



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del Decreto legislativo 8 giugno 2001, n. 231)

adottato con delibera del C.d.A. del ____ / ____ / ____
Revisione 9.11.2023

SOMMARIO

PARTE GENERALE

1	IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231	Pag. 3
1.1	Il regime della responsabilità amministrativa degli Enti	Pag. 3
1.2	Le sanzioni applicabili a carico dell'Ente	Pag. 4
1.2.1	Sanzione pecuniaria	Pag. 4
1.2.2	Sanzioni interdittive	Pag. 5
1.3	I reati presupposto	Pag. 6
1.4	Esenzione dalla responsabilità amministrativa: il Modello di organizzazione, controllo e gestione ex D.Lgs. 231/2001	Pag. 10
2	ADOZIONE DEL MODELLO DA PARTE DI HS HOSPITAL SERVICE S.P.A.	Pag.12
2.1	Obiettivi perseguiti da HS Hospital Service S.p.A. con l'adozione del Modello	Pag.12
2.2	Sistema di <i>Corporate Governance</i> di HS Hospital Service S.p.A.	Pag. 13
2.3	Sistema di deleghe e procure adottate dalla Società	Pag. 14
2.4	Le procedure e il Codice Etico	Pag. 16
2.5	Altri Protocolli di prevenzione	Pag. 16

3	FUNZIONE DEL MODELLO	Pag. 17
3.1	Il Modello di HS Hospital Service S.p.A.	Pag. 17
3.2	Attività preparatoria del Modello	Pag. 18
3.3	Approvazione del Modello e suo recepimento	Pag. 19
3.4	Struttura del Modello: Parte Generale e Parte Speciale in funzione delle diverse aree funzionali impattate	Pag. 19
4	L'ORGANISMO DI VIGILANZA	Pag. 21
4.1	Identificazione dell'Organismo di Vigilanza	Pag. 21
4.2	Modalità di convocazione e tenuta delle riunioni dell'OdV	Pag. 22
4.3	Funzioni e poteri dell'OdV	Pag. 23
4.4	Funzioni dell'OdV: autonomia nei confronti degli organi societari	Pag. 24
4.5	Flussi informativi nei confronti dell'OdV	Pag. 25
4.6	Modalità di funzionamento dell'OdV	Pag. 26
4.7	Flussi informativi alternativi e Sistema Whistleblowing	Pag. 28
5	SELEZIONE, FORMAZIONE E INFORMATIVA	Pag. 31
5.1	Selezione del personale	Pag. 31
5.2	Formazione del personale	Pag. 31
5.3	Diffusione dei contenuti del Modello	Pag. 31
5.4	Informativa ai collaboratori esterni	Pag. 31
6	SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO	Pag. 32
6.1	Principi generali	Pag. 32
6.2	Sanzioni per i lavoratori dipendenti e misure nei confronti degli Amministratori e dei collaboratori esterni	Pag. 33

6.3	Misure nei confronti dei membri degli Amministratori	Pag. 34
6.4	Misure nei confronti dei membri del Collegio Sindacale	Pag. 35
6.5	Misure nei confronti dei collaboratori esterni e partner	Pag. 35
6.6	Misure in caso di violazione degli obblighi di informazione nei confronti dell'OdV	Pag. 36
6.7	Misure nei confronti dei membri dell'ODV in caso di illeciti disciplinari	Pag. 36
6.8	Misure in caso di violazione del Sistema Whistleblowing	Pag. 36

PARTE SPECIALE

INTRODUZIONE. FUNZIONE DELLA PARTE SPECIALE	Pag. 37
--	---------

1	Sezione A	IL CONSIGLIO DI AMMINISTRAZIONE E LA DIREZIONE GENERALE: PRESIDENTE, AMMINISTRATORE DELEGATO, CONSIGLIERI	Pag. 37
	1.1	I reati contro la Pubblica Amministrazione	Pag. 39
	1.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 46
	1.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001)	Pag. 48
		Protocollo 1:	
		• Rapporti anche istituzionali con la Pubblica Amministrazione	
		• Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni	
		• Gestione delle gare e dei bandi pubblici	
		• Accesso a sistemi informatici della Pubblica Amministrazione	Pag. 49
		Protocollo 2:	
		• Scelta di fornitori e consulenti	Pag. 51
		Protocollo 3:	
		• Richiesta ed ottenimento finanziamenti pubblici	Pag. 51
		Protocollo 4:	
		• Assunzione del personale	Pag. 52

	Protocollo 5:	
	• Gestione dei contenziosi giudiziali e stragiudiziali	Pag. 52
	Protocollo 6:	
	• Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi	
	• Spese di rappresentanza	Pag. 53
1.4	Compiti dell'Organismo di Vigilanza	Pag. 53
1.5	Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 54
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 56
1.6	Compiti dell'Organismo di Vigilanza	Pag. 58
1.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto)	Pag. 58
	Protocollo 1:	
	• Commercializzazione di prototipi e/o nuovi prodotti	Pag. 60
	Protocollo 2:	
	• Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla società	Pag. 61
	Protocollo 3:	
	• Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	Pag. 62
1.8	Compiti dell'Organismo di Vigilanza	Pag. 62
1.9	Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001)	Pag. 63
	Protocollo 1:	
	• Predisposizione del bilancio;	
	• Tenuta delle scritture contabili e dei libri sociali;	
	• Gestione degli ordini e delle fatture	Pag. 66
	Protocollo 2:	
	• Gestione delle operazioni societarie (aumento o	Pag. 67

	riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni)	
	• creazione di fondi extracomunitari	
	Protocollo 3:	
	• rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa / contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale	Pag. 68
	Protocollo 4:	
	• Scelta consulenti / fornitori / partner commerciali e rapporti con i clienti;	
	• Gestione della liquidità	Pag. 68
1.10	Compiti dell'Organismo di Vigilanza	Pag. 70
1.11	Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies, D.Lgs. 231/2001).	Pag. 71
1.12	Struttura organizzativa di HS Hospital Service S.p.A.	Pag. 73
1.13	Principi procedurali specifici	Pag. 75
	Protocollo 1:	
	• Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	Pag. 75
1.14	Compiti dell'Organismo di Vigilanza	Pag. 78
1.15	Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	Pag. 79
	Protocollo 1:	
	• Scelta consulenti, fornitori, partner commerciali	Pag. 80
	Protocollo 2:	
	• Gestione dei flussi finanziari / creazione di fondi extracontabili e gestione della liquidità e cassa	Pag. 81
	Protocollo 3:	
	• Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio	Pag. 82
	Protocollo 4:	
	• Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà	Pag. 82
1.16	Compiti dell'Organismo di Vigilanza	Pag. 82
1.17	Regole di comportamento e Protocolli operativi in materia di reati ambientali (art. 25-undecies del Decreto)	Pag. 83

	Protocollo 1:	
	• Rispetto della normativa sull'ambiente	Pag. 86
1.18	Compiti dell'Organismo di Vigilanza	Pag. 91
1.19	Regole di comportamento e Protocolli operativi in materia di reati tributari (art. n25 quinquiesdecies del Decreto)	Pag. 92
	Art. 25 quinquiesdecies – Reati Tributari	Pag. 93
1.20	Tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)	Pag. 95
1.21	Sanzioni nei confronti dell'Ente	Pag. 98
1.22	Aumenti delle sanzioni nei confronti dell'Ente	Pag. 99
1.23	Aree a rischio reato e processi sensibili	Pag. 99
1.24	Regole di comportamento	Pag. 100
1.24.1	Principi generali e standard di controllo	Pag. 100
1.24.2	Principi generali specifici	Pag. 102
	Protocollo 1:	
	Definizione di ruoli e responsabilità	
	Gestione contabilità, Approvvigionamenti di beni e servizi,	
	Gestione buste paga e rimborsi spese ai dipendenti	
	Tenuta e custodia delle scritture contabili e fiscali	
	Gestione delle operazioni straordinarie	Pag. 103
1.24.3	Responsabilità specifiche del Consiglio di Amministrazione (Presidente e Consiglieri)	Pag. 106
1.25	Compiti dell'Organismo di Vigilanza	Pag. 107
1.26	Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25-sexiesdecies del Decreto)	Pag. 108
1.27	Sanzioni nei confronti dell'Ente	Pag. 109
1.28	Aree a rischio reato e processi sensibili	Pag. 110
1.29	Regole di comportamento	Pag. 111
1.29.1	Principi generali e standard di controllo	Pag. 111
1.29.2	Principi procedurali specifici	Pag. 112
	Protocollo 1:	
	Controllo interno sull'emissione e la conservazione dei documenti fiscali	Pag. 112
1.30	Compiti dell'Organismo di Vigilanza	Pag. 112

2	Sezione B SETTORE QUALITY ASSURANCE & REGULATORY AFFAIRS: RESPONSABILE REGULATORY AFFAIRS (RRA), RESPONSABILE DIREZIONE DI QUALITÀ (R.D.Q.), RESPONSABILE ASSICURAZIONE QUALITÀ (R.A.Q.).	Pag. 113
2.1	I reati contro la Pubblica Amministrazione	Pag. 114
2.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 116
2.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A.	Pag. 117
	Protocollo 1:	
	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche ed ispezioni (es. ASL, ARPA, VV.FF., Guardia di Finanza, INAIL ecc.) • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	Pag. 119
2.4	Compiti dell'Organismo di Vigilanza	Pag. 120
2.5	Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 121
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 123
2.6	Compiti dell'Organismo di Vigilanza	Pag. 125
2.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto)	Pag. 125
	Protocollo 1:	
	• Commercializzazione di prototipi e/o nuovi prodotti	Pag. 127
	Protocollo 2:	
	• Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicazione dei prodotti e dei marchi legati alla Società	Pag. 128
	Protocollo 3:	
	• Approvvigionamento, installazione e/o configurazione	Pag. 129

	di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità delle licenze d'uso e dei bollini SIAE	
2.8	Compiti dell'Organismo di Vigilanza	Pag. 130
2.9	Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001) Protocollo 1: • Rapporti con Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i soci nell'attività di verifica della gestione aziendale	Pag. 130
2.10	Compiti dell'Organismo di Vigilanza	Pag. 133
3	Sezione C SETTORE AMMINISTRATIVO, FINANZIARIO E RISORSE UMANE	Pag. 134
3.1	I reati contro la Pubblica Amministrazione	Pag. 136
3.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 143
3.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001) Protocollo 1: • Rapporti anche istituzionali con la Pubblica Amministrazione • Gestione dei rapporti con le Autorità e gli Organi di Controllo anche in occasione di verifiche ed ispezioni • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione Protocollo 2: • Scelta di fornitori e consulenti Protocollo 3: • Richiesta ed ottenimento di finanziamenti pubblici Protocollo 4: • Assunzione del personale Protocollo 5: • Gestione dei contenziosi giudiziali e stragiudiziali Protocollo 6: • Gestione di liberalità (donazioni e sponsorizzazioni) ed omaggi • Spese di rappresentanza	Pag. 144
		Pag. 146
		Pag. 147
		Pag. 147
		Pag. 148
		Pag. 148
		Pag. 149

3.4	Compiti dell'Organismo di Vigilanza	Pag. 149
3.5	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001) Protocollo 1: • Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 150 Pag. 152
3.6	Compiti dell'Organismo di Vigilanza	Pag. 154
3.7	Regole di comportamento e Protocolli operativi in tema di reati societari (art. 25-ter D.Lgs. 231/2001) Protocollo 1: • Predisposizione del bilancio • Tenuta delle scritture contabili e dei libri sociali • Gestione degli ordini e delle fatture Protocollo 2: • Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni) • Creazione di fondi extracontabili Protocollo 3: • Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa / contabile e sul bilancio di esercizio e con i soci nell'attività di verifica della gestione aziendale Protocollo 4: • Scelta consulenti / fornitori / partner commerciali e rapporti con i clienti • Gestione della liquidità	Pag. 154 Pag. 157 Pag. 158 Pag. 158
3.8	Compiti dell'Organismo di Vigilanza	Pag. 161
3.9	Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	Pag. 162
3.10	Struttura organizzativa di HS Hospital Service S.p.A.	Pag. 164
3.11	Principi procedurali specifici Protocollo 1: • Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	Pag. 166 Pag. 166
3.12	Compiti dell'Organismo di Vigilanza	Pag. 169
3.13	Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	Pag. 170

	Protocollo 1:	
	• Scelta consulenti, fornitori, partner commerciali	Pag. 171
	Protocollo 2:	
	• gestione dei flussi finanziari / creazione di fondi extracontabili e gestione della liquidità e cassa	Pag. 172
	Protocollo 3:	
	• negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziarie e brokeraggio	Pag. 172
	Protocollo 4:	
	• realizzazione, promozione e gestione di iniziative umanitarie e solidarietà	Pag. 173
3.14	Compiti dell'Organismo di Vigilanza	Pag. 173
3.15	Regole di comportamento e Protocolli operativi in materia di reati ambientali (art. 25-undecies del Decreto)	Pag. 174
	Protocollo 1:	
	• rispetto della normativa sull'ambiente	Pag. 177
3.16	Compiti dell'Organismo di Vigilanza	Pag. 181
3.17	Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25-quinquiesdecies del Decreto)	Pag. 183
	Art. 25-quinquiesdecies – Reati Tributari	Pag. 184
3.18	La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)	Pag. 186
3.19	Sanzioni nei confronti dell'Ente	Pag. 189
3.20	Aumenti delle sanzioni nei confronti dell'Ente	Pag. 190
3.21	Aree a rischio reato e processi sensibili	Pag. 190
3.22	Regole di comportamento	Pag. 191
3.22.1	Principi generali e standard di controllo	Pag. 191
4	Principi procedurali specifici	Pag. 193
	Protocollo 1:	
	Definizioni di ruoli e responsabilità	
	Gestione contabilità, Approvvigionamenti di beni e servizi,	
	Gestione buste paga e rimborsi spese ai dipendenti	
	Tenuta e custodia delle scritture contabili e fiscali	
	Gestione delle operazioni straordinarie	Pag. 194
4.1	Responsabilità specifiche del Chief Financial Officer (CFO), Direzione Amministrativa (DAM), Direzione Finanziaria (DF)	Pag. 197
4.2	Compiti dell'Organismo di Vigilanza	Pag. 198

4.3	Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25 sexiesdecies del Decreto)	Pag. 199
4.4	Sanzioni nei confronti dell'Ente	Pag. 200
4.5	Aree a rischio reato e processi sensibili	Pag. 202
4.6	Regole di comportamento	Pag. 202
4.6.1	Principi generali e standard di controllo	Pag. 202
5	Principi procedurali specifici	Pag. 203
	Protocollo 1	
	Controllo interno sull'emissione e la conservazione dei documenti fiscali	Pag. 203
5.1	Compiti dell'Organismo di Vigilanza	Pag. 204
4	Sezione D SETTORE RICERCA E SVILUPPO (R&D)	Pag. 204
4.1	I reati contro la Pubblica Amministrazione	Pag. 205
4.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 207
4.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001)	Pag. 208
	Protocollo 1:	
	• Rapporti anche istituzionali con la Pubblica Amministrazione • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV.FF., Guardia di Finanza, INAIL ecc.) • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	Pag. 210
	Protocollo 2:	
	• Scelta di fornitori e consulenti	Pag. 211
	Protocollo 3:	
	• Richiesta e ottenimento di finanziamenti pubblici	Pag. 212
	Protocollo 4:	
	• Assunzione del personale	Pag. 212
	Protocollo 5:	
	• Gestione dei contenziosi giudiziali e stragiudiziali	Pag. 213
	Protocollo 6:	
	• Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi	Pag. 213

	• Spese di rappresentanza	
4.4	Compiti dell'Organismo di Vigilanza	Pag. 213
4.5	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 214
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 216
4.6	Compiti dell'Organismo di Vigilanza	Pag. 218
4.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 24-novies del Decreto)	Pag. 218
	Protocollo 1:	
	• Commercializzazione di prototipi e/o nuovi prodotti	Pag. 220
	Protocollo 2:	
	• Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società	Pag. 221
	Protocollo 3:	
	• Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	Pag. 222
4.8	Compiti dell'Organismo di Vigilanza	Pag. 222
5	Sezione E SETTORE HARDWARE & SOFTWARE	Pag. 223
5.1	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 224
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 226
5.2	Compiti dell'Organismo di Vigilanza	Pag. 228
5.3	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis	Pag. 228

del Decreto) e di Violazione del Diritto d'Autore (art. 24-novies del Decreto)

Protocollo 1:

- Commercializzazione di prototipi e/o nuovi prodotti Pag. 230

Protocollo 2:

- Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società Pag. 231

Protocollo 3:

- Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE Pag. 232

5.4 Compiti dell'Organismo di Vigilanza Pag. 232

5.5 Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001) Pag. 233

5.6 Struttura organizzativa di HS Hospital Service S.p.A. Pag. 235

5.7 Principi procedurali specifici Pag. 237

Protocollo 1:

- Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro Pag. 237

5.8 Compiti dell'Organismo di Vigilanza Pag. 240

6 Sezione F SETTORE TECNICO PRODUTTIVO INTERNO, CRITICAL CARE, ENDO, TERAPIE ABLATIVE Pag. 241

6.1 I reati contro la Pubblica Amministrazione Pag. 243

6.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio Pag. 244

6.3 Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001) Pag. 246

Protocollo 1:

- Rapporti anche istituzionali con la Pubblica Amministrazione
- Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche ed ispezioni Pag. 247

	(es. ASL, ARPA, VV.FF., Guardia di Finanza, INAIL ecc.)	
	• Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
	Protocollo 2:	
	• Scelta di fornitori e consulenti	Pag. 249
	Protocollo 3:	
	• Richiesta e ottenimento di finanziamenti pubblici	Pag. 249
	Protocollo 4:	
	• Assunzione del personale	Pag. 250
	Protocollo 5:	
	• Gestione dei contenziosi giudiziali e stragiudiziali	Pag. 250
	Protocollo 6:	
	• Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi • Spese di rappresentanza	Pag. 250
6.4	Compiti dell'Organismo di Vigilanza	Pag. 251
6.5	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 251
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 253
6.6	Compiti dell'Organismo di Vigilanza	Pag. 255
6.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 24-novies del Decreto)	Pag. 256
	Protocollo 1:	
	• Commercializzazione di prototipi e/o nuovi prodotti	Pag. 257
	Protocollo 2:	
	• Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società	Pag. 258
	Protocollo 3:	
	• Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con	Pag. 259

	particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	
6.8	Compiti dell'Organismo di Vigilanza	Pag. 260
6.9	Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001)	Pag. 260
6.10	Struttura organizzativa di HS Hospital Service S.p.A.	Pag. 262
6.11	Principi procedurali specifici	Pag. 264
	Protocollo 1:	
	• Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	Pag. 265
6.12	Compiti dell'Organismo di Vigilanza	Pag. 268
6.13	Regole di comportamento e Protocolli operativi in materia di reati ambientali (art.25-undecies del Decreto)	Pag. 269
	Protocollo 1:	
	• Rispetto alla normativa sull'ambiente	Pag. 272
6.14	Compiti dell'Organismo di Vigilanza	Pag. 276
7	Sezione G SETTORE ACQUISTI	Pag. 278
7.1	I reati contro la Pubblica Amministrazione	Pag. 279
7.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 285
7.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001)	Pag. 287
	Protocollo 1:	
	• Rapporti anche istituzionali con la Pubblica Amministrazione	
	• Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche ed ispezioni (es. ASL, ARPA, VV.FF., Guardia di Finanza, INAIL ecc.)	
	• Gestione delle gare e dei bandi pubblici	
	• Accesso a sistemi informatici della Pubblica Amministrazione	Pag. 288
	Protocollo 2:	
	• Scelta di fornitori e consulenti	Pag. 290
	Protocollo 3:	
	• Richiesta e ottenimento di finanziamenti pubblici	Pag. 290
	Protocollo 4:	Pag. 291

	Assunzione del personale	
	Protocollo 5:	
	Gestione dei contenziosi giudiziali e stragiudiziali	Pag. 291
	Protocollo 6:	
	- Gestione di liberalità (donazioni e sponsorizzazione) e omaggi - Spese di rappresentanza	Pag. 291
7.4	Compiti dell'Organismo di Vigilanza	Pag. 292
7.5	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 292
	Protocollo 1:	
	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 294
7.6	Compiti dell'Organismo di Vigilanza	Pag. 297
7.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 24-novies del Decreto)	Pag. 297
	Protocollo 1:	
	Commercializzazione di prototipi e/o nuovi prodotti	Pag. 298
	Protocollo 2:	
	Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società	Pag. 299
	Protocollo 3:	
	Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	Pag. 300
7.8	Compiti dell'Organismo di Vigilanza	Pag. 301
7.9	Regole di comportamento e Protocolli operativi in tema di reati societari (art. 25-ter D.Lgs. 231/2001)	Pag. 302
	Protocollo 1:	
	- Predisposizione del bilancio - Tenuta delle scritture contabili e dei Libri Sociali - Gestione degli ordini e delle fatture	Pag. 305

	Protocollo 2:	
	- Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni) - Creazione di fondi extracontabili	Pag. 306
	Protocollo 3:	
	Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale	Pag. 306
	Protocollo 4:	
	- Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti - Gestione della liquidità	Pag. 306
7.10	Compiti dell'Organismo di Vigilanza	Pag. 308
7.11	Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies	Pag. 309
	Protocollo 1:	
	Scelta consulenti, fornitori, partner commerciali	Pag. 310
	Protocollo 2:	
	Gestione dei flussi finanziari/creazione di fondi extracontabili e gestione della liquidità e cassa	Pag. 311
	Protocollo 3:	
	Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio	Pag. 312
	Protocollo 4:	
	Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà	Pag. 312
7.12	Compiti dell'Organismo di Vigilanza	Pag. 312
7.13	Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25 quinquiesdecies del Decreto)	Pag. 313
	Art. 25 quinquiesdecies – Reati tributari	Pag. 314
7.14	La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)	Pag. 316
7.15	Sanzioni nei confronti dell'Ente	Pag. 319
7.16	Aumenti delle sanzioni nei confronti dell'Ente	Pag. 320
7.17	Aree a rischio reato e processi sensibili	Pag. 320
7.18	Regole di comportamento	Pag. 321

7.18.1	Principi generali e standard di controllo	Pag. 321
7.19	Principi procedurali specifici	Pag. 323
	Protocollo 1:	
	Definizioni di ruoli e responsabilità	
	Gestione contabilità, Approvvigionamenti di beni e servizi,	
	Gestione buste paga e rimborsi spese ai dipendenti	
	Tenuta e custodia delle scritture contabili e fiscali	
	Gestione delle operazioni straordinarie	Pag. 324
7.20	Responsabilità specifiche della Direzione Acquisti (DA)	Pag. 327
7.21	Compiti dell'Organismo di Vigilanza	Pag. 327
7.22	Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25 sexiesdecies del Decreto)	Pag. 329
7.23	Sanzioni nei confronti dell'Ente	Pag. 330
7.24	Aree a rischio reato e processi sensibili	Pag. 331
7.25	Regole di comportamento	Pag. 331
7.25.1	Principi generali e standard di controllo	Pag. 331
7.26	Principi procedurali specifici	Pag. 332
	Protocollo 1:	
	Controllo interno sull'emissione e la conservazione dei documenti fiscali	Pag. 333
7.27	Compiti dell'Organismo di Vigilanza	
	7.28 Regole di comportamento e Protocolli operativi con riferimento ai delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	
	Pag.333	
	7.29 La tipologia dei delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori	
	Pag. 338	
	7.30 Sanzioni nei confronti dell'Ente	Pag. 340
	7.31 Area a rischio reato e processi sensibili	Pag. 340
	7.32 Regole di comportamento	Pag. 341
	7.33 Compiti dell'Organismo di Vigilanza	Pag. 341

8	Sezione H DIREZIONE MARKETING E COMMERCIALE	Pag. 342
----------	--	-----------------

8.1	I reati contro la Pubblica Amministrazione	Pag. 343
8.2	Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio	Pag. 350
8.3	Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001)	Pag. 351
	Protocollo 1:	
	• Rapporti anche istituzionali con la Pubblica Amministrazione • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV.FF., Guardia di Finanza, INAIL ecc.) • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	Pag. 353
	Protocollo 2:	
	• Scelta di fornitori e consulenti	Pag. 355
	Protocollo 3:	
	• Richiesta e ottenimento di finanziamenti pubblici	Pag. 355
	Protocollo 4:	
	• Assunzione del personale	Pag. 356
	Protocollo 5:	
	• Gestione dei contenziosi giudiziali e stragiudiziali	Pag. 356
	Protocollo 6:	
	• Gestione di liberalità (donazioni e sponsorizzazione) e omaggi • Spese di rappresentanza	Pag. 356
8.4	Compiti dell'Organismo di Vigilanza	Pag. 357
8.5	Regole di comportamento e Protocolli operativi in tema di delitti informatici (art. 24-bis D.Lgs. 231/2001)	Pag. 357
	Protocollo 1:	
	• Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali	Pag. 360
8.6	Compiti dell'Organismo di Vigilanza	Pag. 362
8.7	Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto)	Pag. 362
	Protocollo 1:	
	• Commercializzazione di prototipi e/o nuovi prodotti	Pag. 364

	Protocollo 2:	
	• Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società	Pag. 365
	Protocollo 3:	
	• Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	Pag. 366
8.8	Compiti dell'Organismo di Vigilanza	Pag. 366
8.9	Regole di comportamento e Protocolli operativi in tema di reati societari (art. 25-ter D.Lgs. 231/2001)	Pag. 367
	Protocollo 1:	
	• Predisposizione del bilancio • Tenuta delle scritture contabili e dei Libri Sociali • Gestione degli ordini e delle fatture	Pag. 370
	Protocollo 2:	
	• Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni) • Creazione di fondi extracontabili	Pag. 371
	Protocollo 3:	
	• Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i soci nell'attività di verifica della gestione aziendale	Pag. 371
	Protocollo 4:	
	• Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti • Gestione della liquidità	Pag. 371
8.10	Compiti dell'Organismo di Vigilanza	Pag. 374
8.11	Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	Pag. 374
	Protocollo 1:	
	• Scelta consulenti/fornitori/partner commerciali	Pag. 375
	Protocollo 2:	
	• Gestione dei flussi finanziari/creazione di fondi	Pag. 376

extracontabili e gestione della liquidità e cassa

Protocollo 3:

- Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio Pag. 377

Protocollo 4:

- Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà Pag. 377

8.12	Compiti dell'Organismo di Vigilanza	Pag. 377
8.13	Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25quinquiesdecies del Decreto) Art. 25 quinquiesdecies – Reati tributari	Pag. 378 Pag. 380
8.14	La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)	Pag. 382
8.15	Sanzioni nei confronti dell'Ente	Pag. 385
8.16	Aumenti delle sanzioni nei confronti dell'Ente	Pag. 386
8.17	Aree a rischio reato e processi sensibili	Pag. 386
8.18	Regole di comportamento	Pag. 387
8.18.1	Principi generali e standard di controllo	Pag. 387
8.18.2	Principi procedurali specifici	Pag. 389

Protocollo 1:

Definizione di ruoli e responsabilità

Gestione contabilità, Approvvigionamenti di beni e servizi,

Gestione buste paga e rimborsi spese ai dipendenti

Tenuta e custodia delle scritture contabili e fiscali

Gestione delle operazioni straordinarie

Pag. 390

8.18.3	Responsabilità specifiche della Direzione Marketing e Commerciale (R. Mktg)	Pag. 393
---------------	---	----------

8.19	Compiti dell'Organismo di Vigilanza	Pag. 393
8.20	Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25 sexiesdecies del Decreto)	Pag. 395
8.21	Sanzioni nei confronti dell'Ente	Pag. 396
8.22	Aree a rischio reato e processi sensibili	Pag. 397
8.23	Regole di comportamento	Pag. 397
8.23.1	Principi generali e standard di controllo	Pag. 397
8.23.2	Principi procedurali specifici	Pag. 398

	Protocollo 1;	
	Controllo interno sull'emissione e la conservazione dei documenti fiscali	Pag. 398
8.24	Compiti dell'Organismo di Vigilanza	Pag. 399
9	Sezione I FUNZIONI AZIENDALI ESTERNALIZZATE: IL RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE (RSPP)	Pag. 400
9.1	Rapporti tra il RSPP e l'Organismo di Vigilanza	Pag. 401

ALLEGATI

CODICE ETICO

Allegato 1 **ELENCO DEI REATI PRESUPPOSTO**

Allegato 2 **LA NORMATIVA DI RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI EX D.LGS. N.231/2001 E I REATI PRESUPPOSTO EX D.LGS. 231/2001 (TESTO DELLE CONDOTTE CRIMINOSE)**

PARTE GENERALE

IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231.

1.1 Il regime della responsabilità amministrativa degli Enti.

Il Decreto Legislativo 8 giugno 2001 n. 231 (di seguito anche il “d.lgs. 231/2001” o il “Decreto”), recante la Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e di altre strutture associative, anche prive di personalità giuridica (c.d. “Enti”), a norma dell’art. 11 della Legge 29 settembre 2000, n. 300, ha introdotto per la prima volta in Italia una responsabilità amministrativa da reato a carico degli Enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

Si tratta di una nuova e più estesa forma di responsabilità, che colpisce l’Ente per i reati commessi, nel suo interesse o vantaggio, da soggetti ad esso funzionalmente legati (soggetti in posizione apicale e soggetti sottoposti alla direzione e vigilanza di costoro).

Il Decreto prevede che gli Enti possano essere ritenuti responsabili, e conseguentemente sanzionati, in relazione esclusiva al compimento di taluni reati (c.d. “reati presupposto”) indicati tassativamente dalla legge, per quanto l’elencazione sia suscettibile di modifiche ed integrazioni da parte del legislatore.

Il Decreto ha inteso adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l’Italia aveva già da tempo aderito¹.

Il primo criterio fondamentale d’imputazione consiste quindi nel fatto che il reato sia stato commesso nell’interesse o a vantaggio dell’ente: ciò significa che la responsabilità dell’ente sorge qualora il fatto sia stato commesso per favorire l’ente, senza che sia necessario il conseguimento effettivo e concreto dell’obiettivo.

L’ente non è responsabile se l’illecito è stato commesso da uno dei soggetti sopra indicati nell’interesse esclusivo proprio o di terzi.

Il secondo criterio fondamentale d’imputazione è costituito dal tipo di soggetti autori del reato, dai quali può derivare una responsabilità amministrativa a carico dell’ente.

Tali soggetti, infatti, possono essere:

– soggetti in posizione apicale (quali, ad es., il legale rappresentante, l’amministratore, il direttore generale o le persone che esercitano, anche di fatto, la gestione o il controllo dell’ente);

¹ Quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione del 26 maggio 1997, anch’essa firmata a Bruxelles, sulla lotta alla corruzione e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

– soggetti subalterni, tipicamente lavoratori dipendenti, ma anche soggetti esterni all'ente, ai quali sia stato affidato un incarico da svolgere sotto la direzione e la sorveglianza dei soggetti apicali.

Qualora più soggetti concorrano alla commissione del reato (art. 110 c.p.) non è necessario che il soggetto “qualificato” ponga in essere direttamente il fatto, ma è sufficiente che fornisca un consapevole contributo causale alla realizzazione del reato stesso.

La responsabilità prevista dal suddetto Decreto si configura anche in relazione ai reati commessi all'estero dall'ente, alle seguenti condizioni:

- il reato è stato commesso da un soggetto funzionalmente legato all'ente, apicale o subordinato, come sopra illustrato;
- l'ente ha la propria sede principale in Italia;
- l'ente può rispondere solo nei casi e alle condizioni previste dagli articoli 7, 8, 9 e 10 c.p. e qualora la legge preveda che la persona fisica colpevole sia punita a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso;
- l'ente risponde solo se nei suoi confronti non procede lo Stato del luogo in cui è stato commesso il reato.

La responsabilità amministrativa dell'ente sorge anche nel caso in cui uno degli illeciti previsti dal Decreto sia commesso anche solo nella forma di tentativo (art. 56 c.p.).

1.2.1 Le sanzioni applicabili a carico dell'Ente.

Le sanzioni previste a carico dell'Ente, in conseguenza della commissione o tentata commissione dei reati presupposto, sono:

1. **Sanzione pecuniaria**: si tratta di una sanzione applicabile a tutti gli illeciti, determinata attraverso un sistema basato su “quote” in numero non inferiore a cento e non superiore a mille, ciascuna di valore tra un minimo di Euro 258,23 ed un massimo di Euro 1.549,37 (perciò la sanzione oscilla tra un minimo di Euro 25.823 ed un massimo di Euro 1.549.370, eccetto per i reati societari le cui sanzioni pecuniarie sono raddoppiate in base a quanto previsto dalla Legge sul Risparmio 262/2005, art. 39, comma 5).

Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente, nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione.

La sanzione pecuniaria è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado:

- a. l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato, ovvero si è comunque efficacemente adoperato in tal senso;
- b. è stato adottato o reso operativo un Modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Inoltre è prevista la riduzione della metà della sanzione pecuniaria se:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità.

Il principio fondamentale che guida l'intera materia della responsabilità dell'Ente, stabilisce che dell'obbligazione per il pagamento della sanzione pecuniaria inflitta all'Ente risponde soltanto l'Ente, con il suo patrimonio o il fondo comune. La norma, dunque, esclude una responsabilità patrimoniale diretta dei soci o degli associati, indipendentemente dalla natura giuridica dell'Ente collettivo.

1.2.2 Sanzioni interdittive:

- 1) interdizione dall'esercizio dell'attività;
- 2) sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- 3) divieto di contrattare con la Pubblica Amministrazione;
- 4) esclusione da agevolazioni, finanziamenti, contributi, sussidi ed eventuale revoca di quelli già concessi;
- 5) divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive sono irrogate, congiuntamente a quella pecuniaria, solo se espressamente previste per quella fattispecie di reato, e soltanto quando ricorre almeno una di queste due condizioni:

- i. la società ha già commesso in precedenza un illecito da reato (reiterazione degli illeciti);
 - ii. la società ha tratto dal reato un profitto di rilevante entità.
2. **Confisca** (e sequestro preventivo in sede cautelare) del profitto e del prezzo del reato, anche in forma per equivalente (confiscando cioè una somma di denaro, beni o altre utilità di valore corrispondenti al prezzo o profitto del reato).
 3. **Pubblicazione della sentenza** che può essere disposta dal giudice quando, nei confronti dell'Ente, viene applicata una sanzione interdittiva.
 4. **Misure cautelari**: il Pubblico Ministero può chiedere l'applicazione delle sanzioni interdittive anche in via cautelare, qualora:
 - a. sussistano gravi indizi della responsabilità dell'Ente;
 - b. vi siano fondati e specifici elementi tali da far ritenere il concreto pericolo che vengano commessi illeciti dello stesso tipo di quello già commesso.

1.3 I reati presupposto

I reati destinati a comportare il regime di responsabilità amministrativa a carico degli Enti (**Allegato 1**), per i quali si applica la disciplina in esame, sono di seguito elencati:

- a) **Reati commessi nei rapporti con la P.A.** - artt. 24 e 25 del Decreto.
- b) **Delitti informatici e trattamento illecito di dati** - art. 24-bis del Decreto.
- c) **Delitti di criminalità organizzata** - art. 24-ter del Decreto.
- d) **Reati in tema di falsità in monete, carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** - art. 25-bis del Decreto.
- e) **Delitti contro l'industria e il commercio** - art. 25-bis.1 del Decreto.
- f) **Reati in materia societaria** - art. 25-ter del Decreto.
- g) **Delitti con finalità di terrorismo o di eversione dell'ordine democratico** - art. 25-quater del Decreto.
- h) **Pratiche di mutilazione degli organi genitali femminili** - art. 25-quater.1 del Decreto.
- i) **Delitti contro la personalità individuale** - art. 25-quinquies del Decreto.

- j) **Reati di abuso di mercato** - art. 25-sexies del Decreto.
- k) **Reati transnazionali** - con Legge 16 Marzo 2006, n. 146 di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, la responsabilità amministrativa degli enti è stata estesa, ai sensi dell'art. 10, ai seguenti reati, purché commessi a livello transnazionale:
- associazione per delinquere (art. 416 c.p.);
 - associazione di tipo mafioso (art. 416-bis c.p.);
 - induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
 - favoreggiamento personale (art. 378 c.p.);
 - associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. 23 Gennaio 1973 n. 43);
 - associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 Ottobre 1990 n. 309);
 - disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-bis, 3-ter e 5 del d.lgs. 25 Luglio 1998, n. 286).
- l) **Reati di omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro** - art. 25-septies del Decreto.
- m) **Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio** - art. 25-octies del Decreto - introdotto dal d.lgs. 21 Novembre 2007 n. 231, estende l'elenco dei reati presupposto a:
- ricettazione (art. 648 c.p.);
 - riciclaggio (art. 648-bis c.p.);
 - impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
 - autoriciclaggio (art. 648-ter 1 c.p.).

Come indicato in precedenza, i reati di riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita erano già rilevanti ai fini del Decreto, ma esclusivamente se realizzati a livello transnazionale (ex art. 10 L. 146/2006).

A seguito dell'introduzione dell'art. 25-octies, i predetti reati – unitamente alla ricettazione – divengono rilevanti anche su base nazionale.

- n) **Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori** – art. 25-octies¹ del Decreto – introdotto dall'art. 3, comma 1, lett.a), D. Lgs. 8 novembre 2021, n. 184, relativo ai delitti di cui agli artt. 493-ter, 493-quater e 640-ter c.p. e modificato a D.L.10 agosto 2023 n. 105 coordinato con la legge di conversione n. 137 del 9 ottobre 2023.
- o) **Delitti in materia di violazione del diritto d'autore** - art. 25-novies del Decreto - aggiunto dalla Legge 23 Luglio 2009, n. 99 (art. 15, comma 7, lett. 5) e relativo ai delitti di cui alla Legge 22 Aprile 1941, n. 633 rubricata "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (artt. 171, primo comma, lett. a-bis) e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies).
- p) **Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** - art. 25-decies del Decreto - introdotto dall'art. 4, comma 1, della Legge 3 Agosto 2009, n. 116, riguarda il delitto di cui all'art. 377-bis c.p. ("Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria").
- q) **Reati ambientali** - art. 25-undecies del Decreto - recante il recepimento delle direttive 2008/99/CE e 2009/123/CE del Parlamento Europeo e del Consiglio. I nuovi reati presupposto sono:
- uccisione, distruzione, cattura, prelievo o possesso di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.);
 - distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
 - importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n. 150/1992, art. 1 e art. 2);
 - scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (d.lgs. n. 152/2006, art. 137);
 - attività di gestione di rifiuti non autorizzata (d.lgs. n. 152/2006, art. 256);
 - traffico illecito di rifiuti (d.lgs. N. 152/2006, art. 259);
 - attività organizzate per il traffico illecito di rifiuti (d.lgs. 152/2006, art. 260);

- inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (d.lgs. n. 152/2006, n. 257);
 - violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (d.lgs. n. 152/2006, art. 258);
 - false dichiarazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel "Registro elettronico nazionale per la tracciabilità dei rifiuti" (ex SISTRI) di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda di area movimentazione nel trasporto di rifiuti (d.lgs. n. 152/2006, art. 260 bis);
 - inquinamento colposo provocato da navi (art. 9 del d.lgs. 202/2007);
 - inquinamento doloso provocato da navi (art. 8 del d.lgs. 202/2007);
 - inquinamento ambientale art. 452bis (legge n. 68/2015);
 - disastro ambientale art. 452 ter (legge n. 68/2015);
 - traffico e abbandono di materiale radioattivo 452quinquies (legge n. 68/2015);
 - impedimento del controllo 452sexies e omessa bonifica 452terdecies (legge n. 68/2015).
- r) **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare** – art. 25-duodecies del Decreto, aggiunto dall'art. 2, comma 1, del d.lgs. 109/2012: impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-bis, d.lgs. 286/1998).
- s) **Razzismo e xenofobia** – Art. 25-terdecies, D.Lgs. n. 231/2001, aggiunto dalla Legge 20 novembre 2017 n. 167 [modificato dal D.Lgs. n. 21/2018 che è andato a sopprimere l'articolo 3 della Legge 654/1975].
- t) **Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** – art. 25-quaterdecies del Decreto, inserito dall'art. 5, L. 03.05.2019, n. 39.
- u) **Reati tributari** – 25-quinquiesdecies, D.Lgs. n. 231/2001, aggiunto dalla Legge 19 dicembre 2019 n. 157.
- v) **Reati di contrabbando** – 25-sexiesdecies, D.Lgs. n. 231/2001, aggiunto dal D.Lgs. 14 luglio 2020, n. 75 ("Attuazione della direttiva (UE) 2017/1371 c.d. "Direttiva PIF",

relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale").

- w) **Delitti contro il patrimonio culturale** – art. 25-septiesdecies del Decreto, inserito dall'art. 3, comma 1, L. 9 marzo 2022, n. 22, a decorrere al 23 marzo 2022, ai sensi di quanto disposto dall'art. 7, comma 1, delle medesima legge n. 22/2022.
- x) **Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** – art. 25-duodevicies del Decreto, inserito dall'art. 3, comma 1, L. 9 marzo 2022, n. 22, a decorrere al 23 marzo 2022, ai sensi di quanto disposto dall'art. 7, comma 1, delle medesima legge n. 22/2022.

Come meglio specificato nel prosieguo, nelle Parti Speciali del presente documento, saranno trattati solo i reati presupposto astrattamente ipotizzabili in capo alla Società.

1.4 Esenzione dalla responsabilità amministrativa: il Modello di Organizzazione, Gestione e Controllo ex d.lgs. 231/2001

Il Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'Ente dimostri di aver adottato tutte le misure organizzative opportune e necessarie al fine di prevenire la commissione dei reati previsti dal Decreto da parte di soggetti che operino per suo conto. La presenza di un'adequata organizzazione è, dunque, misura e segno della diligenza dell'Ente nello svolgere le proprie attività, con particolare riferimento a quelle in cui si manifesta il rischio di commissione dei reati previsti dal Decreto: l'accertata esistenza di un'efficiente ed efficace organizzazione esclude, dunque, la "colpa" dell'Ente a far venir meno la necessità di applicare ad esso le previste sanzioni.

Al Consiglio di Amministrazione compete l'adozione e l'efficace attuazione del Modello di organizzazione, gestione e controllo, ai sensi dell'art. 6, comma 1, lett. a), nonché l'istituzione dell'Organismo di Vigilanza e la nomina dei suoi membri, ai sensi della successiva lett. b).

Il Decreto indica quali sono le componenti di un apparato organizzativo efficace ed effettivo la cui corretta predisposizione porta ad escludere la sua responsabilità.

In particolare, l'Ente va esente da responsabilità se prova:

- di aver *adottato ed efficacemente attuato*, prima della commissione del fatto, modelli di organizzazione e di gestione idonei (di seguito il "Modello") a prevenire i reati della specie di quello verificatosi;
- di aver affidato la vigilanza sul funzionamento e l'osservanza del Modello, nonché il compito di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (di seguito "*Organismo di Vigilanza*");
- che le persone che hanno commesso il reato l'abbiano fatto eludendo fraudolentemente il Modello;
- che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Inoltre, l'art. 6, al secondo comma, indica anche il contenuto del Modello, che dovrà presentare le seguenti caratteristiche:

- a) individuare le attività nel cui ambito esiste la possibilità che siano commessi i reati di cui al Decreto;
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- d) prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (denominati anche linee guida) redatti da associazioni rappresentative di categoria.

Le linee guida vengono comunicate al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni, osservazioni sulla idoneità a prevenire i reati dei Modelli elaborati in conformità alle linee guida delle associazioni di categoria.

È opportuno evidenziare che la mancata conformità a punti specifici delle Linee guida non inficia di per sé la validità del Modello.

Il singolo Modello, infatti, dovendo essere redatto con riguardo alla realtà concreta della società cui si riferisce, ben può discostarsi dalle Linee guida (che, per loro natura, hanno carattere generale), per garantire maggiormente le esigenze tutelate dal Decreto.

In questo senso devono essere valutate anche le osservazioni esemplificative contenute nell'appendice alle predette Linee guida (c.d. "Case Study") nonché la sintetica elencazione degli strumenti di controlli ivi prevista.

2. ADOZIONE DEL MODELLO DA PARTE DI HS HOSPITAL SERVICE S.P.A.

2.1 Obiettivi perseguiti da HS Hospital Service S.p.A. con l'adozione del Modello

HS Hospital Service S.p.A. (di seguito anche "HS" o la "Società") è una società fondata nel 1980 che rappresenta una delle più importanti realtà aziendali italiane nel settore della produzione e commercializzazione di dispositivi per interventistica, *critical care*, terapie interstiziali, chirurgia mini-invasiva e per oncologia, operante sia a livello nazionale che internazionale.

La Società, che ha sede legale in Roma (RM) – Via Zosimo 13 (**verificare se cambiata la sede legale), ha per oggetto sociale principale l'attività di fabbricazione, concessioni, commercio, importazione, esportazione, distribuzione e vendita di qualsiasi prodotto attinente alle cure mediche e cioè di prodotti medicinali, chirurgici, da laboratorio, diagnostici e apparecchiature usati da medici, ospedali, laboratori, industrie, facoltà universitarie, dentisti e veterinari.

HS – sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine e delle aspettative dei propri dipendenti – ha ritenuto conforme alle proprie politiche aziendali procedere all'attuazione del Modello previsto dal d.lgs. n. 231/2001.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello – al di là delle prescrizioni del Decreto, che indicano il Modello stesso come elemento facoltativo e non obbligatorio – possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto della Società, affinché seguano,

nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

Il suddetto Modello è stato predisposto dalla Società tenendo presenti, oltre alle prescrizioni del Decreto, le linee guida elaborate in materia da Confindustria.

Sempre in attuazione di quanto previsto dal Decreto, il Consiglio di Amministrazione, nell'adottare il suddetto Modello, ha affidato ad un Organismo di Vigilanza (di seguito anche "l'Organismo" o "l'OdV") l'incarico di assumere le funzioni di organo di controllo con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

2.2 Sistema di Corporate Governance di HS Hospital Service S.p.A.

Il sistema di *Corporate Governance* di HS (**Allegato 2**) è strutturato in modo tale da assicurare e garantire alla Società la massima efficienza ed efficacia operativa.

Tale sistema è strutturato secondo quello "tradizionale" e, precisamente:

- L'Assemblea dei Soci: è competente a deliberare, in sede ordinaria e straordinaria, sulle materie alla stessa riservata dalla legge o dallo statuto.
- Il Consiglio di Amministrazione:
 - è attualmente composto da un numero di quattro membri;
 - gli Amministratori restano in carica per il periodo stabilito alla loro nomina, oppure fino a revoca o dimissioni, e comunque non oltre tre esercizi e sono rieleggibili;
 - è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, ed ha la facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione ed il raggiungimento dell'oggetto sociale, ad eccezione soltanto di quanto per legge sia espressamente riservato all'Assemblea;
 - può delegare tutti o parte dei suoi poteri ad un comitato esecutivo composto da alcuni dei suoi componenti, ovvero ad uno o più amministratori delegati, anche disgiuntamente, determinandone i poteri e la relativa remunerazione;
- la rappresentanza legale della Società di fronte ai terzi ed in giudizio spetta al Presidente del Consiglio di Amministrazione, il quale ha facoltà di promuovere azioni ed istanze giudiziarie ed amministrative per ogni grado di giurisdizione.
- Il Collegio Sindacale:

- si compone di tre membri effettivi e due supplenti;
- il Collegio vigila sull'osservanza della Legge e dello Statuto ed esercita tutti i poteri ad esso conferiti dalla Legge e dallo Statuto;
- il controllo contabile è stato affidato al Collegio Sindacale.

2.3 Sistema di deleghe e procure adottate dalla Società

Le funzioni presenti in azienda sono:

ACRONIMO		FUNZIONE
1	C.d.A.	Consiglio di Amministrazione: Presidente e Consiglieri
2	R.D.Q. & R.R.A.	Resp. Direzione di Qualità & Resp. Assicurazione Qualità
3	R&D	Resp. Ricerca e Sviluppo
4	RSPP*	Resp. Servizio Prevenzione e Protezione
5	R. H&S	Resp. Hardware e Software
6	RTPI	Resp. Settore Tecnico Produttivo Interno
7	D.A.	Direzione Acquisti
8	R. Mrktg	Responsabile Marketing
9	HR	Risorse Umane
10	DAM	Direzione Amministrativa
11	DF	Direzione Finanziaria
12	IT*	Servizi Informatici

* Le funzioni contrassegnate con l'asterisco sono esercitate da personale esterno all'azienda: in particolare per il ruolo di RSPP è stato incaricato un soggetto esterno all'azienda, mentre i Servizi IT sono esercitati in collaborazione con il personale della Ditta "DESIDERIO TAGLIANTI".

Il sistema di attribuzione delle deleghe e delle procure aziendali è parte integrante del sistema di controllo interno e costituisce, nell'ottica del Modello, un ulteriore presidio alla prevenzione dei reati richiamati dal d.lgs. 231/2001.

La definizione dei criteri per l'assegnazione delle deleghe e delle procure spetta al Consiglio di Amministrazione.

Il sistema delle deleghe e delle procure deve costituire:

- a) uno strumento di gestione per il compimento di atti aventi rilevanza esterna o interna, necessari al perseguimento degli obiettivi aziendali, che sia congruente con le responsabilità gestionali assegnate a ciascun soggetto;
- b) un fattore di prevenzione dell'abuso dei poteri funzionali attribuiti, mediante la definizione dei limiti economici per ciascun atto o serie di atti;
- c) un elemento incontrovertibile di riconducibilità degli atti aziendali, aventi rilevanza esterna o interna, alle persone fisiche che li hanno adottati. Da ciò dipende l'utilità del sistema sia nella prevenzione della commissione di reati che nella identificazione successiva dei soggetti che hanno adottato atti, direttamente o indirettamente connessi alla consumazione del reato.

La politica della Società prevede che solo i soggetti muniti di formali e specifici poteri possano assumere impegni verso terzi in nome e per conto della Società stessa.

Nell'ambito di questo progetto la Società sta predisponendo ed implementando un sistema di deleghe e procure coerente con le responsabilità organizzative assegnate implicanti effettive necessità di rappresentanza e con la previsione, quando opportuno, di una puntuale indicazione di soglie quantitative di spesa stabilite da provvedimenti interni all'azienda.

L'atto attributivo deve rispettare gli specifici requisiti eventualmente richiesti dalla legge (es. delega e subdelega in materia di salute e sicurezza dei lavoratori).

Le unità aziendali interessate, eventualmente con il supporto dell'Organismo di Vigilanza, verificano periodicamente il sistema delle deleghe e procure in vigore, anche attraverso l'esame della documentazione attestante l'attività concretamente posta in essere dai soggetti che operano per conto della Società, suggerendo le necessarie modifiche nel

caso in cui le funzioni di gestione e/o qualifica non corrispondano ai poteri di rappresentanza conferiti.

2.4 Le Procedure e il Codice Etico

A supporto del proprio sistema di controllo interno, la Società ha adottato e sta ulteriormente implementando un sistema di procedure interne volte a disciplinare le attività sensibili e, conseguentemente, a prevenire la commissione dei reati presupposto.

Tali procedure, che costituiscono parte integrante del Modello, vengono aggiornate, di volta in volta, al sorgere di nuove esigenze organizzative e di prevenzione di reati.

Di rilevante importanza per il sistema di *governance* della Società, e a completamento dei principi che devono essere rispettati, è il Codice Etico adottato dalla Società, documento che raccoglie ed esplicita i principi ed i valori etici a cui tutti gli amministratori, i dipendenti ed i collaboratori devono ispirarsi nell'esercizio della propria attività, accettando responsabilità, assetti, ruoli e regole.

Il Codice Etico è pubblicato sul sito internet aziendale, così da renderne possibile la diffusione ai destinatari e ai terzi che intrattengano rapporti con la Società.

Inoltre, tutti i fornitori, gli appaltatori ed i subappaltatori sono invitati, da contratto, a prendere visione del Codice Etico e a rispettare i principi di comportamento in esso richiamati.

2.5 Altri Protocolli di Prevenzione

Il sistema protocollare per la prevenzione dei reati, deve essere realizzato applicando alle singole attività sensibili i seguenti Principi Generali di Prevenzione:

- **Regolamentazione:** esistenza di disposizioni aziendali idonee a fornire principi di comportamento, regole decisionali e modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- **Tracciabilità:** ogni operazione relativa all'attività sensibile deve essere, ove possibile, adeguatamente documentata; il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile *ex post*, anche tramite appositi supporti documentali;

- Separazione dei compiti: separazione delle attività tra chi autorizza, chi esegue e chi controlla. Tale segregazione è garantita dall'intervento, all'interno di uno stesso macro processo aziendale, di più soggetti al fine di garantire indipendenza e obiettività dei processi. [La separazione delle funzioni è attuata anche attraverso l'utilizzo di sistemi informatici che abilitano determinate operazioni solo a persone identificate ed autorizzate];
- Attività di monitoraggio: è finalizzata all'aggiornamento periodico e tempestivo di procure, deleghe di funzioni, procedure, nonché del sistema di controllo, in coerenza con il sistema decisionale e con l'intero impianto della struttura organizzativa. Il monitoraggio sui controlli di processo viene svolto dai Responsabili di Processo.

3. FUNZIONE DEL MODELLO

3.1 Il Modello di HS Hospital Service S.p.A.

Scopo del Modello è la costruzione di un sistema strutturato e organico di procedure e attività di controllo, volto a prevenire la commissione delle diverse tipologie di reati contemplate dal Decreto.

In particolare, mediante l'individuazione delle aree di attività a rischio e la conseguente modalità di svolgimento delle predette attività, il Modello si propone come finalità quelle di:

- determinare, in tutti coloro che operano in nome e per conto di HS nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni da parte dell'azienda così come previsto al successivo paragrafo 6.
- ribadire che tali forme di comportamento illecito sono fortemente condannate da HS in quanto contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui la Società intende attenersi nell'espletamento della propria attività aziendale;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle "aree di attività a rischio", di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Punti cardine del Modello sono, oltre ai principi già indicati:

- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la "mappa delle aree di attività a rischio" dell'azienda, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- l'attribuzione all'OdV di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- la verifica e documentazione delle operazioni a rischio;
- il rispetto del principio della separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico.

3.2 Attività preparatoria del Modello

Per la predisposizione del Modello si è proceduto, come suggerito dalle Linee Guida delle principali associazioni di categoria, attraverso la mappatura specifica delle attività aziendali, volta ad individuare le aree a rischio della Società in relazione ai reati di cui alla normativa in esame.

Tale attività, svolta mediante l'analisi della documentazione aziendale già predisposta dalla Società, è stata effettuata principalmente in tre fasi che si sono succedute in un determinato lasso di tempo:

1. la prima fase è stata effettuata sulla base della conoscenza della Società e delle aree di rischio; l'attività di analisi è stata effettuata dalla Società con il supporto di uno Studio legale esterno all'azienda;
2. la seconda fase si è concretizzata attraverso un'audizione, sempre svolta con il supporto di uno Studio legale esterno, del Presidente e Amministratore Delegato della Società e dei responsabili di funzione, per verificare la sussistenza delle aree di rischio già evidenziate, nonché quella eventuale di ulteriori aree di rischio non ancora considerate;
3. all'esito della terza fase, la Società, sempre con il supporto dello Studio legale esterno ha effettuato una "*gap analysis*", ovvero ha individuato i sistemi di controllo già esistenti a presidio delle aree considerate a rischio reato e li ha confrontati con i

requisiti organizzativi richiesti dal Decreto, anche al fine di procedere alla elaborazione del presente Modello.

3.3 Approvazione del Modello e suo recepimento

E' stato demandato al Consiglio di Amministrazione di HS, sulla base anche di criteri e direttive emanati in tal senso, di provvedere mediante apposita delibera all'adozione di un proprio Modello, in funzione dei profili di rischio configurabili nelle attività svolte dalla Società.

Nell'adottare il Modello, il Consiglio di Amministrazione della Società ha proceduto contestualmente anche alla nomina dell'Organismo di Vigilanza, incaricato di svolgere i compiti di controllo sullo svolgimento delle suddette attività e sull'applicazione del Modello medesimo.

E' rimesso alla Società di predisporre, adottare e aggiornare il Modello in relazione alle esigenze di adeguamento che per esso si verranno nel tempo a determinare. In particolare, è demandato al Consiglio di Amministrazione di HS, anche su proposta dell'OdV, di integrare il presente Modello, ove necessario, mediante apposita delibera, con i reati presupposto così come previsti dalle normative nel tempo vigenti.

E', inoltre, rimessa alla responsabilità della Società l'applicazione del Modello in relazione all'attività dalla stessa in concreto posta in essere. A tal fine è attribuito all'OdV il compito primario di esercitare i controlli sull'attuazione del Modello stesso secondo le procedure in esso descritte.

3.4 Struttura del Modello: Parte Generale e Parte Speciale in funzione delle diverse aree funzionali impattate

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale" predisposta per aree funzionali aziendali in relazione alle diverse tipologie di reato contemplate nel Decreto e ritenute, all'esito dell'attività di *risk assessment* astrattamente ipotizzabili in capo alla Società.

Si rileva, inoltre, che l'introduzione di alcuni reati ha carattere meramente prudenziale in quanto, pur non sussistendo elementi specifici da cui dedurre l'esistenza di attuali rischi, si tratta di reati sui quali la Società intende comunque mantenere un alto livello di attenzione.

La Parte Speciale si compone di diverse aree funzionali raggruppate come segue:

- **Parte Speciale SEZIONE “A”** relativa alla funzione Consiglio di Amministrazione (Presidente, Amministratore Delegato e Consiglieri);
- **Parte Speciale SEZIONE “B”** relativa alle aree funzionali: Regulatory Affairs e Qualità;
- **Parte Speciale SEZIONE “C”** relativa all'area funzionale: Settore Amministrativo, Finanziario e Risorse Umane;
- **Parte Speciale SEZIONE “D”** relativa alla funzione: Settore Ricerca e Sviluppo;
- **Parte Speciale SEZIONE “E”** relativa all'area funzionale: Settore Hardware e Software;
- **Parte Speciale SEZIONE “F”** relativa all'area funzionale: Produzione Interna (funzioni: Responsabile Settore Tecnico Produttivo Interno, Responsabile Camera bianca, Responsabile Magazzino, Responsabile Assembly & Packaging, Resp. Assistenza Tecnica e Controllo Qualità);
- **Parte Speciale SEZIONE “G”** relativa alla funzione: Direzione Acquisti;
- **Parte Speciale SEZIONE “H”** relativa alle aree funzionali: Direzione commerciale e Direzione Marketing (Dir. Vendite Naz. Endosurgery, Dir. Vendite Naz. Interventistica e Terapie ablativie, Dir. Vendite Naz. Critical Care, Dir. Vendite Estero Biopsy & Critical Care, Responsabile Customer Service Italia, Responsabile Customer Service Estero)
- **Parte Speciale SEZIONE “I”** relativa alle funzioni esternalizzate: Responsabile del Servizio di Prevenzione e Protezione.

4. L'ORGANISMO DI VIGILANZA (ODV)

4.1 Identificazione dell'Organismo di Vigilanza

In attuazione di quanto previsto dal Decreto – il quale pone come condizione, per la concessione dell'esimente dalla responsabilità amministrativa, che il compito di vigilare sul

funzionamento e l'osservanza del modello sia affidato a un organismo dell'ente – è stato individuato, nell'ambito di HS, un Organismo di Vigilanza costituito da due membri effettivi, entrambi scelti tra professionisti esterni all'azienda.

L'OdV deve presentare i seguenti requisiti:

1. autonomia: deve avere un'autonomia decisionale, qualificabile come imprescindibile libertà di autodeterminazione e d'azione, con totale esercizio della discrezionalità tecnica nell'espletamento delle proprie funzioni;
2. indipendenza rispetto alla Società: deve essere scevro da condizionamenti dipendenti da legami di sudditanza rispetto al vertice di controllo e deve essere un organo terzo, collocato in posizione di indipendenza anche gerarchica, capace di adottare provvedimenti ed iniziative autonome;
3. professionalità: deve essere professionalmente capace ed affidabile, sia per quanto riguarda i singoli membri che lo compongono, sia nella sua globalità. Deve disporre, come organo, delle cognizioni tecniche e delle professionalità necessarie al fine di espletare al meglio le funzioni affidategli;
4. continuità di azione: deve svolgere le funzioni assegnategli in via continuativa, seppure non in modo esclusivo;
5. onorabilità ed assenza di conflitti di interesse: non può essere nominato membro dell'OdV e, se del caso, decade dalla carica, il soggetto che:
 - sia interdetto, inabilitato o fallito o che sia comunque stato condannato per uno dei reati previsti dal Decreto o, comunque, ad una delle pene che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;
 - abbia rapporti d'affari (intesi, ad esempio, quali rapporti di partnership, contratti di associazione in partecipazione, joint venture, ecc.) con la Società o le altre società controllate o che la controllano.

Tuttavia, qualora un membro dell'OdV abbia un interesse per conto proprio o di terzi in una delibera, dovrà darne comunicazione agli altri membri dell'Organismo, specificandone la natura, i termini, l'origine e la portata. Gli altri membri decideranno se il soggetto interessato dovrà astenersi dalla delibera.

Il Consiglio di Amministrazione di HS nomina i membri effettivi, i quali restano in carica per tre anni.

E' facoltà dell'OdV farsi coadiuvare, nelle sue funzioni di controllo, da soggetti esterni che svolgano professionalmente attività di *audit* e certificazione.

E', altresì, facoltà dell'Organismo scegliere tra i suoi componenti il Presidente, ove questo non sia nominato dal Consiglio di Amministrazione.

Il Presidente coordina i lavori dell'Organismo di Vigilanza e provvede affinché siano fornite a tutti i membri adeguate informazioni sulle materie iscritte all'ordine del giorno.

4.2 Modalità di convocazione e tenuta delle riunioni dell'OdV

L'OdV si raduna tutte le volte che il Presidente o uno dei membri lo ritenga opportuno, oppure quando ne sia fatta richiesta dal Consiglio di Amministrazione o dal Collegio Sindacale e comunque almeno ogni tre mesi.

Le sedute dell'OdV saranno tenute nel luogo designato nell'avviso di convocazione, contenente l'indicazione del giorno, dell'ora e del luogo dell'adunanza e l'elenco delle materie da trattare. L'avviso di convocazione, da comunicare a ciascun membro dell'Organismo (per mezzo di posta ordinaria od elettronica, telegramma, fax, a mano), dovrà essere inviato almeno tre giorni prima di quello fissato per la seduta stessa ovvero, in caso di urgenza, almeno un giorno prima.

Le adunanze dell'OdV potranno essere tenute anche per audio e/o videoconferenza, a condizione che tutti i partecipanti possano essere identificati e sia loro consentito seguire la discussione e intervenire alla trattazione degli argomenti e alla votazione.

Le decisioni dell'OdV sugli argomenti in esame possono essere adottate mediante consultazione scritta ovvero mediante consenso espresso per iscritto.

Tali delibere, così come i rapporti relativi alle verifiche compiute dall'Organismo stesso direttamente o tramite collaboratori esterni, saranno trascritte sul Libro delle Adunanze dell'Organismo.

4.3 Funzioni e poteri dell'OdV

All'Organismo di Vigilanza di HS è affidato il compito di vigilare:

- sull'osservanza delle prescrizioni del Modello da parte dei destinatari, appositamente individuati nelle singole Parti Speciali in relazione alle diverse tipologie di reati contemplate dal Decreto;
- sulla reale efficacia ed effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei reati di cui al Decreto;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali.

Sul piano operativo è affidato all'OdV il compito di:

- attivare le procedure di controllo, tenendo presente che la responsabilità primaria sul controllo delle attività, anche per quelle relative alle aree di attività a rischio, resta comunque demandata al management operativo e forma parte integrante del processo aziendale, il che conferma l'importanza di un processo formativo del personale;
- condurre ricognizioni dell'attività aziendale ai fini della mappatura aggiornata delle aree di attività a rischio nell'ambito del contesto aziendale;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di attività a rischio come definite nelle singole Parti Speciali del Modello;
- promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione organizzativa interna necessaria al fine del funzionamento del Modello stesso, contenente le istruzioni, i chiarimenti o gli aggiornamenti;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV o tenute a sua disposizione;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle aree a rischio. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle suddette aree a rischio, e ha libero accesso a tutta la documentazione aziendale rilevante. All'OdV devono essere, inoltre, segnalate da parte del management eventuali situazioni dell'attività aziendale che possano esporre l'azienda al rischio di commissione di un reato;

- controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di reati. In particolare all'OdV devono essere segnalate le attività più significative o le operazioni contemplate dalle Parti Speciali, devono essere messi a sua disposizione i dati di aggiornamento della documentazione, al fine di consentire l'effettuazione dei controlli;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di reati (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a un aggiornamento degli elementi stessi;
- coordinarsi con i responsabili delle altre funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello (definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, ecc.).

4.4 Funzioni dell'OdV: autonomia nei confronti degli organi societari

L'OdV di HS è organo autonomo rispetto agli organi societari ed esente da vincoli di subordinazione gerarchica.

Tuttavia, ha come referenti aziendali, su base continuativa, il Presidente della Società e, su base periodica, il Consiglio di Amministrazione e/o il Collegio Sindacale.

L'OdV della Società potrà essere chiamato in qualsiasi momento dai suddetti organi - o potrà, a sua volta, presentare richiesta in tal senso - per riferire in merito al funzionamento del Modello o a situazioni specifiche.

Ogni anno, inoltre, l'OdV trasmette al Consiglio di Amministrazione un rapporto scritto sulle attività svolte e sull'attuazione del Modello.

L'OdV è dotato di appropriata autonomia di spesa, essendo previsto un budget annuale pari ad Euro [10.000,00]. Le eventuali spese straordinarie saranno sottoposte all'approvazione del Consiglio di Amministrazione.

4.5 Flussi informativi nei confronti dell'OdV

L'OdV di HS deve essere tempestivamente informato da tutti i soggetti destinatari del Modello in merito a qualsiasi notizia relativa all'esistenza di possibili violazioni del Modello stesso. In particolare, devono segnalare le notizie relative alla commissione o alla possibile commissione dei reati o di deviazioni comportamentali rispetto ai principi contenuti nel Modello.

In ogni caso, devono essere comunicate all'OdV:

a) Le informazioni che possono avere attinenza con potenziali violazioni del Modello quali, a titolo meramente esemplificativo:

- eventuali offerte o richieste di denaro di doni (eccedenti il valore modico) o di altre utilità provenienti da o destinate a pubblici ufficiali o incaricati di pubblico servizio;
- partecipazione a gare d'appalto ed aggiudicazione delle stesse e in genere instaurazione di rapporti con la Pubblica Amministrazione;
- l'eventuale concessione di erogazioni pubbliche, il rilascio di nuove licenze, di autorizzazioni o di altri rilevanti provvedimenti amministrativi;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini per i reati, anche nei confronti di ignoti qualora tali indagini coinvolgano la Società e/o suoi esponenti aziendali e/o dipendenti;
- le richieste di assistenza legale inoltrate dagli esponenti aziendali in caso di avvio di procedimento giudiziario per i reati;
- le notizie relative ai procedimenti sanzionatori effettuati dalle Pubbliche Autorità e alle eventuali misure irrogate (ivi compresi i provvedimenti verso gli esponenti aziendali) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di reati o violazione delle regole di comportamento o procedurali del Modello;
- anomalie di spese emerse dalle richieste di autorizzazione;
- eventuali operazioni finanziarie che assumano particolare rilievo per valore, modalità, rischiosità o atipicità;

- eventuali omissioni o trascuratezze nella tenuta della contabilità su cui si fondano le registrazioni contabili;
- eventuali segnalazioni, non tempestivamente riscontrate dalle funzioni competenti, concernenti sia carenze o inadeguatezze dei luoghi o delle attrezzature di lavoro o dei dispositivi di protezione messi a disposizione della Società, sia ogni altra situazione di pericolo connessa alla sicurezza sul lavoro.

b) Le informazioni attinenti i compiti dell'OdV e che possono assumere rilevanza per l'espletamento delle sue funzioni, quali, ad esempio:

- le notizie relative ai cambiamenti organizzativi della Società;
- notizie concernenti l'attuazione del Modello e alle sanzioni che, in conseguenza della mancata osservazione dello stesso, siano irrogate;
- i rapporti preparati dalle varie funzioni in merito a quelle attività che sono ritenute o che possono ritenersi attinenti ad aree a rischio della Società;
- il bilancio annuale, corredato dalla nota integrativa e la situazione patrimoniale;
- le comunicazioni, da parte del Collegio Sindacale relative a criticità emerse, anche se risolte.

I soggetti che intendono effettuare le segnalazioni, per non subire ritorsioni o discriminazioni di alcun tipo, devono essere tutelati dall'OdV e quindi godere di riservatezza. A questo proposito, al fine di facilitare le segnalazioni, qualsiasi destinatario del Modello potrà inviare la comunicazione all'apposita casella di posta elettronica odvhsspa@gmail.com. Le segnalazioni devono essere conservate presso l'ufficio dell'OdV.

4.6 Modalità di funzionamento dell'OdV

L'OdV programma le attività di controllo periodico in funzione dello stato delle attività aziendali e delle informazioni in suo possesso.

Il programma viene approvato dall'OdV in occasione delle riunioni dello stesso ed indica quali aree e funzioni intende verificare e rispetto a quali criteri ed entro quale data debbano essere svolte tali attività. Le verifiche potranno essere affidate sia ai membri dell'OdV sia affidate, dall'OdV, a consulenti esterni.

Al termine di ogni verifica deve essere predisposto un rapporto che illustri l'attività svolta e le risultanze della stessa. Tra le risultanze devono essere indicate:

- le aree aziendali verificate ed ogni informazione utile ulteriore;
- il livello di conformità ovvero le criticità rilevate rispetto ai criteri dell'*audit*;
- il richiamo ai documenti di controllo;
- le eventuali raccomandazioni;
- ogni altra informazione ritenuta opportuna per la migliore valutazione dell'attività sottoposta a verifica.

In occasione della successiva riunione dell'OdV verranno esaminate le risultanze delle attività. L'OdV, ove lo ritenga opportuno, potrà effettuare degli ulteriori *audit* di approfondimento, anche a mezzo di consulenti esterni, ovvero richiedere all'organo amministrativo della Società di intervenire per riportare il livello di rischio a livelli ritenuti accettabili.

Le raccomandazioni dell'OdV devono trovare tempestivo accoglimento da parte delle funzioni interessate ed è compito del Consiglio di Amministrazione verificarne l'efficace applicazione.

L'OdV solleciterà riunioni periodiche con il Collegio Sindacale per la condivisione delle strategie di controllo e prenderà visione dei verbali di verifica del Collegio Sindacale e a questo invierà le proprie risultanze.

In tutti i casi in cui la Società incarichi un soggetto esterno che svolga professionalmente attività di certificazione, di svolgere attività di verifica e certificazione in merito ad aspetti delle attività aziendali rientranti nella competenza dell'OdV, tale soggetto dovrà predisporre un rapporto che contenga tutte le indicazioni sopra riportate. Il rapporto dovrà essere trasmesso all'OdV con data certa in tempo utile per permettere allo stesso di esaminare tali rapporti e le relative risultanze.

4.7 Flussi informativi alternativi e Sistema Whistleblowing

In ossequio a quanto recentemente introdotto dalla Legge n. 179 del 30 novembre 2017, (GU n. 291 del 14 dicembre 2017), la Società sta implementando un canale ulteriore di flussi di informazione alternativo a quello verso l'Organismo di Vigilanza.

In particolare, la Legge n. 179 del 30 novembre 2017, "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", ha modificato l'art. 6 del d.lgs. 231/2001 ed ha infatti esteso l'istituto del "Whistleblowing", ovvero l'eventuale denuncia di condotte illecite da parte dei dipendenti di una organizzazione, al settore privato, per cui le società dotate di un Modello 231 dovranno individuare uno o più canali che consentano ai dipendenti di presentare segnalazioni circostanziate nel caso in cui vengano a conoscenza di condotte illecite, tenuto conto che almeno un canale informatico deve essere idoneo a garantire la riservatezza del segnalante.

Lo scopo del sistema di Whistleblowing è quello di permettere alla Società di affrontare il problema segnalato il prima possibile, rendendo note situazioni di rischio o di danno e contribuendo alla prevenzione e al contrasto di eventuali illeciti.

Pubblicato in Gazzetta Ufficiale lo scorso 15 Marzo, **il D. LGS. 24/2023 predispone nuove regole circa il whistleblowing**, ovvero la segnalazione di illeciti di cui un dipendente, collaboratore, professionista sia venuto a conoscenza in ragione del rapporto di lavoro. Ad oggi, esistono ovviamente delle procedure legislative volte ad agevolare la pratica. Tali normative, tuttavia, sono state più volte tacciate di attribuire ai segnalanti (o whistleblower) una protezione inadeguata.

Il nuovo decreto si rivela dunque un **importante punto di svolta rispetto a quanto sino ad oggi previsto dalla normativa di settore**.

Approvato durante la seduta del Consiglio dei Ministri del 9 Marzo, il nuovo documento prevede l'implemento delle pratiche già esistenti, l'introduzione di nuove discipline e tutele più blindate per i whistleblower.

Per attuare le nuove disposizioni, sono state comunicate **due deadline**. Per le realtà **con una media di lavoratori dai 250 dipendenti** (a tempo determinato o indeterminato) in poi nell'ultimo anno, la data a cui fare riferimento è stata quella del **15 Luglio 2023**. Per le imprese **con una media di almeno 50 lavoratori** (a tempo determinato o indeterminato) in media nell'ultimo anno, invece, la scadenza è impostata per il **17 Dicembre 2023**.

Nel caso in cui non si effettui l'aggiornamento entro tali date, sono state **disposte pesanti sanzioni amministrative**, il cui importo varierà in base alle singole situazioni. Gli importi definiti vedono multe dai 5mila ai 30mila euro in caso di attività ritorsive, e importi tra i 10mila e i 50mila euro in caso di mancata implementazione dei canali di segnalazione.

LA TUTELA DEL WHISTLEBLOWING PRIMA DEL NUOVO DECRETO

Antecedentemente all'approvazione del D. LGS. 24/2023, nel settore pubblico, la regolamentazione del whistleblowing era garantita dall'art. 54-bis del D. Lgs. 165/2001. Quest'ultimo disponeva espressamente il divieto di ripercussioni per il pubblico dipendente qualora segnalasse al responsabile della prevenzione della corruzione e della trasparenza, all'Autorità Nazionale Anti Corruzione (ANAC) o all'Autorità giudiziaria, condotte illecite da lui apprese.

Per quanto concerne il settore privato, invece, come visto, la disciplina veniva dettata dalla Legge 179/2017. Tale provvedimento richiedeva alle società del settore privato con modelli organizzativi ex D. LGS. 231/2001 di dotarsi obbligatoriamente di canali di segnalazione delle condotte illecite ritenute rilevanti ai sensi della normativa. Allo stesso tempo, le imprese avevano l'onere di garantire il divieto di atti ritorsivi o discriminatori nei confronti del whistleblower per le segnalazioni effettuate.

Il D. LGS. 24/2023 ha abrogato tali disposizioni e imposto una rilettura della disciplina.

Il nuovo documento riconosce infatti alla segnalazione un ruolo chiave nella prevenzione delle violazioni normative e assicura ai segnalanti di imprese sia pubbliche che private, una tutela più strutturata. Il decreto aggiorna così la legislazione italiana, armonizzandola con quelle che sono le norme del Parlamento europeo e del Consiglio circa la protezione delle persone che segnalano violazioni del Diritto dell'Unione e di disposizioni normative nazionali.

Con il D. LGS 24/2023 aumentano infatti le condotte meritevoli di segnalazione: la disciplina prevista dal decreto si estende infatti anche alle violazioni che possano ledere gli interessi dell'Unione Europea. Ricadono nella normativa anche le violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità della Pubblica Amministrazione o dell'ente privato, inclusi gli illeciti amministrativi, contabili, civili o penali. In continuità con il passato, vengono annoverate anche "le condotte illecite rilevanti ai sensi del Decreto legislativo 8 giugno 2001, n. 231 o violazioni dei modelli di organizzazione e di gestione".

Rimangono, invece, **escluse dal decreto le segnalazioni circa i rapporti individuali di lavoro e quelle in materia di sicurezza e difesa nazionale.**

LE SPECIFICHE DEL D. LGS. 24/2023

Il D. LGS. 24/2023 amplia l'**ambito di applicazione soggettivo** della disciplina in materia di whistleblowing. Con questo nuovo decreto, sono adesso **inclusi tra i soggetti tutelabili anche collaboratori autonomi, liberi professionisti, volontari, azionisti e amministratori**.

Il Decreto differenzia inoltre gli enti destinatari della nuova disciplina in **“soggetti del settore pubblico”** e **“soggetti del settore privato”**.

Vediamo quindi quale tipologia di impresa ricade nelle nuove tipologie di classificazione.

Soggetti del settore pubblico

Si intendono come tali le amministrazioni pubbliche, le Autorità indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli enti di diritto privato sottoposti a controllo pubblico, gli organismi di diritto pubblico, i concessionari di pubblico servizio e le società in house, anche se quotate.

Soggetti del settore privato

Questi enti vengono individuati “in negativo” rispetto a quelli del settore pubblico. Il D. LGS. 24/2023 li circoscrive, rivolgendosi, in particolare, a una serie di casi, di seguito riportata.

1. **Realtà aziendali in cui la media dei lavoratori impiegati sia inferiore alle 50 unità** In questi casi, il whistleblower potrà segnalare condotte illecite rilevanti ai sensi del D. LGS. 231/2001 o violazioni del modello organizzativo, facendo ricorso al solo canale di segnalazione interno;
2. **Enti con una media di lavoratori superiore alle 50 unità** Date queste eventualità, invece, il whistleblower avrà la possibilità di segnalare, oltre alle violazioni contemplate dalla nuova normativa, anche quelle attinenti al diritto dell'Unione Europea. L'ente potrà fare ricorso a tutti i canali di segnalazione di cui al D. LGS. 24/2023.

Rispetto alla norme preesistenti, che contemplavano il solo uso di canali di segnalazione interni, il decreto introduce **ulteriori modalità** attraverso cui il whistleblower può **comunicare gli illeciti** di cui sia venuto a conoscenza. Il documento amplia infatti i canali a disposizione, prevedendone **uno di segnalazione esterna, predisposto e gestito dall'ANAC**.

Entro tre mesi dalla data di entrata in vigore del D. Lgs. 24/2023, tale Autorità – sentito il Garante Privacy – dovrà adottare delle linee guida in tema di presentazione e gestione delle segnalazioni

esterne, prevedendo il ricorso a strumenti di crittografia che garantiscano la riservatezza del segnalante e della persona menzionata nella segnalazione - o comunque coinvolta.

5. SELEZIONE, FORMAZIONE E INFORMATIVA

5.1 Selezione del personale

La scelta e la gestione del personale e dei collaboratori esterni (consulenti, partner, fornitori, ecc.) deve rispondere a criteri di ragionevolezza, professionalità, integrità, correttezza e trasparenza in ossequio alle esigenze aziendali in relazione all'applicazione del Decreto.

5.2 Formazione del personale

La formazione del personale è un'attività fondamentale ai fini di una completa ed efficace attuazione del Modello. Pertanto l'OdV provvede a redigere e a realizzare piani di formazione che prevedano anche interventi di tipo diversificato, a seconda della collocazione del personale all'interno della Società o della pertinenza delle rispettive attività ad una delle aree a rischio indicate nel Modello.

5.3 Diffusione dei contenuti del Modello

Il Modello, una volta approvato dal Consiglio di Amministrazione, viene diffuso a tutti i dipendenti ai quali è fatto obbligo di rispettare il documento. Saranno di volta in volta definite le modalità di diffusione del Modello nei confronti degli ulteriori soggetti tenuti al rispetto dei contenuti dello stesso (fornitori, collaboratori esterni e terzi in generale).

5.4 Informativa ai collaboratori esterni

Potranno essere forniti ai collaboratori esterni apposite informative sulle politiche e le procedure adottate dalla Società sulla base del presente Modello, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

6. SISTEMA DISCIPLINARE E MISURE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO

6.1 Principi generali

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'effettività del Modello stesso e per rendere efficiente l'azione di vigilanza dell'OdV.

Al riguardo, infatti, l'art. 6 comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione devono *"introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello"*.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dalla Società in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

Il sistema disciplinare, così come previsto dall'art. 7 comma 1, Legge 300/1970 ("Statuto dei lavoratori"), sarà affisso sulla bacheca aziendale.

L'accertamento delle infrazioni può essere avviato anche d'impulso dell'OdV che abbia, nel corso della sua attività di controllo e vigilanza, rilevato una possibile infrazione del Modello.

L'irrogazione delle sanzioni nei confronti di quadri, impiegati, operai e dirigenti sono di competenza dell'Amministratore Delegato, in conformità alle deleghe lui conferite.

L'OdV può, inoltre, essere chiamato a svolgere una funzione consultiva nel corso dell'intero procedimento disciplinare al fine di acquisire eventuali elementi utili in vista del costante aggiornamento del Modello. L'accertamento delle eventuali responsabilità derivanti dalla violazione del Modello e l'attribuzione della conseguente sanzione devono essere comunque condotti nel rispetto della vigente normativa, della tutela della privacy, della dignità e della reputazione dei soggetti coinvolti.

Il sistema disciplinare viene costantemente monitorato dall'Organismo di Vigilanza e dall'Amministratore Delegato.

6.2 Sanzioni per i lavoratori dipendenti e misure nei confronti degli Amministratori e dei collaboratori esterni

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti come illeciti disciplinari.

In relazione a quanto sopra, il Modello fa riferimento a delle categorie di fatti che descrivono i comportamenti sanzionati, a seconda del rilievo che assumono le singole fattispecie considerate, e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

In particolare, si prevede che:

- a) Incorre nei provvedimenti di RICHIAMO VERBALE, RICHIAMO SCRITTO, MULTA (in misura non eccedente l'importo di 4 ore della normale retribuzione) O SOSPENSIONE DAL LAVORO E DALLA RETRIBUZIONE (per un massimo di giorni 10), secondo la gravità della violazione, il lavoratore che violi le procedure interne previste dal presente Modello o adottati, nell'espletamento delle proprie attività, un comportamento non conforme alle prescrizioni del Modello stesso e del Codice Etico, dovendosi ravvisare in tali comportamenti una violazione del contratto che comporta un pregiudizio alla disciplina e morale dell'azienda;
- b) Incorre nel provvedimento di LICENZIAMENTO PER GIUSTA CAUSA il lavoratore che adottati, nell'espletamento delle proprie attività, un comportamento palesemente in violazione alle prescrizioni del presente Modello tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento il compimento di *"delitti a termini di legge"* o *"atti tali da far venire meno radicalmente la fiducia della Società nei suoi confronti"*, ovvero il verificarsi delle mancanze richiamate ai punti precedenti con la determinazione di un grave pregiudizio morale e/o materiale per la Società.

Il tipo e l'entità delle sanzioni sopra richiamate, comminate al personale dipendente, dovranno, in sede applicativa, essere commisurati al principio di proporzionalità previsto dall'art. 2106 c.c., dovendosi tenere conto per ciascuna fattispecie:

- dell'intenzionalità e del grado di reiterazione del comportamento, del grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- della gravità oggettiva del fatto costituente infrazione disciplinare;
- del comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- delle mansioni del lavoratore;
- della posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- delle altre particolari circostanze che accompagnano la violazione disciplinare.

A titolo esemplificativo e non esaustivo, costituiscono infrazioni disciplinari i seguenti comportamenti:

- la violazione, anche con condotte omissive e in eventuale concorso con altri, dei principi e delle procedure previste dal presente Modello o stabilite per la sua attuazione;
- la redazione, eventualmente in concorso con altri, di documentazione non veritiera;
- l'agevolazione, mediante condotta omissiva, della redazione da parte di altri, di documentazione non veritiera;
- l'omessa redazione della documentazione richiesta dal presente Modello o dalle procedure stabilite per la sua attuazione;
- la sottrazione, la distruzione o l'alterazione della documentazione inerente la procedura per sottrarsi al sistema dei controlli previsto dal Modello;
- l'ostacolo alla attività di vigilanza dell'OdV o dei soggetti dei quali lo stesso si avvale;
- l'impedimento all'accesso alle informazioni e alla documentazione richiesta dai soggetti preposti ai controlli delle procedure e delle decisioni;
- La realizzazione di qualsiasi altra condotta idonea a eludere il sistema di controllo previsto dal Modello.

6.3 Misure nei confronti degli Amministratori

La Società valuta con estremo rigore le infrazioni al presente Modello poste in essere da coloro che rappresentano il vertice della Società e ne manifestano, dunque, l'immagine

verso i dipendenti, gli azionisti, i creditori ed il pubblico. La formazione e il consolidamento di un'etica aziendale sensibile ai valori della correttezza e della trasparenza presuppone, innanzitutto, che tali valori siano fatti propri e rispettati da coloro che guidano le scelte aziendali, in modo da costituire esempio e stimolo per tutti coloro che, a qualsiasi livello, operano per la Società.

In caso di violazione da parte degli Amministratori delle procedure interne e dei principi di comportamento previsti dal presente Modello e/o di adozione, nell'esercizio delle proprie attribuzioni, di provvedimenti che contrastino con le disposizioni o i principi del Modello, l'OdV informa tempestivamente tutti i membri del Consiglio di Amministrazione e tutti i componenti del Collegio sindacale, i quali, a seconda delle rispettive competenze, provvederanno ad assumere le iniziative più opportune ed adeguate coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto (ad es., dichiarazioni nei verbali delle adunanze, convocazione dell'Assemblea dei soci per deliberare in merito ai provvedimenti nei confronti dei soggetti responsabili della violazione tra cui la revoca della nomina di amministratore e l'eventuale adozione delle azioni di responsabilità previste dalla legge, ecc.).

6.4 Misure nei confronti dei membri del Collegio Sindacale

Con riguardo ai membri del Collegio Sindacale, le violazioni delle prescrizioni contenute nel presente Modello sono segnalate tempestivamente dall'OdV, a tutti i componenti del Collegio Sindacale nonché a tutti i membri del Consiglio di Amministrazione. Il Collegio Sindacale assume, sentito il parere del Consiglio di Amministrazione, gli opportuni provvedimenti nei confronti dei Sindaci che hanno compiuto le violazioni contestate.

6.5 Misure nei confronti di collaboratori esterni e partner

Ogni comportamento posto in essere dai collaboratori esterni o dai partner in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, grazie all'attivazione di opportune clausole, la risoluzione del rapporto contrattuale.

6.6 Misure in caso di violazione degli obblighi di informazione nei confronti dell'OdV

In caso di violazioni degli obblighi d'informazione o in caso di mancata risposta alle richieste di informazioni promosse dall'OdV, l'OdV stesso informerà prontamente il Consiglio di Amministrazione, che potrà adottare le sanzioni più opportune.

6.7 Misure nei confronti di membri dell'ODV in caso di illeciti disciplinari

In caso di illeciti disciplinari commessi da membri dell'OdV, il Consiglio di Amministrazione dovrà essere prontamente informato e lo stesso potrà richiamare per iscritto tale membro dell'OdV o revocarlo, a seconda della gravità dell'illecito commesso. Le sanzioni previste per i dipendenti e dirigenti si applicheranno, altresì, ai membri dell'OdV che ricadano in tali categorie.

6.8 Misure in caso di violazione del Sistema Whistleblowing

In ossequio alla legge del Whistleblowing (di cui al precedente punto 4.7), è fatto divieto di ritorsione nei confronti del soggetto segnalante.

Sono, inoltre, previste sanzioni nei confronti di chi dovesse violare dette misure di tutela e di chi, con dolo o colpa grave, dovesse formulare segnalazioni infondate.

Le sanzioni verranno applicate sulla base dello Statuto dei Lavoratori (legge n. 300/1970) e dei singoli Contratti Collettivi Nazionali, differenziando, quindi, tra soggetti dirigenti e dipendenti.

INTRODUZIONE. FUNZIONE DELLA PARTE SPECIALE

Scopo della presente Parte Speciale è fare in modo che tutti i destinatari del Modello (quali, a titolo esemplificativo, i dipendenti, i dirigenti, gli amministratori, i liquidatori, i consulenti, i fornitori, i collaboratori esterni, i partner della Società ecc. e, in generale, tutti coloro che sono tenuti a rispettare il presente Modello, di seguito i “Destinatari”) adottino regole di condotta adeguate e conformi a quanto prescritto al fine di impedire il verificarsi dei reati in essa considerati.

In particolare, la Parte Speciale ha la funzione di:

- a) descrivere i principi procedurali – generali e specifici – che i Destinatari del Modello sono tenuti ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all’Organismo di Vigilanza gli strumenti esecutivi per esercitare l’attività di controllo e verifica previste dal Modello.

Per quanto concerne le seguenti ipotesi di reato previste dal Decreto:

- falsi nummari;
- delitti contro la personalità individuale (riduzione in schiavitù e pedopornografia);
- delitti di criminalità organizzata e reati transnazionali;
- induzione a non rendere dichiarazioni o rendere dichiarazioni mendaci all’autorità giudiziaria;
- delitti con finalità di terrorismo o di eversione dell’ordinamento democratico;
- reato di impiego di cittadini di paesi terzi il cui soggiorno in Italia è irregolare;
- pratiche di mutilazione degli organi genitali femminili,

si ritiene che il rischio di concretizzazione di tali reati sia trascurabile, fermo restando, comunque, la previsione del rinvio a condotte rispettose delle normative in materia, nonché alle regole generali di comportamento di cui al presente Modello.

1. SEZIONE A – Il Consiglio di Amministrazione: Presidente e Consiglieri.

Questa sezione si occuperà di analizzare l’area di rischio relativa al Consiglio di Amministrazione che in HS è composto da Presidente e due Consiglieri. **(VERIFICARE)**

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte dal C.d.A. e nell’ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

CONSIGLIO DI AMMINISTRAZIONE e DIREZIONE GENERALE (Presidente e Consiglieri)	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.); • Gestione delle gare e dei bandi pubblici; • Scelta di fornitori e consulenti; • Richiesta e ottenimento di finanziamenti pubblici; • Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi; • Spese di rappresentanza; • Assunzione del personale; • Accesso ai sistemi informatici della Pubblica Amministrazione; • Gestione dei contenziosi.
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto)	Contraffazione, alterazione o uso di marchi.
Reati societari (art. 25-ter)	• Tenuta delle scritture contabili e dei Libri Sociali; • Creazione di fondi extracontabili; • Gestione degli ordini e delle fatture; • Gestione della liquidità; • Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale; • Scelta consulenti/fornitori/partner commerciali.
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme in materia di sicurezza sul lavoro (Art. 25-septies)	• Documento di Valutazione dei Rischi (DVR); • Gestione delle misure di sicurezza; • Gestione delle gare pubbliche; • Manutenzione delle infrastrutture e sicurezza delle zone di produzione e magazzino; • Formazione del personale.
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	• Scelta consulenti/fornitori/partner commerciali; • Gestione dei flussi finanziari/creazione di fondi extracontabili; • Gestione della liquidità e cassa.
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Gestione delle licenze e dei software per elaboratore.
Reati ambientali (art. 25-undecies del Decreto): • attività gestione rifiuti non autorizzata, • traffico illecito di rifiuti, • attività organizzate per il traffico illecito di rifiuti, • inquinamento del suolo, sottosuolo, delle acque superficiali e sotterranee,	• Tutela del suolo, sottosuolo e delle acque (es. sversamenti da impianto di depurazione); • Gestione dei rifiuti (es. dismissione degli impianti, gestione dei rifiuti di apparecchiature meccaniche, elettriche ed elettroniche, ecc.)

• violazione obblighi di comunicazione, • false indicazioni su natura e composizione dei rifiuti, • inquinamento ambientale art. 452bis c.p., • disastro ambientale art. 452 ter c.p., • traffico e abbandono di materiale radioattivo 452quinquies c.p., • impedimento del controllo 452sexies c.p. • omessa bonifica 452terdecies c.p.)	
Reati tributari (art. 25-quinquiesdecies del Decreto)	• Gestione della contabilità • Acquisto di beni e servizi • Adempimenti fiscali e tributari in genere • Tenuta e custodia delle scritture contabili e fiscali • Gestione di eventuali operazioni straordinarie
Reati di contrabbando (art. 25-sexiesdecies)	• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine; • Scarico e deposito delle merci oltre confine.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

1.1. I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- ✓ **malversazione a danno dello Stato**, (art. 316-bis c.p.): *"Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni"*
- È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **indebita percezione di erogazioni a danno dello Stato**, (art. 316-ter c.p.): *"(Comma 1) Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle*

*Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. **La pena è della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.***² (Comma 2). Quando la somma indebitamente percepita è pari o inferiore a lire sette milioni settecentoquarantacinquemila si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da dieci a cinquanta milioni di lire. Tale sanzione non può comunque superare il triplo del beneficio conseguito” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Truffa** (art. 640, comma 2, n. 1 c.p.): “(Comma 1). Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinquecento a diecimila. 2. La pena è della reclusione da uno a cinque anni e della multa da lire tremila a quindicimila:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea³ o col pretesto di far esonerare taluno dal servizio militare;

2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;

2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

3) Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), “La pena è della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Frode informatica** (art. 640-ter c.p.): “(Comma 1). Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza

² Aggiornamento del D.Lgs. 74/2020.

³ Aggiornamento del D.Lgs. 74/2020.

diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. (Comma 2). La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. (Comma 3). La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Frode nelle pubbliche forniture** (art. 356 c.p.)⁴: *"Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore ad euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- ✓ **Frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale** (art. 2 L. 898/1986): *" (Comma 1). 1. Ove il fatto non configuri il più grave reato previsto dall'articolo 640-bis del codice penale, chiunque, mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il danno o il profitto sono superiori a euro 100.000. Quando la somma indebitamente percepita è pari od inferiore a 5.000 euro si applica soltanto la sanzione amministrativa di cui agli articoli seguenti. (Comma 2). Agli effetti della disposizione del precedente comma 1 e di quella del comma 1 dell'articolo 3, alle erogazioni a carico del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale sono assimilate le quote nazionali previste dalla normativa comunitaria a complemento delle somme a carico di detti Fondi, nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa comunitaria. (Comma 3). Con la sentenza il giudice determina altresì l'importo indebitamente percepito e condanna il colpevole alla restituzione di esso*

⁴ Fattispecie inserita dal D.Lgs. 75/2020.

all'amministrazione che ha disposto la erogazione di cui al comma 1" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote.

L'art. 25⁵ rubricato "Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", elenca le seguenti fattispecie criminose quali reati suscettibili di far scattare la responsabilità dell'Ente ex Decreto:

- ✓ **Peculato** (art. 314, co. 1, c.p.): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro [c.p. 458] o di altra cosa mobile altrui [c.c. 812, 814], se ne appropria, è punito con la reclusione da quattro anni a dieci anni e sei mesi."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Peculato mediante profitto dell'errore altrui** (art. 316): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni. (Comma 2) La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000⁶"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Concussione** (art. 317 c.p.), *"Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;;
- ✓ **Corruzione per l'esercizio della funzione** (art. 318 c.p.), *"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da tre a otto anni"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), *"Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito*

⁵ AGGIORNAMENTO: Il D.lgs. n. 75/2020 modifica l'art. 25 D.Lgs. 231/2001, ampliando il catalogo dei reati con le fattispecie di peculato ex artt. 314 e 316 c.p. e di abuso d'ufficio ex art. 323 c.p.

⁶ Comma aggiunto dall'art. 1, comma 1, lett. a), D.Lgs. n. 75/2020.

con la reclusione da sei a dieci anni.” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Circostanze aggravanti** (art. 319 bis c.p.), *“La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi ” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;*
- ✓ **Corruzione in atti giudiziari** (art. 319-ter c.p.): “ (Comma 1)Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni. (Comma 2)Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote per il comma 1 e fino 800 quote per il comma 2;
- ✓ **Induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), “(Comma 1) Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. (Comma 2) Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;
- ✓ **Corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), “(Comma 1) Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. (Comma 2) In ogni caso, le pene sono ridotte in misura non superiore a un terzo” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote nel caso di commissione art. 318 c.p. e fino a 600 quote in caso di commissione art. 319 c.p.;
- ✓ **Pene per il corruttore** (art. 321 c.p.), *“Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o*

promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;

- ✓ **Istigazione alla corruzione** (art. 322 commi 1 e 3 c.p.): *"(Comma 1) Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo [...]. (Comma 3) La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;*
- ✓ **Istigazione alla corruzione** (art. 322 commi 2 e 4 c.p.): *"(Comma 2) Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo [...]. (Comma 4) La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- ✓ **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): *"Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*
 - 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;*
 - 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;*
 - 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;*
 - 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;*

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitano funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;

5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;

5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;

5-quinquies) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione⁷.

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitano funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi” - Sono previste in capo all'Ente le medesime sanzioni pecuniarie previste per gli artt. 314, 316, da 317 a 320 e 322 terzo e quarto comma c.p.

- ✓ **Traffico di influenze illecite** (art. 346 bis c.p.): tale ipotesi delittuosa punisce chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio. Tale fattispecie può concretizzarsi in attività che pongono in relazione due soggetti privati, (uno dei quali funge da intermediario “illecito” verso un pubblico ufficiale o incaricato di pubblico servizio in

⁷ Numero aggiunto dall'art. 1, comma 1, lett. d), D.Lgs. 14 luglio 2020, n. 75, a decorrere dal 30 luglio 2020.

cambio di un interesse o vantaggio) - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.

- ✓ **Abuso d'ufficio** (art. 323 c.p.), *"Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni⁸. La pena è aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.

1.2. Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio

– Pubblica Amministrazione (di seguito "PA") s'intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;

⁸ Comma così modificato, a decorrere dal 17 luglio 2020, dall'art. 23, comma 1, D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAL, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la P.A. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

- *Pubblici ufficiali e incaricati di un pubblico servizio.* Ai sensi dell’art. 357, primo comma, del codice penale, è considerato pubblico ufficiale “agli effetti della legge penale” colui il quale esercita “una pubblica funzione legislativa, giudiziaria o amministrativa”.

La norma chiarisce solo la nozione di “pubblica funzione amministrativa” (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale “è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”.

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l’art. 358 c.p. definisce i “soggetti incaricati di un pubblico servizio” come quei soggetti “i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della “pubblica funzione”, da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d'ordine e/o la prestazione d'opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

1.3. Regole di comportamento e Protocolli operativi in tema di reati contro la P.A.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
- ✓ porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
- ✓ comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
- ✓ violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;

- ✓ i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
- ✓ tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
- ✓ qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli e responsabilità	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla P.A. (ad es., nel caso di richiesta di un finanziamento agevolato, deve essere ben chiara la segregazione delle funzioni tra (a) chi propone la richiesta di finanziamento (b) chi effettua lo studio di fattibilità per valutare la possibilità di accedere al finanziamento (c) chi raccoglie e dispone la documentazione necessaria e (d) chi approva e sottoscrive la richiesta). • Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: • proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; • porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; • distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; • presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; • presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al

	fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: • sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; • ogni eventuale accordo preso con la P.A. sia documentato; • sia implementato un sistema di verifica (c.d. <i>Activity Check</i>) sulle attività svolte in concreto dai venditori e/o informatori scientifici, nonché sui rapporti da questi intrattenuti con soggetti, potenziali clienti e/o fornitori e/o distributori, appartenenti alla P.A. o con essa collegati, attraverso scambio continuo di documentazione telematica e/o cartacea da parte degli stessi venditori e/o informatori scientifici alla Società, contenente la descrizione delle attività svolte e l'identificazione dei soggetti con i quali vengono intrattenuti rapporti commerciali a nome della Società.
Gestione operativa: Venditori Informatori Scientifici	In caso di proposizione di nuove opportunità commerciali (es. nuovo cliente appartenente alla P.A.) e comunque in caso di rapporti con la P.A. in genere, è necessario che: a) vi sia una verifica sull'esistenza di eventuali conflitti di interesse con riferimento alla possibilità di entrare in trattativa con la P.A. o con soggetti ad essa collegati, b) vi sia un controllo sulle modalità di ingaggio del nuovo cliente/fornitore/distributore, c) vi sia una verifica sul cliente in termini di casellario giudiziale, d) sia previsto <u>un doppio controllo mensile</u> (c.d. <i>Activity Check</i>) sull'attività svolta da venditori e/o informatori scientifici, oltre la possibilità di effettuare dei <i>random check</i> (ovvero controlli casuali) sull'attività di questi ultimi. A tal fine è obbligo dei venditori e/o degli informatori scientifici: • documentare le proprie attività (appuntamenti giornalieri, identità del cliente, attività in concreto svolta con il cliente, ecc.) in formato telematico e/o cartaceo; • inoltrare alla Società due volte al mese l'<i>activity check</i> per via telematica; • informare immediatamente la Società di eventuali proposte o fatti illeciti commessi dal cliente, che possano integrare ipotesi di reato ai danni della Società, come sopra descritte. È, inoltre, fatto divieto di: intrattenere qualsiasi forma di rapporto (commerciale e non) di cui la Società non sia stata previamente messa a conoscenza.
Ispezioni	• Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; • di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; • devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche

	preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: - la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; - specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.

Protocollo 2 – Scelta di fornitori e consulenti	
Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	- I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. - I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. - Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. - Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici	
Transazioni finanziarie	- Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio. - In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; - Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto

	previsto dall'art. 3 della legge n. 136/2010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che dovrà essere necessariamente corredata da idonea documentazione giustificativa.
Irregolarità anomalie	o Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di irregolarità o anomalie.

Protocollo 4 – Assunzione del personale

Assunzione, gestione, formazione e incentivazione dei dipendenti e collaboratori	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato.
---	--

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali

Contenziosi/ Contestazioni	• Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. • Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.
---------------------------------------	--

Protocollo 6 • Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi • Spese di rappresentanza	
Omaggi/Donazioni	Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico. A tal fine è si prevede la creazione di una procedura sulle liberalità che: • indichi i soggetti che possono da un lato autorizzarle e dall'altro riceverle; • definisca il valore massimo per ogni omaggio ed i casi in cui le liberalità possono essere eseguite; È, inoltre, fatto obbligo che qualora gli omaggi vengano elargiti a soggetti appartenenti la P.A., questo sia comunicato immediatamente al C.d.A. In ogni caso, nessun omaggio e/o donazione potrà essere effettuato se non quelli espressamente approvati dal C.d.A.

1.4. Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

1.5. Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta DESIDERIO TAGLIENTI, la quale sta implementando un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito la Società implementando le proprie procedure interne in materia di protezione dei dati personali, attraverso l'adozione un software che permette:

- l'identificazione univoca degli utenti, attraverso un ID, un Identity Provider utilizzabile per eseguire l'accesso e l'autenticazione a norma a tutti gli applicativi e servizi in cloud;
- la crittazione dei dati sensibili, (ad es. dichiarazioni di appartenenza ad organizzazioni sindacali, dati relativi allo stato di salute, ecc.), attraverso cifratura delle informazioni per rendere i dati inaccessibili al di fuori dell'applicazione software, tenendo conto anche del contesto e delle finalità del trattamento, nonché del rischio per i diritti degli interessati;
- il log delle attività per l'archiviazione e la consultazione dei log delle attività previsti dalla nuova normativa.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

La presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali
Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica

In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato:

- introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili;
- acquisire, possedere o utilizzare strumenti *software e/o hardware* che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le *password*, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società;
- divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti;
- distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (*vulnerability test*, *penetration test*) e previsto nei propri compiti lavorativi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono

	utilizzati; Inoltre: • l'utilizzo del servizio aziendale di posta elettronica deve essere effettuato nel rispetto del Codice Etico aziendale, impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software, ecc.</i>); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che
--	--

	soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	---

1.6. Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.
- c. comunicare eventuali violazioni della presente Parte speciale al DPO in carica e

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

1.7. Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di

responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative

di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti

Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti

La regolamentazione dell'attività descritta deve prevedere che:

- i Destinatari si accertino che i dipartimenti di *patent e trademark* internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto;
- in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di *patent e trademark* internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto.
- I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti.

Inoltre, è fatto espressamente divieto di:

- contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati;
- contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati;
- introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati;
- detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto;

	• consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche.
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche,
---	--

	musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; • importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	---

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE

Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
------------------------------	--

1.8. Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- d. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- e. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

1.9. Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001).

Nell'ambito della riforma del diritto societario, il Decreto Legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter del Decreto, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. "reati societari".

I reati societari sono reati propri e, in quanto tali, possono essere commessi direttamente da:

- Consiglio di Amministrazione;
- Sindaci;
- Liquidatori;
- Sottoposti alla direzione e alla vigilanza dei soggetti sopra elencati nel caso di corruzione tra privati;
- nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

Le fattispecie di reati societari considerate sono:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- falso in prospetto (art. 173-bis, T.U.F.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3 c.c.) [modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019];
- istigazione alla corruzione tra privati (art. 2635-bis c.c.) [introdotto dal D.Lgs. n. 38/2017];
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-ter del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

- a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società. A questo proposito, è fatto espresso divieto di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Società;
 - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
- c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività aziendale, fino alle fasi eventuali di liquidazione o cessazione della Società;
- e. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
- a. omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
 - b. esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
 - c. porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- g. predisporre procedure per la preparazione del bilancio e la gestione delle risorse finanziarie; inoltre,
- h. il presente Modello deve essere portato adeguatamente a conoscenza di tutto il personale, non solo dirigente, e appositi meccanismi di comunicazione (ad esempio tramite poster nelle sale comuni o pubblicazioni periodiche) devono essere predisposti in modo da permettere la conoscenza di modifiche e/o aggiornamenti del Modello stesso e deve essere attivato un

programma di informazione/formazione a favore del personale addetto atto a prevenire la commissione di reati societari;

- i. tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o di conflitto di interesse, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili, le attività finalizzate alla formazione del bilancio e le altre comunicazioni sociali siano accurati e trasparenti.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente contabile esterno non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1	
• Predisposizione del bilancio; • Tenuta delle scritture contabili e dei Libri Sociali; • Gestione degli ordini e delle fatture.	
Definizione dei ruoli e responsabilità	Devono essere osservate specifiche procedure che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione della contabilità, predisposizione dei bilanci, dei rendiconti, prevedendo controlli in ordine alla completezza e veridicità delle informazioni contenute nei singoli documenti finali; • individuino la funzione e il soggetto deputato a gestire per conto di HS la contabilità ed il processo di formazione dei documenti contabili, cui conferire apposita delega e procura scritta. Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere

	adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione Operativa	In aggiunta ai presidi aziendali già esistenti, si dispone: - la trasmissione agli amministratori e al collegio sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del consiglio di amministrazione o sui quali esso debba esprimere un parere ai sensi di legge; - la previsione di riunioni periodiche tra il collegio sindacale e l'Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di <i>Corporate Governance</i>. Inoltre, per la predisposizione delle comunicazioni ai Soci relative alla situazione economica, patrimoniale e finanziaria della Società, si dispone che la redazione delle stesse sia effettuata determinando in maniera chiara e completa: - i dati e le informazioni che ciascuna funzione deve fornire; - i criteri contabili per l'elaborazione dei dati; - la tempistica per la loro consegna alle aree aziendali responsabili. Infine, in caso di comunicati stampa e ogniqualvolta vengano diffuse all'esterno notizie aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società, si dispone che chi diffonde tali informazioni, oltre ad osservare i principi suindicati, deve attenersi esclusivamente alle informazioni desumibili da documenti già approvati e resi pubblici.

Protocollo 2 Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni); Creazione di fondi extracontabili.	
Gestione operativa	- Le modalità di gestione delle operazioni societarie devono essere condotte in maniera veritiera e corretta, coerentemente e nel rispetto dei principi di <i>Corporate Governance</i> adottati dal Consiglio di Amministrazione. - Deve esistere una segregazione di ruoli e responsabilità tra chi evidenzia la necessità di un'operazione, chi la esegue e chi effettua il relativo controllo. - Per ogni documentazione predisposta deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi. - Tutta la documentazione deve contenere elementi assolutamente veritieri e devono essere coerenti all'oggetto per cui sono stati richiesti. A tal fine tutta la documentazione relativa alle operazioni societarie deve essere archiviata in un apposito fascicolo con sottoscrizione del responsabile della funzione. - E' inoltre necessario che sia previsto quanto segue: - un programma di formazione – informazione del personale impiegato nella predisposizione della documentazione attinente le operazioni societarie; - un monitoraggio dei poteri anche con riferimento alla verifica delle firme dei documenti inerenti le operazioni societarie; - la documentazione redatta ed in genere ogni altra informazione formalizzata deve contenere solo elementi assolutamente veritieri.

Protocollo 3 – Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale

Identificazione dei soggetti responsabili	Nella gestione dei rapporti con il collegio sindacale, società di revisione e soci devono essere osservate le seguenti disposizioni: • identificazione del personale all'interno di HS preposto ad interloquire con il collegio sindacale e alla trasmissione della relativa documentazione; • possibilità per il Collegio Sindacale e della società di revisione di prendere contatto con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possono presentare aspetti di criticità in relazione ai reati societari.
--	---

Protocollo 4

- **Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti;**
- **Gestione della liquidità.**

Gestione del processo di acquisizione di nuova clientela e di gestione della clientela acquisita	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con clienti o altre controparti contrattuali; • garantire una segregazione di funzioni e responsabilità e una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione delle vendite, in particolare tra responsabilità nei rapporti con il cliente (cd. <i>account manager</i>), responsabilità nella definizione del prezzo di offerta e delle condizioni/tempi di pagamento (e relative penali), responsabilità nella definizione di eventuali risoluzioni transattive in caso di controversie; • individuare criteri generali e trasparenti per la determinazione di un prezzo massimo di offerta per singolo prodotto o servizio, di modo che qualunque anomalia possa essere agevolmente rilevata. In caso di qualsivoglia criticità sorta nell'ambito dei rapporti sopra descritti, deve essere informato l'Organismo di Vigilanza con nota scritta. In particolare, vi è l'obbligo di comunicare: • le operazioni di vendita superiori ad un dato importo che potrà rappresentare la soglia di rischio; • le operazioni di vendita superiori di una data percentuale rispetto al prezzo medio del prodotto, come risultante dai criteri generali suddetti; • tutte le operazioni di incasso al di sotto dei termini standard di pagamento (ad esempio, fatture pagate a vista).
Assegnazione/gestione degli incarichi e delle consulenze esterne	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con fornitori o altre controparti contrattuali; • garantire una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione degli acquisti, in particolare tra funzione che individua e seleziona il fornitore, il consulente o il prestatore di servizi, funzione che ratifica la c.d. entrata merci, funzione che autorizza il pagamento e funzione che effettua il controllo di gestione e la tracciabilità delle operazioni; • effettuare una pianificazione dell'attività di <i>benchmarking</i> (raffronto con i valori

	economici di mercato); • predisporre adeguati protocolli aziendali per acquisti di beni e servizi, affidamento di consulenza ed altre prestazioni professionali e gestione del magazzino.
Selezione e gestione del personale	La regolamentazione dell'attività descritta deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • il monitoraggio di ogni eventuale conflitto di interessi da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato.
Gestione del marketing ed eventuale omaggistica clienti comprese le organizzazioni no profit	Con riguardo alla formazione del personale dipendente e amministrativo, sono prescritte le seguenti e ulteriori regole di comportamento: • divieto di offrire, sollecitare, istigare o ricevere da terzi, direttamente o indirettamente, o di accettare la promessa di ricevere omaggi, benefici o altre utilità, a meno che questi omaggi, benefici e utilità abbiano "modico valore" e rientrino nei limiti della normale cortesia e non abbiano lo scopo di influenzare decisioni aziendali o creare obblighi nei confronti di terzi o di compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. In particolare: – le spese di rappresentanza devono essere limitate a pranzi o cene di lavoro; – i c.d. omaggi a clienti sono da limitare alla gadgetistica o ad oggetti di puro valore simbolico, meglio ancora se riportanti il marchio dell'azienda per collegarli a finalità pur sempre commerciali, con la previsione di un listino; • proibire liberalità che non siano inquadrare in programmi generali di <i>social responsibility</i>, come sponsorizzazioni sportive di club, associazioni, ecc. riconducibili ad un ente/cliente o a suoi singoli manager; • prevedere una chiara casistica ed un flusso di comunicazioni verso l'Organismo di Vigilanza affinché si possa vigilare su eventuali abusi, attraverso l'analisi incrociata con altri dati, ad esempio quelli relativi alle commesse acquisite; • prevedere che chiunque riceva tali richieste o offerte, eccezione fatta per omaggi di modico valore, debba informarne "il responsabile della funzione aziendale competente"; • prevedere, nell'informativa comunicata ai clienti/fornitori, che ogni violazione dei principi contenuti nel Codice Etico rappresenta una violazione contrattuale; • prevedere l'obbligo per i clienti/fornitori di conformarsi al Codice Etico prima di poter avere rapporti commerciali con la società.

Partecipazione a gare indette da soggetti privati e gestione dei rapporti con il cliente in caso di vittoria di una gara	È necessario che sia previsto quanto segue: • una corretta applicazione della procedura di partecipazione ai bandi privati sia con riferimento alla fase di ricezione (fonte interna e/o fonte esterna) dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui su è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, che alla predisposizione e spedizione della documentazione all'Ente (o alla capofila) che indica il relativo bando; • una verifica dell'esistenza di eventuali conflitti di interessi con riferimento anche alla possibilità di partecipare o meno al bando. Inoltre, devono essere previste regole di comportamento che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione delle varie fasi dei rapporti con partner/terze parti ed altri soggetti privati in genere, prevedendo controlli in ordine alla regolarità dei requisiti di ammissione degli stessi ad eventuali bandi di gara privati o all'ottenimento di contributi, sovvenzioni e finanziamenti privati; • individuino la funzione e la persona fisica deputata a rappresentare l'azienda nei confronti dei terzi privati, cui conferire apposita delega e procura e stabiliscano forme di riporto periodico dell'attività svolta verso il responsabile della funzione competente a gestire tali rapporti; Infine, il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
--	---

1.10. Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato *reporting* verso gli organi deputati, ecc.);
- monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;
- verificare annualmente i principali atti societari ed in particolare la relazione del Collegio Sindacale e della Società di Revisione nonché il rispetto delle procedure per la diffusione delle comunicazioni rivolte ai Soci, dei comunicati stampa e delle notizie scritte rivolte all'esterno aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società al fine di verificare l'osservanza della presente Parte Speciale nonché la sua idoneità a prevenire i reati ivi elencati;

- d. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- e. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- f. curare l'aggiornamento del Modello, indicando al consiglio di amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

1.11 Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies, D.Lgs. 231/2001).

I reati in materia di salute e sicurezza sul lavoro che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-septies del d.lgs. 231/2001 sono i seguenti:

- Omicidio Colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590, comma III, c.p.).

Le Linee Guida di Confindustria nell'ambito dei reati trattati nella presente Parte Speciale evidenziano l'impossibilità di escludere a priori alcun ambito di attività della società, in quanto i reati in esame potrebbero riguardare tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Ne consegue che le potenziali aree a rischio reato che HS ha individuato nell'ambito di tali reati riguardano tutte le attività svolte nei siti della Società.

In particolare, la Società ha la sede legale in Roma (RM) – Via Zosimo 13, e unità operative e locali in:

- Aprilia (Latina), Via Angela Vacchi 23/25, CAP 04011 – Stabilimento di produzione.

Inoltre, sono considerate aree a rischio anche tutte le attività svolte dal personale di HS che opera esternamente in qualità di *supporters* tecnici all'interno di strutture e aziende sanitarie, (nello specifico in sale operatorie). Particolare attenzione deve essere dedicata a quelle attività realizzate in associazione con partner commerciali (in caso di joint venture, anche in forma di ATI, consorzi, ecc.) o tramite la stipula di contratti di somministrazione, appalto o con società di consulenza o liberi professionisti.

Anche ai fini della redazione della presente Parte Speciale si devono pertanto considerare i fattori riportati nel Documento di Valutazione dei Rischi (di seguito anche DVR) tenuto conto che lo

stesso non esaurisce le procedure di seguito previste, finalizzate a costituire il complessivo sistema di gestione della sicurezza sul lavoro e dare attuazione al disposto dell'art. 30 d.lgs. 81/08 secondo i principi espressi dalle Linee Guida UNI – INAIL.

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso in una delle aree sensibili indicate al precedente paragrafo 1, si ritiene particolarmente importante:

- a) determinare le politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;
- b) identificare e applicare in modo corretto le prescrizioni delle leggi e dei regolamenti applicabili in tema di salute e sicurezza sul lavoro;
- c) identificare e valutare i rischi per tutte le categorie di lavoratori, con particolare riferimento alla redazione:
 - del DVR;
 - dei contratti di appalto;
 - della valutazione dei rischi derivanti dalle interferenze;
 - nel caso in cui la Società fosse costruttrice, dei Piani di Sicurezza e Coordinamento, Fascicolo dell'Opera e Piani Operativi di Sicurezza;
- d) fissare gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elaborare dei programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività del Servizio Prevenzione e Protezione e del Medico Competente;
 - attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori;
- e) sensibilizzare la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti esposti a rischi specifici (es. addetti alla Camera Bianca);

- f) attuare adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
 - coerenza tra attività svolta e competenze possedute;
- g) attuare le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- h) effettuare un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione per la sicurezza del lavoro e la tutela della salute nel raggiungere gli obiettivi prefissati, nonché l'adequatezza di questi ultimi rispetto sia alla specifica realtà della Società che ad eventuali cambiamenti nell'attività.

1.12 Struttura organizzativa di HS Hospital Service S.p.A.

In materia di salute e sicurezza sul lavoro la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente di cui al d.lgs. 81/2008 e successive modifiche (di seguito anche "Decreto Sicurezza"), al fine di eliminare o, per lo meno di limitare, i rischi per i lavoratori.

Nell'ambito di tale struttura organizzativa operano:

A) Il Datore di Lavoro. È il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

B) Il Servizio di Prevenzione e Protezione (SPP). Insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori. La Società ha proceduto alla nomina di un Responsabile del Servizio di Prevenzione e Protezione (RSPP), in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 d.lgs. 81/08 e designata dal Datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi (art. 2 d.lgs. 81/2008).

C) Responsabile dei Lavori. La persona che può essere incaricata dal Committente/Datore di Lavoro Committente per svolgere i compiti ad essa attribuiti dal d.lgs. 81/2008.

D) Addetti al primo soccorso. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili del soccorso in azienda, in caso di infortuni.

E) Addetti antincendio. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili dell'attuazione delle misure antincendio e di evacuazione, in caso di emergenza.

F) Il Medico Competente. Medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 d.lgs. 81/08 che collabora, secondo quanto previsto all'articolo 29, comma 1, con il Datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al Decreto Sicurezza (art. 2 d.lgs. 81/08).

G) Il Rappresentante dei Lavoratori per la Sicurezza (RLS). Persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro (art. 2 comma 1, lett. i d.lgs. 81/2008).

H) Lavoratore. Persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione della Società, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite. I lavoratori di aziende che svolgono per HS attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

I) Gestione degli appalti e dei fornitori. Nei contratti di appalto intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione, il Datore di Lavoro in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno della propria azienda o Unità produttiva, in conformità alle procedure aziendali, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

- verificare, con il supporto delle Unità interessate, l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;
- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici

anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture. L'obbligo di redazione del suddetto documento non sussiste in caso di appalto di servizi di natura intellettuale, mere forniture di materiali o attrezzature, nonché per i lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza delle sostanze di cui all'allegato XI del d.lgs. 81/2008.

1.13 Principi procedurali specifici

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei lavoratori così come individuati dall'art. 15 del Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del suddetto decreto si prevede quanto segue.

Protocollo 1 – Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	
Politiche aziendali in tema di sicurezza	La politica per la sicurezza e salute sul lavoro adottata da HS deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte da HS e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i Lavoratori. A tal fine, è predisposto un adeguato sistema di designazioni o deleghe di funzioni in materia di salute e sicurezza secondo i principi di: • effettività, sussistenza e compresenza di autonomia decisionale e finanziaria del delegato; • idoneità tecnico-professionale del delegato; • vigilanza sull'attività del delegato, non acquiescenza, non ingerenza; • certezza, specificità e consapevolezza. La designazione / delega di funzioni da parte del datore di lavoro deve: • risultare da atto scritto recante data certa; • essere diretta ad un soggetto che possieda tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;

	• essere accettata dal delegato per iscritto. Il soggetto delegato deve essere consapevole delle funzioni ad esso delegate. La politica per la sicurezza e salute sul lavoro è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.
Processo di pianificazione	HS nell'ambito del processo di pianificazione degli obiettivi in tema di salute e sicurezza, con cadenza annuale: • definisce gli obiettivi finalizzati al mantenimento e/o miglioramento del sistema; • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	• La Società ha definito un sistema di comunicazioni interne che assicura che le informazioni relative alla sicurezza fluiscano "dall'alto verso il basso", ma anche "dal basso verso l'alto" ed orizzontalmente rispetto alle varie parti dell'organizzazione. Lo scambio di informazioni tra i differenti livelli e settori aziendali è attuato attraverso l'individuazione di referenti interni e di idonei strumenti di comunicazione. Gli strumenti di comunicazione interna possono variare in funzione del tipo di informazione che è necessario fornire avendo però sempre presente che il requisito indispensabile è che le informazioni siano fornite usando una forma ed un modo che le rendano comprensibili alle persone che le devono ricevere. • La Società è convinta che il processo di prevenzione e miglioramento della sicurezza debba vedere coinvolto tutto il personale aziendale. A tale fine ogni lavoratore è incoraggiato a segnalare al proprio responsabile di funzione o direttamente al RSPP eventuali anomalie o proposte di miglioramento. Tali segnalazioni sono raccolte dal RSPP che provvede ad effettuarne un'analisi ed è responsabile di mettere in atto le eventuali azioni conseguenti; la decisione presa in merito è registrata dal RSPP. Il RSPP organizza anche le riunioni periodiche sulla sicurezza prevista dalle norme vigenti e redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione. • È stata definita una procedura per regolamentare le attività di formazione, informazione e addestramento da erogare a: - personale dipendente; - lavoratori con contratto di somministrazione; - stagisti. La procedura definisce anche le modalità in caso di nuove assunzioni e cambi di mansione. I contenuti della procedura specificano modalità e responsabilità in merito a: - l'individuazione delle necessità di formazione e addestramento;

		- la pianificazione e attuazione della formazione; - la registrazione delle attività formative; - la verifica della loro efficacia; - l'informazione e sensibilizzazione del personale sull'igiene e la sicurezza del lavoro. • In merito all'attività di documentazione, HS dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, dei seguenti documenti: - la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro; - il registro degli infortuni; - il Documento di Valutazione dei Rischi indicante la metodologia con la quale si è proceduto alla valutazione dei rischi e contenente il programma delle misure di mantenimento e di miglioramento; - nel caso in cui la Società sia appaltatrice di lavori di costruzione: la documentazione contratti; Piano di Sicurezza e Coordinamento; Fascicolo dell'Opera; verbali di coordinamento relativi alla verifica dell'applicazione da parte delle imprese esecutrici delle disposizioni contenute nel PSC; Piani Operativi di Sicurezza. • HS è altresì chiamata a garantire che: - il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente; - venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente; - venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica; - venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale; - venga conservata la documentazione inerente a regolamenti ed accordi aziendali; - vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori; - venga conservata ogni procedura adottata da HS per la gestione della salute e sicurezza sui luoghi di lavoro; - tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.
Attività monitoraggio	di	HS deve assicurare un costante ed efficace monitoraggio del sistema per la gestione della salute e della sicurezza sui luoghi di lavoro. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere.

	Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta HS, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. HS garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.
Riesame del sistema	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema adottato da HS per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame annuale da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.
Gestione operativa degli appalti	HS deve predisporre e tenere aggiornato un elenco delle aziende con le quali stipula eventuali contratti di appalto. Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti dai quali devono risultare espressi riferimenti agli adempimenti di cui all'art. 26 del Decreto Sicurezza. Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori e le organizzazioni sindacali dei lavoratori. Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

1.14 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-septies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di HS eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la tutela della salute e della sicurezza nei luoghi di lavoro, in coerenza con quanto stabilito nel presente Modello e all'art. 30 del Decreto Sicurezza;

- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati da HS tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il Delegato della Sicurezza Aziendale e il RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

HS garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti di HS (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; gli Addetti al Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso).

1.15 Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies).

I reati di cui all'art. 25-octies del d.lgs. 231/2001 sono i seguenti:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
- Autoriciclaggio (art. 648-ter 1 c.p.)

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di:

- a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-octies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente diventarlo;
- b) intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della

liceità quali, a titolo esemplificativo, persone legate all'ambiente del riciclaggio, del terrorismo, al traffico di droga, all'usura, ecc.;

- c) utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti;
- d) accettare rapporti contrattuali con clienti o altre controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI;
- e) effettuare elargizioni in denaro ad individui, società od organizzazioni condannate per aver svolto attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico;
- f) avere contatti con individui inseriti nelle *black list* antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea.

Inoltre è previsto, a carico dei Destinatari, l'espresso obbligo di:

- g) richiedere tutte le informazioni necessarie al fine di valutare l'affidabilità, la solidità economica e l'attendibilità commerciale/ professionale dei fornitori e del partner;
- h) assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- i) tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti;
- j) prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri.

Protocollo 1 - Scelta consulenti, fornitori, partner commerciali

Selezione dei partner e dei fornitori	Si riportano di seguito specifiche regole di comportamento da tenere in osservanza del Decreto: • la Società procede alla selezione dei Partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri oggettivi e documentabili, verificandone l'attendibilità commerciale attraverso: – verifica ex ante, conservando evidenza dei dati raccolti, che i soggetti con cui intrattiene rapporti contrattuali, anche lavorativi, abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI e non siano inseriti nelle <i>blacklist</i> antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea., della Commissione Europea. – visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni estere; – referenze da parte di altri soggetti già in rapporti con la Società o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione; – ove possibile, certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere; • la Società inserisce nei contratti con i Partner commerciali una specifica clausola con
--	---

	la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali di HS e dei principi contenuti nel Modello e si impegnano al rispetto degli stessi; il mancato rispetto dei comportamenti etici o false dichiarazioni relative alla situazione del Partner comporteranno l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto; • la Società verifica l'attendibilità commerciale e professionale dei Fornitori, perlomeno di una certa rilevanza (da concordare un limite di importo di fornitura superato il quale procedere alle verifiche) attraverso: – visure ordinarie presso la Camera di Commercio o certificati equivalenti per Fornitori stranieri; – certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti per fornitori stranieri; – analisi del Fornitore per verificarne la coerenza con le prestazioni richieste dalla Società. Inoltre, è previsto, a carico dei Destinatari, l'espresso obbligo di tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

Protocollo 2 – Gestione dei flussi finanziari/creazione di fondi extracontabili e gestione della liquidità e cassa	
Gestione di investimenti	Si prevede l'espresso divieto di: • utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti; • effettuare elargizioni in denaro, in particolare ad individui, società od organizzazioni condannate per aver svolto attività illecite. Inoltre, è previsto l'obbligo di assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
Monitoraggio flussi finanziari	La Società effettua un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie. Inoltre, si prevede che: • nel caso di elargizioni di danaro ad individui, società o organizzazioni è necessario controllare la serietà e la professionalità del destinatario del denaro. Inoltre deve essere redatto un piano d'investimento a giustificazione dell'investimento, comprensivo di controlli periodici dell'avanzamento del piano; • in caso di <i>Joint Venture</i>, la Società proceda alla verifica della congruità economica dell'investimento, avendo riguardo, nello specifico, al rispetto dei prezzi medi di mercato, all'utilizzo di professionisti di fiducia per l'effettuazione della <i>due diligence</i>; • la Società presti particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti/partner/fornitori esteri.

	Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 3 – Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio

Gestione organizzativa ed operativa	L'eventuale coinvolgimento di consulenti, intermediari, agenti, promotori finanziari e broker a supporto della prestazione dei servizi della Società presuppone un'adeguata conoscenza degli stessi e la verifica, anche mediante attestazione degli interessati, della sussistenza dei requisiti di onorabilità previsti dalla legge e dell'assenza di situazioni di conflitto di interesse in capo ad essi. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 4 – Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà

Gestione organizzativa ed operativa	La Società deve definire e rispettare i criteri che regolano la scelta delle associazioni/fondazioni in favore delle quali effettuare donazioni od erogazioni liberali di qualsiasi tipo, in modo che sia possibile accertare l'effettiva finalizzazione dell'iniziativa a scopi umanitari che non dissimolino attività di riciclaggio o terrorismo. In particolare: • donazioni e/o erogazioni liberali di qualsiasi tipo sono effettuate sulla base di una lista di associazioni/fondazioni accreditate quali potenziali beneficiarie. Le modalità d'inserimento, mantenimento ed eliminazione delle associazioni/ fondazioni da tale lista sono debitamente formalizzate; • donazioni ed erogazioni liberali di qualsiasi tipo sono operate solo ove adeguatamente autorizzate, formalizzate e rendicontate; • la Società non effettua donazioni né erogazioni liberali di qualsiasi tipo tramite versamenti in contanti o su conti correnti cifrati. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

1.16 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-octies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di reati di riciclaggio, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

1.17 Regole di comportamento e Protocolli operativi in materia di reati ambientali (art. 25-undecies del Decreto)

I reati ambientali che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-undecies del d.lgs. 231/2001 sono i seguenti:

- scarichi di acque reflue (art. 137, comma 2, 3, 5, 11, 13 d.lgs. 3 aprile 2006, n. 152);
- attività di gestione di rifiuti non autorizzata (art. 256 comma 1, 3, 5, 6, e artt. 208, 209, 210, 211, 212, 214, 215, 216 d.lgs. 3 aprile 2006, n. 152);
- bonifica dei siti (art. 257 comma 1 e 2, d.lgs. 3 aprile 2006, n. 152);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (articolo 258 del d.lgs. 3 aprile 2006, n. 152);
- traffico illecito di rifiuti (art. 259 d.lgs. 3 aprile 2006 n. 152);
- attività organizzate per il traffico illecito di rifiuti (art. 260 d.lgs. 3 aprile 2006 n. 152);
- sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis d.lgs. 3 aprile 2006 n. 152);
- violazione dei valori limite di emissione (art. 279 d.lgs. 3 aprile 2006 n. 152);
- cessazione e riduzione dell'impiego di sostanze ozono lesive (art. 3 l. 28 dicembre 1993 n. 549).
- inquinamento ambientale art. 452bis c.p.,
- disastro ambientale art. 452 ter c.p.,
- traffico e abbandono di materiale radioattivo 452quinquies c.p.,
- impedimento del controllo 452sexies c.p.,
- omessa bonifica 452terdecies c.p.

Le potenziali aree a rischio reato che la Società ha individuato con riferimento ai reati ambientali riguardano tutte le attività svolte nei propri siti e nelle sedi amministrative e societarie nelle quali si svolgono le attività aziendali da parte del personale dipendente. Sono inoltre considerate aree a rischio anche tutte le attività svolte dal personale esterno incidenti sui processi produttivi o

comunque sul sistema di gestione ambiente e sicurezza (ad es., fornitori di beni o servizi in base a contratti d'appalto, d'opera o somministrazione).

Le attività sono considerate sensibili avuto riguardo al loro svolgimento sia da parte del personale aziendale, sia da parte di terzi che agiscano su incarico o per conto della Società, ovvero che intrattengano un rapporto contrattuale con la Società, con particolare riferimento al perimetro delle attività loro assegnate ed esercitate sotto la direzione o vigilanza della Società.

Sono da considerare attività sensibili ai fini del presente Modello quelle che possano produrre impatti ambientali significativi sulle matrici ambientali (acqua, aria, suolo, rifiuti, flora, fauna) o comunque tali da imporre misure per il loro contenimento.

In particolare, dovranno considerarsi attività aziendali significative per la tutela delle matrici ambientali le aree nelle quali possano verificarsi condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti ai sensi delle Direttive 2008/99 CE e 2009/123 CE, in quanto provochino o possano provocare il decesso o lesioni gravi alle persone o danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora. Più specificamente, sono considerate sensibili le attività con impatto ambientale diretto (attività industriali, attività produttive, attività dalle quali si originano rifiuti, reflui o emissioni) o indiretto (quali, a titolo esemplificativo, le attività manutentive). Rientrano in tale ambito anche le attività che si svolgono in luoghi ove siano adottate misure a tutela della salute e sicurezza dell'ambiente di lavoro oggetto della valutazione ex art 18, comma 1, lett. q) d.lgs. 81/2008 nonché le attività soggette a procedimenti amministrativi di abilitazione, iscrizione, autorizzazione, nonché a specifici divieti ai sensi del d.lgs. n. 152/2006.

In conformità ai principi generali del Codice Etico e della Politica Ambiente e Sicurezza è preminente e specifico interesse della Società quello di sviluppare i propri investimenti in modo compatibile con il rispetto dell'ambiente, riconosciuto quale bene primario da salvaguardare, perseguendo il miglior equilibrio tra la propria iniziativa economica e la tutela delle esigenze ambientali attraverso il contenimento dell'impatto delle proprie attività ed il rispetto della normativa ambientale.

La Società considera pertanto ogni condotta che direttamente o indirettamente possa generare un pregiudizio anche potenziale all'ambiente come contraria al proprio interesse e respinge ogni condotta elusiva delle procedure aziendali ed inosservante della normativa vigente, dichiarando espressamente che a tali eventuali condotte non corrisponde alcun vantaggio per la Società, bensì la compromissione di ideali e patrimonio aziendali.

In tale contesto, la presente Parte Speciale prevede l'espresso divieto per tutti i Destinatari (i) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *undecies* del Decreto) e (ii) di violare i principi illustrati nel presente Modello e porre in essere condotte difformi dalle procedure aziendali previste.

Conseguentemente, i soggetti sopra indicati hanno l'obbligo di rispettare scrupolosamente tutta la normativa vigente ed in particolare di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure in tutte le attività aziendali adottate dalla Società, di astenersi dal porre in essere o dare causa a violazioni dei principi comportamentali, dei protocolli e delle procedure aziendali, di rispettare le misure organizzative e preventive dettate per lo svolgimento delle attività produttive ad impatto ambientale ed i relativi oneri informativi, partecipando diligentemente alle sessioni formative ed informative connesse con le mansioni a ciascuno affidate dalla Società.

In tale contesto, ed ai fini di cui sopra, la Società:

- a. determina le politiche ambientali volte a definire gli impegni generali assunti per garantire il rispetto dell'ambiente e l'osservanza delle pertinenti norme applicabili nonché la riduzione degli impatti ambientali connessi alle attività svolte dalla Società;
- b. identifica le norme applicabili in tema di protezione dell'ambiente ed opera in conformità alle stesse;
- c. identifica e valuta i fattori che si originano dall'attività produttiva e che possono modificare lo stato dell'ambiente, la loro significatività, nonché le componenti ambientali che sono influenzate da tali azioni;
- d. fissa gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elabora dei programmi per il raggiungimento di tali obiettivi con la definizione di priorità, tempi ed attribuzione delle relative responsabilità – con assegnazione delle necessarie risorse - in materia di protezione dell'ambiente, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività di tutti i soggetti su cui ricade la responsabilità dell'attuazione delle misure per la protezione dell'ambiente;
- e. sensibilizza la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;

- formazione differenziata per soggetti investiti di specifiche funzioni in materia di protezione dell'ambiente e per soggetti addetti a mansioni dalle quali possono derivare impatti ambientali;
- f. attua adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia delle procedure e dei sistemi di gestione ambientale adottati, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme;
 - coerenza tra attività svolta e competenze possedute;
- g. attua le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- h. effettua un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione ambientale nel raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alla specifica realtà della Società sia ad eventuali mutamenti nell'attività.

In particolare, in conformità ai principi di prevenzione e di precauzione, l'obiettivo del rispetto delle norme comportamentali e delle relative procedure interne prescritte per la tutela dell'ambiente sarà quello di prevenire condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora, ovvero che provochino o possano provocare il decesso o lesioni gravi alle persone.

In relazione alle aree a rischio individuate nella presente Parte Speciale, e a integrazione dei presidi e delle procedure aziendali già esistenti, si riportano di seguito specifici principi di comportamento da tenere in osservanza del Decreto.

Protocollo 1 – Rispetto della normativa sull'ambiente	
Politiche aziendali in tema di protezione dell'ambiente	La politica per la protezione dell'ambiente adottata dalla Società deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte dalla Società e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della riduzione degli impatti sull'ambiente. Tale politica contiene: • l'individuazione di un approccio strutturato alla riduzione dell'impatto ambientale e all'incremento della sicurezza che tenga conto di tutte le implicazioni di carattere organizzativo, tecnico, economico, normativo; • l'individuazione dello sviluppo sostenibile della Società e del territorio nel quale essa opera come missione primaria della Società; • l'impegno a ridurre i consumi energetici e di materie prime, privilegiando l'utilizzo di processi e materie prime a minore impatto ambientale; • l'impegno a commercializzare prodotti sempre più compatibili con l'ambiente e sicuri

	per gli utilizzatori; • l'identificazione e la valutazione degli effetti ambientali e dei rischi dovuti a incidenti, fatti accidentali potenziali, situazioni di emergenza; • l'impegno alla prevenzione ed al miglioramento continuo delle proprie capacità organizzative e tecniche in grado di ridurre l'impatto ambientale e i rischi legati all'attività della Società; • l'impegno a fornire le risorse umane e strumentali necessarie; • l'impegno ad un riesame periodico della politica per l'ambiente al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società, nonché alla normativa vigente in materia ed alle migliori prassi internazionali; • l'adeguamento continuo alle crescenti esigenze sociali e legislative nel campo della tutela dell'ambiente e della sicurezza, precorrendole, ove possibile, mediante un'adeguata pianificazione delle attività e iniziative in tali campi; • l'impegno a definire e diffondere all'interno della Società la conoscenza delle problematiche di tutela dell'ambiente, delle relative discipline tecnico-organizzative nonché gli obiettivi del sistema di gestione ambiente e sicurezza ed i relativi programmi di attuazione. La politica è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario. Le procedure interne devono inoltre essere caratterizzate dai seguenti elementi: • separatezza, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni"); • traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità"); • adeguato livello di formalizzazione. La Società predispone ed adotta inoltre procedure finalizzate ad individuare le modalità e le funzioni responsabili della gestione dei rapporti con le competenti Autorità amministrative, nonché delle ispezioni e degli accertamenti in materia di tutela ambientale e dell'elevazione di contestazioni. In particolare, dovrà essere: • conferita procura speciale ai responsabili delle funzioni coinvolte in ispezioni e/o accertamenti al fine di dotarli del potere di rappresentare la Società dinanzi alla pubblica Autorità (in particolare, Ufficio delle Entrate, Guardia di Finanza, ARPA, ASL, NOE, CFS, MIPAF, NAS, nonché le altre Forze dell'Ordine delegate in materia ambientale) in caso di ispezione e/o accertamento; • conferita apposita delega alla funzione deputata a rappresentare la Società nei confronti dell'Ente di Pubblica Amministrazione concedente un provvedimento amministrativo o nei confronti del quale sia diretta una comunicazione; • prevista la redazione da parte dei procuratori sopra indicati di un report informativo dell'attività svolta nel corso dell'ispezione; • prevista una metodologia di archiviazione della documentazione relativa all'attività in oggetto; • prevista una modalità di comunicazione preventiva dell'avviso di ispezioni (anche periodiche, ad esempio in materia di A.I.A.) ai soggetti responsabili preposti per materia nonché il ruolo di questi ultimi nell'indirizzo, supervisione e controllo; • individuata la modalità con la quale evadere le richieste di informazioni da parte delle Autorità di vigilanza, nonché il flusso informativo verso eventuali ulteriori funzioni o, in
--	---

	caso di necessità ed urgenza, le modalità con le quali informare CDA; • prevista un'apposita forma di rendiconto periodico sulla gestione di tali fasi all'Organismo di Vigilanza. Devono inoltre essere osservati i seguenti ulteriori principi procedurali specifici, da integrarsi con le procedure di sistema e istruzioni di processo, di controllo operativo ed emergenze previste dal sistema integrato di gestione ambiente e sicurezza adottato dalla Società: • devono essere specificamente individuate e rigorosamente rispettate le procedure di monitoraggio dei processi produttivi e le procedure di emergenza previste per il caso di incidenti; • devono essere individuate e rigorosamente osservate specifiche procedure di monitoraggio e controllo delle emissioni e degli scarichi; • devono essere previste e rigorosamente rispettate le procedure operative di gestione dei rifiuti adottate dalla Società in conformità alle disposizioni di cui al d.lgs. n. 152/06 nonché le procedure amministrative di gestione dei rifiuti applicabili alle diverse tipologie di rifiuti prodotti dalla Società, con particolare riferimento agli adempimenti di comunicazione, tenuta dei registri obbligatori e dei formulari e/o agli adempimenti prescritti dal sistema informatico di controllo della tracciabilità dei rifiuti (ex SISTRI oggi "Registro elettronico nazionale per la tracciabilità dei rifiuti"); • devono essere definiti e rigorosamente osservati specifici protocolli relativi all'assunzione delle misure di prevenzione e messa in sicurezza di emergenza che si rendano eventualmente necessarie nell'ipotesi di eventi idonei a determinare situazioni di potenziale contaminazione di suolo, sottosuolo, acque superficiali o sotterranee e/o di potenziale impatto sulla flora e fauna; • non devono essere utilizzate o detenute le sostanze di cui alla tabella A allegata alla legge 28 dicembre 1993, n. 549. La Società: • svolge, a favore dei Destinatari, in modo differenziato ed adeguato ai rispettivi compiti e responsabilità, un'attività di formazione finalizzata alla conoscenza della normativa applicabile ai processi e delle procedure di gestione ambientale adottate dalla Società; • adotta i necessari presidi affinché i processi produttivi si svolgano in condizioni controllate; • predispone le procedure atte a definire, per i processi produttivi suscettibili di dar luogo a impatti sull'ambiente, le modalità di lavoro, i valori dei parametri operativi, i criteri di accettabilità, le registrazioni da produrre; • adotta procedure di emergenza volte a evitare o mitigare gli effetti di incidenti; • definisce le condizioni per tenere sotto controllo i parametri dei processi produttivi; • predispone ed attua programmi di formazione.
Processo di pianificazione e	La Società, nell'ambito del processo di pianificazione degli obiettivi in tema di protezione dell'ambiente, con cadenza annuale: • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od

	implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	<u>L'informazione</u> L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a: • l'importanza di rispettare la politica ambientale e gli obiettivi individuati dalla Società; • le conseguenze derivanti dallo svolgimento della propria attività in modo non conforme alla politica ambientale e agli obiettivi individuati dalla Società; • il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità alla politica aziendale ed alle procedure in materia di protezione dell'ambiente e ad ogni altra prescrizione relativa al sistema di gestione ambientale adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale. Ciò premesso, la Società in considerazione dei diversi ruoli e responsabilità dei Destinatari, è tenuta ai seguenti oneri informativi: • la Società deve fornire adeguata informazione ai Destinatari circa i rischi di impatti negativi sull'ambiente derivanti dall'attività dell'impresa, sulle conseguenze di questi e sulle procedure operative da adottare; • la Società deve organizzare periodici incontri tra le funzioni preposte alla protezione dell'ambiente; • la Società deve coinvolgere i responsabili di settore nell'organizzazione dell'attività di rilevazione e valutazione dei rischi e di prevenzione. Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione. <u>Formazione</u> • La Società deve fornire adeguata formazione al personale addetto ad attività che possono avere un'incidenza sull'ambiente; • i responsabili per la Sicurezza sul Lavoro devono partecipare alla stesura del piano di formazione; • la formazione erogata deve prevedere questionari di valutazione; • la formazione deve essere adeguata ai contenuti della mansione cui il lavoratore è in concreto assegnato ed ai possibili impatti della relativa attività sull'ambiente; • deve essere predisposto uno specifico piano di formazione per i lavoratori addetti ad attività da cui possano derivare impatti ambientali significativi; • i lavoratori che cambiano mansione e quelli trasferiti a compiti da cui possano derivare impatti ambientali devono fruire di formazione preventiva, aggiuntiva e specifica; • gli addetti a specifici compiti in materia di protezione dell'ambiente devono ricevere specifica formazione; • la Società deve effettuare periodiche esercitazioni finalizzate all'adozione del corretto comportamento in caso di incidenti o di emergenze di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze). Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente. Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione ambientale, la Società deve garantire un adeguato livello di circolazione e condivisione

	delle informazioni tra tutti i Destinatari. Pertanto, la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi: • dal basso verso l'alto: è garantito dalla Società il diritto-dovere dei Destinatari di portare a conoscenza proposte ed esigenze di miglioria inerenti alla gestione ambientale; • dall'alto verso il basso: ha lo scopo di diffondere a tutti i Destinatari la conoscenza del sistema adottato dalla Società per la gestione ambientale. A tale scopo la Società garantisce agli esponenti aziendali (ovvero gli amministratori, i dirigenti, i componenti del Collegio Sindacale e i dipendenti della Società) un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto: • nuovi rischi in materia di protezione dell'ambiente; • modifiche nella struttura organizzativa adottata dalla Società per la gestione dell'ambiente; • contenuti delle procedure aziendali adottate per la gestione dell'ambiente; • ogni altro aspetto inerente alla gestione dell'ambiente. <u>Documentazione</u> La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, oltre ai documenti sopra indicati, anche dei seguenti documenti: • la documentazione inerente alle norme relative alla protezione dell'ambiente rilevanti per l'attività aziendale; • le autorizzazioni ambientali relative all'esercizio dell'attività della Società; • i registri relativi a taratura e manutenzione delle apparecchiature di sorveglianza; • la documentazione relativa all'attività di sorveglianza ed alle misurazioni; • i piani di emergenza; • le informazioni relative ai Fornitori; • il registro degli incidenti e delle azioni correttive attuate; • tutta la documentazione relativa alle attività di Informazione e Formazione che dovrà essere conservata a cura del responsabile per la Sicurezza sul Lavoro.
Attività di monitoraggio	La Società deve assicurare un costante ed efficace monitoraggio del sistema di gestione ambientale. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte nell'ambito del sistema di gestione ambiente e sicurezza; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione ambiente e sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni incidente verificatosi, al fine di individuare eventuali lacune nel sistema di gestione ambientale e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta la Società, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. La Società garantisce che gli eventuali interventi correttivi necessari vengano predisposti nel più breve tempo possibile.
Riesame del sistema	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema di gestione ambientale adottato dalla Società è sottoposto ad un riesame annuale da parte della Società, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il

	raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.
--	--

1.18 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-undecies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti della Società eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla protezione dell'ambiente, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la protezione dell'ambiente, in coerenza con quanto stabilito nel presente Modello e nel sistema di gestione ambiente e sicurezza adottato dalla Società;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla tutela dell'ambiente valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il responsabile per la Sicurezza sul Lavoro.
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

La Società garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli incidenti verificatisi, delle modifiche dei processi produttivi aventi un impatto sull'ambiente, nonché delle implementazioni dei sistemi di gestione ambiente e sicurezza.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti della Società.

1.19 Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25-quinquiesdecies del Decreto)

Il Decreto Legge n. 124 del 26 ottobre 2019, convertito con modificazioni nella Legge n. 157 del 19 dicembre 2019, ha introdotto i reati tributari nell'elenco dei reati presupposto della responsabilità amministrativa degli enti.

Con l'inserimento nel Decreto 231 dell'art. 25-quinquiesdecies viene prevista, dunque, una nuova responsabilità nei confronti dell'ente in caso di commissione, nel suo interesse o a suo vantaggio, di alcuni dei reati tributari contemplati nel D.Lgs. 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205".

Successivamente, il 30 luglio 2020, il D.Lgs. 75/2020 (in adempimento alla Direttiva UE/2017/1371 c.d. "PIF") ha esteso ulteriormente il catalogo dei reati tributari presupposto per la responsabilità dell'ente.

Sotto il profilo strettamente fiscale, la Direttiva PIF prevede come soglia minima di tutela la repressione di gravi frodi IVA, ossia di tutte quelle *"azioni od omissioni di carattere intenzionale secondo la definizione di cui all'art. 3, paragrafo 2, lettera d), [che] siano connesse al territorio di due*

o più Stati membri dell'Unione e comportino un danno complessivo pari ad almeno 10 mln di euro", ferma restando la facoltà per la legislazione nazionale di mantenere o adottare norme più rigorose.

Al fine di comprendere cosa possa essere considerato come *"frode che lede gli interessi finanziari dell'Unione"* la menzionata Direttiva, all'art. 3, paragrafo 2, lettera d), precisa che la suddetta frode è l'azione od omissione commessa in sistemi fraudolenti transfrontalieri in relazione:

- "i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti relativi all'IVA, cui consegua la diminuzione di risorse del bilancio dell'Unione;*
- ii) alla mancata comunicazione di un'informazione relativa all'IVA in violazione di un obbligo specifico, cui consegua lo stesso effetto;*
- iii) alla presentazione di dichiarazioni esatte relative all'IVA per dissimulare in maniera fraudolenta il mancato pagamento o la costituzione illecita di diritti a rimborsi dell'IVA".*

Si riporta di seguito il testo dell'art. 25-quinquiesdecies del D. Lgs. 231/2001.

Art. 25-quinquiesdecies**Reati tributari**

* * *

1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
- d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
- g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
- b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
- c) per il delitto di indebita compensazione previsto dall'articolo 10 quater, la sanzione pecuniaria fino a quattrocento quote.
- d) Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) ”.

Ai fini della normativa tributaria di cui al Decreto Legislativo 10 marzo 2000, n. 74 rubricato “Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell’articolo 9 della Legge 25 giugno 1999, n. 205”, si applicano le seguenti definizioni di carattere generale applicabili a tutti i reati tributari:

- per *"fatture o altri documenti per operazioni inesistenti"* si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, (i) emessi a fronte di operazioni non realmente effettuate in tutto o in parte o (ii) che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero (iii) che riferiscono l'operazione a soggetti diversi da quelli effettivi;
- per *"elementi attivi o passivi"* si intendono (i) le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e (ii) le componenti che incidono sulla determinazione dell'imposta dovuta;
- per *"dichiarazioni"* si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
- il *"fine di evadere le imposte"* e il *"fine di consentire a terzi l'evasione"* si intendono comprensivi, rispettivamente, anche (i) del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e (ii) del fine di consentirli a terzi;
- riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il *"fine di evadere le imposte"* ed il *"fine di sottrarsi al pagamento"* si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
- per *"imposta evasa"* si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

- le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
- per *“operazioni simulate oggettivamente o soggettivamente”* si intendono (i) le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero (ii) le operazioni riferite a soggetti fittiziamente interposti;
- per *“mezzi fraudolenti”* si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

1.20 La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)

Le nuove fattispecie di reati tributari introdotte nell'elenco dei reati suscettibili di rilevare secondo il Decreto 231, sono dunque le seguenti:

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74).

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

- **Dichiarazione fraudolenta mediante altri artifici** (art. 3, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si configura allorché, fuori dai casi previsti dall'articolo 2 (di cui sopra), al fine di evadere le imposte sui redditi o sul valore aggiunto, il soggetto autore del reato - (i) compiendo operazioni simulate oggettivamente o soggettivamente ovvero (ii) avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria - indichi in una delle dichiarazioni relative a dette imposte (a) *elementi attivi per un ammontare inferiore a quello effettivo* o (b) *elementi passivi fittizi* o (c) *crediti e ritenute fittizi*, quando, congiuntamente:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;

- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, (i) è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, (ii) è superiore a euro un milione cinquecentomila, ovvero (iii) qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della norma non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

- **Emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma 1 e comma 2-bis, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Ai fini di quanto sopra indicato, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

- **Occultamento o distruzione di documenti contabili** (art. 10, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, (i) al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero (ii) di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

- **Sottrazione fraudolenta al pagamento di imposte** (art. 11, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza:

a) allorché un soggetto - (i) al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero (ii) di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila - aliena simulatamente o compie altri atti

fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

b) allorché un soggetto - al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori - indica nella documentazione presentata ai fini della procedura di transazione fiscale (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

- **Dichiarazione infedele ex art. 4 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Si realizza qualora un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- b. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Tale illecito è rilevante per la Società solo nel caso in cui sia commesso ***“nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro”***, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Omessa dichiarazione ex art. 5 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Tale fattispecie punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. Punisce, altresì, chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Tale illecito è rilevante per la Società solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Indebita compensazione ex art. 10-quater D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).

Tale ipotesi delittuosa si configura qualora un soggetto non versi le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti o crediti inesistenti, per un importo annuo superiore a cinquantamila euro.

Tale illecito è rilevante per la Società solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

1.21 Sanzioni nei confronti dell’Ente.

In relazione alla commissione dei reati sopra elencati si applicano le seguenti sanzioni pecuniarie:

- art. 2 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 3 - Dichiarazione fraudolenta mediante altri artifici: sanzione pecuniaria fino a 500 quote;
- art. 8 - Emissione di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 10 - Occultamento o distruzione di documenti contabili: sanzione pecuniaria fino a 400 quote;
- art. 11 - Sottrazione fraudolenta al pagamento di imposte: sanzione pecuniaria fino a 400 quote;
- art. 4 - Dichiarazione infedele: sanzione pecuniaria fino a 300 quote;
- art. 5 - Omessa dichiarazione: sanzione pecuniaria fino a 400 quote;
- art. 10-quater - Indebita compensazione: sanzione pecuniaria fino a 400 quote.

Nei casi previsti dai commi 1 e 2 dell'art. 25-quinquiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

1.22 Aumenti delle sanzioni nei confronti dell'ente

Le sanzioni pecuniarie sono aumentate di un terzo qualora, a seguito alla commissione dei delitti di cui trattasi (indicati nel comma 1 dell'art. 25-quinquiesdecies), l'ente abbia conseguito un profitto di rilevante entità.

1.23 Aree a rischio reato e processi sensibili

I processi sensibili individuati da HS che presentano il rischio di commissione dei reati di cui alla presente sezione riguardano le seguenti attività:

- Gestione della contabilità: con riferimento alla gestione della fatturazione attiva e passiva e all'emissione e contabilizzazione di fatture e altra documentazione afferente alla contabilità;
- Acquisto di beni e servizi - con riferimento all'attività di selezione e gestione dei fornitori esterni e di eventuali subappaltatori;
- Adempimenti fiscali e tributari in genere: con riferimento a i) predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere, ii) calcolo obbligazioni tributarie, iii) gestione adempimenti dichiarativi e contributivi e iv) pagamento delle imposte;
- Tenuta e custodia delle scritture contabili e fiscali: con riferimento alla conservazione, tracciabilità ed archiviazione di tutta la documentazione contabile e fiscale;
- Gestione di eventuali operazioni straordinarie: con riferimento ad eventuali trasformazioni, fusioni, scissioni, cessioni e/o conferimenti d'azienda, vendite di assets aziendali, ecc.

La tabella che segue indica in modo sintetico processi sensibili e relativi possibili reati tributari.

Processi sensibili	Reato
• <u>Gestione della contabilità</u> • <u>Acquisto di beni e servizi</u> • <u>Adempimenti fiscali e tributari in genere</u>	• Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 10 marzo 2000, n. 74);

• <u>Tenuta e custodia delle scritture contabili e fiscali</u> • <u>Gestione di eventuali operazioni straordinarie</u>	• Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 10 marzo 2000, n. 74); • Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 10 marzo 2000, n. 74); • Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione infedele ex art. 4 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Omessa dichiarazione ex art. 5 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Indebita compensazione ex art. 10-quater D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).
---	---

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

1.24 Regole di comportamento.

1.24.1 Principi generali e standard di controllo.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Sezione prevede l'espresso divieto di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-quinquiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;
2. comunicare all'Agenzia delle Entrate e/o alle Autorità fiscali dati non rispondenti al vero, con il divieto di predisporre e fornire documenti falsi, omettere le informazioni dovute.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a:
 - diffondere i principi di HS previsti dal Codice Etico;
 - promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati;
 - rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con l'Agenzia delle Entrate e le Autorità fiscali;
 - rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con l'Agenzia delle Entrate e le Autorità fiscali, deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che si occupano della predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria, dell'emissione di documentazione afferente alla contabilità, del ricevimento di documentazione afferente alla contabilità o del pagamento di imposte, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per evitare il rischio di violazioni in materia tributaria;
- ✓ tutti i consulenti in materia fiscale di HS devono essere informati circa le linee guida contro la commissione di reati tributari;
- ✓ qualunque criticità sorga nell'ambito del rapporto con l'Agenzia delle Entrate e le Autorità fiscali, deve essere immediatamente comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

È, inoltre, sancito l'espresso obbligo di:

- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- garantire un corretto e trasparente processo di gestione delle operazioni straordinarie, compresa la vendita di eventuali asset aziendali;

- assicurare la veridicità dei dati predisposti;
- assicurare la trasparente gestione delle forniture, di beni e servizi;
- garantire il flusso informativo tra le funzioni coinvolte nei processi sensibili in materia contabile-fiscale con il Collegio Sindacale e l'Organismo di Vigilanza;
- svolgere un'adeguata attività di selezione dei fornitori;
- acquistare beni di provenienza garantita e servizi e/o qualsiasi altra utilità ad un prezzo che, salvo casi eccezionali e certificati (quali ad esempio acquisti da aste giudiziarie o da fallimenti), sia commisurato alla qualità e quantità dei beni stessi in base al valore di mercato;
- rispettare la normativa fiscale-tributaria;
- garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali.

Gli standard di controllo da considerare ed applicare con riferimento alle attività sensibili di cui alla presente sezione sono:

- **previsione di procedure interne** idonee a fornire i principi di riferimento generali per la regolamentazione dell'attività sensibile;
- **tracciabilità**: tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali/informatici;
- **segregazione dei compiti**: lo standard concerne l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di un sistema di segregazione delle funzioni coerente** con le responsabilità organizzative assegnate: sono previste regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

1.24.2 Principi procedurali specifici

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto

all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1 Definizione di ruoli e responsabilità Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti. Tenuta e custodia delle scritture contabili e fiscali Gestione delle operazioni straordinarie	
Definizione di ruoli e responsabilità	- Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare all'Agenzia delle Entrate o alle altre Autorità fiscali [ad es., nel caso di predisposizione della documentazione ai fini di dichiarazioni e comunicazioni concernenti la materia tributaria, deve essere ben chiara la segregazione delle funzioni tra (i) chi è preposto alla elaborazione e raccolta della documentazione da presentare, (ii) chi verifica, approva e sottoscrive la documentazione da presentare. - Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti	È fatto obbligo di: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni nelle fasi di autorizzazione / esecuzione / controllo per i seguenti ambiti: - gestione della fatturazione e relativa registrazione - gestione dei pagamenti - gestione delle note di credito - gestione degli acquisti, di beni e servizi - gestione buste paga e rimborsi spesa ai dipendenti - tenere tracciate tutte le fasi di gestione dei flussi finanziari e archiviare in maniera completa i relativi documenti giustificativi; - prevedere un sistema di backup dell'archiviazione dei documenti contabili; - verificare l'effettiva e corretta esecuzione della prestazione richiesta (sia verso fornitori di beni che di servizi), nel rispetto del principio di segregazione delle funzioni, prima di autorizzare il pagamento della relativa fattura; - tenere traccia e registrare ogni richiesta di ordine e relativo preventivo inoltrato, sia che sia stato mandato via e-mail che telefonici (in quest'ultimo caso andrà compilato apposito modulo di richiesta ordine); - verificare che gli incassi siano sempre supportati da un contratto o un ordine autorizzato e conseguentemente non accettare beni e/o altre utilità a fronte delle quali non vi sia un contratto o un ordine adeguatamente autorizzato;

- verificare che l'importo effettivamente incassato corrisponda a quello fatturato e che non vi siano anomalie al riguardo;
- rispettare le procedure adottate che regolano la gestione della contabilità;
- rispettare il sistema di deleghe e procure adottato che indica i poteri ed i limiti di spesa dei soggetti coinvolti;
- verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività;
- svolgere un'attenta attività di selezione dei potenziali fornitori (sia di beni che di servizi), rispettando i criteri tecnico-economici ed espletando un'adeguata attività selettiva e di obiettiva comparazione tra più offerte;
- a seconda del servizio richiesto, richiedere al fornitore tutta la documentazione o le certificazioni previste dalla legge di riferimento;
- formalizzare tutti i contratti/accordi con fornitori e/o consulenti, allegando la relativa documentazione;
- qualora si faccia uso di soggetti terzi intermediari, verificare con attenzione l'esistenza effettiva, la solidità e l'affidabilità del soggetto;
- monitorare il mantenimento dei requisiti richiesti in capo al fornitore;
- inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali);
- identificare i ruoli e le responsabilità per la gestione dei rimborsi spese ai dipendenti nel rispetto del principio di segregazione di ruoli nelle fasi di autorizzazione / esecuzione / controllo;
- controllare che ogni richiesta di rimborso spese sia accompagnata dalla relativa documentazione giustificativa e conseguentemente non riconoscere alcuna somma che non sia supportata da relativo giustificativo.

Inoltre, ai fini preventivi, si ribadisce che:

- è assolutamente vietato:
 - contabilizzare e registrare fatture per operazioni/prestazioni inesistenti;
 - autorizzare pagamenti a fornitori per operazioni inesistenti o privi dell'evidenza dell'effettuazione del servizio reso;
 - autorizzare rimborsi spesa privi della necessaria documentazione giustificativa;
 - predisporre o comunque utilizzare documenti palesemente falsi;
- ogni pagamento deve corrispondere esattamente a quanto indicato nel contratto e/o nel preventivo formulato al cliente;
- nessun pagamento e nessun incasso di denaro verso/da Paesi inseriti nelle principali black list internazionali, può avvenire senza adeguata documentazione comprovante la reale e specifica necessità;
- nessun pagamento può essere effettuato in favore di un soggetto diverso dalla controparte contrattuale. Eventuali eccezioni a tale divieto sono ammesse solo a fronte della presentazione di una regolare documentazione che giustifichi e consente il pagamento nei confronti di un terzo (es. in caso di cessione del credito o pignoramento presso terzi);
- nessun acquisto deve essere effettuato attraverso il ricorso a mercati non

	consolidati; • nessun contratto di fornitura può essere stipulato in assenza di un'adeguata attività di selezione o in mancanza della relativa documentazione richiesta dalla legge; • tutti gli incassi devono provenire dalla controparte contrattuale. Eventuali eccezioni sono ammesse solo a fronte della presentazione di una regolare documentazione giustificativa (es. pignoramento presso terzi); • ogni importo effettivamente incassato deve corrispondere a quanto fatturato. Qualora sia necessario restituire un pagamento o parte di esso indebitamente ricevuto, questo deve essere disposto esclusivamente verso il conto corrente di provenienza, tenendo traccia dei documenti giustificativi; • occorre tenere l'evidenza scritta di ogni pagamento; • occorre archiviare tutti i documenti contabili nel rispetto dei principi di <u>correttezza, completezza e attenzione della relativa tenuta.</u>
Tenuta e custodia delle scritture contabili e fiscali	In merito alla tenuta delle scritture contabili, è fatto obbligo: • identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni per i seguenti ambiti: - gestione degli adempimenti fiscali e tributari; - gestione del calcolo delle obbligazioni tributarie e dei relativi obblighi dichiarativi; - gestione e tenuta delle scritture contabili e fiscali; • tenere tracciate tutte le fasi di gestione dei citati processi e archiviare in maniera completa i relativi documenti; • prevedere un sistema di back up dell'archiviazione dei documenti contabili e fiscali; • prevedere modalità di aggiornamento, anche tramite consulenti esterni, sulle novità in ambito fiscale e tributario; • provvedere al regolare adempimento degli obblighi fiscali-tributari cui la società è tenuta (tributi, contributi, Iva etc.); • prevedere uno scadenziario che preveda i termini entro i quali occorre provvedere ai vari adempimenti fiscali-tributari. È, inoltre, vietato: • occultare o distruggere, in tutto o in parte, documenti contabili, fiscali o di cui è comunque obbligatoria la conservazione; • omettere o fornire dati ed informazioni inesatte o non complete imposte dalla legge sulla situazione economica, patrimoniale e finanziaria della società; • violare, eludere, evadere obblighi di dichiarazione, attestazione, certificazione di natura tributaria previsti dalla legge; • non adempiere le prescrizioni di legge in materia contabile, di informazione societaria, di valutazione di cespiti e di redazione del bilancio; • occultare in contabilità redditi conseguiti soggetti a tassazione, rappresentare falsamente spese non reali, emettere fatture per prestazioni inesistenti, effettuare stime, valutazioni e determinazione di poste di bilancio con modalità e criteri valutativi difforni da quelli richiesti dalla legge; • porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da

	parte degli organi di controllo; ostacolare, in ogni modo, l'effettuazione di verifiche, accertamenti ed ispezioni da parte dell'Agenzia delle Entrate o delle altre Autorità fiscali o giudiziarie.
Gestione delle operazioni straordinarie	Con riferimento a tale attività è fatto obbligo di: - garantire l'esplicita approvazione, da parte dell'Assemblea dei Soci, di ogni attività relativa ad operazioni straordinarie, comprese le cessioni e dismissioni di assets aziendali, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni, qualora per il compimento delle suddette operazioni si renda necessaria od opportuna l'approvazione dell'Assemblea; - identificare in maniera chiara e precisa i ruoli ed i soggetti competenti alla predisposizione della documentazione destinata agli organi sociali a supporto delle deliberazioni relative ad operazioni straordinarie; - identificare in maniera chiara ruoli e responsabilità in merito alla tenuta ed archiviazione degli atti di delibera e dei relativi documenti predisposti; - garantire una corretta tenuta ed archiviazione della documentazione relativa alle operazioni, prevedendo anche sistemi di back up.; È, inoltre, assolutamente vietato: - alienare simulatamente beni o assets aziendali al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; - compiere qualsiasi altro atto fraudolento al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; - indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

1.24.3 Responsabilità specifiche del Consiglio di Amministrazione (Presidente e Consiglieri)

Con riferimento alla prevenzione del rischio di commissione dei reati tributari sarà compito del CDA:

- verificare ed approvare il progetto di bilancio e nota integrativa nonché le situazioni patrimoniali in occasione delle operazioni straordinarie prima che siano sottoposti all'Assemblea dei soci;
- valutare la fattibilità ed approvare le operazioni straordinarie;
- redigere ed approvare la Relazione sulla Gestione sulla base delle informazioni raccolte dalle Funzioni aziendali coinvolte;
- supportare e verificare le valutazioni contabili effettuate dall'ufficio amministrativo;
- autorizzare l'apertura o la chiusura dei conti correnti bancari;
- autorizzare l'emissione di assegni;
- autorizzare gli ordini di bonifici bancari;
- autorizzare l'emissione e l'utilizzo di carte di credito aziendali;

- autorizzare nuovi finanziamenti.

Il CDA o il Presidente ove lo ritengano opportuno, per la migliore e più agile gestione aziendale, fermo restando il loro potere (e connessa responsabilità) autorizzativo, possono delegare espressamente alla firma (in loro vece) di ogni e qualsivoglia strumento finanziario (apertura conti correnti bancari, sconto fatture, versamenti in c/c bancario, bonifici bancari anche in home banking, firma di assegni, ecc.) in qualità di mero portatore della loro volontà, sempre con apposita procura notarile. Le autorizzazioni del CDA o del Presidente di cui alla presente procedura possono essere anche generali e preventive per tipologie di operazioni di routine (i.e., quale indicazione non esaustiva: pagamento stipendi, pagamento di fatture e note pro forma di consulenti e fornitori di servizi - anche professionali - in presenza di contratti o lettere d'incarico recanti compensi forfetizzati e ripetitivi nel tempo, piccole spese di cassa).

1.25 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'esito di eventuali audit effettuati sulla gestione delle attività sensibili sopra indicate, sia da parte di funzioni interne che da parte di soggetti esterni (ad es. consulenti fiscali, commercialisti, ecc.);
- l'avviso di eventuali ispezioni da parte dell'Agenzia delle Entrate o di altre autorità fiscali o giudiziarie con relativo verbale;
- eventuali comunicazioni provenienti dal Collegio Sindacale relativamente a criticità emerse, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-quinquiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente - con il supporto delle funzioni competenti - il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od

opportuni;

- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

L'Organismo di Vigilanza deve riportare i risultati della sua attività di vigilanza e controllo, con cadenza periodica semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale.

Peraltro, nel caso in cui dagli accertamenti svolti dall'Organismo di Vigilanza emergano elementi che facciano risalire la violazione dei principi e protocolli contenuti nella presente Parte Speciale del Modello, la commissione del reato, o il tentativo di commissione del reato, direttamente al Presidente, l'Organismo di Vigilanza dovrà riferire al Consiglio di Amministrazione ed al Collegio Sindacale, ai quali compete la decisione sull'eventuale applicazione dei meccanismi previsti dalla legge.

1.26 Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25-sexiesdecies del Decreto)

Il reato di contrabbando, previsto all'art. 25-sexiesdecies del Decreto, è stato introdotto dal D.Lgs. 14 luglio 2020, n. 75 ("Attuazione della direttiva (UE) 2017/1371 c.d. "Direttiva PIF", relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale").

L'art. 25-sexiesdecies del D.Lgs. 231/01 dispone che: *"1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.*

2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

La Società ha ritenuto di dover mappare il rischio connesso alla commissione di reati di contrabbando stante la ingente attività di import ed export con diversi paesi UE ed extra UE.

A tal fine, si ritiene necessaria una breve premessa con riferimento alla materia doganale.

I dazi doganali rappresentano una risorsa propria dell'Unione europea e confluiscono nel bilancio unitario, ad esclusione di una percentuale del 25% che viene trattenuta dallo Stato di entrata delle merci a copertura delle spese di riscossione (fonte: dossier di documentazione parlamentare).

La normativa doganale è contenuta nel Decreto del Presidente della Repubblica 23 gennaio 1973 n. 43 (Testo Unico Doganale, "TUD").

Si considerano "diritti doganali" tutti quei diritti che la dogana è tenuta a riscuotere in forza di una legge, in relazione alle operazioni doganali. Fra i diritti doganali costituiscono "diritti di confine" (art. 34 del TUD):

- i dazi di importazione e quelli di esportazione;
- i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione;
- i diritti di monopolio, le sovrimposte di confine ed ogni altra imposta o sovrimposta di consumo a favore dello Stato (per quanto concerne le merci in importazione).

Per le merci soggette a diritti di confine, il presupposto dell'obbligazione tributaria è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e, relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso (art. 36 del TUD).

1.27 Sanzioni nei confronti dell'Ente.

In relazione alla commissione dei reati di cui sopra si applicano all'ente le seguenti sanzioni pecuniarie:

1. fino a 200 quote in relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica n. 43/1973, ovvero ai delitti del Titolo VII Capo I, intendendosi per tali i fatti ivi previsti (ma solo se superano 10mila euro di diritti di confine evasi) ed in particolare:
 - Articolo 282 (Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali)
 - Articolo 283 (Contrabbando nel movimento delle merci nei laghi di confine)
 - Articolo 284 (Contrabbando nel movimento marittimo delle merci)
 - Articolo 285 (Contrabbando nel movimento delle merci per via aerea)
 - Articolo 286 (Contrabbando nelle zone extra-doganali)
 - Articolo 287 (Contrabbando per indebito uso di merci importate con agevolazioni doganali)
 - Articolo 288 (Contrabbando nei depositi doganali)
 - Articolo 289 (Contrabbando nel cabotaggio e nella circolazione)

- Articolo 290 (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti).
- Articolo 291 (Contrabbando nell'importazione od esportazione temporanea)
- Articolo 291-bis (Contrabbando di tabacchi lavorati esteri)
- Articolo 291-ter (Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri)
- Articolo 291-quater (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri)
- Articolo 292 (Altri casi di contrabbando)
- Articolo 294 (Pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato)
- alle contravvenzioni del Titolo VII Capo II, cioè ai fatti ivi previsti ma solo se superano i 10mila euro di diritti di confine evasi (articoli 302 e seguenti).

2. fino a 400 quote qualora i diritti di confine dovuti superino i 100.000 Euro.

Nei casi previsti dai commi 1 e 2 dell'art. 25-sexiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

1.28 Aree a rischio reato e processi sensibili

I processi sensibili che presentano il rischio di commissione dei reati di cui al presente paragrafo riguardano le seguenti attività:

- vendita, acquisto, commercializzazione e scambio di prodotti oltre confine;
- scarico e deposito delle merci oltre confine.

Le potenziali aree a rischio reato che HS ha astrattamente individuato sono quelle relative alle seguenti attività:

Processi sensibili	Reato
• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine • Scarico e deposito delle merci oltre confine	• Contrabbando (Decreto del Presidente della Repubblica n. 43/1973);

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

1.29 Regole di comportamento

1.29.1. Principi generali e standard di controllo

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-sexiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;

Inoltre, è fatto specifico divieto di:

- introdurre merci estere attraverso il confine di terra in violazione delle prescrizioni, divieti e limitazioni;
- introdurre merci estere via mare in violazione delle prescrizioni, divieti e limitazioni;
- scaricare o depositare merci estere nello spazio intermedio tra la frontiera e la più vicina dogana;
- nascondere merci estere sulla persona o nei bagagli o fra merci di altro genere od in qualunque mezzo di trasporto, per sottrarle alla visita doganale;
- asportare merci dagli spazi doganali senza aver pagato i diritti dovuti senza averne garantito il pagamento;
- portare fuori del territorio doganale merci nazionali o nazionalizzate soggette a diritti di confine;
- detenere merci estere, quando ricorrano le circostanze previste nel secondo comma dell'art. 25-sexiesdecies per il delitto di contrabbando (ovvero, "*Quando i diritti di confine dovuti superano centomila euro*").

1.29.2. Principi procedurali specifici.

Protocollo 1 Controllo interno sull'emissione e la conservazione dei documenti fiscali	
Applicazione di misure idonee ad evitare l'emissione di documentazione contabile non coerente con la prestazione o la distruzione di documenti fiscali al fine di eventuali controlli da parte delle Autorità Doganali	Devono essere osservate specifiche misure che consentano di: • evitare di introdurre o esportare merci che violino prescrizioni, divieti e limitazioni di cui al Testo unico delle disposizioni legislative in materia doganale; • conservare la documentazione doganale; • non sottrarsi alle visite doganali; • pagare i diritti dovuti o garantire i dovuti pagamenti.

Con riferimento e per l'espletamento delle operazioni doganali di import ed export la HS si affida a società selezionate per la notorietà e l'esperienza nel settore delle spedizioni e della consulenza per logistica e trasporti a livello internazionale nonché per le pratiche doganali in import/export. L'affidamento di tali incarichi viene fatto a mezzo contratti di mandato e consulenza annuali e/o a tempo indeterminato.

Dovrà essere cura dei Destinatari della presente sezione di verificare la validità e la vigenza dei suddetti contratti di mandato.

1.30 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'avviso di eventuali ispezioni da parte delle Autorità doganali o di altre autorità giudiziarie sempre relativamente alla materia doganale;
- eventuali comunicazioni provenienti dalle Autorità doganali o di altre autorità giudiziarie relativamente a criticità emerse in materia doganale, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-sexiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- ✓ verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- ✓ esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- ✓ comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- ✓ curare l'aggiornamento del Modello, indicando al CDA le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

2. SEZIONE B – SETTORE QUALITY ASSURANCE & REGULATORY AFFAIRS: RESPONSABILE REGULATORY AFFAIRS (RRA), RESPONSABILE DIREZIONE DI QUALITÀ (R.D.Q.), RESPONSABILE ASSICURAZIONE QUALITÀ (R.A.Q.).

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Quality Assurance & Regulatory Affairs: relativamente a quest'area nella Società si distinguono le funzioni di Responsabile Regulatory Affairs (RRA), Responsabile Direzione di Qualità (R.D.Q.), Responsabile Assicurazione Qualità (R.A.Q.).

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte dal Responsabile Regulatory Affairs (RRA), dal Responsabile Direzione di Qualità (R.D.Q.), nonché dal Responsabile Assicurazione Qualità (R.A.Q.) e nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

SETTORE QUALITY ASSURANCE & REGULATORY AFFAIRS [Responsabile Regulatory Affairs (RRA), Responsabile Direzione di Qualità (R.D.Q.), Responsabile Assicurazione Qualità (R.A.Q.)]	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.); • Gestione delle gare e dei bandi pubblici; • Accesso ai sistemi informatici della Pubblica Amministrazione;

Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto)	Contraffazione, alterazione o uso di marchi.
Reati societari (art. 25-ter)	Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale;
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Gestione delle licenze e dei software per elaboratore.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

2.1 I reati contro la Pubblica Amministrazione

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti.

Essi sono:

- **malversazione a danno dello Stato**, di altro ente pubblico o comunitario (art. 316-bis c.p.), che punisce la mancata destinazione di contributi, sovvenzioni o simili alle finalità per cui erano stati destinati;
- **indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato**, di altro ente pubblico o da parte di ente comunitario (art. 316-ter c.p.) mediante l'utilizzo di documenti falsi o il rilascio di dichiarazioni attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute; [modificato dalla L. n. 3/2019]
- **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), che consiste nella percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato, di altro ente pubblico o da parte di ente comunitario mediante artifici o raggiri diversi dall'utilizzo di documenti falsi, dichiarazioni false od omissione di informazioni dovute;
- **truffa aggravata in danno dello Stato o di altro ente pubblico** (art. 640, comma 2, n. 1 c.p.), che punisce l'impiego di artifici e raggiri per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;

- **frode informatica in danno dello Stato o di altro ente pubblico** (art. 640-ter c.p.), che incrimina l'ipotesi di alterazione del funzionamento di un sistema informatico o telematico, ovvero l'intervento senza diritto su dati, informazioni o programmi contenuti in un sistema informatico, per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;
- **concussione** (art. 317 c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della propria qualità o del proprio potere, costringe o induce il privato a dare o promettere denaro o altra utilità;
- **corruzione per l'esercizio della funzione** (art. 318 c.p.), ossia il caso in cui il pubblico ufficiale riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità, in cambio dell'esercizio delle sue funzioni o poteri; [modificato dalla L. n. 3/2019]
- **corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), ossia il caso in cui il pubblico ufficiale, per omettere o ritardare un atto dell'ufficio o compierne uno contrario ai propri doveri, riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità;
- **corruzione in atti giudiziari** (art. 319-ter c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi di chi riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità al fine di favorire o danneggiare una parte di un processo civile, amministrativo o penale;
- **concussione per induzione, ovvero induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità; la responsabilità penale si estende anche a chi dà o promette denaro o altra utilità;
- **corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), ossia le ipotesi di reato previste dagli artt. 318 e 319 c.p. commesse nei confronti di un incaricato di pubblico servizio;
- **istigazione alla corruzione** (art. 322 c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi che il pubblico ufficiale non accetti di ricevere o il privato si rifiuti di dare denaro o altra utilità;
- **peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): l'ipotesi prevista dal legislatore è quella dei reati contemplati in rubrica commessi nei confronti di funzionari esteri. [modificato dalla L. n. 3/2019]
- **traffico di influenze illecite** (art. 346 bis c.p.) [introdotto con la L. n. 3/2019] Con la riforma del 2019 (legge 3/2019), che ha abrogato l'art. 346 c.p., i fatti fino ad allora qualificabili come

millantato credito possono essere sussunti sotto il nuovo art. 346-bis c.p. Infatti, la condotta punita non consiste solo più nello sfruttamento di relazioni esistenti, ma anche nella vanteria di relazioni «asserite» con un pubblico ufficiale, un incaricato di pubblico servizio o, ancora, con uno dei soggetti elencati all'art. 322-bis c.p.

2.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio.

– Pubblica Amministrazione (di seguito “PA”) s'intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di

reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

- Pubblici ufficiali e incaricati di un pubblico servizio Ai sensi dell’art. 357, primo comma, del codice penale, è considerato pubblico ufficiale “agli effetti della legge penale” colui il quale esercita “una pubblica funzione legislativa, giudiziaria o amministrativa”.

La norma chiarisce solo la nozione di “pubblica funzione amministrativa” (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale “è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”.

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l’art. 358 c.p. definisce i “soggetti incaricati di un pubblico servizio” come quei soggetti “i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della “pubblica funzione”, da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d’ordine e/o la prestazione d’opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

2.3 Regole di comportamento e Protocolli operativi in tema di reati contro la P.A.

Nell’espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
- ✓ porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
- ✓ comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
- ✓ violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
- ✓ tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
- ✓ qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;

- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli e responsabilità	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla P.A. (ad es., nel caso di richiesta di elaborazione di dichiarazioni tecnico-commerciali al fine di partecipare a gare di appalto, deve essere ben chiara la segregazione delle funzioni tra (a) chi formula la richiesta specificandone le finalità (b) chi redige le dichiarazioni tecnico-commerciali (c) chi raccoglie e predispone la documentazione necessaria e (d) chi approva e sottoscrive la dichiarazione). • Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: • porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; • presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; • presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: • sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; • ogni eventuale accordo preso con la P.A. sia documentato.
Ispezioni	• Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; • di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; • devono essere osservate specifiche procedure che disciplinino le modalità di

	partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: • la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; • specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.

2.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

2.5 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;

- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta Cianfanelli Simona, nominata anche Amministratore di Sistema (c.d. ADS), la quale ha supportato la Società nell'implementazione un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito HS, nel rispetto del principio di responsabilizzazione (c.d. *accountability*), ha adottato procedure e misure di sicurezza idonee ad assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica

In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato:

- introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili;
- acquisire, possedere o utilizzare strumenti *software e/o hardware* che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le *password*, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);
- ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società;
- divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti;
- distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;
- effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (*vulnerability test*, *penetration test*) e previsto nei propri compiti lavorativi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;
- comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

	Inoltre: • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato nel rispetto del Codice Etico aziendale, nonché di quanto previsto dalle procedure interne in materia di trattamento dei dati personali (così come previsto dal Regolamento UE 2016/679 c.d. GDPR); • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software</i>, ecc.); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che
--	---

	soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	---

2.6 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

2.7 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative

di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti		
Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti		La regolamentazione dell'attività descritta deve prevedere che: • i Destinatari si accertino che i dipartimenti di <i>patent e trademark</i> internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto; • in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di <i>patent e trademark</i> internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto. • I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti. Inoltre, è fatto espressamente divieto di: • contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati; • contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati; • introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati; • detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto;

	• consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	---

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero
---	---

	ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; • importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	--

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE

Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
------------------------------	--

2.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- d. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- e. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

2.9 Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001).

Nell'ambito della riforma del diritto societario, il Decreto Legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter del Decreto, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. "reati societari".

I reati societari sono reati propri e, in quanto tali, possono essere commessi direttamente da:

- Consiglio di Amministrazione;
- Amministratori;
- Direttori Generali;
- Sindaci;

- Liquidatori;
- Sottoposti alla direzione e alla vigilanza dei soggetti sopra elencati nel caso di corruzione tra privati;
- nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

Le fattispecie di reati societari considerate sono:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- falso in prospetto (art. 173-bis, T.U.F.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3 c.c.) [modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019];
- istigazione alla corruzione tra privati (art. 2635-bis c.c.) [introdotto dal D.Lgs. n. 38/2017];
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-ter del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

- a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società. A questo proposito, è fatto espresso divieto di:
 - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Società;
 - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
- c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività aziendale, fino alle fasi eventuali di liquidazione o cessazione della Società;
- e. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
 - d. omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
 - e. esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
 - f. porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);

- g. predisporre procedure per la preparazione del bilancio e la gestione delle risorse finanziarie; inoltre,
- h. il presente Modello deve essere portato adeguatamente a conoscenza di tutto il personale, non solo dirigente, e appositi meccanismi di comunicazione (ad esempio tramite poster nelle sale comuni o pubblicazioni periodiche) devono essere predisposti in modo da permettere la conoscenza di modifiche e/o aggiornamenti del Modello stesso e deve essere attivato un programma di informazione/formazione a favore del personale addetto atto a prevenire la commissione di reati societari;
- i. tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o di conflitto di interesse, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili, le attività finalizzate alla formazione del bilancio e le altre comunicazioni sociali siano accurati e trasparenti.

Protocollo 1 – Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale	
Identificazione dei soggetti responsabili	Nella gestione dei rapporti con il collegio sindacale, società di revisione e soci devono essere osservate le seguenti disposizioni: • identificazione del personale all'interno di HS preposto ad interloquire con il collegio sindacale e alla trasmissione della relativa documentazione; • possibilità per il Collegio Sindacale e della società di revisione di prendere contatto con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possono presentare aspetti di criticità in relazione ai reati societari.

2.10 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato *reporting* verso gli organi deputati, ecc.);
- b. monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;

- c. verificare annualmente i principali atti societari ed in particolare la relazione del Collegio Sindacale e della Società di Revisione nonché il rispetto delle procedure per la diffusione delle comunicazioni rivolte ai Soci, dei comunicati stampa e delle notizie scritte rivolte all'esterno aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società al fine di verificare l'osservanza della presente Parte Speciale nonché la sua idoneità a prevenire i reati ivi elencati;
- d. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- e. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- f. curare l'aggiornamento del Modello, indicando al consiglio di amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

3. SEZIONE C - SETTORE AMMINISTRATIVO, FINANZIARIO E RISORSE UMANE.

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Amministrativo, Finanziario e Risorse Umane: relativamente a quest'area si distinguono le funzioni di Chief Financial Officer (CFO), Direzione Amministrativa (DAM), Direzione Finanziaria (DF) e Responsabile delle Risorse Umane (RU).

Dette funzioni, benché distinte, vengono svolte nella Società da un unico soggetto responsabile delle predette.

Le potenziali aree sensibili che HS ha individuato in relazione alle suddette funzioni e nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.); • Gestione delle gare e dei bandi pubblici; • Scelta di fornitori e consulenti; • Richiesta e ottenimento di finanziamenti pubblici; • Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi;

	• Spese di rappresentanza; • Assunzione del personale; • Accesso ai sistemi informatici della Pubblica Amministrazione; • Gestione dei contenziosi.
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Reati societari (art. 25-ter)	• Predisposizione del Bilancio e tenuta delle scritture contabili e dei Libri Sociali; • Creazione di fondi extracontabili; • Gestione degli ordini e delle fatture; • Gestione della liquidità; • Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale; • Scelta consulenti/fornitori/partner commerciali.
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme in materia di sicurezza sul lavoro (Art. 25-septies)	• Sistema di deleghe ex art. 16 D.Lgs. 81/2008; • Documento di Valutazione dei Rischi (DVR); • Gestione delle misure di sicurezza; • Gestione delle gare pubbliche; • Manutenzione delle infrastrutture e sicurezza delle zone di produzione e magazzino; • Formazione del personale.
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	• Scelta consulenti/fornitori/partner commerciali; • Gestione dei flussi finanziari/creazione di fondi extracontabili; • Gestione della liquidità e cassa.
Reati ambientali (art. 25-undecies del Decreto): • attività gestione rifiuti non autorizzata, • traffico illecito di rifiuti, • attività organizzate per il traffico illecito di rifiuti, • inquinamento del suolo, sottosuolo, delle acque superficiali e sotterranee, • violazione obblighi di comunicazione, • false indicazioni su natura e composizione dei rifiuti, • inquinamento ambientale art.	• Tutela del suolo, sottosuolo e delle acque (es. sversamenti da impianto di depurazione); • Gestione dei rifiuti (es. dismissione degli impianti, gestione dei rifiuti di apparecchiature meccaniche, elettriche ed elettroniche, ecc.).

452bis, disastro ambientale art. 452 ter, - traffico e abbandono di materiale radioattivo 452quinqies, - impedimento del controllo 452sexies - omessa bonifica 452terdecies)	
Reati tributari (art. 25-quinquiesdecies del Decreto)	- Gestione della contabilità - Acquisto di beni e servizi - Adempimenti fiscali e tributari in genere - Tenuta e custodia delle scritture contabili e fiscali - Gestione di eventuali operazioni straordinarie
Reati di contrabbando (art. 25-sexiesdecies)	- Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine; - Scarico e deposito delle merci oltre confine.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

3.1 I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- ✓ **malversazione a danno dello Stato**, (art. 316-bis c.p.): *"Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- ✓ **indebita percezione di erogazioni a danno dello Stato**, (art. 316-ter c.p.): *"(Comma 1) Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. La pena è*

della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.⁹ (Comma 2). Quando la somma indebitamente percepita è pari o inferiore a lire sette milioni settecentoquarantacinquemila si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da dieci a cinquanta milioni di lire. Tale sanzione non può comunque superare il triplo del beneficio conseguito" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Truffa** (art. 640, comma 2, n. 1 c.p.): "(Comma 1). Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinquecento a diecimila. 2. La pena è della reclusione da uno a cinque anni e della multa da lire tremila a quindicimila:
 - se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea¹⁰ o col pretesto di far esonerare taluno dal servizio militare;
 - se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;
 - 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).
- ✓ (Comma 3). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), "La pena è della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **Frode informatica** (art. 640-ter c.p.): "(Comma 1). Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro.

⁹ Aggiornamento del D.Lgs. 74/2020.

¹⁰ Aggiornamento del D.Lgs. 74/2020.

(Comma 2). La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. (Comma 3). La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **Frode nelle pubbliche forniture** (art. 356 c.p.)¹¹: “Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore ad euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **Frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale** (art. 2 L. 898/1986): “ (Comma 1). 1. Ove il fatto non configuri il più grave reato previsto dall'articolo 640-bis del codice penale, chiunque, mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il danno o il profitto sono superiori a euro 100.000. Quando la somma indebitamente percepita è pari od inferiore a 5.000 euro si applica soltanto la sanzione amministrativa di cui agli articoli seguenti. (Comma 2). Agli effetti della disposizione del precedente comma 1 e di quella del comma 1 dell'articolo 3, alle erogazioni a carico del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale sono assimilate le quote nazionali previste dalla normativa comunitaria a complemento delle somme a carico di detti Fondi, nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa comunitaria. (Comma 3). Con la sentenza il giudice determina altresì l'importo indebitamente percepito e condanna il colpevole alla restituzione di esso all'amministrazione che ha disposto la erogazione di cui al comma 1” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote.

¹¹ Fattispecie inserita dal D.Lgs. 75/2020.

L'art. 25¹² rubricato "Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", elenca le seguenti fattispecie criminose quali reati suscettibili di far scattare la responsabilità dell'Ente ex Decreto:

- ✓ **Peculato** (art. 314, co. 1, c.p.): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro [c.p. 458] o di altra cosa mobile altrui [c.c. 812, 814], se ne appropriava, è punito con la reclusione da quattro anni a dieci anni e sei mesi."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Peculato mediante profitto dell'errore altrui** (art. 316): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni. (Comma 2) La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000¹³"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Concussione** (art. 317 c.p.), *"Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;;
- ✓ **Corruzione per l'esercizio della funzione** (art. 318 c.p.), *"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da tre a otto anni"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), *"Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **Circostanze aggravanti** (art. 319 bis c.p.), *"La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene"*

¹² AGGIORNAMENTO: Il D.lgs. n. 75/2020 modifica l'art. 25 D.Lgs. 231/2001, ampliando il catalogo dei reati con le fattispecie di peculato ex artt. 314 e 316 c.p. e di abuso d'ufficio ex art. 323 c.p.

¹³ Comma aggiunto dall'art. 1, comma 1, lett. a), D.Lgs. n. 75/2020.

nonché il pagamento o il rimborso di tributi " - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;

- ✓ **Corruzione in atti giudiziari** (art. 319-ter c.p.): "*(Comma 1) Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni. (Comma 2) Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni*" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote per il comma 1 e fino 800 quote per il comma 2;
- ✓ **Induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), "*(Comma 1) Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. (Comma 2) Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000*" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;
- ✓ **Corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), "*(Comma 1) Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. (Comma 2) In ogni caso, le pene sono ridotte in misura non superiore a un terzo*" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote nel caso di commissione art. 318 c.p. e fino a 600 quote in caso di commissione art. 319 c.p.;
- ✓ **Pene per il corruttore** (art. 321 c.p.), "*Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità*" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;
- ✓ **Istigazione alla corruzione** (art. 322 commi 1 e 3 c.p.): "*(Comma 1) Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo [...]. (Comma 3) La pena di cui al primo comma si applica al pubblico ufficiale o*

all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;

- ✓ **Istigazione alla corruzione** (art. 322 commi 2 e 4 c.p.): *"(Comma 2) Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo [...]. (Comma 4) La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*

- ✓ **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): *"Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;

5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;

5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;

5-quinquies) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione¹⁴.

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

- 1) alle persone indicate nel primo comma del presente articolo;*
- 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.*

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi" - Sono previste in capo all'Ente le medesime sanzioni pecuniarie previste per gli artt. 314, 316, da 317 a 320 e 322 terzo e quarto comma c.p.

- ✓ **Traffico di influenze illecite** (art. 346 bis c.p.): tale ipotesi delittuosa punisce chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio. Tale fattispecie può concretizzarsi in attività che pongono in relazione due soggetti privati, (uno dei quali funge da intermediario "illecito" verso un pubblico ufficiale o incaricato di pubblico servizio in cambio di un interesse o vantaggio) - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.
- ✓ **Abuso d'ufficio** (art. 323 c.p.), *"Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni¹⁵. La pena è*

¹⁴ Numero aggiunto dall'art. 1, comma 1, lett. d), D.Lgs. 14 luglio 2020, n. 75, a decorrere dal 30 luglio 2020.

¹⁵ Comma così modificato, a decorrere dal 17 luglio 2020, dall'art. 23, comma 1, D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità” - È prevista nei confronti dell’Ente una sanzione pecuniaria fino a 200 quote.

3.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio.

- **Pubblica Amministrazione** (di seguito “PA”) s’intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell’interesse della collettività, e quindi nell’interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l’Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d’Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAL, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

- **Pubblici ufficiali e incaricati di un pubblico servizio** Ai sensi dell'art. 357, primo comma, del codice penale, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

La norma chiarisce solo la nozione di "pubblica funzione amministrativa" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l'art. 358 c.p. definisce i "soggetti incaricati di un pubblico servizio" come quei soggetti "i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della "pubblica funzione", da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d'ordine e/o la prestazione d'opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

3.3 Regole di comportamento e Protocolli operativi in tema di reati contro la P.A.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
2. porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
3. comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
4. violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

5. il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
6. tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
7. i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
8. tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
9. qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
10. su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli e responsabilità	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla P.A. (ad es., nel caso di pagamenti effettuati e/o ricevuti, deve essere ben chiara la segregazione delle funzioni tra (a) chi riceve i pagamenti (b) chi effettua il controllo sui pagamenti [ad es. verifica della corrispondenza tra il soggetto che deve ricevere il pagamento e quello che ha effettuato la prestazione] (c) chi raccoglie e dispone la documentazione necessaria per la fatturazione e (d) chi approva e sottoscrive l'autorizzazione di pagamento). • Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: • proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; • porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; • distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; • presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; • presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: • sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; • ogni eventuale accordo preso con la P.A. sia documentato.
Ispezioni	• Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; • di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con

	nota scritta da parte del responsabile della funzione coinvolta; devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: - la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; - specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.

Protocollo 2 – Scelta di fornitori e consulenti	
Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	- I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. - I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. - Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. - Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici	
Transazioni finanziarie	Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione

	nelle prescritte voci di bilancio. • In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; • Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto previsto dall'art. 3 della legge n. 136/12010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che dovrà essere necessariamente corredata da idonea documentazione giustificativa.
Irregolarità anomalie	o Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di

Protocollo 4 – Assunzione del personale	
Assunzione, gestione, formazione incentivazione dei dipendenti e collaboratori	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato. Il personale che si occupa di transazioni con funzionari pubblici nazionali o stranieri ha l'obbligo di eseguire una certificazione periodica di non aver violato la Parte Speciale del presente Modello.

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali	
Contenziosi/ Contestazioni	• Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni

	responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.
--	---

Protocollo 6 Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi Spese di rappresentanza	
Omaggi/Donazioni	Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico. A tal fine si prevede la creazione di una procedura sulle liberalità che: - indichi i soggetti che possono da un lato autorizzarle e dall'altro riceverle; - definisca il valore massimo per ogni omaggio ed i casi in cui le liberalità possono essere eseguite; È, inoltre, fatto obbligo che qualora gli omaggi vengano elargiti a soggetti appartenenti la P.A., questo sia comunicato immediatamente al C.d.A. In ogni caso, nessun omaggio e/o donazione potrà essere effettuato se non quelli espressamente approvati dal C.d.A.

3.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

3.5 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, in ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta DESIDERIO TAGLIENTI, la quale stanno implementando un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito la Società implementando le proprie procedure interne in materia di protezione dei dati personali, attraverso l'adozione un software che permette:

- l'identificazione univoca degli utenti, attraverso un ID, un Identity Provider utilizzabile per eseguire l'accesso e l'autenticazione a norma a tutti gli applicativi e servizi in cloud;
- la crittazione dei dati sensibili, (ad es. dichiarazioni di appartenenza ad organizzazioni sindacali, dati relativi allo stato di salute, ecc.), attraverso cifratura delle informazioni per rendere i dati inaccessibili al di fuori dell'applicazione software, tenendo conto anche del contesto e delle finalità del trattamento, nonché del rischio per i diritti degli interessati;
- il log delle attività per l'archiviazione e la consultazione dei log delle attività previsti dalla nuova normativa.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica	In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test</i>, <i>penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati; Inoltre: • l'utilizzo del servizio aziendale di posta elettronica che deve essere
--	--

	effettuato nel rispetto del Codice Etico aziendale, impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software</i>, ecc.); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante <i>username e password</i> al quale corrisponda un profilo limitato della gestione
--	--

	di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	--

3.6 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

3.7 Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001).

Nell'ambito della riforma del diritto societario, il Decreto Legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter del Decreto, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. "reati societari".

I reati societari sono reati propri e, in quanto tali, possono essere commessi direttamente da:

- Consiglio di Amministrazione;
- Amministratori;
- Direttori Generali;
- Sindaci;
- Liquidatori;
- Sottoposti alla direzione e alla vigilanza dei soggetti sopra elencati nel caso di corruzione tra privati;
- nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

Le fattispecie di reati societari considerate sono:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- falso in prospecto (art. 173-bis, T.U.F.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3 c.c.) [modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019];
- istigazione alla corruzione tra privati (art. 2635-bis c.c.) [introdotto dal D.Lgs. n. 38/2017];
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-ter del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

- a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società. A questo proposito, è fatto espresso divieto di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Società;
 - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
- c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività aziendale, fino alle fasi eventuali di liquidazione o cessazione della Società;
- e. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
- g. omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
 - h. esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
 - i. porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- g. predisporre procedure per la preparazione del bilancio e la gestione delle risorse finanziarie; inoltre,
- h. il presente Modello deve essere portato adeguatamente a conoscenza di tutto il personale, non solo dirigente, e appositi meccanismi di comunicazione (ad esempio tramite poster nelle sale comuni o pubblicazioni periodiche) devono essere predisposti in modo da permettere la conoscenza di modifiche e/o aggiornamenti del Modello stesso e deve essere attivato un

programma di informazione/formazione a favore del personale addetto atto a prevenire la commissione di reati societari;

- i. tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o di conflitto di interesse, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili, le attività finalizzate alla formazione del bilancio e le altre comunicazioni sociali siano accurati e trasparenti.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente contabile esterno non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1	
• Predisposizione del bilancio; • Tenuta delle scritture contabili e dei Libri Sociali; • Gestione degli ordini e delle fatture.	
Definizione dei ruoli e responsabilità	Devono essere osservate specifiche procedure che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione della contabilità, predisposizione dei bilanci, dei rendiconti, prevedendo controlli in ordine alla completezza e veridicità delle informazioni contenute nei singoli documenti finali; • individuino la funzione e il soggetto deputato a gestire per conto di HS la contabilità ed il processo di formazione dei documenti contabili, cui conferire apposita delega e procura scritta. Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere

	adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione Operativa	In aggiunta ai presidi aziendali già esistenti, si dispone: - la trasmissione agli amministratori e al collegio sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del consiglio di amministrazione o sui quali esso debba esprimere un parere ai sensi di legge; - la previsione di riunioni periodiche tra il collegio sindacale e l'Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di <i>Corporate Governance</i>. Inoltre, per la predisposizione delle comunicazioni ai Soci relative alla situazione economica, patrimoniale e finanziaria della Società, si dispone che la redazione delle stesse sia effettuata determinando in maniera chiara e completa: - i dati e le informazioni che ciascuna funzione deve fornire; - i criteri contabili per l'elaborazione dei dati; - la tempistica per la loro consegna alle aree aziendali responsabili. Infine, in caso di comunicati stampa e ogniqualvolta vengano diffuse all'esterno notizie aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società, si dispone che chi diffonde tali informazioni, oltre ad osservare i principi suindicati, deve attenersi esclusivamente alle informazioni desumibili da documenti già approvati e resi pubblici.

Protocollo 2 Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni); Creazione di fondi extracontabili.	
Gestione operativa	- Le modalità di gestione delle operazioni societarie devono essere condotte in maniera veritiera e corretta, coerentemente e nel rispetto dei principi di <i>Corporate Governance</i> adottati dal Consiglio di Amministrazione. - Deve esistere una segregazione di ruoli e responsabilità tra chi evidenzia la necessità di un'operazione, chi la esegue e chi effettua il relativo controllo. - Per ogni documentazione predisposta deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi. - Tutta la documentazione deve contenere elementi assolutamente veritieri e devono essere coerenti all'oggetto per cui sono stati richiesti. A tal fine tutta la documentazione relativa alle operazioni societarie deve essere archiviata in un apposito fascicolo con sottoscrizione del responsabile della funzione. - E' inoltre necessario che sia previsto quanto segue: - un programma di formazione – informazione del personale impiegato nella predisposizione della documentazione attinente le operazioni societarie; - un monitoraggio dei poteri anche con riferimento alla verifica delle firme dei documenti inerenti le operazioni societarie; - la documentazione redatta ed in genere ogni altra informazione formalizzata deve contenere solo elementi assolutamente veritieri.

Protocollo 3 – Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale	
Identificazione dei	Nella gestione dei rapporti con il collegio sindacale, società di revisione e soci devono

soggetti responsabili	essere osservate le seguenti disposizioni: • identificazione del personale all'interno di HS preposto ad interloquire con il collegio sindacale e alla trasmissione della relativa documentazione; • possibilità per il Collegio Sindacale e della società di revisione di prendere contatto con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possono presentare aspetti di criticità in relazione ai reati societari.
------------------------------	---

Protocollo 4 • Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti; • Gestione della liquidità.	
Gestione del processo di acquisizione di nuova clientela e di gestione della clientela acquisita	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con clienti o altre controparti contrattuali; • garantire una segregazione di funzioni e responsabilità e una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione delle vendite, in particolare tra responsabilità nei rapporti con il cliente (cd. <i>account manager</i>), responsabilità nella definizione del prezzo di offerta e delle condizioni/tempi di pagamento (e relative penali), responsabilità nella definizione di eventuali risoluzioni transattive in caso di controversie; • individuare criteri generali e trasparenti per la determinazione di un prezzo massimo di offerta per singolo prodotto o servizio, di modo che qualunque anomalia possa essere agevolmente rilevata. In caso di qualsivoglia criticità sorta nell'ambito dei rapporti sopra descritti, deve essere informato l'Organismo di Vigilanza con nota scritta. In particolare, vi è l'obbligo di comunicare: • le operazioni di vendita superiori ad un dato importo che potrà rappresentare la soglia di rischio; • le operazioni di vendita superiori di una data percentuale rispetto al prezzo medio del prodotto, come risultante dai criteri generali suddetti; • tutte le operazioni di incasso al di sotto dei termini standard di pagamento (ad esempio, fatture pagate a vista).
Assegnazione/gestione degli incarichi e delle consulenze esterne	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con fornitori o altre controparti contrattuali; • garantire una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione degli acquisti, in particolare tra funzione che individua e seleziona il fornitore, il consulente o il prestatore di servizi, funzione che ratifica la c.d. entrata merci, funzione che autorizza il pagamento e funzione che effettua il controllo di gestione e la tracciabilità delle operazioni; • effettuare una pianificazione dell'attività di <i>benchmarking</i> (raffronto con i valori economici di mercato); • predisporre adeguati protocolli aziendali per acquisti di beni e servizi, affidamento di consulenza ed altre prestazioni professionali e gestione del magazzino.

Selezione e gestione del personale	La regolamentazione dell'attività descritta deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • il monitoraggio di ogni eventuale conflitto di interessi da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato.
Gestione del marketing ed eventuale omaggistica clienti comprese le organizzazioni no profit	Con riguardo alla formazione del personale dipendente e amministrativo, sono prescritte le seguenti e ulteriori regole di comportamento: • divieto di offrire, sollecitare, istigare o ricevere da terzi, direttamente o indirettamente, o di accettare la promessa di ricevere omaggi, benefici o altre utilità, a meno che questi omaggi, benefici e utilità abbiano "modico valore" e rientrino nei limiti della normale cortesia e non abbiano lo scopo di influenzare decisioni aziendali o creare obblighi nei confronti di terzi o di compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. In particolare: – le spese di rappresentanza devono essere limitate a pranzi o cene di lavoro; – i c.d. omaggi a clienti sono da limitare alla gadgettistica o ad oggetti di puro valore simbolico, meglio ancora se riportanti il marchio dell'azienda per collegarli a finalità pur sempre commerciali, con la previsione di un listino; • proibire liberalità che non siano inquadrare in programmi generali di <i>social responsibility</i>, come sponsorizzazioni sportive di club, associazioni, ecc. riconducibili ad un ente/cliente o a suoi singoli manager; • prevedere una chiara casistica ed un flusso di comunicazioni verso l'Organismo di Vigilanza affinché si possa vigilare su eventuali abusi, attraverso l'analisi incrociata con altri dati, ad esempio quelli relativi alle commesse acquisite; • prevedere che chiunque riceva tali richieste o offerte, eccezione fatta per omaggi di modico valore, debba informarne "il responsabile della funzione aziendale competente"; • prevedere, nell'informativa comunicata ai clienti/fornitori, che ogni violazione dei principi contenuti nel Codice Etico rappresenta una violazione contrattuale; • prevedere l'obbligo per i clienti/fornitori di conformarsi al Codice Etico prima di poter avere rapporti commerciali con la società.
Partecipazione a gare indette da soggetti privati e gestione dei rapporti con il cliente in caso di vittoria di una gara	È necessario che sia previsto quanto segue: • una corretta applicazione della procedura di partecipazione ai bandi privati sia con riferimento alla fase di ricezione (fonte interna e/o fonte esterna) dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui su è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, che alla predisposizione e spedizione della documentazione all'Ente (o alla capofila) che indica il relativo bando; • una verifica dell'esistenza di eventuali conflitti di interessi con riferimento anche alla possibilità di partecipare o meno al bando.

	Inoltre, devono essere previste regole di comportamento che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione delle varie fasi dei rapporti con partner/terze parti ed altri soggetti privati in genere, prevedendo controlli in ordine alla regolarità dei requisiti di ammissione degli stessi ad eventuali bandi di gara privati o all'ottenimento di contributi, sovvenzioni e finanziamenti privati; • individuino la funzione e la persona fisica deputata a rappresentare l'azienda nei confronti dei terzi privati, cui conferire apposita delega e procura e stabiliscano forme di riporto periodico dell'attività svolta verso il responsabile della funzione competente a gestire tali rapporti; Infine, il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
--	---

3.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato *reporting* verso gli organi deputati, ecc.);
- b. monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;
- c. verificare annualmente i principali atti societari ed in particolare la relazione del Collegio Sindacale e della Società di Revisione nonché il rispetto delle procedure per la diffusione delle comunicazioni rivolte ai Soci, dei comunicati stampa e delle notizie scritte rivolte all'esterno aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società al fine di verificare l'osservanza della presente Parte Speciale nonché la sua idoneità a prevenire i reati ivi elencati;
- d. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- e. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;

- f. curare l'aggiornamento del Modello, indicando al consiglio di amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

3.9 Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies, D.Lgs. 231/2001).

I reati in materia di salute e sicurezza sul lavoro che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-septies del d.lgs. 231/2001 sono i seguenti:

- Omicidio Colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590, comma III, c.p.).

Le Linee Guida di Confindustria nell'ambito dei reati trattati nella presente Parte Speciale evidenziano l'impossibilità di escludere a priori alcun ambito di attività della società, in quanto i reati in esame potrebbero riguardare tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Ne consegue che le potenziali aree a rischio reato che HS ha individuato nell'ambito di tali reati riguardano tutte le attività svolte nei siti della Società.

In particolare, la Società ha la sede legale in Roma (RM) – Via Zosimo 13, e unità operative e locali in:

- Aprilia (Latina), Via Angela Vacchi 23/25, CAP 04011 – Stabilimento di produzione.

Inoltre, sono considerate aree a rischio anche tutte le attività svolte dal personale di HS che opera esternamente in qualità di *supporters* tecnici all'interno di strutture e aziende sanitarie, (nello specifico in sale operatorie). Particolare attenzione deve essere dedicata a quelle attività realizzate in associazione con partner commerciali (in caso di joint venture, anche in forma di ATI, consorzi, ecc.) o tramite la stipula di contratti di somministrazione, appalto o con società di consulenza o liberi professionisti.

Anche ai fini della redazione della presente Parte Speciale si devono pertanto considerare i fattori riportati nel Documento di Valutazione dei Rischi (di seguito anche DVR) tenuto conto che lo stesso non esaurisce le procedure di seguito previste, finalizzate a costituire il complessivo sistema di gestione della sicurezza sul lavoro e dare attuazione al disposto dell'art. 30 d.lgs. 81/08 secondo i principi espressi dalle Linee Guida UNI – INAIL.

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso in una delle aree sensibili indicate al precedente paragrafo 1, si ritiene particolarmente importante:

- a) determinare le politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;
- b) identificare e applicare in modo corretto le prescrizioni delle leggi e dei regolamenti applicabili in tema di salute e sicurezza sul lavoro;
- c) identificare e valutare i rischi per tutte le categorie di lavoratori, con particolare riferimento alla redazione:
 - del DVR;
 - dei contratti di appalto;
 - della valutazione dei rischi derivanti dalle interferenze;
 - nel caso in cui la Società fosse costruttrice, dei Piani di Sicurezza e Coordinamento, Fascicolo dell'Opera e Piani Operativi di Sicurezza;
- d) fissare gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elaborare dei programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività del Servizio Prevenzione e Protezione e del Medico Competente;
 - attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori;
- e) sensibilizzare la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti esposti a rischi specifici (es. addetti alla Camera Bianca);
- f) attuare adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;

- gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
 - coerenza tra attività svolta e competenze possedute;
- g) attuare le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- h) effettuare un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione per la sicurezza del lavoro e la tutela della salute nel raggiungere gli obiettivi prefissati, nonché l'adequatezza di questi ultimi rispetto sia alla specifica realtà della Società che ad eventuali cambiamenti nell'attività.

3.10 Struttura organizzativa di HS Hospital Service S.p.A.

In materia di salute e sicurezza sul lavoro la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente di cui al d.lgs. 81/2008 e successive modifiche (di seguito anche "Decreto Sicurezza"), al fine di eliminare o, per lo meno di limitare, i rischi per i lavoratori.

Nell'ambito di tale struttura organizzativa operano:

A) Il Datore di Lavoro. È il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

B) Il Servizio di Prevenzione e Protezione (SPP). Insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori. La Società ha proceduto alla nomina di un Responsabile del Servizio di Prevenzione e Protezione (RSPP), in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 d.lgs. 81/08 e designata dal Datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi (art. 2 d.lgs. 81/2008).

C) Responsabile dei Lavori. La persona che può essere incaricata dal Committente/Datore di Lavoro Committente per svolgere i compiti ad essa attribuiti dal d.lgs. 81/2008.

D) Addetti al primo soccorso. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili del soccorso in azienda, in caso di infortuni.

E) Addetti antincendio. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili dell'attuazione delle misure antincendio e di evacuazione, in caso di emergenza.

F) Il Medico Competente. Medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 d.lgs. 81/08 che collabora, secondo quanto previsto all'articolo

29, comma 1, con il Datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al Decreto Sicurezza (art. 2 d.lgs. 81/08).

G) Il Rappresentante dei Lavoratori per la Sicurezza (RLS). Persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro (art. 2 comma 1, lett. i d.lgs. 81/2008).

H) Lavoratore. Persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione della Società, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite. I lavoratori di aziende che svolgono per HS attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

I) Gestione degli appalti e dei fornitori. Nei contratti di appalto intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione, il Datore di Lavoro in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno della propria azienda o Unità produttiva, in conformità alle procedure aziendali, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

- verificare, con il supporto delle Unità interessate, l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;
- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i

rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture. L'obbligo di redazione del suddetto documento non sussiste in caso di appalto di servizi di natura intellettuale, mere forniture di materiali o attrezzature, nonché per i lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza delle sostanze di cui all'allegato XI del d.lgs. 81/2008.

3.11 Principi procedurali specifici

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei lavoratori così come individuati dall'art. 15 del Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del suddetto decreto si prevede quanto segue.

Protocollo 1 – Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	
Politiche aziendali in tema di sicurezza	La politica per la sicurezza e salute sul lavoro adottata da HS deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte da HS e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i Lavoratori. A tal fine, è predisposto un adeguato sistema di designazioni o deleghe di funzioni in materia di salute e sicurezza secondo i principi di: • effettività, sussistenza e compresenza di autonomia decisionale e finanziaria del delegato; • idoneità tecnico-professionale del delegato; • vigilanza sull'attività del delegato, non acquiescenza, non ingerenza; • certezza, specificità e consapevolezza. La designazione / delega di funzioni da parte del datore di lavoro deve: • risultare da atto scritto recante data certa; • essere diretta ad un soggetto che possieda tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate; • essere accettata dal delegato per iscritto. Il soggetto delegato deve essere consapevole delle funzioni ad esso delegate. La politica per la sicurezza e salute sul lavoro è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.

Processo pianificazione	di HS nell'ambito del processo di pianificazione degli obiettivi in tema di salute e sicurezza, con cadenza annuale: • definisce gli obiettivi finalizzati al mantenimento e/o miglioramento del sistema; • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	• La Società ha definito un sistema di comunicazioni interne che assicura che le informazioni relative alla sicurezza fluiscano "dall'alto verso il basso", ma anche "dal basso verso l'alto" ed orizzontalmente rispetto alle varie parti dell'organizzazione. Lo scambio di informazioni tra i differenti livelli e settori aziendali è attuato attraverso l'individuazione di referenti interni e di idonei strumenti di comunicazione. Gli strumenti di comunicazione interna possono variare in funzione del tipo di informazione che è necessario fornire avendo però sempre presente che il requisito indispensabile è che le informazioni siano fornite usando una forma ed un modo che le rendano comprensibili alle persone che le devono ricevere. • La Società è convinta che il processo di prevenzione e miglioramento della sicurezza debba vedere coinvolto tutto il personale aziendale. A tale fine ogni lavoratore è incoraggiato a segnalare al proprio responsabile di funzione o direttamente al RSPP eventuali anomalie o proposte di miglioramento. Tali segnalazioni sono raccolte dal RSPP che provvede ad effettuarne un'analisi ed è responsabile di mettere in atto le eventuali azioni conseguenti; la decisione presa in merito è registrata dal RSPP. Il RSPP organizza anche le riunioni periodiche sulla sicurezza prevista dalle norme vigenti e redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione. • È stata definita una procedura per regolamentare le attività di formazione, informazione e addestramento da erogare a: - personale dipendente; - lavoratori con contratto di somministrazione; - stagisti. La procedura definisce anche le modalità in caso di nuove assunzioni e cambi di mansione I contenuti della procedura specificano modalità e responsabilità in merito a: - l'individuazione delle necessità di formazione e addestramento; - la pianificazione e attuazione della formazione; - la registrazione delle attività formative; - la verifica della loro efficacia; - l'informazione e sensibilizzazione del personale sull'igiene e la sicurezza del lavoro. • In merito all'attività di documentazione, HS dovrà provvedere alla conservazione,

		sia su supporto cartaceo che informatico, dei seguenti documenti: - la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro; - il registro degli infortuni; - il Documento di Valutazione dei Rischi indicante la metodologia con la quale si è proceduto alla valutazione dei rischi e contenente il programma delle misure di mantenimento e di miglioramento; - nel caso in cui la Società sia appaltatrice di lavori di costruzione: la documentazione contratti; Piano di Sicurezza e Coordinamento; Fascicolo dell'Opera; verbali di coordinamento relativi alla verifica dell'applicazione da parte delle imprese esecutrici delle disposizioni contenute nel PSC; Piani Operativi di Sicurezza. • HS è altresì chiamata a garantire che: - il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente; - venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente; - venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica; - venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale; - venga conservata la documentazione inerente a regolamenti ed accordi aziendali; - vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori; - venga conservata ogni procedura adottata da HS per la gestione della salute e sicurezza sui luoghi di lavoro; - tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.
Attività monitoraggio	di	HS deve assicurare un costante ed efficace monitoraggio del sistema per la gestione della salute e della sicurezza sui luoghi di lavoro. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta HS, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. HS garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.

<i>Riesame del sistema</i>	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema adottato da HS per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame annuale da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.
<i>Gestione operativa degli appalti</i>	HS deve predisporre e tenere aggiornato un elenco delle aziende con le quali stipula eventuali contratti di appalto. Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti dai quali devono risultare espressi riferimenti agli adempimenti di cui all'art. 26 del Decreto Sicurezza. Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori e le organizzazioni sindacali dei lavoratori. Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

3.12 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-septies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di HS eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la tutela della salute e della sicurezza nei luoghi di lavoro, in coerenza con quanto stabilito nel presente Modello e all'art. 30 del Decreto Sicurezza;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati da HS tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il Delegato della Sicurezza Aziendale e il RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

HS garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti di HS (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; gli Addetti al Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso).

3.13 Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies).

I reati di cui all'art. 25-octies del d.lgs. 231/2001 sono i seguenti:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
- Autoriciclaggio (art. 648-ter 1 c.p.)

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di:

- a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-octies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente diventarlo;
- b) intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo, persone legate all'ambiente del riciclaggio, del terrorismo, al traffico di droga, all'usura, ecc.;
- c) utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti;

- d) accettare rapporti contrattuali con clienti o altre controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI;
- e) effettuare elargizioni in denaro ad individui, società od organizzazioni condannate per aver svolto attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico;
- f) avere contatti con individui inseriti nelle *black list* antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea.

Inoltre è previsto, a carico dei Destinatari, l'espresso obbligo di:

- g) richiedere tutte le informazioni necessarie al fine di valutare l'affidabilità, la solidità economica e l'attendibilità commerciale/ professionale dei fornitori e del partner;
- h) assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- i) tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti;
- j) prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri.

Protocollo 1 - Scelta consulenti, fornitori, partner commerciali

Selezione dei partner e dei fornitori

Si riportano di seguito specifiche regole di comportamento da tenere in osservanza del Decreto:

- la Società procede alla selezione dei Partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri oggettivi e documentabili, verificandone l'attendibilità commerciale attraverso:
 - verifica ex ante, conservando evidenza dei dati raccolti, che i soggetti con cui intrattiene rapporti contrattuali, anche lavorativi, abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI e non siano inseriti nelle *black list* antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea.
 - visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni estere;
 - referenze da parte di altri soggetti già in rapporti con la Società o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione;
 - ove possibile, certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere;
- la Società inserisce nei contratti con i Partner commerciali una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali di HS e dei principi contenuti nel Modello e si impegnano al rispetto degli stessi; il mancato rispetto dei comportamenti etici o false dichiarazioni relative alla situazione del Partner comporteranno l'applicazione di una penale o, a seconda della gravità, la risoluzione

	del contratto; - la Società verifica l'attendibilità commerciale e professionale dei Fornitori, perlomeno di una certa rilevanza (da concordare un limite di importo di fornitura superato il quale procedere alle verifiche) attraverso: - visure ordinarie presso la Camera di Commercio o certificati equivalenti per Fornitori stranieri; - certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti per fornitori stranieri; - analisi del Fornitore per verificarne la coerenza con le prestazioni richieste dalla Società. Inoltre, è previsto, a carico dei Destinatari, l'espresso obbligo di tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 2 – Gestione dei flussi finanziari/creazione di fondi extracontabili e gestione della liquidità e cassa	
Gestione di investimenti	Si prevede l'espresso divieto di: - utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti; - effettuare elargizioni in denaro, in particolare ad individui, società od organizzazioni condannate per aver svolto attività illecite. Inoltre, è previsto l'obbligo di assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
Monitoraggio flussi finanziari	La Società effettua un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie. Inoltre, si prevede che: - nel caso di elargizioni di danaro ad individui, società o organizzazioni è necessario controllare la serietà e la professionalità del destinatario del denaro. Inoltre deve essere redatto un piano d'investimento a giustificazione dell'investimento, comprensivo di controlli periodici dell'avanzamento del piano; - in caso di <i>Joint Venture</i>, la Società proceda alla verifica della congruità economica dell'investimento, avendo riguardo, nello specifico, al rispetto dei prezzi medi di mercato, all'utilizzo di professionisti di fiducia per l'effettuazione della <i>due diligence</i>; - la Società presti particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti/partner/fornitori esteri. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.

Protocollo 3 – Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio

Gestione organizzativa ed operativa	L'eventuale coinvolgimento di consulenti, intermediari, agenti, promotori finanziari e <i>broker</i> a supporto della prestazione dei servizi della Società presuppone un'adeguata conoscenza degli stessi e la verifica, anche mediante attestazione degli interessati, della sussistenza dei requisiti di onorabilità previsti dalla legge e dell'assenza di situazioni di conflitto di interesse in capo ad essi. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

Protocollo 4 – Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà

Gestione organizzativa ed operativa	La Società deve definire e rispettare i criteri che regolano la scelta delle associazioni/fondazioni in favore delle quali effettuare donazioni od erogazioni liberali di qualsiasi tipo, in modo che sia possibile accertare l'effettiva finalizzazione dell'iniziativa a scopi umanitari che non dissimolino attività di riciclaggio o terrorismo. In particolare: • donazioni e/o erogazioni liberali di qualsiasi tipo sono effettuate sulla base di una lista di associazioni/fondazioni accreditate quali potenziali beneficiarie. Le modalità d'inserimento, mantenimento ed eliminazione delle associazioni/ fondazioni da tale lista sono debitamente formalizzate; • donazioni ed erogazioni liberali di qualsiasi tipo sono operate solo ove adeguatamente autorizzate, formalizzate e rendicontate; • la Società non effettua donazioni né erogazioni liberali di qualsiasi tipo tramite versamenti in contanti o su conti correnti cifrati. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

3.14 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-octies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di reati di riciclaggio, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

3.15 Regole di comportamento e Protocolli operativi in materia di reati ambientali (art. 25-undecies del Decreto).

I reati ambientali che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-undecies del d.lgs. 231/2001 sono i seguenti:

- scarichi di acque reflue (art. 137, comma 2, 3, 5, 11, 13 d.lgs. 3 aprile 2006, n. 152);
- attività di gestione di rifiuti non autorizzata (art. 256 comma 1, 3, 5, 6, e artt. 208, 209, 210, 211, 212, 214, 215, 216 d.lgs. 3 aprile 2006, n. 152);
- bonifica dei siti (art. 257 comma 1 e 2, d.lgs. 3 aprile 2006, n. 152);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (articolo 258 del d.lgs. 3 aprile 2006, n. 152);
- traffico illecito di rifiuti (art. 259 d.lgs. 3 aprile 2006 n. 152);
- attività organizzate per il traffico illecito di rifiuti (art. 260 d.lgs. 3 aprile 2006 n. 152);
- sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis d.lgs. 3 aprile 2006 n. 152);
- violazione dei valori limite di emissione (art. 279 d.lgs. 3 aprile 2006 n. 152);
- cessazione e riduzione dell'impiego di sostanze ozono lesive (art. 3 l. 28 dicembre 1993 n. 549).
- inquinamento ambientale art. 452bis c.p.,
- disastro ambientale art. 452 ter c.p.,
- traffico e abbandono di materiale radioattivo 452quinquies c.p.,
- impedimento del controllo 452sexies c.p.,
- omessa bonifica 452terdecies c.p.

Le potenziali aree a rischio reato che la Società ha individuato con riferimento ai reati ambientali riguardano tutte le attività svolte nei propri siti e nelle sedi amministrative e societarie nelle quali si svolgono le attività aziendali da parte del personale dipendente. Sono inoltre considerate aree a rischio anche tutte le attività svolte dal personale esterno incidenti sui processi produttivi o comunque sul sistema di gestione ambiente e sicurezza (ad es., fornitori di beni o servizi in base a contratti d'appalto, d'opera o somministrazione).

Le attività sono considerate sensibili avuto riguardo al loro svolgimento sia da parte del personale aziendale, sia da parte di terzi che agiscano su incarico o per conto della Società, ovvero che intrattengono un rapporto contrattuale con la Società, con particolare riferimento al perimetro delle attività loro assegnate ed esercitate sotto la direzione o vigilanza della Società.

Sono da considerare attività sensibili ai fini del presente Modello quelle che possano produrre impatti ambientali significativi sulle matrici ambientali (acqua, aria, suolo, rifiuti, flora, fauna) o comunque tali da imporre misure per il loro contenimento.

In particolare, dovranno considerarsi attività aziendali significative per la tutela delle matrici ambientali le aree nelle quali possano verificarsi condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti ai sensi delle Direttive 2008/99 CE e 2009/123 CE, in quanto provochino o possano provocare il decesso o lesioni gravi alle persone o danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora. Più specificamente, sono considerate sensibili le attività con impatto ambientale diretto (attività industriali, attività produttive, attività dalle quali si originano rifiuti, reflui o emissioni) o indiretto (quali, a titolo esemplificativo, le attività manutentive). Rientrano in tale ambito anche le attività che si svolgono in luoghi ove siano adottate misure a tutela della salute e sicurezza dell'ambiente di lavoro oggetto della valutazione ex art 18, comma 1, lett. q) d.lgs. 81/2008 nonché le attività soggette a procedimenti amministrativi di abilitazione, iscrizione, autorizzazione, nonché a specifici divieti ai sensi del d.lgs. n. 152/2006.

In conformità ai principi generali del Codice Etico e della Politica Ambiente e Sicurezza è preminente e specifico interesse della Società quello di sviluppare i propri investimenti in modo compatibile con il rispetto dell'ambiente, riconosciuto quale bene primario da salvaguardare, perseguendo il miglior equilibrio tra la propria iniziativa economica e la tutela delle esigenze ambientali attraverso il contenimento dell'impatto delle proprie attività ed il rispetto della normativa ambientale.

La Società considera pertanto ogni condotta che direttamente o indirettamente possa generare un pregiudizio anche potenziale all'ambiente come contraria al proprio interesse e respinge ogni condotta elusiva delle procedure aziendali ed inosservante della normativa vigente, dichiarando espressamente che a tali eventuali condotte non corrisponde alcun vantaggio per la Società, bensì la compromissione di ideali e patrimonio aziendali.

In tale contesto, la presente Parte Speciale prevede l'espresso divieto per tutti i Destinatari (i) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *undecies* del Decreto) e (ii) di violare i principi illustrati nel presente Modello e porre in essere condotte difformi dalle procedure aziendali previste.

Conseguentemente, i soggetti sopra indicati hanno l'obbligo di rispettare scrupolosamente tutta la normativa vigente ed in particolare di tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure in tutte le attività aziendali adottate dalla Società, di astenersi dal porre in essere o dare causa a violazioni dei principi comportamentali, dei protocolli e delle procedure aziendali, di rispettare le misure organizzative e preventive dettate per lo svolgimento delle attività produttive ad impatto ambientale ed i relativi oneri informativi, partecipando diligentemente alle sessioni formative ed informative connesse con le mansioni a ciascuno affidate dalla Società.

In tale contesto, ed ai fini di cui sopra, la Società:

- a. determina le politiche ambientali volte a definire gli impegni generali assunti per garantire il rispetto dell'ambiente e l'osservanza delle pertinenti norme applicabili nonché la riduzione degli impatti ambientali connessi alle attività svolte dalla Società;
- b. identifica le norme applicabili in tema di protezione dell'ambiente ed opera in conformità alle stesse;
- c. identifica e valuta i fattori che si originano dall'attività produttiva e che possono modificare lo stato dell'ambiente, la loro significatività, nonché le componenti ambientali che sono influenzate da tali azioni;
- d. fissa gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elabora dei programmi per il raggiungimento di tali obiettivi con la definizione di priorità, tempi ed attribuzione delle relative responsabilità – con assegnazione delle necessarie risorse - in materia di protezione dell'ambiente, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività di tutti i soggetti su cui ricade la responsabilità dell'attuazione delle misure per la protezione dell'ambiente;
- e. sensibilizza la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti investiti di specifiche funzioni in materia di protezione dell'ambiente e per soggetti addetti a mansioni dalle quali possono derivare impatti ambientali;
- f. attua adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia delle procedure e dei sistemi di gestione ambientale adottati, in particolare per ciò che concerne:

- misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme;
 - coerenza tra attività svolta e competenze possedute;
- g. attua le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- h. effettua un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione ambientale nel raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alla specifica realtà della Società sia ad eventuali mutamenti nell'attività.

In particolare, in conformità ai principi di prevenzione e di precauzione, l'obiettivo del rispetto delle norme comportamentali e delle relative procedure interne prescritte per la tutela dell'ambiente sarà quello di prevenire condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora, ovvero che provochino o possano provocare il decesso o lesioni gravi alle persone.

In relazione alle aree a rischio individuate nella presente Parte Speciale, e a integrazione dei presidi e delle procedure aziendali già esistenti, si riportano di seguito specifici principi di comportamento da tenere in osservanza del Decreto.

Protocollo 1 – Rispetto della normativa sull'ambiente	
Politiche aziendali in tema di protezione dell'ambiente	La politica per la protezione dell'ambiente adottata dalla Società deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte dalla Società e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della riduzione degli impatti sull'ambiente. Tale politica contiene: • l'individuazione di un approccio strutturato alla riduzione dell'impatto ambientale e all'incremento della sicurezza che tenga conto di tutte le implicazioni di carattere organizzativo, tecnico, economico, normativo; • l'individuazione dello sviluppo sostenibile della Società e del territorio nel quale essa opera come missione primaria della Società; • l'impegno a ridurre i consumi energetici e di materie prime, privilegiando l'utilizzo di processi e materie prime a minore impatto ambientale; • l'impegno a commercializzare prodotti sempre più compatibili con l'ambiente e sicuri per gli utilizzatori; • l'identificazione e la valutazione degli effetti ambientali e dei rischi dovuti a incidenti, fatti accidentali potenziali, situazioni di emergenza; • l'impegno alla prevenzione ed al miglioramento continuo delle proprie capacità organizzative e tecniche in grado di ridurre l'impatto ambientale e i rischi legati all'attività della Società; • l'impegno a fornire le risorse umane e strumentali necessarie; • l'impegno ad un riesame periodico della politica per l'ambiente al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società, nonché alla normativa vigente in materia ed alle migliori prassi internazionali;

- l'adeguamento continuo alle crescenti esigenze sociali e legislative nel campo della tutela dell'ambiente e della sicurezza, precorrendole, ove possibile, mediante un'adeguata pianificazione delle attività e iniziative in tali campi;
- l'impegno a definire e diffondere all'interno della Società la conoscenza delle problematiche di tutela dell'ambiente, delle relative discipline tecnico-organizzative nonché gli obiettivi del sistema di gestione ambiente e sicurezza ed i relativi programmi di attuazione.

La politica è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.

Le procedure interne devono inoltre essere caratterizzate dai seguenti elementi:

- separatezza, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni");
- traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità");
- adeguato livello di formalizzazione.

La Società predispone ed adotta inoltre procedure finalizzate ad individuare le modalità e le funzioni responsabili della gestione dei rapporti con le competenti Autorità amministrative, nonché delle ispezioni e degli accertamenti in materia di tutela ambientale e dell'elevazione di contestazioni.

In particolare, dovrà essere:

- conferita procura speciale ai responsabili delle funzioni coinvolte in ispezioni e/o accertamenti al fine di dotarli del potere di rappresentare la Società dinanzi alla pubblica Autorità (in particolare, Ufficio delle Entrate, Guardia di Finanza, ARPA, ASL, NOE, CFS, MIPAF, NAS, nonché le altre Forze dell'Ordine delegate in materia ambientale) in caso di ispezione e/o accertamento;
- conferita apposita delega alla funzione deputata a rappresentare la Società nei confronti dell'Ente di Pubblica Amministrazione concedente un provvedimento amministrativo o nei confronti del quale sia diretta una comunicazione;
- prevista la redazione da parte dei procuratori sopra indicati di un report informativo dell'attività svolta nel corso dell'ispezione;
- prevista una metodologia di archiviazione della documentazione relativa all'attività in oggetto;
- prevista una modalità di comunicazione preventiva dell'avviso di ispezioni (anche periodiche, ad esempio in materia di A.I.A.) ai soggetti responsabili preposti per materia nonché il ruolo di questi ultimi nell'indirizzo, supervisione e controllo;
- individuata la modalità con la quale evadere le richieste di informazioni da parte delle Autorità di vigilanza, nonché il flusso informativo verso eventuali ulteriori funzioni o, in caso di necessità ed urgenza, le modalità con le quali informare l'Amministratore Delegato;
- prevista un'apposita forma di rendiconto periodico sulla gestione di tali fasi all'Organismo di Vigilanza.

Devono inoltre essere osservati i seguenti ulteriori principi procedurali specifici, da integrarsi con le procedure di sistema e istruzioni di processo, di controllo operativo ed emergenze previste dal sistema integrato di gestione ambiente e sicurezza adottato dalla Società:

- devono essere specificamente individuate e rigorosamente rispettate le procedure di monitoraggio dei processi produttivi e le procedure di emergenza previste per il caso di incidenti;
- devono essere individuate e rigorosamente osservate specifiche procedure di monitoraggio e controllo delle emissioni e degli scarichi;
- devono essere previste e rigorosamente rispettate le procedure operative di gestione dei rifiuti adottate dalla Società in conformità alle disposizioni di cui al d.lgs. n. 152/06 nonché le procedure amministrative di gestione dei rifiuti applicabili alle diverse tipologie di rifiuti prodotti

	dalla Società, con particolare riferimento agli adempimenti di comunicazione, tenuta dei registri obbligatori e dei formulari e/o agli adempimenti prescritti dal sistema informatico di controllo della tracciabilità dei rifiuti (ex SISTRI oggi "Registro elettronico nazionale per la tracciabilità dei rifiuti"); • devono essere definiti e rigorosamente osservati specifici protocolli relativi all'assunzione delle misure di prevenzione e messa in sicurezza di emergenza che si rendano eventualmente necessarie nell'ipotesi di eventi idonei a determinare situazioni di potenziale contaminazione di suolo, sottosuolo, acque superficiali o sotterranee e/o di potenziale impatto sulla flora e fauna; • non devono essere utilizzate o detenute le sostanze di cui alla tabella A allegata alla legge 28 dicembre 1993, n. 549. La Società: • svolge, a favore dei Destinatari, in modo differenziato ed adeguato ai rispettivi compiti e responsabilità, un'attività di formazione finalizzata alla conoscenza della normativa applicabile ai processi e delle procedure di gestione ambientale adottate dalla Società; • adotta i necessari presidi affinché i processi produttivi si svolgano in condizioni controllate; • predispone le procedure atte a definire, per i processi produttivi suscettibili di dar luogo a impatti sull'ambiente, le modalità di lavoro, i valori dei parametri operativi, i criteri di accettabilità, le registrazioni da produrre; • adotta procedure di emergenza volte a evitare o mitigare gli effetti di incidenti; • definisce le condizioni per tenere sotto controllo i parametri dei processi produttivi; • predispone ed attua programmi di formazione.
Processo di pianificazione	La Società, nell'ambito del processo di pianificazione degli obiettivi in tema di protezione dell'ambiente, con cadenza annuale: • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	<u>L'informazione</u> L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a: • l'importanza di rispettare la politica ambientale e gli obiettivi individuati dalla Società; • le conseguenze derivanti dallo svolgimento della propria attività in modo non conforme alla politica ambientale e agli obiettivi individuati dalla Società ; • il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità alla politica aziendale ed alle procedure in materia di protezione dell'ambiente e ad ogni altra prescrizione relativa al sistema di gestione ambientale adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale. Ciò premesso, la Società in considerazione dei diversi ruoli e responsabilità dei Destinatari, è tenuta ai seguenti oneri informativi: • la Società deve fornire adeguata informazione ai Destinatari circa i rischi di impatti negativi

sull'ambiente derivanti dall'attività dell'impresa, sulle conseguenze di questi e sulle procedure operative da adottare;

- la Società deve organizzare periodici incontri tra le funzioni preposte alla protezione dell'ambiente;
- la Società deve coinvolgere i responsabili di settore nell'organizzazione dell'attività di rilevazione e valutazione dei rischi e di prevenzione.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

Formazione

- La Società deve fornire adeguata formazione al personale addetto ad attività che possono avere un'incidenza sull'ambiente;
- i responsabili per la Sicurezza sul Lavoro devono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai contenuti della mansione cui il lavoratore è in concreto assegnato ed ai possibili impatti della relativa attività sull'ambiente;
- deve essere predisposto uno specifico piano di formazione per i lavoratori addetti ad attività da cui possano derivare impatti ambientali significativi;
- i lavoratori che cambiano mansione e quelli trasferiti a compiti da cui possano derivare impatti ambientali devono fruire di formazione preventiva, aggiuntiva e specifica;
- gli addetti a specifici compiti in materia di protezione dell'ambiente devono ricevere specifica formazione;
- la Società deve effettuare periodiche esercitazioni finalizzate all'adozione del corretto comportamento in caso di incidenti o di emergenze di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione ambientale, la Società deve garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Destinatari.

Pertanto, la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

- dal basso verso l'alto: è garantito dalla Società il diritto-dovere dei Destinatari di portare a conoscenza proposte ed esigenze di miglioria inerenti alla gestione ambientale;
- dall'alto verso il basso: ha lo scopo di diffondere a tutti i Destinatari la conoscenza del sistema adottato dalla Società per la gestione ambientale.

A tale scopo la Società garantisce agli esponenti aziendali (ovvero gli amministratori, i dirigenti, i componenti del Collegio Sindacale e i dipendenti della Società) un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- nuovi rischi in materia di protezione dell'ambiente;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione dell'ambiente;
- contenuti delle procedure aziendali adottate per la gestione dell'ambiente;
- ogni altro aspetto inerente alla gestione dell'ambiente.

Documentazione

La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, oltre ai

	documenti sopra indicati, anche dei seguenti documenti: • la documentazione inerente alle norme relative alla protezione dell'ambiente rilevanti per l'attività aziendale; • le autorizzazioni ambientali relative all'esercizio dell'attività della Società; • i registri relativi a taratura e manutenzione delle apparecchiature di sorveglianza; • la documentazione relativa all'attività di sorveglianza ed alle misurazioni; • i piani di emergenza; • le informazioni relative ai Fornitori; • il registro degli incidenti e delle azioni correttive attuate; • tutta la documentazione relativa alle attività di Informazione e Formazione che dovrà essere conservata a cura del responsabile per la Sicurezza sul Lavoro.
Attività di monitoraggio	La Società deve assicurare un costante ed efficace monitoraggio del sistema di gestione ambientale. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte nell'ambito del sistema di gestione ambiente e sicurezza; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione ambiente e sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni incidente verificatosi, al fine di individuare eventuali lacune nel sistema di gestione ambientale e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta la Società, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. La Società garantisce che gli eventuali interventi correttivi necessari vengano predisposti nel più breve tempo possibile.
Riesame del sistema	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema di gestione ambientale adottato dalla Società è sottoposto ad un riesame annuale da parte della Società, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.

3.16 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-undecies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti della Società eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla

protezione dell'ambiente, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la protezione dell'ambiente, in coerenza con quanto stabilito nel presente Modello e nel sistema di gestione ambiente e sicurezza adottato dalla Società;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla tutela dell'ambiente valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il responsabile per la Sicurezza sul Lavoro.
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

La Società garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli incidenti verificatisi, delle modifiche dei processi produttivi aventi un impatto sull'ambiente, nonché delle implementazioni dei sistemi di gestione ambiente e sicurezza.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti della Società.

3.17 Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25-quinquiesdecies del Decreto).

Il Decreto Legge n. 124 del 26 ottobre 2019, convertito con modificazioni nella Legge n. 157 del 19 dicembre 2019, ha introdotto i reati tributari nell'elenco dei reati presupposto della responsabilità amministrativa degli enti.

Con l'inserimento nel Decreto 231 dell'art. 25-quinquiesdecies viene prevista, dunque, una nuova responsabilità nei confronti dell'ente in caso di commissione, nel suo interesse o a suo vantaggio, di alcuni dei reati tributari contemplati nel D.Lgs. 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205".

Successivamente, il 30 luglio 2020, il D.Lgs. 75/2020 (in adempimento alla Direttiva UE/2017/1371 c.d. "PIF") ha esteso ulteriormente il catalogo dei reati tributari presupposto per la responsabilità dell'ente.

Sotto il profilo strettamente fiscale, la Direttiva PIF prevede come soglia minima di tutela la repressione di gravi frodi IVA, ossia di tutte quelle *"azioni od omissioni di carattere intenzionale secondo la definizione di cui all'art. 3, paragrafo 2, lettera d), [che] siano connesse al territorio di due o più Stati membri dell'Unione e comportino un danno complessivo pari ad almeno 10 mln di euro"*, ferma restando la facoltà per la legislazione nazionale di mantenere o adottare norme più rigorose.

Al fine di comprendere cosa possa essere considerato come *"frode che lede gli interessi finanziari dell'Unione"* la menzionata Direttiva, all'art. 3, paragrafo 2, lettera d), precisa che la suddetta frode è l'azione od omissione commessa in sistemi fraudolenti transfrontalieri in relazione:

- "i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti relativi all'IVA, cui consegua la diminuzione di risorse del bilancio dell'Unione;*
- ii) alla mancata comunicazione di un'informazione relativa all'IVA in violazione di un obbligo specifico, cui consegua lo stesso effetto;*
- iii) alla presentazione di dichiarazioni esatte relative all'IVA per dissimulare in maniera fraudolenta il mancato pagamento o la costituzione illecita di diritti a rimborsi dell'IVA".*

Si riporta di seguito il testo dell'art. 25-quinquiesdecies del D. Lgs. 231/2001.

Art. 25-quinquiesdecies

Reati tributari

* * *

"1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

- a. per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- b. per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- c. per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
- d. per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- e. per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- f. per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
- g. per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

- a. per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
- b. per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
- c. per il delitto di indebita compensazione previsto dall'articolo 10 quater, la sanzione pecuniaria fino a quattrocento quote.

d. Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) ”.

Ai fini della normativa tributaria di cui al Decreto Legislativo 10 marzo 2000, n. 74 rubricato “Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205”, si applicano le seguenti definizioni di carattere generale applicabili a tutti i reati tributari:

- per "fatture o altri documenti per operazioni inesistenti" si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, (i) emessi a fronte di operazioni non realmente effettuate in tutto o in parte o (ii) che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero (iii) che riferiscono l'operazione a soggetti diversi da quelli effettivi;
- per "elementi attivi o passivi" si intendono (i) le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e (ii) le componenti che incidono sulla determinazione dell'imposta dovuta;
- per "dichiarazioni" si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
- il "fine di evadere le imposte" e il "fine di consentire a terzi l'evasione" si intendono comprensivi, rispettivamente, anche (i) del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e (ii) del fine di consentirli a terzi;
- riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il "fine di evadere le imposte" ed il "fine di sottrarsi al pagamento" si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
- per "imposta evasa" si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non

effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

- le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
- per "operazioni simulate oggettivamente o soggettivamente" si intendono (i) le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero (ii) le operazioni riferite a soggetti fittiziamente interposti;
- per "mezzi fraudolenti" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

3.18 La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto).

Le nuove fattispecie di reati tributari introdotte nell'elenco dei reati suscettibili di rilevare secondo il Decreto 231, sono dunque le seguenti:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74).

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

- Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si configura allorché, fuori dai casi previsti dall'articolo 2 (di cui sopra), al fine di evadere le imposte sui redditi o sul valore aggiunto, il soggetto autore del reato - (i) compiendo operazioni simulate oggettivamente o soggettivamente ovvero (ii) avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria - indichi in una delle dichiarazioni relative a dette imposte (a) elementi attivi per un ammontare inferiore a quello effettivo o (b) elementi passivi fittizi o (c) crediti e ritenute fittizi, quando, congiuntamente:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, (i) è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, (ii) è superiore a euro un milione cinquecentomila, ovvero (iii) qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della norma non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

- **Emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma 1 e comma 2-bis, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Ai fini di quanto sopra indicato, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

- **Occultamento o distruzione di documenti contabili** (art. 10, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, (i) al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero (ii) di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

- **Sottrazione fraudolenta al pagamento di imposte** (art. 11, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza:

- a) allorché un soggetto - (i) al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero (ii) di interessi o sanzioni amministrative relativi a dette imposte di ammontare

complessivo superiore ad euro cinquantamila - aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

b) allorché un soggetto - al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori - indica nella documentazione presentata ai fini della procedura di transazione fiscale (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

- **Dichiarazione infedele ex art. 4 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Si realizza qualora un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- c. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- d. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Omessa dichiarazione ex art. 5 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Tale fattispecie punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. Punisce, altresì, chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Indebita compensazione ex art. 10-quater D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).

Tale ipotesi delittuosa si configura qualora un soggetto non versi le somme dovute, utilizzando in compensazione, ai sensi dell’articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti o crediti inesistenti, per un importo annuo superiore a cinquantamila euro.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

3.19 Sanzioni nei confronti dell’Ente.

In relazione alla commissione dei reati sopra elencati si applicano le seguenti sanzioni pecuniarie:

- art. 2 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 3 - Dichiarazione fraudolenta mediante altri artifici: sanzione pecuniaria fino a 500 quote;
- art. 8 - Emissione di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 10 - Occultamento o distruzione di documenti contabili: sanzione pecuniaria fino a 400 quote;
- art. 11 - Sottrazione fraudolenta al pagamento di imposte: sanzione pecuniaria fino a 400 quote;
- art. 4 - Dichiarazione infedele: sanzione pecuniaria fino a 300 quote;
- art. 5 - Omessa dichiarazione: sanzione pecuniaria fino a 400 quote;
- art. 10-quater - Indebita compensazione: sanzione pecuniaria fino a 400 quote.

Nei casi previsti dai commi 1 e 2 dell'art. 25-quinquiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

3.20 Aumenti delle sanzioni nei confronti dell'Ente.

Le sanzioni pecuniarie sono aumentate di un terzo qualora, a seguito alla commissione dei delitti di cui trattasi (indicati nel comma 1 dell'art. 25-quinquiesdecies), l'ente abbia conseguito un profitto di rilevante entità.

3.21 Aree a rischio reato e processi sensibili.

I processi sensibili individuati da HS che presentano il rischio di commissione dei reati di cui alla presente sezione riguardano le seguenti attività:

- Gestione della contabilità: con riferimento alla gestione della fatturazione attiva e passiva e all'emissione e contabilizzazione di fatture e altra documentazione afferente alla contabilità;
- Acquisto di beni e servizi - con riferimento all'attività di selezione e gestione dei fornitori esterni e di eventuali subappaltatori;
- Adempimenti fiscali e tributari in genere: con riferimento a i) predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere, ii) calcolo obbligazioni tributarie, iii) gestione adempimenti dichiarativi e contributivi e iv) pagamento delle imposte;
- Tenuta e custodia delle scritture contabili e fiscali: con riferimento alla conservazione, tracciabilità ed archiviazione di tutta la documentazione contabile e fiscale;
- Gestione di eventuali operazioni straordinarie: con riferimento ad eventuali trasformazioni, fusioni, scissioni, cessioni e/o conferimenti d'azienda, vendite di assets aziendali, ecc.

La tabella che segue indica in modo sintetico processi sensibili e relativi possibili reati tributari.

Processi sensibili	Reato
• <u>Gestione della contabilità</u> • <u>Acquisto di beni e servizi</u> • <u>Adempimenti fiscali e tributari in genere</u> • <u>Tenuta e custodia delle scritture</u>	• Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 10 marzo 2000, n. 74); • Emissione di fatture o altri documenti per

<u>contabili e fiscali</u> • <u>Gestione di eventuali operazioni straordinarie</u>	operazioni inesistenti (art. 8, D.Lgs. 10 marzo 2000, n. 74); • Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 10 marzo 2000, n. 74); • Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione infedele ex art. 4 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Omessa dichiarazione ex art. 5 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Indebita compensazione ex art. 10-quater D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).
---	--

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

3.22 Regole di comportamento.

3.22.1 Principi generali e standard di controllo.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Sezione prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-quinquiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;
- ✓ comunicare all'Agenzia delle Entrate e/o alle Autorità fiscali dati non rispondenti al vero, con il divieto di predisporre e fornire documenti falsi, omettere le informazioni dovute.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a:

- diffondere i principi di HS previsti dal Codice Etico;
 - promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati;
 - rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con l'Agenzia delle Entrate e le Autorità fiscali;
 - rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con l'Agenzia delle Entrate e le Autorità fiscali, deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che si occupano della predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria, dell'emissione di documentazione afferente alla contabilità, del ricevimento di documentazione afferente alla contabilità o del pagamento di imposte, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per evitare il rischio di violazioni in materia tributaria;
- ✓ tutti i consulenti in materia fiscale di HS devono essere informati circa le linee guida contro la commissione di reati tributari;
- ✓ qualunque criticità sorga nell'ambito del rapporto con l'Agenzia delle Entrate e le Autorità fiscali, deve essere immediatamente comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

È, inoltre, sancito l'espresso obbligo di:

- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- garantire un corretto e trasparente processo di gestione delle operazioni straordinarie, compresa la vendita di eventuali assets aziendali;
- assicurare la veridicità dei dati predisposti;
- assicurare la trasparente gestione delle forniture, di beni e servizi;

- garantire il flusso informativo tra le funzioni coinvolte nei processi sensibili in materia contabile-fiscale con il Collegio Sindacale e l'Organismo di Vigilanza;
- svolgere un'adeguata attività di selezione dei fornitori;
- acquistare beni di provenienza garantita e servizi e/o qualsiasi altra utilità ad un prezzo che, salvo casi eccezionali e certificati (quali ad esempio acquisti da aste giudiziarie o da fallimenti), sia commisurato alla qualità e quantità dei beni stessi in base al valore di mercato;
- rispettare la normativa fiscale-tributaria;
- garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali.

Gli standard di controllo da considerare ed applicare con riferimento alle attività sensibili di cui alla presente sezione sono:

- **previsione di procedure interne** idonee a fornire i principi di riferimento generali per la regolamentazione dell'attività sensibile;
- **tracciabilità**: tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali/informatici;
- **segregazione dei compiti**: lo standard concerne l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di un sistema di segregazione delle funzioni coerente** con le responsabilità organizzative assegnate: sono previste regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

4Principi procedurali specifici.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1 Definizione di ruoli e responsabilità Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti. Tenuta e custodia delle scritture contabili e fiscali Gestione delle operazioni straordinarie	
Definizione di ruoli e responsabilità	- Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare all'Agenzia delle Entrate o alle altre Autorità fiscali [ad es., nel caso di predisposizione della documentazione ai fini di dichiarazioni e comunicazioni concernenti la materia tributaria, deve essere ben chiara la segregazione delle funzioni tra (i) chi è preposto alla elaborazione e raccolta della documentazione da presentare, (ii) chi verifica, approva e sottoscrive la documentazione da presentare. - Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti	È fatto obbligo di: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni nelle fasi di autorizzazione / esecuzione / controllo per i seguenti ambiti: - gestione della fatturazione e relativa registrazione - gestione dei pagamenti - gestione delle note di credito - gestione degli acquisti, di beni e servizi - gestione buste paga e rimborsi spesa ai dipendenti - tenere tracciate tutte le fasi di gestione dei flussi finanziari e archiviare in maniera completa i relativi documenti giustificativi; - prevedere un sistema di backup dell'archiviazione dei documenti contabili; - verificare l'effettiva e corretta esecuzione della prestazione richiesta (sia verso fornitori di beni che di servizi), nel rispetto del principio di segregazione delle funzioni, prima di autorizzare il pagamento della relativa fattura; - tenere traccia e registrare ogni richiesta di ordine e relativo preventivo inoltrato, sia che sia stato mandato via e-mail che telefonici (in quest'ultimo caso andrà compilato apposito modulo di richiesta ordine); - verificare che gli incassi siano sempre supportati da un contratto o un ordine autorizzato e conseguentemente non accettare beni e/o altre utilità a fronte delle quali non vi sia un contratto o un ordine adeguatamente autorizzato; - verificare che l'importo effettivamente incassato corrisponda a quello fatturato e che non vi siano anomalie al riguardo; - rispettare le procedure adottate che regolano la gestione della contabilità;

	• rispettare il sistema di deleghe e procure adottato che indica i poteri ed i limiti di spesa dei soggetti coinvolti; • verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività; • svolgere un'attenta attività di selezione dei potenziali fornitori (sia di beni che di servizi), rispettando i criteri tecnico-economici ed espletando un'adeguata attività selettiva e di obiettiva comparazione tra più offerte; • a seconda del servizio richiesto, richiedere al fornitore tutta la documentazione o le certificazioni previste dalla legge di riferimento; • formalizzare tutti i contratti/accordi con fornitori e/o consulenti, allegando la relativa documentazione; • qualora si faccia uso di soggetti terzi intermediari, verificare con attenzione l'esistenza effettiva, la solidità e l'affidabilità del soggetto; • monitorare il mantenimento dei requisiti richiesti in capo al fornitore; • inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali); • identificare i ruoli e le responsabilità per la gestione dei rimborsi spese ai dipendenti nel rispetto del principio di segregazione di ruoli nelle fasi di autorizzazione / esecuzione / controllo; • controllare che ogni richiesta di rimborso spese sia accompagnata dalla relativa documentazione giustificativa e conseguentemente non riconoscere alcuna somma che non sia supportata da relativo giustificativo. Inoltre, ai fini preventivi, si ribadisce che: • è assolutamente vietato: - contabilizzare e registrare fatture per operazioni/prestazioni inesistenti; - autorizzare pagamenti a fornitori per operazioni inesistenti o privi dell'evidenza dell'effettuazione del servizio reso; - autorizzare rimborsi spesa privi della necessaria documentazione giustificativa; - predisporre o comunque utilizzare documenti palesemente falsi; • ogni pagamento deve corrispondere esattamente a quanto indicato nel contratto e/o nel preventivo formulato al cliente; • nessun pagamento e nessun incasso di denaro verso/da Paesi inseriti nelle principali black list internazionali, può avvenire senza adeguata documentazione comprovante la reale e specifica necessità; • nessun pagamento può essere effettuato in favore di un soggetto diverso dalla controparte contrattuale. Eventuali eccezioni a tale divieto sono ammesse solo a fronte della presentazione di una regolare documentazione che giustifichi e consente il pagamento nei confronti di un terzo (es. in caso di cessione del credito o pignoramento presso terzi); • nessun acquisto deve essere effettuato attraverso il ricorso a mercati non consolidati; • nessun contratto di fornitura può essere stipulato in assenza di un'adeguata attività di selezione o in mancanza della relativa documentazione richiesta dalla
--	--

	legge; - tutti gli incassi devono provenire dalla controparte contrattuale. Eventuali eccezioni sono ammesse solo a fronte della presentazione di una regolare documentazione giustificativa (es. pignoramento presso terzi); - ogni importo effettivamente incassato deve corrispondere a quanto fatturato. Qualora sia necessario restituire un pagamento o parte di esso indebitamente ricevuto, questo deve essere disposto esclusivamente verso il conto corrente di provenienza, tenendo traccia dei documenti giustificativi; - occorre tenere l'evidenza scritta di ogni pagamento; - occorre archiviare tutti i documenti contabili nel rispetto dei principi di correttezza, completezza e attenzione della relativa tenuta.
Tenuta e custodia delle scritture contabili e fiscali	In merito alla tenuta delle scritture contabili, è fatto obbligo: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni per i seguenti ambiti: - gestione degli adempimenti fiscali e tributari; - gestione del calcolo delle obbligazioni tributarie e dei relativi obblighi dichiarativi; - gestione e tenuta delle scritture contabili e fiscali; - tenere tracciate tutte le fasi di gestione dei citati processi e archiviare in maniera completa i relativi documenti; - prevedere un sistema di back up dell'archiviazione dei documenti contabili e fiscali; - prevedere modalità di aggiornamento, anche tramite consulenti esterni, sulle novità in ambito fiscale e tributario; - provvedere al regolare adempimento degli obblighi fiscali-tributari cui la società è tenuta (tributi, contributi, Iva etc.); - prevedere uno scadenziario che preveda i termini entro i quali occorre provvedere ai vari adempimenti fiscali-tributari. È, inoltre, vietato: - occultare o distruggere, in tutto o in parte, documenti contabili, fiscali o di cui è comunque obbligatoria la conservazione; - omettere o fornire dati ed informazioni inesatte o non complete imposte dalla legge sulla situazione economica, patrimoniale e finanziaria della società; - violare, eludere, evadere obblighi di dichiarazione, attestazione, certificazione di natura tributaria previsti dalla legge; - non adempiere le prescrizioni di legge in materia contabile, di informazione societaria, di valutazione di cespiti e di redazione del bilancio; - occultare in contabilità redditi conseguiti soggetti a tassazione, rappresentare falsamente spese non reali, emettere fatture per prestazioni inesistenti, effettuare stime, valutazioni e determinazione di poste di bilancio con modalità e criteri valutativi difforni da quelli richiesti dalla legge; - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da parte degli organi di controllo; - ostacolare, in ogni modo, l'effettuazione di verifiche, accertamenti ed ispezioni da parte dell'Agenzia delle Entrate o delle altre Autorità fiscali o

	giudiziarie.
Gestione delle operazioni straordinarie	Con riferimento a tale attività è fatto obbligo di: • garantire l'esplicita approvazione, da parte dell'Assemblea dei Soci, di ogni attività relativa ad operazioni straordinarie, comprese le cessioni e dismissioni di asset aziendali, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni, qualora per il compimento delle suddette operazioni si renda necessaria od opportuna l'approvazione dell'Assemblea; • identificare in maniera chiara e precisa i ruoli ed i soggetti competenti alla predisposizione della documentazione destinata agli organi sociali a supporto delle deliberazioni relative ad operazioni straordinarie; • identificare in maniera chiara ruoli e responsabilità in merito alla tenuta ed archiviazione degli atti di delibera e dei relativi documenti predisposti; • garantire una corretta tenuta ed archiviazione della documentazione relativa alle operazioni, prevedendo anche sistemi di back up.; È, inoltre, assolutamente vietato: • alienare simulatamente beni o assets aziendali al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; • compiere qualsiasi altro atto fraudolento al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; • indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

4.18 Responsabilità specifiche del Chief Financial Officer (CFO), Direzione Amministrativa (DAM), Direzione Finanziaria (DF).

Con riferimento alla prevenzione del rischio di commissione dei reati tributari sarà compito del CFO, della Direzione Amministrativa e la Direzione Finanziaria:

- effettuare le attività di verifica e monitoraggio sulle registrazioni contabili sia del ciclo attivo che del ciclo passivo;
- effettuare le valutazioni contabili di propria pertinenza nel rispetto dei principi comportamentali e dei principi contabili italiani e aziendali richiamati dalla presente procedura;
- predisporre il calendario delle attività di chiusura contabile e di redazione del progetto di bilancio inviandolo a tutti i soggetti aziendali interessati;
- monitorare e sollecitare le informazioni contabili inviate da altre Funzioni;
- effettuare tutte le attività di verifica necessarie in fase di chiusura contabile in modo tale da garantire la correttezza e la completezza dei dati di bilancio;

- predisporre le scritture di chiusura di propria competenza nel rispetto dei principi comportamentali e dei principi contabili italiani e aziendali richiamati dalla presente procedura;
- archiviare e conservare tutta la documentazione a supporto delle registrazioni contabili e del bilancio;
- custodire i valori di cassa centrale;
- gestire le operazioni di cassa centrale;
- registrare le operazioni in contabilità generale;
- effettuare giornalmente la conta fisica di cassa e la quadratura con la scheda contabile;
- verificare i giustificativi inviati ed approvati;
- verificare i giustificativi per le spese effettuate mediante carta di credito (verifica dell'inerenza con l'attività aziendale);
- effettuare le riconciliazioni dei conti correnti bancari.

Con specifico riferimento al Chief Financial Officer (CFO), quest'ultimo dovrà:

- monitorare e verificare tutte le suddette attività svolte da DAM e DF;
- approvare le riconciliazioni bancarie;
- pianificare e proporre le operazioni di finanziamento;
- verificare le condizioni di conto corrente;
- verificare mensilmente la conta fisica della cassa centrale e la relativa quadratura con la scheda contabile;
- gestire le attività operative di apertura, gestione e chiusura dei conti correnti bancari.

4.19 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'esito di eventuali audit effettuati sulla gestione delle attività sensibili sopra indicate, sia da parte di funzioni interne che da parte di soggetti esterni (ad es. consulenti fiscali, commercialisti, ecc.);
- l'avviso di eventuali ispezioni da parte dell'Agenzia delle Entrate o di altre autorità fiscali o giudiziarie con relativo verbale;
- eventuali comunicazioni provenienti dal Collegio Sindacale relativamente a criticità emerse, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-quinquiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente - con il supporto delle funzioni competenti - il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

L'Organismo di Vigilanza deve riportare i risultati della sua attività di vigilanza e controllo, con cadenza periodica semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale.

Pertanto, nel caso in cui dagli accertamenti svolti dall'Organismo di Vigilanza emergano elementi che facciano risalire la violazione dei principi e protocolli contenuti nella presente Parte Speciale del Modello, la commissione del reato, o il tentativo di commissione del reato, direttamente al Presidente, l'Organismo di Vigilanza dovrà riferire al Consiglio di Amministrazione ed al Collegio Sindacale, ai quali compete la decisione sull'eventuale applicazione dei meccanismi previsti dalla legge.

4.20 Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25-sexiesdecies del Decreto).

Il reato di contrabbando, previsto all'art. 25-sexiesdecies del Decreto, è stato introdotto dal D.Lgs. 14 luglio 2020, n. 75 ("Attuazione della direttiva (UE) 2017/1371 c.d. "Direttiva PIF", relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale").

L'art. 25-sexiesdecies del D.Lgs. 231/01 dispone che: *"1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.*

2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

La Società ha ritenuto di dover mappare il rischio connesso alla commissione di reati di contrabbando stante la ingente attività di import ed export con diversi paesi UE ed extra UE.

A tal fine, si ritiene necessaria una breve premessa con riferimento alla materia doganale.

I dazi doganali rappresentano una risorsa propria dell'Unione europea e confluiscono nel bilancio unitario, ad esclusione di una percentuale del 25% che viene trattenuta dallo Stato di entrata delle merci a copertura delle spese di riscossione (fonte: dossier di documentazione parlamentare).

La normativa doganale è contenuta nel Decreto del Presidente della Repubblica 23 gennaio 1973 n. 43 (Testo Unico Doganale, "TUD").

Si considerano "diritti doganali" tutti quei diritti che la dogana è tenuta a riscuotere in forza di una legge, in relazione alle operazioni doganali. Fra i diritti doganali costituiscono "diritti di confine" (art. 34 del TUD):

- i dazi di importazione e quelli di esportazione;
- i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione;
- i diritti di monopolio, le sovrimposte di confine ed ogni altra imposta o sovrimposta di consumo a favore dello Stato (per quanto concerne le merci in importazione).

Per le merci soggette a diritti di confine, il presupposto dell'obbligazione tributaria è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e, relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso (art. 36 del TUD).

4.21 Sanzioni nei confronti dell'Ente.

In relazione alla commissione dei reati di cui sopra si applicano all'ente le seguenti sanzioni pecuniarie:

✓ fino a 200 quote in relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica n. 43/1973, ovvero ai delitti del Titolo VII Capo I, intendendosi per tali i fatti ivi previsti (ma solo se superano 10mila euro di diritti di confine evasi) ed in particolare:

- Articolo 282 (Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali)
- Articolo 283 (Contrabbando nel movimento delle merci nei laghi di confine)
- Articolo 284 (Contrabbando nel movimento marittimo delle merci)
- Articolo 285 (Contrabbando nel movimento delle merci per via aerea)
- Articolo 286 (Contrabbando nelle zone extra-doganali)
- Articolo 287 (Contrabbando per indebito uso di merci importate con agevolazioni doganali)
- Articolo 288 (Contrabbando nei depositi doganali)
- Articolo 289 (Contrabbando nel cabotaggio e nella circolazione)
- Articolo 290 (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti).
- Articolo 291 (Contrabbando nell'importazione od esportazione temporanea)
- Articolo 291-bis (Contrabbando di tabacchi lavorati esteri)
- Articolo 291-ter (Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri)
- Articolo 291-quater (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri)
- Articolo 292 (Altri casi di contrabbando)
- Articolo 294 (Pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato)
- alle contravvenzioni del Titolo VII Capo II, cioè ai fatti ivi previsti ma solo se superano i 10mila euro di diritti di confine evasi (articoli 302 e seguenti).

✓ fino a 400 quote qualora i diritti di confine dovuti superino i 100.000 Euro.

Nei casi previsti dai commi 1 e 2 dell'art. 25-sexiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

4.22 Aree a rischio reato e processi sensibili.

I processi sensibili che presentano il rischio di commissione dei reati di cui al presente paragrafo riguardano le seguenti attività:

- vendita, acquisto, commercializzazione e scambio di prodotti oltre confine;
- scarico e deposito delle merci oltre confine.

Le potenziali aree a rischio reato che HS ha astrattamente individuato sono quelle relative alle seguenti attività:

Processi sensibili	Reato
• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine • Scarico e deposito delle merci oltre confine	• Contrabbando (Decreto del Presidente della Repubblica n. 43/1973);

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

4.23 Regole di comportamento

4.23.1 Principi generali e standard di controllo

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-sexiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;

Inoltre, è fatto specifico divieto di:

- introdurre merci estere attraverso il confine di terra in violazione delle prescrizioni, divieti e limitazioni;
- introdurre merci estere via mare in violazione delle prescrizioni, divieti e limitazioni;
- scaricare o depositare merci estere nello spazio intermedio tra la frontiera e la più vicina dogana;

- nascondere merci estere sulla persona o nei bagagli o fra merci di altro genere od in qualunque mezzo di trasporto, per sottrarle alla visita doganale;
- asportare merci dagli spazi doganali senza aver pagato i diritti dovuti senza averne garantito il pagamento;
- portare fuori del territorio doganale merci nazionali o nazionalizzate soggette a diritti di confine;
- detenere merci estere, quando ricorrano le circostanze previste nel secondo comma dell'art. 25-sexiesdecies per il delitto di contrabbando (ovvero, *"Quando i diritti di confine dovuti superano centomila euro"*).

5 Principi procedurali specifici.

Protocollo 1 Controllo interno sull'emissione e la conservazione dei documenti fiscali	
Applicazione di misure idonee ad evitare l'emissione di documentazione contabile non coerente con la prestazione o la distruzione di documenti fiscali al fine di eventuali controlli da parte delle Autorità Doganali	Devono essere osservate specifiche misure che consentano di: • evitare di introdurre o esportare merci che violino prescrizioni, divieti e limitazioni di cui al Testo unico delle disposizioni legislative in materia doganale; • conservare la documentazione doganale; • non sottrarsi alle visite doganali; • pagare i diritti dovuti o garantire i dovuti pagamenti.

Con riferimento e per l'espletamento delle operazioni doganali di import ed export la HS si affida a società selezionate per la notorietà e l'esperienza nel settore delle spedizioni e della consulenza per logistica e trasporti a livello internazionale nonché per le pratiche doganali in import/export. L'affidamento di tali incarichi viene fatto a mezzo contratti di mandato e consulenza annuali e/o a tempo indeterminato.

Dovrà essere cura dei Destinatari della presente sezione di verificare la validità e la vigenza dei suddetti contratti di mandato.

5.18 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'avviso di eventuali ispezioni da parte delle Autorità doganali o di altre autorità giudiziarie sempre relativamente alla materia doganale;
- eventuali comunicazioni provenienti dalle Autorità doganali o di altre autorità giudiziarie relativamente a criticità emerse in materia doganale, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-sexiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- ✓ verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- ✓ esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- ✓ comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- ✓ curare l'aggiornamento del Modello, indicando al CDA le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

4 SEZIONE D – SETTORE RICERCA E SVILUPPO (R&D).

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Ricerca e Sviluppo che in HS è composto da il Responsabile e da una Unità di Ricerca e Progettazione.

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte in questo settore dal Responsabile ed i suoi sottoposti e nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

SETTORE RICERCA E SVILUPPO (R&D) (Responsabile Ricerca e Sviluppo)	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Richiesta e ottenimento di finanziamenti pubblici; • Accesso ai sistemi informatici della Pubblica Amministrazione;
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto)	Contraffazione, alterazione o uso di marchi.
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Gestione delle licenze e dei software per elaboratore.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

4.1 I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- **malversazione a danno dello Stato**, di altro ente pubblico o comunitario (art. 316-bis c.p.), che punisce la mancata destinazione di contributi, sovvenzioni o simili alle finalità per cui erano stati destinati;
- **indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato**, di altro ente pubblico o da parte di ente comunitario (art. 316-ter c.p.) mediante l'utilizzo di documenti falsi o il rilascio di dichiarazioni attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute; [modificato dalla L. n. 3/2019]
- **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), che consiste nella percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato, di altro ente pubblico o da parte di ente comunitario mediante artifici o raggiri diversi dall'utilizzo di documenti falsi, dichiarazioni false od omissione di informazioni dovute;
- **truffa aggravata in danno dello Stato o di altro ente pubblico** (art. 640, comma 2, n. 1 c.p.), che punisce l'impiego di artifici e raggiri per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;

- **frode informatica in danno dello Stato o di altro ente pubblico** (art. 640-ter c.p.), che incrimina l'ipotesi di alterazione del funzionamento di un sistema informatico o telematico, ovvero l'intervento senza diritto su dati, informazioni o programmi contenuti in un sistema informatico, per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;
- **concussione** (art. 317 c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della propria qualità o del proprio potere, costringe o induce il privato a dare o promettere denaro o altra utilità;
- **corruzione per l'esercizio della funzione** (art. 318 c.p.), ossia il caso in cui il pubblico ufficiale riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità, in cambio dell'esercizio delle sue funzioni o poteri; [modificato dalla L. n. 3/2019];
- **corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), ossia il caso in cui il pubblico ufficiale, per omettere o ritardare un atto dell'ufficio o compierne uno contrario ai propri doveri, riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità;
- **corruzione in atti giudiziari** (art. 319-ter c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi di chi riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità al fine di favorire o danneggiare una parte di un processo civile, amministrativo o penale;
- **concussione per induzione, ovvero induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità; la responsabilità penale si estende anche a chi dà o promette denaro o altra utilità;
- **corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), ossia le ipotesi di reato previste dagli artt. 318 e 319 c.p. commesse nei confronti di un incaricato di pubblico servizio;
- **istigazione alla corruzione** (art. 322 c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi che il pubblico ufficiale non accetti di ricevere o il privato si rifiuti di dare denaro o altra utilità;
- **peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): l'ipotesi prevista dal legislatore è quella dei reati contemplati in rubrica commessi nei confronti di funzionari esteri. [modificato dalla L. n. 3/2019]
- **traffico di influenze illecite** (art. 346 bis c.p.) [introdotto con la L. n. 3/2019] Con la riforma del 2019 (legge 3/2019), che ha abrogato l'art. 346 c.p., i fatti fino ad allora qualificabili come

millantato credito possono essere sussunti sotto il nuovo art. 346-bis c.p. Infatti, la condotta punita non consiste solo più nello sfruttamento di relazioni esistenti, ma anche nella vanteria di relazioni «asserite» con un pubblico ufficiale, un incaricato di pubblico servizio o, ancora, con uno dei soggetti elencati all'art. 322-bis c.p.

4.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio.

– Pubblica Amministrazione (di seguito “PA”) s’intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell’interesse della collettività, e quindi nell’interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l’Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d’Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPSAI, INPSAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti

enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

- Pubblici ufficiali e incaricati di un pubblico servizio Ai sensi dell’art. 357, primo comma, del codice penale, è considerato pubblico ufficiale “agli effetti della legge penale” colui il quale esercita “una pubblica funzione legislativa, giudiziaria o amministrativa”.

La norma chiarisce solo la nozione di “pubblica funzione amministrativa” (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale “è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”.

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l’art. 358 c.p. definisce i “soggetti incaricati di un pubblico servizio” come quei soggetti “i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della “pubblica funzione”, da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d’ordine e/o la prestazione d’opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

4.3 Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001).

Nell’espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e

ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
- ✓ porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
- ✓ comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
- ✓ violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
- ✓ tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
- ✓ qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;

- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli e responsabilità	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla P.A. (ad es., nel caso di richiesta di un finanziamento agevolato per la realizzazione di un progetto di ricerca, deve essere ben chiara la segregazione delle funzioni tra (a) chi propone la richiesta di finanziamento (b) chi effettua lo studio di fattibilità per valutare la possibilità di accedere al finanziamento (c) chi raccoglie e dispone la documentazione necessaria relativa al progetto e alla richiesta di finanziamento e (d) chi approva e sottoscrive la richiesta). • Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: • proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; • porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; • distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; • presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; • presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: • sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; • ogni eventuale accordo preso con la P.A. sia documentato.
Ispezioni	• Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche

	tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; • di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; • devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: • la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; • specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.

Protocollo 2 – Scelta di fornitori e consulenti	
Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	• I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. • I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. • Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. • Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici	
Transazioni finanziarie	• Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio. • In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; • Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto previsto dall'art. 3 della legge n. 136/12010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che dovrà essere necessariamente corredata da idonea documentazione giustificativa.
Irregolarità anomalie	o Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di

Protocollo 4 – Assunzione del personale	
Assunzione, gestione, formazione incentivazione dei dipendenti e collaboratori	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato. Il personale che si occupa di transazioni con funzionari pubblici nazionali o stranieri

	ha l'obbligo di eseguire una certificazione periodica di non aver violato la Parte Speciale del presente Modello.
--	---

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali	
Contenziosi/ Contestazioni	- Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. - Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.

Protocollo 6	
Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi Spese di rappresentanza	
Omaggi/Donazioni	Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico.

4.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

4.5 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta Cianfanelli Simona, nominata anche Amministratore di Sistema (c.d. ADS), la quale ha supportato la Società nell'implementazione un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito HS, nel rispetto del principio di responsabilizzazione (c.d. *accountability*), ha adottato procedure e misure di sicurezza idonee ad assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica	In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test, penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati; Inoltre: • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato nel rispetto del Codice Etico aziendale, nonché di quanto previsto dalle procedure interne in materia di trattamento dei dati personali (così come previsto dal Regolamento UE 2016/679 c.d. GDPR); • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale;
--	---

	• ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software, ecc.</i>); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante <i>username e password</i> al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	--

4.6 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

4.7 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001) in materia di contraffazione (art. 25-bis lett. f-bis del Decreto) e Violazione del diritto d'autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi,

ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti	
Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti	La regolamentazione dell'attività descritta deve prevedere che: • i Destinatari si accertino che i dipartimenti di <i>patent e trademark</i> internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto; • in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di <i>patent e trademark</i> internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto. • I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti. Inoltre, è fatto espressamente divieto di: • contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati; • contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati; • introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati; • detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto; • consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni

	realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941;
---	--

	importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	--

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE

Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: - l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; - tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: - duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); - riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
------------------------------	--

4.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- ✓ proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;

- ✓ esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- ✓ proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- ✓ esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

5 SEZIONE E – SETTORE HARDWARE & SOFTWARE.

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Hardware e Software di HS.

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte dal Responsabile del predetto settore e nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

SETTORE HARDWARE & SOFTWARE	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto) e in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto)	Contraffazione, alterazione o uso di marchi.
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme in materia di sicurezza sul lavoro (Art. 25-septies)	• Gestione delle misure di sicurezza; • Manutenzione delle infrastrutture e sicurezza delle zone di produzione e magazzino; • Formazione del personale.
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Gestione delle licenze e dei software per elaboratore.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

5.1 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24.bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;

- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta Cianfanelli Simona, nominata anche Amministratore di Sistema (c.d. ADS), la quale ha supportato la Società nell'implementazione un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito HS, nel rispetto del principio di responsabilizzazione (c.d. *accountability*), ha adottato procedure e misure di sicurezza idonee ad assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica	In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test</i>, <i>penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;
--	---

	Inoltre: • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato nel rispetto del Codice Etico aziendale, nonché di quanto previsto dalle procedure interne in materia di trattamento dei dati personali (così come previsto dal Regolamento UE 2016/679 c.d. GDPR); • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software, ecc.</i>); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che
--	---

	soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	---

5.2 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- c. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

5.3 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001) in materia di contraffazione (art. 25-bis lett. f-bis del Decreto) e Violazione del diritto d'autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti	
Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti	La regolamentazione dell'attività descritta deve prevedere che: • i Destinatari si accertino che i dipartimenti di <i>patent e trademark</i> internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto; • in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di <i>patent e trademark</i> internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto. • I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti. Inoltre, è fatto espressamente divieto di: • contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati; • contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati; • introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati; • detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto; • consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti

	industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere
---	--

	collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; • importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	---

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE

Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
------------------------------	--

5.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a

verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- ✓ proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- ✓ esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- ✓ proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- ✓ esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

5.5 Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies D.Lgs. 231/2001).

I reati in materia di salute e sicurezza sul lavoro che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-septies del d.lgs. 231/2001 sono i seguenti:

- Omicidio Colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590, comma III, c.p.).

Le Linee Guida di Confindustria nell'ambito dei reati trattati nella presente Parte Speciale evidenziano l'impossibilità di escludere a priori alcun ambito di attività della società, in quanto i reati in esame potrebbero riguardare tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Ne consegue che le potenziali aree a rischio reato che HS ha individuato nell'ambito di tali reati riguardano tutte le attività svolte nei siti della Società.

In particolare, la Società ha la sede legale in Roma (RM) – Via Zosimo 13, e unità operative e locali in:

- Aprilia (Latina), Via Angela Vacchi 23/25, CAP 04011 – Stabilimento di produzione.

Inoltre, sono considerate aree a rischio anche tutte le attività svolte dal personale di HS che opera esternamente in qualità di *supporters* tecnici all'interno di strutture e aziende sanitarie, (nello

specifico in sale operatorie). Particolare attenzione deve essere dedicata a quelle attività realizzate in associazione con partner commerciali (in caso di joint venture, anche in forma di ATI, consorzi, ecc.) o tramite la stipula di contratti di somministrazione, appalto o con società di consulenza o liberi professionisti.

Anche ai fini della redazione della presente Parte Speciale si devono pertanto considerare i fattori riportati nel Documento di Valutazione dei Rischi (di seguito anche DVR) tenuto conto che lo stesso non esaurisce le procedure di seguito previste, finalizzate a costituire il complessivo sistema di gestione della sicurezza sul lavoro e dare attuazione al disposto dell'art. 30 d.lgs. 81/08 secondo i principi espressi dalle Linee Guida UNI – INAIL.

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso in una delle aree sensibili indicate al precedente paragrafo 1, si ritiene particolarmente importante:

- determinare le politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;
- identificare e applicare in modo corretto le prescrizioni delle leggi e dei regolamenti applicabili in tema di salute e sicurezza sul lavoro;
- identificare e valutare i rischi per tutte le categorie di lavoratori, con particolare riferimento alla redazione:
 - del DVR;
 - dei contratti di appalto;
 - della valutazione dei rischi derivanti dalle interferenze;
 - nel caso in cui la Società fosse costruttrice, dei Piani di Sicurezza e Coordinamento, Fascicolo dell'Opera e Piani Operativi di Sicurezza;
- fissare gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elaborare dei programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività del Servizio Prevenzione e Protezione e del Medico Competente;
 - attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori;

- sensibilizzare la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti esposti a rischi specifici (es. addetti alla Camera Bianca);
- attuare adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
 - coerenza tra attività svolta e competenze possedute;
- attuare le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- effettuare un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione per la sicurezza del lavoro e la tutela della salute nel raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alla specifica realtà della Società che ad eventuali cambiamenti nell'attività.

5.6 Struttura organizzativa di HS Hospital Service S.p.A.

In materia di salute e sicurezza sul lavoro la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente di cui al d.lgs. 81/2008 e successive modifiche (di seguito anche "Decreto Sicurezza"), al fine di eliminare o, per lo meno di limitare, i rischi per i lavoratori.

Nell'ambito di tale struttura organizzativa operano:

A) Il Datore di Lavoro. È il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

B) Il Servizio di Prevenzione e Protezione (SPP). Insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori. La Società ha proceduto alla nomina di un Responsabile del Servizio di Prevenzione e Protezione (RSPP), in possesso delle capacità e dei requisiti professionali di cui all'articolo 32

d.lgs. 81/08 e designata dal Datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi (art. 2 d.lgs. 81/2008).

C) Responsabile dei Lavori. La persona che può essere incaricata dal Committente/Datore di Lavoro Committente per svolgere i compiti ad essa attribuiti dal d.lgs. 81/2008.

D) Addetti al primo soccorso. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili del soccorso in azienda, in caso di infortuni.

E) Addetti antincendio. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili dell'attuazione delle misure antincendio e di evacuazione, in caso di emergenza.

F) Il Medico Competente. Medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 d.lgs. 81/08 che collabora, secondo quanto previsto all'articolo 29, comma 1, con il Datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al Decreto Sicurezza (art. 2 d.lgs. 81/08).

G) Il Rappresentante dei Lavoratori per la Sicurezza (RLS). Persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro (art. 2 comma 1, lett. i d.lgs. 81/2008).

H) Lavoratore. Persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione della Società, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite. I lavoratori di aziende che svolgono per HS attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

I) Gestione degli appalti e dei fornitori. Nei contratti di appalto intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione, il Datore di Lavoro in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno della propria azienda o Unità produttiva, in conformità alle procedure aziendali, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

- verificare, con il supporto delle Unità interessate, l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;

- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture. L'obbligo di redazione del suddetto documento non sussiste in caso di appalto di servizi di natura intellettuale, mere forniture di materiali o attrezzature, nonché per i lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza delle sostanze di cui all'allegato XI del d.lgs. 81/2008.

5.7 Principi procedurali specifici.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei lavoratori così come individuati dall'art. 15 del Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del suddetto decreto si prevede quanto segue.

Protocollo 1 – Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	
Politiche aziendali in tema di sicurezza	La politica per la sicurezza e salute sul lavoro adottata da HS deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte da HS e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i Lavoratori. A tal fine, è predisposto un adeguato sistema di designazioni o deleghe di funzioni in materia di salute e sicurezza secondo i principi di: • effettività, sussistenza e compresenza di autonomia decisionale e finanziaria del delegato; • idoneità tecnico-professionale del delegato; • vigilanza sull'attività del delegato, non acquiescenza, non ingerenza;

	• certezza, specificità e consapevolezza. La designazione / delega di funzioni da parte del datore di lavoro deve: • risultare da atto scritto recante data certa; • essere diretta ad un soggetto che possieda tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate; • essere accettata dal delegato per iscritto. Il soggetto delegato deve essere consapevole delle funzioni ad esso delegate. La politica per la sicurezza e salute sul lavoro è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.
Processo di pianificazione	HS nell'ambito del processo di pianificazione degli obiettivi in tema di salute e sicurezza, con cadenza annuale: • definisce gli obiettivi finalizzati al mantenimento e/o miglioramento del sistema; • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	• La Società ha definito un sistema di comunicazioni interne che assicura che le informazioni relative alla sicurezza fluiscano "dall'alto verso il basso", ma anche "dal basso verso l'alto" ed orizzontalmente rispetto alle varie parti dell'organizzazione. Lo scambio di informazioni tra i differenti livelli e settori aziendali è attuato attraverso l'individuazione di referenti interni e di idonei strumenti di comunicazione. Gli strumenti di comunicazione interna possono variare in funzione del tipo di informazione che è necessario fornire avendo però sempre presente che il requisito indispensabile è che le informazioni siano fornite usando una forma ed un modo che le rendano comprensibili alle persone che le devono ricevere. • La Società è convinta che il processo di prevenzione e miglioramento della sicurezza debba vedere coinvolto tutto il personale aziendale. A tale fine ogni lavoratore è incoraggiato a segnalare al proprio responsabile di funzione o direttamente al RSPP eventuali anomalie o proposte di miglioramento. Tali segnalazioni sono raccolte dal RSPP che provvede ad effettuarne un'analisi ed è responsabile di mettere in atto le eventuali azioni conseguenti; la decisione presa in merito è registrata dal RSPP. Il RSPP organizza anche le riunioni periodiche sulla sicurezza prevista dalle norme vigenti e redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione.

	• È stata definita una procedura per regolamentare le attività di formazione, informazione e addestramento da erogare a: - personale dipendente; - lavoratori con contratto di somministrazione; - stagisti. La procedura definisce anche le modalità in caso di nuove assunzioni e cambi di mansione I contenuti della procedura specificano modalità e responsabilità in merito a: - l'individuazione delle necessità di formazione e addestramento; - la pianificazione e attuazione della formazione; - la registrazione delle attività formative; - la verifica della loro efficacia; - l'informazione e sensibilizzazione del personale sull'igiene e la sicurezza del lavoro. • In merito all'attività di documentazione, HS dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, dei seguenti documenti: - la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro; - il registro degli infortuni; - il Documento di Valutazione dei Rischi indicante la metodologia con la quale si è proceduto alla valutazione dei rischi e contenente il programma delle misure di mantenimento e di miglioramento; - nel caso in cui la Società sia appaltatrice di lavori di costruzione: la documentazione contratti; Piano di Sicurezza e Coordinamento; Fascicolo dell'Opera; verbali di coordinamento relativi alla verifica dell'applicazione da parte delle imprese esecutrici delle disposizioni contenute nel PSC; Piani Operativi di Sicurezza. • HS è altresì chiamata a garantire che: - il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente; - venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente; - venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica; - venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale; - venga conservata la documentazione inerente a regolamenti ed accordi aziendali; - vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori; - venga conservata ogni procedura adottata da HS per la gestione della salute e sicurezza sui luoghi di lavoro; - tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.
Attività di monitoraggio	HS deve assicurare un costante ed efficace monitoraggio del sistema per la gestione della salute e della sicurezza sui luoghi di lavoro. A tale scopo:

	• assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta HS, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. HS garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.
Riesame del sistema	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema adottato da HS per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame annuale da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.
Gestione operativa degli appalti	HS deve predisporre e tenere aggiornato un elenco delle aziende con le quali stipula eventuali contratti di appalto. Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti dai quali devono risultare espressi riferimenti agli adempimenti di cui all'art. 26 del Decreto Sicurezza. Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori e le organizzazioni sindacali dei lavoratori. Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

5.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-septies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di HS eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla

tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la tutela della salute e della sicurezza nei luoghi di lavoro, in coerenza con quanto stabilito nel presente Modello e all'art. 30 del Decreto Sicurezza;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati da HS tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il Delegato della Sicurezza Aziendale e il RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

HS garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti di HS (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; gli Addetti al Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso).

6 SEZIONE F – SETTORE TECNICO PRODUTTIVO INTERNO, CRITICAL CARE, ENDO, TERAPIE ABLATIVE.

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Tecnico Produttivo Interno di HS relativamente alle tre linee di produzione Critical Care, Endo e Terapie Ablative.

Nell'ambito di questo settore e sotto la direzione del Responsabile vi sono:

- una Unità di assistenza tecnica e controllo qualità;
- il reparto di Inventory control in comunicazione con il Settore Acquisti;
- il reparto di Camera Bianca;
- il magazzino;
- il reparto Assemblaggio ed Imballaggio (c.d. Assembly & Packaging).

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte dal Responsabile e dalle varie unità sottoposte, nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

SETTORE TECNICO PRODUTTIVO INTERNO, CRITICAL CARE, ENDO, TERAPIE ABLATIVE (Responsabile settore Tecnico produttivo Interno [RSPT])	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.);
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto)	Contraffazione, alterazione o uso di marchi.
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme in materia di sicurezza sul lavoro (Art. 25-septies)	- Gestione delle misure di sicurezza; - Manutenzione delle infrastrutture e sicurezza delle zone di produzione e magazzino; - Formazione del personale.
Reati ambientali (art. 25-undecies del Decreto): - attività gestione rifiuti non autorizzata, - traffico illecito di rifiuti, - attività organizzate per il traffico illecito di rifiuti, - inquinamento del suolo, sottosuolo, delle acque superficiali e sotterranee, - violazione obblighi di comunicazione, - false indicazioni su natura e composizione dei rifiuti, - inquinamento ambientale art. 452bis c.p., - disastro ambientale art. 452 ter c.p., - traffico e abbandono di materiale radioattivo 452quinqies c.p., - impedimento del controllo 452sexies c.p., - omessa bonifica 452terdecies c.p.)	- Tutela del suolo, sottosuolo e delle acque (es. sversamenti da impianto di depurazione); - Gestione dei rifiuti (es. dismissione degli impianti, gestione dei rifiuti di apparecchiature meccaniche, elettriche ed elettroniche, ecc.)

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

6.18 I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- **malversazione a danno dello Stato**, di altro ente pubblico o comunitario (art. 316-bis c.p.), che punisce la mancata destinazione di contributi, sovvenzioni o simili alle finalità per cui erano stati destinati;
- **indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato**, di altro ente pubblico o da parte di ente comunitario (art. 316-ter c.p.) mediante l'utilizzo di documenti falsi o il rilascio di dichiarazioni attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute; [modificato dalla L. n. 3/2019]
- **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), che consiste nella percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato, di altro ente pubblico o da parte di ente comunitario mediante artifici o raggiri diversi dall'utilizzo di documenti falsi, dichiarazioni false od omissione di informazioni dovute;
- **truffa aggravata in danno dello Stato o di altro ente pubblico** (art. 640, comma 2, n. 1 c.p.), che punisce l'impiego di artifici e raggiri per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;
- **frode informatica in danno dello Stato o di altro ente pubblico** (art. 640-ter c.p.), che incrimina l'ipotesi di alterazione del funzionamento di un sistema informatico o telematico, ovvero l'intervento senza diritto su dati, informazioni o programmi contenuti in un sistema informatico, per ottenere un ingiusto profitto a danno dello Stato o di altro ente pubblico;
- **concussione** (art. 317 c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della propria qualità o del proprio potere, costringe o induce il privato a dare o promettere denaro o altra utilità;
- **corruzione per l'esercizio della funzione** (art. 318 c.p.), ossia il caso in cui il pubblico ufficiale riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità, in cambio dell'esercizio delle sue funzioni o poteri; [modificato dalla L. n. 3/2019];
- **corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), ossia il caso in cui il pubblico ufficiale, per omettere o ritardare un atto dell'ufficio o compierne uno contrario ai propri doveri, riceve (o accetta di ricevere) per sé o per altri denaro o altra utilità;

- **corruzione in atti giudiziari** (art. 319-ter c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi di chi riceve (o accetti di ricevere) per sé o per altri denaro o altra utilità al fine di favorire o danneggiare una parte di un processo civile, amministrativo o penale;
- **concussione per induzione, ovvero induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), ossia il caso in cui il pubblico ufficiale o l'incaricato di un pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità; la responsabilità penale si estende anche a chi dà o promette denaro o altra utilità;
- **corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), ossia le ipotesi di reato previste dagli artt. 318 e 319 c.p. commesse nei confronti di un incaricato di pubblico servizio;
- **istigazione alla corruzione** (art. 322 c.p.): in entrambi i casi di corruzione sopra definiti, tale norma incrimina l'ipotesi che il pubblico ufficiale non accetti di ricevere o il privato si rifiuti di dare denaro o altra utilità;
- **peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): l'ipotesi prevista dal legislatore è quella dei reati contemplati in rubrica commessi nei confronti di funzionari esteri. [modificato dalla L. n. 3/2019]
- **traffico di influenze illecite** (art. 346 bis c.p.) [introdotto con la L. n. 3/2019] Con la riforma del 2019 (legge 3/2019), che ha abrogato l'art. 346 c.p., i fatti fino ad allora qualificabili come millantato credito possono essere sussunti sotto il nuovo art. 346-bis c.p. Infatti, la condotta punita non consiste solo più nello sfruttamento di relazioni esistenti, ma anche nella vanteria di relazioni «asserite» con un pubblico ufficiale, un incaricato di pubblico servizio o, ancora, con uno dei soggetti elencati all'art. 322-bis c.p.

6.19 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio

– Pubblica Amministrazione (di seguito “PA”) s'intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAL, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

- **Pubblici ufficiali e incaricati di un pubblico servizio** Ai sensi dell'art. 357, primo comma, del codice penale, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

La norma chiarisce solo la nozione di "pubblica funzione amministrativa" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l'art. 358 c.p. definisce i “soggetti incaricati di un pubblico servizio” come quei soggetti “i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della “pubblica funzione”, da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d'ordine e/o la prestazione d'opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

6.20 Regole di comportamento e protocolli operativi in tema di reati contro la P.A. (Artt. 24 e 25, D.Lgs. 231/01).

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
- ✓ porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
- ✓ comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;

- ✓ violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
- ✓ tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
- ✓ qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1

- **Rapporti anche istituzionali con la Pubblica Amministrazione.**
- **Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.).**
- **Gestione delle gare e dei bandi pubblici**
- **Accesso a sistemi informatici della Pubblica Amministrazione**

Definizione dei ruoli	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la
------------------------------	--

responsabilità	documentazione da presentare alla P.A. (ad es., nel caso di ispezione, deve essere ben chiara la segregazione delle funzioni tra (a) chi è autorizzato a seguire le operazioni di ispezione e ad interloquire con la P.A. (b) chi raccoglie e dispone la documentazione necessaria richiesta dalla P.A.). Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: - proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; - porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; - distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; - presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; - presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: - sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; - ogni eventuale accordo preso con la P.A. sia documentato.
Ispezioni	- Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; - di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; - devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle

	principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; • specifici protocolli di controllo e verifica della veridicità e correttezza dei documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.
--	---

Protocollo 2 – Scelta di fornitori e consulenti	
Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	• I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. • I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. • Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. • Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici	
Transazioni finanziarie	• Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio. • In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; • Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto previsto dall'art. 3 della legge n. 136/12010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che

		dovrà essere necessariamente corredata da idonea documentazione giustificativa.
Irregolarità anomalie	o	Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di

Protocollo 4 – Assunzione del personale		
Assunzione, gestione, formazione incentivazione dei dipendenti e collaboratori	e	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato. Il personale che si occupa di transazioni con funzionari pubblici nazionali o stranieri ha l'obbligo di eseguire una certificazione periodica di non aver violato la Parte Speciale del presente Modello.

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali		
Contenziosi/ Contestazioni		• Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. • Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.

Protocollo 6		
• Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi • Spese di rappresentanza		
Omaggi/Donazioni		Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero,

	ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico.
--	---

6.21 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- c. esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- d. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- e. curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

6.22 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001)

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);

- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta Cianfanelli Simona, nominata anche Amministratore di Sistema (c.d. ADS), la quale ha supportato la Società nell'implementazione un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito HS, nel rispetto del principio di responsabilizzazione (c.d. *accountability*), ha adottato procedure e misure di sicurezza idonee ad assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento dei dati.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno

rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali		
Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica		In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di

	clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test</i>, <i>penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati; Inoltre: • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato nel rispetto del Codice Etico aziendale, nonché di quanto previsto dalle procedure interne in materia di trattamento dei dati personali (così come previsto dal Regolamento UE 2016/679 c.d. GDPR); • l'utilizzo della rete e del servizio di posta elettronica aziendale deve essere effettuato impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet)
--	--

	esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software</i>, ecc.); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	---

6.23 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

6.24 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti	
Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti	La regolamentazione dell'attività descritta deve prevedere che: • i Destinatari si accertino che i dipartimenti di <i>patent e trademark</i> internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto; • in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di <i>patent e trademark</i> internazionali l'incarico di rilevare qualsiasi criticità del marchio o del

	brevetto. • I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti. Inoltre, è fatto espressamente divieto di: • contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati; • contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati; • introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati; • detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto; • consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non
---	--

	destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; • importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	---

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	
Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in

	pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
--	--

6.25 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- d. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- e. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

6.26 Regole di comportamento e Protocolli operativi in materia di Salute e Sicurezza sul lavoro (art. 25-septies, D.Lgs. 231/2001).

I reati in materia di salute e sicurezza sul lavoro che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-septies del d.lgs. 231/2001 sono i seguenti:

- Omicidio Colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590, comma III, c.p.).

Le Linee Guida di Confindustria nell'ambito dei reati trattati nella presente Parte Speciale evidenziano l'impossibilità di escludere a priori alcun ambito di attività della società, in quanto i reati in esame potrebbero riguardare tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Ne consegue che le potenziali aree a rischio reato che HS ha individuato nell'ambito di tali reati riguardano tutte le attività svolte nei siti della Società.

In particolare, la Società ha la sede legale in Roma (RM) – Via Zosimo 13, e unità operative e locali in:

- Aprilia (Latina), Via Angela Vacchi 23/25, CAP 04011 – Stabilimento di produzione.

Inoltre, sono considerate aree a rischio anche tutte le attività svolte dal personale di HS che opera esternamente in qualità di *supporters* tecnici all'interno di strutture e aziende sanitarie, (nello specifico in sale operatorie). Particolare attenzione deve essere dedicata a quelle attività realizzate in associazione con partner commerciali (in caso di joint venture, anche in forma di ATI, consorzi, ecc.) o tramite la stipula di contratti di somministrazione, appalto o con società di consulenza o liberi professionisti.

Anche ai fini della redazione della presente Parte Speciale si devono pertanto considerare i fattori riportati nel Documento di Valutazione dei Rischi (di seguito anche DVR) tenuto conto che lo stesso non esaurisce le procedure di seguito previste, finalizzate a costituire il complessivo sistema di gestione della sicurezza sul lavoro e dare attuazione al disposto dell'art. 30 d.lgs. 81/08 secondo i principi espressi dalle Linee Guida UNI – INAIL.

Con riguardo all'inosservanza delle norme poste a tutela della salute e sicurezza dei lavoratori, da cui possa discendere l'evento dannoso in una delle aree sensibili indicate al precedente paragrafo 1, si ritiene particolarmente importante:

- determinare le politiche di salute e sicurezza sul lavoro volte a definire gli impegni generali assunti dalla Società per la prevenzione dei rischi ed il miglioramento progressivo della salute e sicurezza;
- identificare e applicare in modo corretto le prescrizioni delle leggi e dei regolamenti applicabili in tema di salute e sicurezza sul lavoro;
- identificare e valutare i rischi per tutte le categorie di lavoratori, con particolare riferimento alla redazione:
 - del DVR;

- dei contratti di appalto;
- della valutazione dei rischi derivanti dalle interferenze;
- nel caso in cui la Società fosse costruttrice, dei Piani di Sicurezza e Coordinamento, Fascicolo dell'Opera e Piani Operativi di Sicurezza;
- fissare gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elaborare dei programmi per il raggiungimento di tali obiettivi con relativa definizione di priorità, tempi ed attribuzione delle rispettive responsabilità - con assegnazione delle necessarie risorse - in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività del Servizio Prevenzione e Protezione e del Medico Competente;
 - attività di tutti gli altri soggetti su cui ricade la responsabilità dell'attuazione delle misure per la salute e sicurezza dei lavoratori;
- sensibilizzare la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti esposti a rischi specifici (es. addetti alla Camera Bianca);
- attuare adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia del suddetto sistema di gestione della salute e sicurezza sul lavoro, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, relativi a provvedimenti disciplinari;
 - coerenza tra attività svolta e competenze possedute;
- attuare le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- effettuare un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione per la sicurezza del lavoro e la tutela della salute nel raggiungere gli obiettivi prefissati, nonché l'adequatezza di questi ultimi rispetto sia alla specifica realtà della Società che ad eventuali cambiamenti nell'attività.

6.27 Struttura organizzativa di HS Hospital Service S.p.A.

In materia di salute e sicurezza sul lavoro la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa vigente di cui al d.lgs. 81/2008 e successive modifiche

(di seguito anche "Decreto Sicurezza"), al fine di eliminare o, per lo meno di limitare, i rischi per i lavoratori.

Nell'ambito di tale struttura organizzativa operano:

A) Il Datore di Lavoro. È il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa.

B) Il Servizio di Prevenzione e Protezione (SPP). Insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori. La Società ha proceduto alla nomina di un Responsabile del Servizio di Prevenzione e Protezione (RSPP), in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 d.lgs. 81/08 e designata dal Datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi (art. 2 d.lgs. 81/2008).

C) Responsabile dei Lavori. La persona che può essere incaricata dal Committente/Datore di Lavoro Committente per svolgere i compiti ad essa attribuiti dal d.lgs. 81/2008.

D) Addetti al primo soccorso. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili del soccorso in azienda, in caso di infortuni.

E) Addetti antincendio. Sono le persone designate dal Datore di lavoro ed adeguatamente formate, responsabili dell'attuazione delle misure antincendio e di evacuazione, in caso di emergenza.

F) Il Medico Competente. Medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 d.lgs. 81/08 che collabora, secondo quanto previsto all'articolo 29, comma 1, con il Datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al Decreto Sicurezza (art. 2 d.lgs. 81/08).

G) Il Rappresentante dei Lavoratori per la Sicurezza (RLS). Persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro (art. 2 comma 1, lett. i d.lgs. 81/2008).

H) Lavoratore. Persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione della Società, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite. I lavoratori

di aziende che svolgono per HS attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

I) Gestione degli appalti e dei fornitori. Nei contratti di appalto intesi come contratto di appalto d'opera, di servizi o contratto d'opera o di somministrazione, il Datore di Lavoro in caso di affidamento di lavori, servizi e forniture all'impresa appaltatrice o a Lavoratori autonomi all'interno della propria azienda o Unità produttiva, in conformità alle procedure aziendali, e sempre che abbia la disponibilità giuridica dei luoghi in cui si svolge l'appalto o la prestazione di lavoro autonomo, è chiamato a:

- verificare, con il supporto delle Unità interessate, l'idoneità tecnico-professionale delle imprese appaltatrici o dei Lavoratori autonomi in relazione alle attività da affidare in appalto;
- mettere a disposizione degli appaltatori informazioni dettagliate circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i Lavoratori, attraverso un costante scambio di informazioni con i datori di lavoro delle imprese appaltatrici anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva.

Il Datore di Lavoro committente promuove la cooperazione ed il coordinamento di cui ai punti precedenti elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo i rischi da interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento, e va adeguato in funzione dell'evoluzione dei lavori, dei servizi e delle forniture. L'obbligo di redazione del suddetto documento non sussiste in caso di appalto di servizi di natura intellettuale, mere forniture di materiali o attrezzature, nonché per i lavori o servizi la cui durata non sia superiore ai due giorni, sempre che essi non comportino rischi derivanti dalla presenza delle sostanze di cui all'allegato XI del d.lgs. 81/2008.

6.28 Principi procedurali specifici.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei lavoratori così come individuati dall'art. 15 del Decreto Sicurezza ed in ottemperanza a quanto previsto dagli artt. 18, 19 e 20 del suddetto decreto si prevede quanto segue.

Protocollo 1 – Gestione dei rischi in materia di salute e sicurezza sul luogo di lavoro	
Politiche aziendali in tema di sicurezza	La politica per la sicurezza e salute sul lavoro adottata da HS deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte da HS e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i Lavoratori. A tal fine, è predisposto un adeguato sistema di designazioni o deleghe di funzioni in materia di salute e sicurezza secondo i principi di: • effettività, sussistenza e compresenza di autonomia decisionale e finanziaria del delegato; • idoneità tecnico-professionale del delegato; • vigilanza sull'attività del delegato, non acquiescenza, non ingerenza; • certezza, specificità e consapevolezza. La designazione / delega di funzioni da parte del datore di lavoro deve: • risultare da atto scritto recante data certa; • essere diretta ad un soggetto che possieda tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate; • attribuire al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate; • essere accettata dal delegato per iscritto. Il soggetto delegato deve essere consapevole delle funzioni ad esso delegate. La politica per la sicurezza e salute sul lavoro è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario.
Processo di pianificazione	HS nell'ambito del processo di pianificazione degli obiettivi in tema di salute e sicurezza, con cadenza annuale: • definisce gli obiettivi finalizzati al mantenimento e/o miglioramento del sistema; • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	• La Società ha definito un sistema di comunicazioni interne che assicura che le informazioni relative alla sicurezza fluiscano "dall'alto verso il basso", ma anche "dal basso verso l'alto" ed orizzontalmente rispetto alle varie parti dell'organizzazione. Lo scambio di informazioni tra i differenti livelli e settori

	aziendali è attuato attraverso l'individuazione di referenti interni e di idonei strumenti di comunicazione. Gli strumenti di comunicazione interna possono variare in funzione del tipo di informazione che è necessario fornire avendo però sempre presente che il requisito indispensabile è che le informazioni siano fornite usando una forma ed un modo che le rendano comprensibili alle persone che le devono ricevere. • La Società è convinta che il processo di prevenzione e miglioramento della sicurezza debba vedere coinvolto tutto il personale aziendale. A tale fine ogni lavoratore è incoraggiato a segnalare al proprio responsabile di funzione o direttamente al RSPP eventuali anomalie o proposte di miglioramento. Tali segnalazioni sono raccolte dal RSPP che provvede ad effettuarne un'analisi ed è responsabile di mettere in atto le eventuali azioni conseguenti; la decisione presa in merito è registrata dal RSPP. Il RSPP organizza anche le riunioni periodiche sulla sicurezza prevista dalle norme vigenti e redige e fa sottoscrivere un verbale, mettendolo a disposizione dei partecipanti per la sua consultazione. • È stata definita una procedura per regolamentare le attività di formazione, informazione e addestramento da erogare a: - personale dipendente; - lavoratori con contratto di somministrazione; - stagisti. La procedura definisce anche le modalità in caso di nuove assunzioni e cambi di mansione I contenuti della procedura specificano modalità e responsabilità in merito a: - l'individuazione delle necessità di formazione e addestramento; - la pianificazione e attuazione della formazione; - la registrazione delle attività formative; - la verifica della loro efficacia; - l'informazione e sensibilizzazione del personale sull'igiene e la sicurezza del lavoro. • In merito all'attività di documentazione, HS dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, dei seguenti documenti: - la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro; - il registro degli infortuni; - il Documento di Valutazione dei Rischi indicante la metodologia con la quale si è proceduto alla valutazione dei rischi e contenente il programma delle misure di mantenimento e di miglioramento; - nel caso in cui la Società sia appaltatrice di lavori di costruzione: la documentazione contratti; Piano di Sicurezza e Coordinamento; Fascicolo dell'Opera; verbali di coordinamento relativi alla verifica dell'applicazione da parte delle imprese esecutrici delle disposizioni contenute nel PSC; Piani Operativi di Sicurezza. • HS è altresì chiamata a garantire che: - il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente; - venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal Medico Competente; - venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato
--	---

		medico e data inoltro della pratica; - venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale; - venga conservata la documentazione inerente a regolamenti ed accordi aziendali; - vengano conservati i manuali e le istruzioni per l'uso di macchine, attrezzature e dispositivi di protezione individuale forniti dai costruttori; - venga conservata ogni procedura adottata da HS per la gestione della salute e sicurezza sui luoghi di lavoro; - tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.
Attività di monitoraggio	di	HS deve assicurare un costante ed efficace monitoraggio del sistema per la gestione della salute e della sicurezza sui luoghi di lavoro. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione della salute e della sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta HS, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. HS garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.
Riesame sistema	del	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema adottato da HS per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame annuale da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.
Gestione operativa degli appalti		HS deve predisporre e tenere aggiornato un elenco delle aziende con le quali stipula eventuali contratti di appalto. Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti dai quali devono risultare espressi riferimenti agli adempimenti di cui all'art. 26 del Decreto Sicurezza. Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro derivanti dalle interferenze delle lavorazioni. A tali dati possono accedere, su richiesta, il rappresentante dei lavoratori e le organizzazioni sindacali dei lavoratori. Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

6.29 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-septies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti di HS eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla tutela della salute e sicurezza sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la tutela della salute e della sicurezza nei luoghi di lavoro, in coerenza con quanto stabilito nel presente Modello e all'art. 30 del Decreto Sicurezza;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati da HS tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il Delegato della Sicurezza Aziendale e il RSPP;
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

HS garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti di HS (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; gli Addetti al Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso).

6.30 Regole di comportamento e Protocolli operativi in materia di reati ambientali (art. 25-undecies del Decreto).

I reati ambientali che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-undecies del d.lgs. 231/2001 sono i seguenti:

- scarichi di acque reflue (art. 137, comma 2, 3, 5, 11, 13 d.lgs. 3 aprile 2006, n. 152);
- attività di gestione di rifiuti non autorizzata (art. 256 comma 1, 3, 5, 6, e artt. 208, 209, 210, 211, 212, 214, 215, 216 d.lgs. 3 aprile 2006, n. 152);
- bonifica dei siti (art. 257 comma 1 e 2, d.lgs. 3 aprile 2006, n. 152);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (articolo 258 del d.lgs. 3 aprile 2006, n. 152);
- traffico illecito di rifiuti (art. 259 d.lgs. 3 aprile 2006 n. 152);
- attività organizzate per il traffico illecito di rifiuti (art. 260 d.lgs. 3 aprile 2006 n. 152);
- sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis d.lgs. 3 aprile 2006 n. 152);
- violazione dei valori limite di emissione (art. 279 d.lgs. 3 aprile 2006 n. 152);
- cessazione e riduzione dell'impiego di sostanze ozono lesive (art. 3 l. 28 dicembre 1993 n. 549).
- inquinamento ambientale art. 452bis, c.p.,
- disastro ambientale art. 452 ter, c.p.,
- traffico e abbandono di materiale radioattivo 452quinqies, c.p.,
- impedimento del controllo 452sexies, c.p.,
- omessa bonifica 452terdecies, c.p.

Le potenziali aree a rischio reato che la Società ha individuato con riferimento ai reati ambientali riguardano tutte le attività svolte nei propri siti e nelle sedi amministrative e societarie nelle quali si svolgono le attività aziendali da parte del personale dipendente. Sono inoltre considerate aree a rischio anche tutte le attività svolte dal personale esterno incidenti sui processi produttivi o comunque sul sistema di gestione ambiente e sicurezza (ad es., fornitori di beni o servizi in base a contratti d'appalto, d'opera o somministrazione).

Le attività sono considerate sensibili avuto riguardo al loro svolgimento sia da parte del personale aziendale, sia da parte di terzi che agiscano su incarico o per conto della Società, ovvero che intrattengono un rapporto contrattuale con la Società, con particolare riferimento al perimetro delle attività loro assegnate ed esercitate sotto la direzione o vigilanza della Società.

Sono da considerare attività sensibili ai fini del presente Modello quelle che possano produrre impatti ambientali significativi sulle matrici ambientali (acqua, aria, suolo, rifiuti, flora, fauna) o comunque tali da imporre misure per il loro contenimento.

In particolare, dovranno considerarsi attività aziendali significative per la tutela delle matrici ambientali le aree nelle quali possano verificarsi condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti ai sensi delle Direttive 2008/99 CE e 2009/123 CE, in quanto provochino o possano provocare il decesso o lesioni gravi alle persone o danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora. Più specificamente, sono considerate sensibili le attività con impatto ambientale diretto (attività industriali, attività produttive, attività dalle quali si originano rifiuti, reflui o emissioni) o indiretto (quali, a titolo esemplificativo, le attività manutentive). Rientrano in tale ambito anche le attività che si svolgono in luoghi ove siano adottate misure a tutela della salute e sicurezza dell'ambiente di lavoro oggetto della valutazione ex art 18, comma 1, lett. q) d.lgs. 81/2008 nonché le attività soggette a procedimenti amministrativi di abilitazione, iscrizione, autorizzazione, nonché a specifici divieti ai sensi del d.lgs. n. 152/2006.

In conformità ai principi generali del Codice Etico e della Politica Ambiente e Sicurezza è preminente e specifico interesse della Società quello di sviluppare i propri investimenti in modo compatibile con il rispetto dell'ambiente, riconosciuto quale bene primario da salvaguardare, perseguendo il miglior equilibrio tra la propria iniziativa economica e la tutela delle esigenze ambientali attraverso il contenimento dell'impatto delle proprie attività ed il rispetto della normativa ambientale.

La Società considera pertanto ogni condotta che direttamente o indirettamente possa generare un pregiudizio anche potenziale all'ambiente come contraria al proprio interesse e respinge ogni condotta elusiva delle procedure aziendali ed inosservante della normativa vigente, dichiarando espressamente che a tali eventuali condotte non corrisponde alcun vantaggio per la Società, bensì la compromissione di ideali e patrimonio aziendali.

In tale contesto, la presente Parte Speciale prevede l'espresso divieto per tutti i Destinatari (i) di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 *undecies* del Decreto) e (ii) di violare i principi illustrati nel presente Modello e porre in essere condotte difformi dalle procedure aziendali previste.

Conseguentemente, i soggetti sopra indicati hanno l'obbligo di rispettare scrupolosamente tutta la normativa vigente ed in particolare di tenere un comportamento corretto, trasparente e

collaborativo, nel rispetto delle norme di legge e delle procedure in tutte le attività aziendali adottate dalla Società, di astenersi dal porre in essere o dare causa a violazioni dei principi comportamentali, dei protocolli e delle procedure aziendali, di rispettare le misure organizzative e preventive dettate per lo svolgimento delle attività produttive ad impatto ambientale ed i relativi oneri informativi, partecipando diligentemente alle sessioni formative ed informative connesse con le mansioni a ciascuno affidate dalla Società.

In tale contesto, ed ai fini di cui sopra, la Società:

- a. determina le politiche ambientali volte a definire gli impegni generali assunti per garantire il rispetto dell'ambiente e l'osservanza delle pertinenti norme applicabili nonché la riduzione degli impatti ambientali connessi alle attività svolte dalla Società;
- b. identifica le norme applicabili in tema di protezione dell'ambiente ed opera in conformità alle stesse;
- c. identifica e valuta i fattori che si originano dall'attività produttiva e che possono modificare lo stato dell'ambiente, la loro significatività, nonché le componenti ambientali che sono influenzate da tali azioni;
- d. fissa gli obiettivi allineati con gli impegni generali definiti nelle politiche di cui al punto a) ed elabora dei programmi per il raggiungimento di tali obiettivi con la definizione di priorità, tempi ed attribuzione delle relative responsabilità – con assegnazione delle necessarie risorse - in materia di protezione dell'ambiente, con particolare riferimento a:
 - attribuzioni di compiti e doveri;
 - attività di tutti i soggetti su cui ricade la responsabilità dell'attuazione delle misure per la protezione dell'ambiente;
- e. sensibilizza la struttura aziendale, a tutti i livelli, al fine di garantire il raggiungimento degli obiettivi prefissati anche attraverso la programmazione di piani di formazione con particolare riferimento a:
 - monitoraggio, periodicità, fruizione e apprendimento;
 - formazione differenziata per soggetti investiti di specifiche funzioni in materia di protezione dell'ambiente e per soggetti addetti a mansioni dalle quali possono derivare impatti ambientali;
- f. attua adeguate attività di monitoraggio, verifica ed ispezione al fine di assicurare l'efficacia delle procedure e dei sistemi di gestione ambientale adottati, in particolare per ciò che concerne:
 - misure di mantenimento e miglioramento;
 - gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme;

- coerenza tra attività svolta e competenze possedute;
- g. attua le necessarie azioni correttive e preventive in funzione degli esiti del monitoraggio;
- h. effettua un periodico riesame al fine di valutare l'efficacia ed efficienza del sistema di gestione ambientale nel raggiungere gli obiettivi prefissati, nonché l'adeguatezza di questi ultimi rispetto sia alla specifica realtà della Società sia ad eventuali mutamenti nell'attività.

In particolare, in conformità ai principi di prevenzione e di precauzione, l'obiettivo del rispetto delle norme comportamentali e delle relative procedure interne prescritte per la tutela dell'ambiente sarà quello di prevenire condotte intenzionali ovvero di grave negligenza alle quali possano conseguire pregiudizi o pericoli di danni rilevanti alla qualità dell'aria, del suolo o delle acque, ovvero alla fauna o alla flora, ovvero che provochino o possano provocare il decesso o lesioni gravi alle persone.

In relazione alle aree a rischio individuate nella presente Parte Speciale, e a integrazione dei presidi e delle procedure aziendali già esistenti, si riportano di seguito specifici principi di comportamento da tenere in osservanza del Decreto.

Protocollo 1 – Rispetto della normativa sull'ambiente	
Politiche aziendali in tema di protezione dell'ambiente	La politica per la protezione dell'ambiente adottata dalla Società deve costituire un riferimento fondamentale per i Destinatari e per tutti coloro che, al di fuori della Società, intrattengono rapporti con la stessa. Tale politica deve essere applicata a tutte le attività svolte dalla Società e deve porsi come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della riduzione degli impatti sull'ambiente. Tale politica contiene: • l'individuazione di un approccio strutturato alla riduzione dell'impatto ambientale e all'incremento della sicurezza che tenga conto di tutte le implicazioni di carattere organizzativo, tecnico, economico, normativo; • l'individuazione dello sviluppo sostenibile della Società e del territorio nel quale essa opera come missione primaria della Società; • l'impegno a ridurre i consumi energetici e di materie prime, privilegiando l'utilizzo di processi e materie prime a minore impatto ambientale; • l'impegno a commercializzare prodotti sempre più compatibili con l'ambiente e sicuri per gli utilizzatori; • l'identificazione e la valutazione degli effetti ambientali e dei rischi dovuti a incidenti, fatti accidentali potenziali, situazioni di emergenza; • l'impegno alla prevenzione ed al miglioramento continuo delle proprie capacità organizzative e tecniche in grado di ridurre l'impatto ambientale e i rischi legati all'attività della Società; • l'impegno a fornire le risorse umane e strumentali necessarie; • l'impegno ad un riesame periodico della politica per l'ambiente al fine di garantire la sua costante adeguatezza alla struttura organizzativa della Società, nonché alla normativa vigente in materia ed alle migliori prassi internazionali; • l'adeguamento continuo alle crescenti esigenze sociali e legislative nel campo della tutela dell'ambiente e della sicurezza, precorrendole, ove possibile, mediante un'adeguata

	pianificazione delle attività e iniziative in tali campi; • l'impegno a definire e diffondere all'interno della Società la conoscenza delle problematiche di tutela dell'ambiente, delle relative discipline tecnico-organizzative nonché gli obiettivi del sistema di gestione ambiente e sicurezza ed i relativi programmi di attuazione. La politica è riesaminata annualmente in base ai risultati del monitoraggio del sistema. Il riesame, il cui esito non dovrà comportare necessariamente delle modifiche alla suddetta politica, potrà inoltre avvenire a seguito di possibili eventi o situazioni che lo rendano necessario. Le procedure interne devono inoltre essere caratterizzate dai seguenti elementi: • separatezza, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni"); • traccia scritta di ciascun passaggio rilevante del processo (c.d. "tracciabilità"); • adeguato livello di formalizzazione. La Società predispone ed adotta inoltre procedure finalizzate ad individuare le modalità e le funzioni responsabili della gestione dei rapporti con le competenti Autorità amministrative, nonché delle ispezioni e degli accertamenti in materia di tutela ambientale e dell'elevazione di contestazioni. In particolare, dovrà essere: • conferita procura speciale ai responsabili delle funzioni coinvolte in ispezioni e/o accertamenti al fine di dotarli del potere di rappresentare la Società dinanzi alla pubblica Autorità (in particolare, Ufficio delle Entrate, Guardia di Finanza, ARPA, ASL, NOE, CFS, MIPAF, NAS, nonché le altre Forze dell'Ordine delegate in materia ambientale) in caso di ispezione e/o accertamento; • conferita apposita delega alla funzione deputata a rappresentare la Società nei confronti dell'Ente di Pubblica Amministrazione concedente un provvedimento amministrativo o nei confronti del quale sia diretta una comunicazione; • prevista la redazione da parte dei procuratori sopra indicati di un report informativo dell'attività svolta nel corso dell'ispezione; • prevista una metodologia di archiviazione della documentazione relativa all'attività in oggetto; • prevista una modalità di comunicazione preventiva dell'avviso di ispezioni (anche periodiche, ad esempio in materia di A.I.A.) ai soggetti responsabili preposti per materia nonché il ruolo di questi ultimi nell'indirizzo, supervisione e controllo; • individuata la modalità con la quale evadere le richieste di informazioni da parte delle Autorità di vigilanza, nonché il flusso informativo verso eventuali ulteriori funzioni o, in caso di necessità ed urgenza, le modalità con le quali informare l'Amministratore Delegato; • prevista un'apposita forma di rendiconto periodico sulla gestione di tali fasi all'Organismo di Vigilanza. Devono inoltre essere osservati i seguenti ulteriori principi procedurali specifici, da integrarsi con le procedure di sistema e istruzioni di processo, di controllo operativo ed emergenze previste dal sistema integrato di gestione ambiente e sicurezza adottato dalla Società: • devono essere specificamente individuate e rigorosamente rispettate le procedure di monitoraggio dei processi produttivi e le procedure di emergenza previste per il caso di incidenti; • devono essere individuate e rigorosamente osservate specifiche procedure di monitoraggio e controllo delle emissioni e degli scarichi; • devono essere previste e rigorosamente rispettate le procedure operative di gestione dei rifiuti adottate dalla Società in conformità alle disposizioni di cui al d.lgs. n. 152/06 nonché le procedure amministrative di gestione dei rifiuti applicabili alle diverse tipologie di rifiuti prodotti dalla Società, con particolare riferimento agli adempimenti di comunicazione, tenuta dei registri obbligatori e dei formulari e/o agli adempimenti prescritti dal sistema informatico di controllo
--	---

	della tracciabilità dei rifiuti (ex SISTRI oggi "Registro elettronico nazionale per la tracciabilità dei rifiuti"); • devono essere definiti e rigorosamente osservati specifici protocolli relativi all'assunzione delle misure di prevenzione e messa in sicurezza di emergenza che si rendano eventualmente necessarie nell'ipotesi di eventi idonei a determinare situazioni di potenziale contaminazione di suolo, sottosuolo, acque superficiali o sotterranee e/o di potenziale impatto sulla flora e fauna; • non devono essere utilizzate o detenute le sostanze di cui alla tabella A allegata alla legge 28 dicembre 1993, n. 549. La Società: • svolge, a favore dei Destinatari, in modo differenziato ed adeguato ai rispettivi compiti e responsabilità, un'attività di formazione finalizzata alla conoscenza della normativa applicabile ai processi e delle procedure di gestione ambientale adottate dalla Società; • adotta i necessari presidi affinché i processi produttivi si svolgano in condizioni controllate; • predispone le procedure atte a definire, per i processi produttivi suscettibili di dar luogo a impatti sull'ambiente, le modalità di lavoro, i valori dei parametri operativi, i criteri di accettabilità, le registrazioni da produrre; • adotta procedure di emergenza volte a evitare o mitigare gli effetti di incidenti; • definisce le condizioni per tenere sotto controllo i parametri dei processi produttivi; • predispone ed attua programmi di formazione.
Processo di pianificazione	La Società, nell'ambito del processo di pianificazione degli obiettivi in tema di protezione dell'ambiente, con cadenza annuale: • determina i criteri di valutazione idonei a dimostrare l'effettivo raggiungimento degli obiettivi stessi; • predispone un piano per il raggiungimento di ciascun obiettivo, l'individuazione delle figure/strutture coinvolte nella realizzazione del suddetto piano e l'attribuzione dei relativi compiti e responsabilità; • definisce le risorse, anche economiche, necessarie, verificandone l'adeguatezza con riguardo all'impiego ed al raggiungimento degli obiettivi attraverso le attribuzioni dell'annualità precedente e disponendo ogni eventuale adeguamento od implementazione delle risorse stesse; • prevede le modalità di controllo periodico e consuntivo dell'effettivo ed efficace raggiungimento degli obiettivi attraverso la verifica della finalizzazione dell'impiego delle risorse attribuite alle competenti funzioni.
Informazione, formazione, documentazione	<u>L'informazione</u> L'informazione che la Società riserva ai Destinatari deve essere facilmente comprensibile e deve consentire agli stessi di acquisire la necessaria consapevolezza in merito a: • l'importanza di rispettare la politica ambientale e gli obiettivi individuati dalla Società; • le conseguenze derivanti dallo svolgimento della propria attività in modo non conforme alla politica ambientale e agli obiettivi individuati dalla Società ; • il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità alla politica aziendale ed alle procedure in materia di protezione dell'ambiente e ad ogni altra prescrizione relativa al sistema di gestione ambientale adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale. Ciò premesso, la Società in considerazione dei diversi ruoli e responsabilità dei Destinatari, è tenuta ai seguenti oneri informativi: • la Società deve fornire adeguata informazione ai Destinatari circa i rischi di impatti negativi sull'ambiente derivanti dall'attività dell'impresa, sulle conseguenze di questi e sulle procedure operative da adottare;

- la Società deve organizzare periodici incontri tra le funzioni preposte alla protezione dell'ambiente;
- la Società deve coinvolgere i responsabili di settore nell'organizzazione dell'attività di rilevazione e valutazione dei rischi e di prevenzione.

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione.

Formazione

- La Società deve fornire adeguata formazione al personale addetto ad attività che possono avere un'incidenza sull'ambiente;
- i responsabili per la Sicurezza sul Lavoro devono partecipare alla stesura del piano di formazione;
- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai contenuti della mansione cui il lavoratore è in concreto assegnato ed ai possibili impatti della relativa attività sull'ambiente;
- deve essere predisposto uno specifico piano di formazione per i lavoratori addetti ad attività da cui possano derivare impatti ambientali significativi;
- i lavoratori che cambiano mansione e quelli trasferiti a compiti da cui possano derivare impatti ambientali devono fruire di formazione preventiva, aggiuntiva e specifica;
- gli addetti a specifici compiti in materia di protezione dell'ambiente devono ricevere specifica formazione;
- la Società deve effettuare periodiche esercitazioni finalizzate all'adozione del corretto comportamento in caso di incidenti o di emergenze di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, anche mediante apposita verbalizzazione, e deve essere ripetuta periodicamente.

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione ambientale, la Società deve garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Destinatari.

Pertanto, la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

- dal basso verso l'alto: è garantito dalla Società il diritto-dovere dei Destinatari di portare a conoscenza proposte ed esigenze di miglioria inerenti alla gestione ambientale;
- dall'alto verso il basso: ha lo scopo di diffondere a tutti i Destinatari la conoscenza del sistema adottato dalla Società per la gestione ambientale.

A tale scopo la Società garantisce agli esponenti aziendali (ovvero gli amministratori, i dirigenti, i componenti del Collegio Sindacale e i dipendenti della Società) un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- nuovi rischi in materia di protezione dell'ambiente;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione dell'ambiente;
- contenuti delle procedure aziendali adottate per la gestione dell'ambiente;
- ogni altro aspetto inerente alla gestione dell'ambiente.

Documentazione

La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, oltre ai documenti sopra indicati, anche dei seguenti documenti:

- la documentazione inerente alle norme relative alla protezione dell'ambiente rilevanti per

	l'attività aziendale; • le autorizzazioni ambientali relative all'esercizio dell'attività della Società; • i registri relativi a taratura e manutenzione delle apparecchiature di sorveglianza; • la documentazione relativa all'attività di sorveglianza ed alle misurazioni; • i piani di emergenza; • le informazioni relative ai Fornitori; • il registro degli incidenti e delle azioni correttive attuate; • tutta la documentazione relativa alle attività di Informazione e Formazione che dovrà essere conservata a cura del responsabile per la Sicurezza sul Lavoro.
Attività di monitoraggio	La Società deve assicurare un costante ed efficace monitoraggio del sistema di gestione ambientale. A tale scopo: • assicura un costante monitoraggio delle misure preventive e protettive predisposte nell'ambito del sistema di gestione ambiente e sicurezza; • assicura un costante monitoraggio dell'adeguatezza e della funzionalità del sistema di gestione ambiente e sicurezza a raggiungere gli obiettivi prefissati e della sua corretta applicazione; • compie approfondita analisi con riferimento ad ogni incidente verificatosi, al fine di individuare eventuali lacune nel sistema di gestione ambientale e di identificare le eventuali azioni correttive da intraprendere. Al fine di adempiere adeguatamente all'attività di monitoraggio ora descritta la Società, laddove la specificità del campo di intervento lo richiedesse, farà affidamento a risorse esterne con elevato livello di specializzazione. La Società garantisce che gli eventuali interventi correttivi necessari vengano predisposti nel più breve tempo possibile.
Riesame del sistema	Al termine dell'attività di monitoraggio di cui al precedente paragrafo, il sistema di gestione ambientale adottato dalla Società è sottoposto ad un riesame annuale da parte della Società, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. Della suddetta attività di riesame e degli esiti della stessa deve essere data evidenza su base documentale.

6.31 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- effettuare verifiche periodiche sul rispetto della presente Parte Speciale, valutando periodicamente l'efficacia della stessa a prevenire la commissione dei Reati di cui all'art. 25-undecies del Decreto. A questo proposito, l'Organismo di Vigilanza - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà ai soggetti competenti della Società eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle norme sulla

protezione dell'ambiente, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale, volte ad assicurare la protezione dell'ambiente, in coerenza con quanto stabilito nel presente Modello e nel sistema di gestione ambiente e sicurezza adottato dalla Società;
- c. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati dalla Società tra le funzioni preposte alla tutela dell'ambiente valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- incontrare periodicamente il responsabile per la Sicurezza sul Lavoro.
- accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

La Società garantisce, a favore dell'Organismo di Vigilanza, flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli incidenti verificatisi, delle modifiche dei processi produttivi aventi un impatto sull'ambiente, nonché delle implementazioni dei sistemi di gestione ambiente e sicurezza.

Nell'espletamento delle attività di cui sopra, l'Organismo di Vigilanza può avvalersi di tutte le risorse competenti della Società.

3 SEZIONE G – SETTORE ACQUISTI.

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Acquisti di HS.

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte dal responsabile e dai suoi sottoposti del predetto settore, sono quelle descritte nella tabella che segue:

SETTORE ACQUISTI (Responsabile Direzione Acquisti [D.A.])	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.); • Gestione delle gare e dei bandi pubblici; • Scelta di fornitori e consulenti;
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto)	Contraffazione, alterazione o uso di marchi.
Reati societari (art. 25-ter)	• Creazione di fondi extracontabili; • Gestione degli ordini e delle fatture; • Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale; • Scelta consulenti/fornitori/partner commerciali.
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	• Scelta consulenti/fornitori/partner commerciali; • Gestione dei flussi finanziari/creazione di fondi extracontabili; • Gestione della liquidità e cassa.
Reati tributari (art. 25-quinquiesdecies del Decreto)	• Gestione della contabilità • Acquisto di beni e servizi • Adempimenti fiscali e tributari in genere • Tenuta e custodia delle scritture contabili e fiscali • Gestione di eventuali operazioni straordinarie •
Reati di contrabbando (art. 25-sexiesdecies)	• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine; • Scarico e deposito delle merci oltre confine • • • •
Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1 del Decreto)	• Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti • Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti • Frode informatica nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale • Ogni altro delitto contro la fede pubblica, contro il patrimonio o che

	comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti
--	---

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

7.1 I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- **malversazione a danno dello Stato**, (art. 316-bis c.p.): *“Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- **indebita percezione di erogazioni a danno dello Stato**, (art. 316-ter c.p.): *“(Comma 1) Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. **La pena è della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.**¹⁶ (Comma 2). Quando la somma indebitamente percepita è pari o inferiore a lire sette milioni settecentoquarantacinquemila si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da dieci a cinquanta milioni di lire. Tale sanzione non può comunque superare il triplo del beneficio conseguito” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- **Truffa** (art. 640, comma 2, n. 1 c.p.): *“(Comma 1). Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la*

¹⁶ Aggiornamento del D.Lgs. 74/2020.

reclusione da sei mesi a tre anni e con la multa da lire cinquecento a diecimila. 2. La pena è della reclusione da uno a cinque anni e della multa da lire tremila a quindicimila:

*1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o **dell'Unione europea**¹⁷ o col pretesto di far esonerare taluno dal servizio militare;*

2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;

2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

(Comma 3). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), *"La pena è della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- **Frode informatica** (art. 640-ter c.p.): *"(Comma 1). Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sè o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. (Comma 2). La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. (Comma 3). La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- **Frode nelle pubbliche forniture** (art. 356 c.p.)¹⁸: *"Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non*

¹⁷ Aggiornamento del D.Lgs. 74/2020.

¹⁸ Fattispecie inserita dal D.Lgs. 75/2020.

inferiore ad euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- **Frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale** (art. 2 L. 898/1986): " (Comma 1). 1. Ove il fatto non configuri il più grave reato previsto dall'articolo 640-bis del codice penale, chiunque, mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il danno o il profitto sono superiori a euro 100.000. Quando la somma indebitamente percepita è pari od inferiore a 5.000 euro si applica soltanto la sanzione amministrativa di cui agli articoli seguenti. (Comma 2). Agli effetti della disposizione del precedente comma 1 e di quella del comma 1 dell'articolo 3, alle erogazioni a carico del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale sono assimilate le quote nazionali previste dalla normativa comunitaria a complemento delle somme a carico di detti Fondi, nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa comunitaria. (Comma 3). Con la sentenza il giudice determina altresì l'importo indebitamente percepito e condanna il colpevole alla restituzione di esso all'amministrazione che ha disposto la erogazione di cui al comma 1" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote.

L'art. 25¹⁹ rubricato "Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", elenca le seguenti fattispecie criminose quali reati suscettibili di far scattare la responsabilità dell'Ente ex Decreto:

- **Peculato** (art. 314, co. 1, c.p.): "Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro [c.p. 458] o di altra cosa mobile altrui [c.c. 812, 814] , se ne appropria, è punito con la reclusione da quattro anni a dieci anni e sei mesi." - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- **Peculato mediante profitto dell'errore altrui** (art. 316): "Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], il quale, nell'esercizio delle funzioni o del

¹⁹ AGGIORNAMENTO: Il D.lgs. n. 75/2020 modifica l'art. 25 D.Lgs. 231/2001, ampliando il catalogo dei reati con le fattispecie di peculato ex artt. 314 e 316 c.p. e di abuso d'ufficio ex art. 323 c.p.

servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni. (Comma 2) La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000²⁰ - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;

- **Concussione** (art. 317 c.p.), *"Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni." - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;;*
- **Corruzione per l'esercizio della funzione** (art. 318 c.p.), *"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da tre a otto anni" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;*
- **Corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), *"Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni." - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- **Circostanze aggravanti** (art. 319 bis c.p.), *"La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene nonché il pagamento o il rimborso di tributi " - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;*
- **Corruzione in atti giudiziari** (art. 319-ter c.p.): *" (Comma 1) Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni. (Comma 2) Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote per il comma 1 e fino a 800 quote per il comma 2;*
- **Induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), *"(Comma 1) Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che,*

²⁰ Comma aggiunto dall'art. 1, comma 1, lett. a), D.Lgs. n. 75/2020.

abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. (Comma 2) Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;

- **Corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), "(Comma 1) Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. (Comma 2) In ogni caso, le pene sono ridotte in misura non superiore a un terzo" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote nel caso di commissione art. 318 c.p. e fino a 600 quote in caso di commissione art. 319 c.p.;
- **Pene per il corruttore** (art. 321 c.p.), "Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;
- **Istigazione alla corruzione** (art. 322 commi 1 e 3 c.p.): "(Comma 1) Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo [...]. (Comma 3) La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- **Istigazione alla corruzione** (art. 322 commi 2 e 4 c.p.): "(Comma 2) Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo [...]. (Comma 4) La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.):** *“Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*
 - 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;*
 - 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;*
 - 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;*
 - 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;*
 - 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;*
 - 5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;*
 - 5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;*
 - 5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;*
 - 5-quinquies) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione²¹.**

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

- 1) alle persone indicate nel primo comma del presente articolo;*

²¹ Numero aggiunto dall'art. 1, comma 1, lett. d), D.Lgs. 14 luglio 2020, n. 75, a decorrere dal 30 luglio 2020.

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi” - Sono previste in capo all'Ente le medesime sanzioni pecuniarie previste per gli artt. 314, 316, da 317 a 320 e 322 terzo e quarto comma c.p.

- **Traffico di influenze illecite** (art. 346 bis c.p.): tale ipotesi delittuosa punisce chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio. Tale fattispecie può concretizzarsi in attività che pongono in relazione due soggetti privati, (uno dei quali funge da intermediario “illecito” verso un pubblico ufficiale o incaricato di pubblico servizio in cambio di un interesse o vantaggio) - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.
- **Abuso d'ufficio** (art. 323 c.p.), “*Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni²². La pena è aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.*

7.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio.

–Pubblica Amministrazione (di seguito “PA”) s'intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

²² Comma così modificato, a decorrere dal 17 luglio 2020, dall'art. 23, comma 1, D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAL, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

- **Pubblici ufficiali e incaricati di un pubblico servizio** Ai sensi dell'art. 357, primo comma, del codice penale, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

La norma chiarisce solo la nozione di "pubblica funzione amministrativa" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da “norme di diritto pubblico”, ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l'art. 358 c.p. definisce i “soggetti incaricati di un pubblico servizio” come quei soggetti “i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”.

Il legislatore puntualizza la nozione di “pubblico servizio” attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della “pubblica funzione”, da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d'ordine e/o la prestazione d'opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

7.3 Regole di comportamento e Protocolli operativi in tema di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001).

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

1. porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
2. porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
3. comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;

4. violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

5. il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
6. tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
7. i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
8. tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
9. qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
10. su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la

responsabilità	documentazione da presentare alla P.A. Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: - proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; - porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; - distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; - presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; - presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: - sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; - ogni eventuale accordo preso con la P.A. sia documentato.
Ispezioni	- Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; - di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; - devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: - la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; - specifici protocolli di controllo e verifica della veridicità e correttezza dei

	documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.
--	--

Protocollo 2 – Scelta di fornitori e consulenti

Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	• I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. • I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. • Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. • Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici

Transazioni finanziarie	• Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio. • In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; • Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto previsto dall'art. 3 della legge n. 136/12010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che dovrà essere necessariamente corredata da idonea documentazione giustificativa.
--------------------------------	--

Irregolarità anomalie	o Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di
----------------------------------	---

Protocollo 4 – Assunzione del personale

Assunzione, gestione, formazione incentivazione dei dipendenti e collaboratori	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato. Il personale che si occupa di transazioni con funzionari pubblici nazionali o stranieri ha l'obbligo di eseguire una certificazione periodica di non aver violato la Parte Speciale del presente Modello.
---	---

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali

Contenziosi/ Contestazioni	• Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. • Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.
---------------------------------------	--

Protocollo 6

- **Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi**
- **Spese di rappresentanza**

Omaggi/Donazioni	Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico.
-------------------------	--

7.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- c. esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- d. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- e. curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

7.5 Regole di comportamento e Protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta DESIDERIO TAGLIENTI, la quale stanno implementando un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito la Società implementando le proprie procedure interne in materia di protezione dei dati personali, attraverso l'adozione un software che permette:

- l'identificazione univoca degli utenti, attraverso un ID, un Identity Provider utilizzabile per eseguire l'accesso e l'autenticazione a norma a tutti gli applicativi e servizi in *cloud*;
- la crittazione dei dati sensibili, (ad es. dichiarazioni di appartenenza ad organizzazioni sindacali, dati relativi allo stato di salute, ecc.), attraverso cifratura delle informazioni per rendere i dati inaccessibili al di fuori dell'applicazione software, tenendo conto anche del contesto e delle finalità del trattamento, nonché del rischio per i diritti degli interessati;
- il log delle attività per l'archiviazione e la consultazione dei log delle attività previsti dalla nuova normativa.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;
- e. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali		
Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica		In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il

	traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test</i>, <i>penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati; Inoltre: • l'utilizzo del servizio aziendale di posta elettronica che deve essere effettuato nel rispetto del Codice Etico aziendale, impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale; • ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
--	--

	• impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software, ecc.</i>); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	--

7.6 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

7.7 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con apposita clausola sottoscritta dal cliente, la Società non si riservi, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti

Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti	La regolamentazione dell'attività descritta deve prevedere che: • i Destinatari si accertino che i dipartimenti di <i>patent e trademark</i> internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al
---	--

	deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto; • in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di <i>patent</i> e <i>trademark</i> internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto. • I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti. Inoltre, è fatto espressamente divieto di: • contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati; • contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati; • introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati; • detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto; • consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita; • porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto; • adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto; • contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari; • introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: • abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102-quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; • riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre
---	--

	cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; • in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; • detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; • duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; • riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; • pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; • importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	---

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE	
Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o

	imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
--	--

7.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

7.9 Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001).

Nell'ambito della riforma del diritto societario, il Decreto Legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter del Decreto, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. "reati societari".

I reati societari sono reati propri e, in quanto tali, possono essere commessi direttamente da:

- Consiglio di Amministrazione;
- Amministratori;
- Direttori Generali;
- Sindaci;
- Liquidatori;
- Sottoposti alla direzione e alla vigilanza dei soggetti sopra elencati nel caso di corruzione tra privati;
- nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

Le fattispecie di reati societari considerate sono:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- falso in prospetto (art. 173-bis, T.U.F.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3 c.c.) [modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019];
- istigazione alla corruzione tra privati (art. 2635-bis c.c.) [introdotto dal D.Lgs. n. 38/2017];
- illecita influenza sull'assemblea (art. 2636 c.c.);

- aggrottaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-ter del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

- a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società. A questo proposito, è fatto espresso divieto di:
 - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Società;
 - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;
- c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività aziendale, fino alle fasi eventuali di liquidazione o cessazione della Società;
- e. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

- f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
 - esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
 - porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
 - predisporre procedure per la preparazione del bilancio e la gestione delle risorse finanziarie;
 - inoltre,
 - il presente Modello deve essere portato adeguatamente a conoscenza di tutto il personale, non solo dirigente, e appositi meccanismi di comunicazione (ad esempio tramite poster nelle sale comuni o pubblicazioni periodiche) devono essere predisposti in modo da permettere la conoscenza di modifiche e/o aggiornamenti del Modello stesso e deve essere attivato un programma di informazione/formazione a favore del personale addetto atto a prevenire la commissione di reati societari;
 - tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o di conflitto di interesse, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili, le attività finalizzate alla formazione del bilancio e le altre comunicazioni sociali siano accurati e trasparenti.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi

settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente contabile esterno non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1 • Predisposizione del bilancio; • Tenuta delle scritture contabili e dei Libri Sociali; • Gestione degli ordini e delle fatture.	
Definizione dei ruoli e responsabilità	Devono essere osservate specifiche procedure che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione della contabilità, predisposizione dei bilanci, dei rendiconti, prevedendo controlli in ordine alla completezza e veridicità delle informazioni contenute nei singoli documenti finali; • individuino la funzione e il soggetto deputato a gestire per conto di HS la contabilità ed il processo di formazione dei documenti contabili, cui conferire apposita delega e procura scritta. Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione Operativa	In aggiunta ai presidi aziendali già esistenti, si dispone: • la trasmissione agli amministratori e al collegio sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del consiglio di amministrazione o sui quali esso debba esprimere un parere ai sensi di legge; • la previsione di riunioni periodiche tra il collegio sindacale e l'Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di <i>Corporate Governance</i>. Inoltre, per la predisposizione delle comunicazioni ai Soci relative alla situazione economica, patrimoniale e finanziaria della Società, si dispone che la redazione delle stesse sia effettuata determinando in maniera chiara e completa: • i dati e le informazioni che ciascuna funzione deve fornire; • i criteri contabili per l'elaborazione dei dati; • la tempistica per la loro consegna alle aree aziendali responsabili. Infine, in caso di comunicati stampa e ogniqualvolta vengano diffuse all'esterno notizie aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società, si dispone che chi diffonde tali informazioni, oltre ad osservare i principi suindicati, deve attenersi esclusivamente alle informazioni desumibili da documenti già approvati e resi pubblici.

Protocollo 2

- **Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni);**
- **Creazione di fondi extracontabili.**

Gestione operativa

- Le modalità di gestione delle operazioni societarie devono essere condotte in maniera veritiera e corretta, coerentemente e nel rispetto dei principi di *Corporate Governance* adottati dal Consiglio di Amministrazione.
- Deve esistere una segregazione di ruoli e responsabilità tra chi evidenzia la necessità di un'operazione, chi la esegue e chi effettua il relativo controllo.
- Per ogni documentazione predisposta deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi.
- Tutta la documentazione deve contenere elementi assolutamente veritieri e devono essere coerenti all'oggetto per cui sono stati richiesti. A tal fine tutta la documentazione relativa alle operazioni societarie deve essere archiviata in un apposito fascicolo con sottoscrizione del responsabile della funzione.
- E' inoltre necessario che sia previsto quanto segue:
 - un programma di formazione – informazione del personale impiegato nella predisposizione della documentazione attinente le operazioni societarie;
 - un monitoraggio dei poteri anche con riferimento alla verifica delle firme dei documenti inerenti le operazioni societarie;
 - la documentazione redatta ed in genere ogni altra informazione formalizzata deve contenere solo elementi assolutamente veritieri.

Protocollo 3 – Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale
Identificazione dei soggetti responsabili

- Nella gestione dei rapporti con il collegio sindacale, società di revisione e soci devono essere osservate le seguenti disposizioni:
- identificazione del personale all'interno di HS preposto ad interloquire con il collegio sindacale e alla trasmissione della relativa documentazione;
 - possibilità per il Collegio Sindacale e della società di revisione di prendere contatto con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possono presentare aspetti di criticità in relazione ai reati societari.

Protocollo 4

- **Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti;**
- **Gestione della liquidità.**

Gestione del processo di acquisizione di nuova clientela e di gestione della clientela acquisita

- In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento:
- agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con clienti o altre controparti contrattuali;
 - garantire una segregazione di funzioni e responsabilità e una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione delle vendite, in particolare tra responsabilità nei rapporti con il cliente (cd. *account manager*), responsabilità nella definizione del prezzo di offerta e delle condizioni/tempi di pagamento (e relative penali), responsabilità nella definizione di eventuali risoluzioni transattive in caso di controversie;

	- individuare criteri generali e trasparenti per la determinazione di un prezzo massimo di offerta per singolo prodotto o servizio, di modo che qualunque anomalia possa essere agevolmente rilevata. In caso di qualsivoglia criticità sorta nell'ambito dei rapporti sopra descritti, deve essere informato l'Organismo di Vigilanza con nota scritta. In particolare, vi è l'obbligo di comunicare: - le operazioni di vendita superiori ad un dato importo che potrà rappresentare la soglia di rischio; - le operazioni di vendita superiori di una data percentuale rispetto al prezzo medio del prodotto, come risultante dai criteri generali suddetti; - tutte le operazioni di incasso al di sotto dei termini standard di pagamento (ad esempio, fatture pagate a vista).
Assegnazione/gestione degli incarichi e delle consulenze esterne	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: - agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con fornitori o altre controparti contrattuali; - garantire una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione degli acquisti, in particolare tra funzione che individua e seleziona il fornitore, il consulente o il prestatore di servizi, funzione che ratifica la c.d. entrata merci, funzione che autorizza il pagamento e funzione che effettua il controllo di gestione e la tracciabilità delle operazioni; - effettuare una pianificazione dell'attività di <i>benchmarking</i> (raffronto con i valori economici di mercato); - predisporre adeguati protocolli aziendali per acquisti di beni e servizi, affidamento di consulenza ed altre prestazioni professionali e gestione del magazzino.
Selezione e gestione del personale	La regolamentazione dell'attività descritta deve prevedere: - una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; - un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; - l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; - la gestione dell'incentivazione dei dipendenti e collaboratori; - la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; - il monitoraggio di ogni eventuale conflitto di interessi da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato.
Gestione del marketing ed eventuale omaggistica clienti comprese le organizzazioni no profit	Con riguardo alla formazione del personale dipendente e amministrativo, sono prescritte le seguenti e ulteriori regole di comportamento: - divieto di offrire, sollecitare, istigare o ricevere da terzi, direttamente o indirettamente, o di accettare la promessa di ricevere omaggi, benefici o altre utilità, a meno che questi omaggi, benefici e utilità abbiano "modico valore" e rientrino nei limiti della normale cortesia e non abbiano lo scopo di influenzare decisioni aziendali o creare obblighi nei confronti di terzi o di compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. In particolare: - le spese di rappresentanza devono essere limitate a pranzi o cene di lavoro; - i c.d. omaggi a clienti sono da limitare alla gadgettistica o ad oggetti di puro

	valore simbolico, meglio ancora se riportanti il marchio dell'azienda per collegarli a finalità pur sempre commerciali, con la previsione di un listino; • proibire liberalità che non siano inquadrare in programmi generali di <i>social responsibility</i>, come sponsorizzazioni sportive di club, associazioni, ecc. riconducibili ad un ente/cliente o a suoi singoli manager; • prevedere una chiara casistica ed un flusso di comunicazioni verso l'Organismo di Vigilanza affinché si possa vigilare su eventuali abusi, attraverso l'analisi incrociata con altri dati, ad esempio quelli relativi alle commesse acquisite; • prevedere che chiunque riceva tali richieste o offerte, eccezione fatta per omaggi di modico valore, debba informarne "il responsabile della funzione aziendale competente"; • prevedere, nell'informativa comunicata ai clienti/fornitori, che ogni violazione dei principi contenuti nel Codice Etico rappresenta una violazione contrattuale; • prevedere l'obbligo per i clienti/fornitori di conformarsi al Codice Etico prima di poter avere rapporti commerciali con la società.
Partecipazione a gare indette da soggetti privati e gestione dei rapporti con il cliente in caso di vittoria di una gara	È necessario che sia previsto quanto segue: • una corretta applicazione della procedura di partecipazione ai bandi privati sia con riferimento alla fase di ricezione (fonte interna e/o fonte esterna) dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui su è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, che alla predisposizione e spedizione della documentazione all'Ente (o alla capofila) che indica il relativo bando; • una verifica dell'esistenza di eventuali conflitti di interessi con riferimento anche alla possibilità di partecipare o meno al bando. Inoltre, devono essere previste regole di comportamento che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione delle varie fasi dei rapporti con partner/terze parti ed altri soggetti privati in genere, prevedendo controlli in ordine alla regolarità dei requisiti di ammissione degli stessi ad eventuali bandi di gara privati o all'ottenimento di contributi, sovvenzioni e finanziamenti privati; • individuino la funzione e la persona fisica deputata a rappresentare l'azienda nei confronti dei terzi privati, cui conferire apposita delega e procura e stabiliscano forme di riporto periodico dell'attività svolta verso il responsabile della funzione competente a gestire tali rapporti; Infine, il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.

7.10 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a

rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato *reporting* verso gli organi deputati, ecc.);

- b. monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;
- c. verificare annualmente i principali atti societari ed in particolare la relazione del Collegio Sindacale e della Società di Revisione nonché il rispetto delle procedure per la diffusione delle comunicazioni rivolte ai Soci, dei comunicati stampa e delle notizie scritte rivolte all'esterno aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società al fine di verificare l'osservanza della presente Parte Speciale nonché la sua idoneità a prevenire i reati ivi elencati;
- d. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- e. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- f. curare l'aggiornamento del Modello, indicando al consiglio di amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

7.11 Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies).

I reati di cui all'art. 25-octies del d.lgs. 231/2001 sono i seguenti:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
- Autoriciclaggio (art. 648-ter 1 c.p.)

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di:

- a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-octies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente diventarlo;

- b) intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo, persone legate all'ambiente del riciclaggio, del terrorismo, al traffico di droga, all'usura, ecc.;
- c) utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti;
- d) accettare rapporti contrattuali con clienti o altre controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI;
- e) effettuare elargizioni in denaro ad individui, società od organizzazioni condannate per aver svolto attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico;
- f) avere contatti con individui inseriti nelle *black list* antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea.

Inoltre è previsto, a carico dei Destinatari, l'espresso obbligo di:

- g) richiedere tutte le informazioni necessarie al fine di valutare l'affidabilità, la solidità economica e l'attendibilità commerciale/ professionale dei fornitori e del partner;
- h) assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- i) tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti;
- j) prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri.

Protocollo 1 - Scelta consulenti, fornitori, partner commerciali

Selezione dei partner e dei fornitori	Si riportano di seguito specifiche regole di comportamento da tenere in osservanza del Decreto: • la Società procede alla selezione dei Partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri oggettivi e documentabili, verificandone l'attendibilità commerciale attraverso: – verifica ex ante, conservando evidenza dei dati raccolti, che i soggetti con cui intrattiene rapporti contrattuali, anche lavorativi, abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI e non siano inseriti nelle <i>black list</i> antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea. – visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni estere; – referenze da parte di altri soggetti già in rapporti con la Società o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione;
--	--

	– ove possibile, certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere; • la Società inserisce nei contratti con i Partner commerciali una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali di HS e dei principi contenuti nel Modello e si impegnano al rispetto degli stessi; il mancato rispetto dei comportamenti etici o false dichiarazioni relative alla situazione del Partner comporteranno l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto; • la Società verifica l'attendibilità commerciale e professionale dei Fornitori, perlomeno di una certa rilevanza (da concordare un limite di importo di fornitura superato il quale procedere alle verifiche) attraverso: – visure ordinarie presso la Camera di Commercio o certificati equivalenti per Fornitori stranieri; – certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti per fornitori stranieri; – analisi del Fornitore per verificarne la coerenza con le prestazioni richieste dalla Società. Inoltre, è previsto, a carico dei Destinatari, l'espresso obbligo di tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 2 – Gestione dei flussi finanziari/creazione di fondi extracontabili e gestione della liquidità e cassa	
Gestione di investimenti	Si prevede l'espresso divieto di: • utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti; • effettuare elargizioni in denaro, in particolare ad individui, società od organizzazioni condannate per aver svolto attività illecite. Inoltre, è previsto l'obbligo di assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
Monitoraggio flussi finanziari	La Società effettua un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo), degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie. Inoltre, si prevede che: • nel caso di elargizioni di danaro ad individui, società o organizzazioni è necessario controllare la serietà e la professionalità del destinatario del denaro. Inoltre deve essere redatto un piano d'investimento a giustificazione dell'investimento, comprensivo di controlli periodici dell'avanzamento del piano; • in caso di <i>Joint Venture</i>, la Società proceda alla verifica della congruità economica dell'investimento, avendo riguardo, nello specifico, al rispetto dei prezzi medi di mercato, all'utilizzo di professionisti di fiducia per l'effettuazione della <i>due diligence</i>; • la Società presti particolare attenzione ai pagamenti ricevuti da istituti di

	credito/clienti/partner/fornitori esteri. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 3 – Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio

Gestione organizzativa ed operativa	L'eventuale coinvolgimento di consulenti, intermediari, agenti, promotori finanziari e broker a supporto della prestazione dei servizi della Società presuppone un'adeguata conoscenza degli stessi e la verifica, anche mediante attestazione degli interessati, della sussistenza dei requisiti di onorabilità previsti dalla legge e dell'assenza di situazioni di conflitto di interesse in capo ad essi. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

Protocollo 4 – Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà

Gestione organizzativa ed operativa	La Società deve definire e rispettare i criteri che regolano la scelta delle associazioni/fondazioni in favore delle quali effettuare donazioni od erogazioni liberali di qualsiasi tipo, in modo che sia possibile accertare l'effettiva finalizzazione dell'iniziativa a scopi umanitari che non dissimolino attività di riciclaggio o terrorismo. In particolare: • donazioni e/o erogazioni liberali di qualsiasi tipo sono effettuate sulla base di una lista di associazioni/fondazioni accreditate quali potenziali beneficiarie. Le modalità d'inserimento, mantenimento ed eliminazione delle associazioni/ fondazioni da tale lista sono debitamente formalizzate; • donazioni ed erogazioni liberali di qualsiasi tipo sono operate solo ove adeguatamente autorizzate, formalizzate e rendicontate; • la Società non effettua donazioni né erogazioni liberali di qualsiasi tipo tramite versamenti in contanti o su conti correnti cifrati. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

7.12 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-octies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di reati di riciclaggio, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

7.13 Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25-quinquiesdecies del Decreto).

Il Decreto Legge n. 124 del 26 ottobre 2019, convertito con modificazioni nella Legge n. 157 del 19 dicembre 2019, ha introdotto i reati tributari nell'elenco dei reati presupposto della responsabilità amministrativa degli enti.

Con l'inserimento nel Decreto 231 dell'art. 25-quinquiesdecies viene prevista, dunque, una nuova responsabilità nei confronti dell'ente in caso di commissione, nel suo interesse o a suo vantaggio, di alcuni dei reati tributari contemplati nel D.Lgs. 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205".

Successivamente, il 30 luglio 2020, il D.Lgs. 75/2020 (in adempimento alla Direttiva UE/2017/1371 c.d. "PIF") ha esteso ulteriormente il catalogo dei reati tributari presupposto per la responsabilità dell'ente.

Sotto il profilo strettamente fiscale, la Direttiva PIF prevede come soglia minima di tutela la repressione di gravi frodi IVA, ossia di tutte quelle *"azioni od omissioni di carattere intenzionale secondo la definizione di cui all'art. 3, paragrafo 2, lettera d), [che] siano connesse al territorio di due o più Stati membri dell'Unione e comportino un danno complessivo pari ad almeno 10 mln di euro"*, ferma restando la facoltà per la legislazione nazionale di mantenere o adottare norme più rigorose.

Al fine di comprendere cosa possa essere considerato come *"frode che lede gli interessi finanziari dell'Unione"* la menzionata Direttiva, all'art. 3, paragrafo 2, lettera d), precisa che la suddetta frode è l'azione od omissione commessa in sistemi fraudolenti transfrontalieri in relazione:

- i) *all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti relativi all'IVA, cui consegua la diminuzione di risorse del bilancio dell'Unione;*
- ii) *alla mancata comunicazione di un'informazione relativa all'IVA in violazione di un obbligo specifico, cui consegua lo stesso effetto;*

iii) alla presentazione di dichiarazioni esatte relative all'IVA per dissimulare in maniera fraudolenta il mancato pagamento o la costituzione illecita di diritti a rimborsi dell'IVA".

Si riporta di seguito il testo dell'art. 25-quinquiesdecies del D. Lgs. 231/2001.

art. 25-quinquiesdecies

Reati tributari

* * *

"1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
- d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
- g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
- b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;

c) per il delitto di indebita compensazione previsto dall'articolo 10 quater, la sanzione pecuniaria fino a quattrocento quote.

d) Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

3. Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) ”.

Ai fini della normativa tributaria di cui al Decreto Legislativo 10 marzo 2000, n. 74 rubricato “Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell’articolo 9 della Legge 25 giugno 1999, n. 205”, si applicano le seguenti definizioni di carattere generale applicabili a tutti i reati tributari:

- per *"fatture o altri documenti per operazioni inesistenti"* si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, (i) emessi a fronte di operazioni non realmente effettuate in tutto o in parte o (ii) che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero (iii) che riferiscono l'operazione a soggetti diversi da quelli effettivi;
- per *"elementi attivi o passivi"* si intendono (i) le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e (ii) le componenti che incidono sulla determinazione dell'imposta dovuta;
- per *"dichiarazioni"* si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
- il *"fine di evadere le imposte"* e il *"fine di consentire a terzi l'evasione"* si intendono comprensivi, rispettivamente, anche (i) del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e (ii) del fine di consentirli a terzi;
- riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il *"fine di evadere le imposte"* ed il *"fine di sottrarsi al pagamento"* si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
- per *"imposta evasa"* si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della

scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

- le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
- per "*operazioni simulate oggettivamente o soggettivamente*" si intendono (i) le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero (ii) le operazioni riferite a soggetti fittiziamente interposti;
- per "*mezzi fraudolenti*" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

7.14 La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto).

Le nuove fattispecie di reati tributari introdotte nell'elenco dei reati suscettibili di rilevare secondo il Decreto 231, sono dunque le seguenti:

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74).

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

- **Dichiarazione fraudolenta mediante altri artifici** (art. 3, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si configura allorché, fuori dai casi previsti dall'articolo 2 (di cui sopra), al fine di evadere le imposte sui redditi o sul valore aggiunto, il soggetto autore del reato - (i) compiendo operazioni simulate oggettivamente o soggettivamente ovvero (ii) avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria - indichi in una delle dichiarazioni relative a dette imposte (a) *elementi attivi per un ammontare inferiore a quello effettivo* o (b) *elementi passivi fittizi* o (c) *crediti e ritenute fittizi*, quando, congiuntamente:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, (i) è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, (ii) è superiore a euro un milione cinquecentomila, ovvero (iii) qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della norma non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

- **Emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma 1 e comma 2-bis, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Ai fini di quanto sopra indicato, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

- **Occultamento o distruzione di documenti contabili** (art. 10, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, (i) al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero (ii) di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

- **Sottrazione fraudolenta al pagamento di imposte** (art. 11, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza:

a) allorché un soggetto - (i) al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero (ii) di interessi o sanzioni amministrative relativi a dette imposte di ammontare

complessivo superiore ad euro cinquantamila - aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

b) allorché un soggetto - al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori - indica nella documentazione presentata ai fini della procedura di transazione fiscale (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

- **Dichiarazione infedele ex art. 4 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Si realizza qualora un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- a. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- b. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso ***“nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro”***, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Omessa dichiarazione ex art. 5 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Tale fattispecie punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. Punisce, altresì, chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Indebita compensazione ex art. 10-quater D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).

Tale ipotesi delittuosa si configura qualora un soggetto non versi le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti o crediti inesistenti, per un importo annuo superiore a cinquantamila euro.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

7.15 Sanzioni nei confronti dell’Ente.

In relazione alla commissione dei reati sopra elencati si applicano le seguenti sanzioni pecuniarie:

- art. 2 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 3 - Dichiarazione fraudolenta mediante altri artifici: sanzione pecuniaria fino a 500 quote;
- art. 8 - Emissione di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 10 - Occultamento o distruzione di documenti contabili: sanzione pecuniaria fino a 400 quote;
- art. 11 - Sottrazione fraudolenta al pagamento di imposte: sanzione pecuniaria fino a 400 quote;
- art. 4 - Dichiarazione infedele: sanzione pecuniaria fino a 300 quote;
- art. 5 - Omessa dichiarazione: sanzione pecuniaria fino a 400 quote;
- art. 10-quater - Indebita compensazione: sanzione pecuniaria fino a 400 quote.

Nei casi previsti dai commi 1 e 2 dell'art. 25-quinquiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

7.16 Aumenti delle sanzioni nei confronti dell'ente

Le sanzioni pecuniarie sono aumentate di un terzo qualora, a seguito alla commissione dei delitti di cui trattasi (indicati nel comma 1 dell'art. 25-quinquiesdecies), l'ente abbia conseguito un profitto di rilevante entità.

7.17 Aree a rischio reato e processi sensibili

I processi sensibili individuati da HS che presentano il rischio di commissione dei reati di cui alla presente sezione riguardano le seguenti attività:

- Gestione della contabilità: con riferimento alla gestione della fatturazione attiva e passiva e all'emissione e contabilizzazione di fatture e altra documentazione afferente alla contabilità;
- Acquisto di beni e servizi - con riferimento all'attività di selezione e gestione dei fornitori esterni e di eventuali subappaltatori;
- Adempimenti fiscali e tributari in genere: con riferimento a i) predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere, ii) calcolo obbligazioni tributarie, iii) gestione adempimenti dichiarativi e contributivi e iv) pagamento delle imposte;
- Tenuta e custodia delle scritture contabili e fiscali: con riferimento alla conservazione, tracciabilità ed archiviazione di tutta la documentazione contabile e fiscale;
- Gestione di eventuali operazioni straordinarie: con riferimento ad eventuali trasformazioni, fusioni, scissioni, cessioni e/o conferimenti d'azienda, vendite di assets aziendali, ecc.

La tabella che segue indica in modo sintetico processi sensibili e relativi possibili reati tributari.

Processi sensibili	Reato
• <u>Gestione della contabilità</u> • <u>Acquisto di beni e servizi</u> • <u>Adempimenti fiscali e tributari in genere</u>	• Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 10 marzo 2000, n. 74);

• <u>Tenuta e custodia delle scritture contabili e fiscali</u> • <u>Gestione di eventuali operazioni straordinarie</u>	• Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 10 marzo 2000, n. 74); • Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 10 marzo 2000, n. 74); • Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione infedele ex art. 4 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Omessa dichiarazione ex art. 5 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Indebita compensazione ex art. 10-quater D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).
---	---

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

7.18 Regole di comportamento.

7.18.1 Principi generali e standard di controllo.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Sezione prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-quinquiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;
- ✓ comunicare all'Agenzia delle Entrate e/o alle Autorità fiscali dati non rispondenti al vero, con il divieto di predisporre e fornire documenti falsi, omettere le informazioni dovute.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a:
 - diffondere i principi di HS previsti dal Codice Etico;
 - promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati;
 - rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con l'Agenzia delle Entrate e le Autorità fiscali;
 - rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con l'Agenzia delle Entrate e le Autorità fiscali, deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che si occupano della predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria, dell'emissione di documentazione afferente alla contabilità, del ricevimento di documentazione afferente alla contabilità o del pagamento di imposte, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per evitare il rischio di violazioni in materia tributaria;
- ✓ tutti i consulenti in materia fiscale di HS devono essere informati circa le linee guida contro la commissione di reati tributari;
- ✓ qualunque criticità sorga nell'ambito del rapporto con l'Agenzia delle Entrate e le Autorità fiscali, deve essere immediatamente comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

È, inoltre, sancito l'espresso obbligo di:

- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- garantire un corretto e trasparente processo di gestione delle operazioni straordinarie, compresa la vendita di eventuali asset aziendali;

- assicurare la veridicità dei dati predisposti;
- assicurare la trasparente gestione delle forniture, di beni e servizi;
- garantire il flusso informativo tra le funzioni coinvolte nei processi sensibili in materia contabile-fiscale con il Collegio Sindacale e l'Organismo di Vigilanza;
- svolgere un'adeguata attività di selezione dei fornitori;
- acquistare beni di provenienza garantita e servizi e/o qualsiasi altra utilità ad un prezzo che, salvo casi eccezionali e certificati (quali ad esempio acquisti da aste giudiziarie o da fallimenti), sia commisurato alla qualità e quantità dei beni stessi in base al valore di mercato;
- rispettare la normativa fiscale-tributaria;
- garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali.

Gli standard di controllo da considerare ed applicare con riferimento alle attività sensibili di cui alla presente sezione sono:

- **previsione di procedure interne** idonee a fornire i principi di riferimento generali per la regolamentazione dell'attività sensibile;
- **tracciabilità**: tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali/informatici;
- **segregazione dei compiti**: lo standard concerne l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di un sistema di segregazione delle funzioni coerente** con le responsabilità organizzative assegnate: sono previste regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

7.19 Principi procedurali specifici.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto

all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1	
- Definizione di ruoli e responsabilità - Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti. - Tenuta e custodia delle scritture contabili e fiscali - Gestione delle operazioni straordinarie	
Definizione di ruoli e responsabilità	- Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare all'Agenzia delle Entrate o alle altre Autorità fiscali [ad es., nel caso di predisposizione della documentazione ai fini di dichiarazioni e comunicazioni concernenti la materia tributaria, deve essere ben chiara la segregazione delle funzioni tra (i) chi è preposto alla elaborazione e raccolta della documentazione da presentare, (ii) chi verifica, approva e sottoscrive la documentazione da presentare. - Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti	È fatto obbligo di: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni nelle fasi di autorizzazione / esecuzione / controllo per i seguenti ambiti: - gestione della fatturazione e relativa registrazione - gestione dei pagamenti - gestione delle note di credito - gestione degli acquisti, di beni e servizi - gestione buste paga e rimborsi spesa ai dipendenti - tenere tracciate tutte le fasi di gestione dei flussi finanziari e archiviare in maniera completa i relativi documenti giustificativi; - prevedere un sistema di backup dell'archiviazione dei documenti contabili; - verificare l'effettiva e corretta esecuzione della prestazione richiesta (sia verso fornitori di beni che di servizi), nel rispetto del principio di segregazione delle funzioni, prima di autorizzare il pagamento della relativa fattura; - tenere traccia e registrare ogni richiesta di ordine e relativo preventivo inoltrato, sia che sia stato mandato via e-mail che telefonici (in quest'ultimo caso andrà compilato apposito modulo di richiesta ordine); - verificare che gli incassi siano sempre supportati da un contratto o un ordine autorizzato e conseguentemente non accettare beni e/o altre utilità a fronte delle quali non vi sia un contratto o un ordine adeguatamente autorizzato;

- verificare che l'importo effettivamente incassato corrisponda a quello fatturato e che non vi siano anomalie al riguardo;
- rispettare le procedure adottate che regolano la gestione della contabilità;
- rispettare il sistema di deleghe e procure adottato che indica i poteri ed i limiti di spesa dei soggetti coinvolti;
- verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività;
- svolgere un'attenta attività di selezione dei potenziali fornitori (sia di beni che di servizi), rispettando i criteri tecnico-economici ed espletando un'adeguata attività selettiva e di obiettiva comparazione tra più offerte;
- a seconda del servizio richiesto, richiedere al fornitore tutta la documentazione o le certificazioni previste dalla legge di riferimento;
- formalizzare tutti i contratti/accordi con fornitori e/o consulenti, allegando la relativa documentazione;
- qualora si faccia uso di soggetti terzi intermediari, verificare con attenzione l'esistenza effettiva, la solidità e l'affidabilità del soggetto;
- monitorare il mantenimento dei requisiti richiesti in capo al fornitore;
- inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali);
- identificare i ruoli e le responsabilità per la gestione dei rimborsi spese ai dipendenti nel rispetto del principio di segregazione di ruoli nelle fasi di autorizzazione / esecuzione / controllo;
- controllare che ogni richiesta di rimborso spese sia accompagnata dalla relativa documentazione giustificativa e conseguentemente non riconoscere alcuna somma che non sia supportata da relativo giustificativo.

Inoltre, ai fini preventivi, si ribadisce che:

- è assolutamente vietato:
 - contabilizzare e registrare fatture per operazioni/prestazioni inesistenti;
 - autorizzare pagamenti a fornitori per operazioni inesistenti o privi dell'evidenza dell'effettuazione del servizio reso;
 - autorizzare rimborsi spesa privi della necessaria documentazione giustificativa;
 - predisporre o comunque utilizzare documenti palesemente falsi;
- ogni pagamento deve corrispondere esattamente a quanto indicato nel contratto e/o nel preventivo formulato al cliente;
- nessun pagamento e nessun incasso di denaro verso/da Paesi inseriti nelle principali black list internazionali, può avvenire senza adeguata documentazione comprovante la reale e specifica necessità;
- nessun pagamento può essere effettuato in favore di un soggetto diverso dalla controparte contrattuale. Eventuali eccezioni a tale divieto sono ammesse solo a fronte della presentazione di una regolare documentazione che giustifichi e consente il pagamento nei confronti di un terzo (es. in caso di cessione del credito o pignoramento presso terzi);
- nessun acquisto deve essere effettuato attraverso il ricorso a mercati non

	consolidati; • nessun contratto di fornitura può essere stipulato in assenza di un'adeguata attività di selezione o in mancanza della relativa documentazione richiesta dalla legge; • tutti gli incassi devono provenire dalla controparte contrattuale. Eventuali eccezioni sono ammesse solo a fronte della presentazione di una regolare documentazione giustificativa (es. pignoramento presso terzi); • ogni importo effettivamente incassato deve corrispondere a quanto fatturato. Qualora sia necessario restituire un pagamento o parte di esso indebitamente ricevuto, questo deve essere disposto esclusivamente verso il conto corrente di provenienza, tenendo traccia dei documenti giustificativi; • occorre tenere l'evidenza scritta di ogni pagamento; • occorre archiviare tutti i documenti contabili nel rispetto dei principi di correttezza, completezza e attenzione della relativa tenuta.
Tenuta e custodia delle scritture contabili e fiscali	In merito alla tenuta delle scritture contabili, è fatto obbligo: • identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni per i seguenti ambiti: - gestione degli adempimenti fiscali e tributari; - gestione del calcolo delle obbligazioni tributarie e dei relativi obblighi dichiarativi; - gestione e tenuta delle scritture contabili e fiscali; • tenere tracciate tutte le fasi di gestione dei citati processi e archiviare in maniera completa i relativi documenti; • prevedere un sistema di back up dell'archiviazione dei documenti contabili e fiscali; • prevedere modalità di aggiornamento, anche tramite consulenti esterni, sulle novità in ambito fiscale e tributario; • provvedere al regolare adempimento degli obblighi fiscali-tributari cui la società è tenuta (tributi, contributi, Iva etc.); • prevedere uno scadenziario che preveda i termini entro i quali occorre provvedere ai vari adempimenti fiscali-tributari. È, inoltre, vietato: • occultare o distruggere, in tutto o in parte, documenti contabili, fiscali o di cui è comunque obbligatoria la conservazione; • omettere o fornire dati ed informazioni inesatte o non complete imposte dalla legge sulla situazione economica, patrimoniale e finanziaria della società; • violare, eludere, evadere obblighi di dichiarazione, attestazione, certificazione di natura tributaria previsti dalla legge; • non adempiere le prescrizioni di legge in materia contabile, di informazione societaria, di valutazione di cespiti e di redazione del bilancio; • occultare in contabilità redditi conseguiti soggetti a tassazione, rappresentare falsamente spese non reali, emettere fatture per prestazioni inesistenti, effettuare stime, valutazioni e determinazione di poste di bilancio con modalità e criteri valutativi difforni da quelli richiesti dalla legge; • porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da

	parte degli organi di controllo; • ostacolare, in ogni modo, l'effettuazione di verifiche, accertamenti ed ispezioni da parte dell'Agenzia delle Entrate o delle altre Autorità fiscali o giudiziarie.
Gestione delle operazioni straordinarie	Con riferimento a tale attività è fatto obbligo di: • garantire l'esplicita approvazione, da parte dell'Assemblea dei Soci, di ogni attività relativa ad operazioni straordinarie, comprese le cessioni e dismissioni di assets aziendali, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni, qualora per il compimento delle suddette operazioni si renda necessaria od opportuna l'approvazione dell'Assemblea; • identificare in maniera chiara e precisa i ruoli ed i soggetti competenti alla predisposizione della documentazione destinata agli organi sociali a supporto delle deliberazioni relative ad operazioni straordinarie; • identificare in maniera chiara ruoli e responsabilità in merito alla tenuta ed archiviazione degli atti di delibera e dei relativi documenti predisposti; • garantire una corretta tenuta ed archiviazione della documentazione relativa alle operazioni, prevedendo anche sistemi di back up.; È, inoltre, assolutamente vietato: • alienare simulatamente beni o assets aziendali al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; • compiere qualsiasi altro atto fraudolento al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; • indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

7.20 Responsabilità specifiche della Direzione Acquisti (DA)

Con riferimento alla prevenzione del rischio di commissione dei reati tributari sarà compito della DA:

- supervisionare l'attività dell'ufficio acquisti;
- accedere agli estratti conto;
- individuare potenziali fornitori, richiedere offerte;
- contattare i fornitori prescelti e negoziare i termini di acquisto e le condizioni della fornitura: quantità, tempi, prezzi, modalità di consegna;
- registrare correttamente sul software gestionale in uso all'azienda tutte le condizioni di fornitura contrattate con terze parti che diventeranno oggetto di fatturazione passiva.

7.21 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'esito di eventuali audit effettuati sulla gestione delle attività sensibili sopra indicate,

sia da parte di funzioni interne che da parte di soggetti esterni (ad es. consulenti fiscali, commercialisti, ecc.);

- l'avviso di eventuali ispezioni da parte dell'Agenzia delle Entrate o di altre autorità fiscali o giudiziarie con relativo verbale;
- eventuali comunicazioni provenienti dal Collegio Sindacale relativamente a criticità emerse, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-quinquiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente - con il supporto delle funzioni competenti - il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

L'Organismo di Vigilanza deve riportare i risultati della sua attività di vigilanza e controllo, con cadenza periodica semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale.

Pertanto, nel caso in cui dagli accertamenti svolti dall'Organismo di Vigilanza emergano elementi che facciano risalire la violazione dei principi e protocolli contenuti nella presente Parte Speciale del Modello, la commissione del reato, o il tentativo di commissione del reato, direttamente al Presidente, l'Organismo di Vigilanza dovrà riferire al Consiglio di Amministrazione ed al Collegio Sindacale, ai quali compete la decisione sull'eventuale applicazione dei meccanismi previsti dalla legge.

7.22 Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25-sexiesdecies del Decreto)

Il reato di contrabbando, previsto all'art. 25-sexiesdecies del Decreto, è stato introdotto dal D.Lgs. 14 luglio 2020, n. 75 ("Attuazione della direttiva (UE) 2017/1371 c.d. "Direttiva PIF", relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale").

L'art. 25-sexiesdecies del D.Lgs. 231/01 dispone che: *"1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.*

2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

La Società ha ritenuto di dover mappare il rischio connesso alla commissione di reati di contrabbando stante la ingente attività di import ed export con diversi paesi UE ed extra UE.

A tal fine, si ritiene necessaria una breve premessa con riferimento alla materia doganale.

I dazi doganali rappresentano una risorsa propria dell'Unione europea e confluiscono nel bilancio unitario, ad esclusione di una percentuale del 25% che viene trattenuta dallo Stato di entrata delle merci a copertura delle spese di riscossione (fonte: dossier di documentazione parlamentare).

La normativa doganale è contenuta nel Decreto del Presidente della Repubblica 23 gennaio 1973 n. 43 (Testo Unico Doganale, "TUD").

Si considerano "diritti doganali" tutti quei diritti che la dogana è tenuta a riscuotere in forza di una legge, in relazione alle operazioni doganali. Fra i diritti doganali costituiscono "diritti di confine" (art. 34 del TUD):

- i dazi di importazione e quelli di esportazione;
- i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione;
- i diritti di monopolio, le sovrimposte di confine ed ogni altra imposta o sovrimposta di consumo a favore dello Stato (per quanto concerne le merci in importazione).

Per le merci soggette a diritti di confine, il presupposto dell'obbligazione tributaria è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e,

relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso (art. 36 del TUD).

7.23 Sanzioni nei confronti dell'Ente.

In relazione alla commissione dei reati di cui sopra si applicano all'ente le seguenti sanzioni pecuniarie:

- ✓ fino a 200 quote in relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica n. 43/1973, ovvero ai delitti del Titolo VII Capo I, intendendosi per tali i fatti ivi previsti (ma solo se superano 10mila euro di diritti di confine evasi) ed in particolare:
 - Articolo 282 (Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali)
 - Articolo 283 (Contrabbando nel movimento delle merci nei laghi di confine)
 - Articolo 284 (Contrabbando nel movimento marittimo delle merci)
 - Articolo 285 (Contrabbando nel movimento delle merci per via aerea)
 - Articolo 286 (Contrabbando nelle zone extra-doganali)
 - Articolo 287 (Contrabbando per indebito uso di merci importate con agevolazioni doganali)
 - Articolo 288 (Contrabbando nei depositi doganali)
 - Articolo 289 (Contrabbando nel cabotaggio e nella circolazione)
 - Articolo 290 (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti).
 - Articolo 291 (Contrabbando nell'importazione od esportazione temporanea)
 - Articolo 291-bis (Contrabbando di tabacchi lavorati esteri)
 - Articolo 291-ter (Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri)
 - Articolo 291-quater (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri)
 - Articolo 292 (Altri casi di contrabbando)
 - Articolo 294 (Pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato)
 - alle contravvenzioni del Titolo VII Capo II, cioè ai fatti ivi previsti ma solo se superano i 10mila euro di diritti di confine evasi (articoli 302 e seguenti).

- ✓ fino a 400 quote qualora i diritti di confine dovuti superino i 100.000 Euro.

Nei casi previsti dai commi 1 e 2 dell'art. 25-sexiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

7.24 Aree a rischio reato e processi sensibili

I processi sensibili che presentano il rischio di commissione dei reati di cui al presente paragrafo riguardano le seguenti attività:

- vendita, acquisto, commercializzazione e scambio di prodotti oltre confine;
- scarico e deposito delle merci oltre confine.

Le potenziali aree a rischio reato che HS ha astrattamente individuato sono quelle relative alle seguenti attività:

Processi sensibili	Reato
• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine • Scarico e deposito delle merci oltre confine	• Contrabbando (Decreto del Presidente della Repubblica n. 43/1973);

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

7.25 Regole di comportamento.

7.25.1 Principi generali e standard di controllo.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-sexiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;

Inoltre, è fatto specifico divieto di:

- introdurre merci estere attraverso il confine di terra in violazione delle prescrizioni, divieti e limitazioni;
- introdurre merci estere via mare in violazione delle prescrizioni, divieti e limitazioni;
- scaricare o depositare merci estere nello spazio intermedio tra la frontiera e la più vicina dogana;
- nascondere merci estere sulla persona o nei bagagli o fra merci di altro genere od in qualunque mezzo di trasporto, per sottrarle alla visita doganale;
- asportare merci dagli spazi doganali senza aver pagato i diritti dovuti senza averne garantito il pagamento;
- portare fuori del territorio doganale merci nazionali o nazionalizzate soggette a diritti di confine;
- detenere merci estere, quando ricorrano le circostanze previste nel secondo comma dell'art. 25-sexiesdecies per il delitto di contrabbando (ovvero, *"Quando i diritti di confine dovuti superano centomila euro"*).

7.26 Principi procedurali specifici.

Protocollo 1 Controllo interno sull'emissione e la conservazione dei documenti fiscali	
Applicazione di misure idonee ad evitare l'emissione di documentazione contabile non coerente con la prestazione o la distruzione di documenti fiscali al fine di eventuali controlli da parte delle Autorità Doganali	Devono essere osservate specifiche misure che consentano di: • evitare di introdurre o esportare merci che violino prescrizioni, divieti e limitazioni di cui al Testo unico delle disposizioni legislative in materia doganale; • conservare la documentazione doganale; • non sottrarsi alle visite doganali; • pagare i diritti dovuti o garantire i dovuti pagamenti.

Con riferimento e per l'espletamento delle operazioni doganali di import ed export la HS si affida a società selezionate per la notorietà e l'esperienza nel settore delle spedizioni e della consulenza per logistica e trasporti a livello internazionale nonché per le pratiche doganali in import/export. L'affidamento di tali incarichi viene fatto a mezzo contratti di mandato e consulenza annuali e/o a tempo indeterminato.

Dovrà essere cura dei Destinatari della presente sezione di verificare la validità e la vigenza dei suddetti contratti di mandato.

7.27 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'avviso di eventuali ispezioni da parte delle Autorità doganali o di altre autorità giudiziarie sempre relativamente alla materia doganale;
- eventuali comunicazioni provenienti dalle Autorità doganali o di altre autorità giudiziarie relativamente a criticità emerse in materia doganale, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-sexiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- ✓ verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- ✓ esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- ✓ comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- ✓ curare l'aggiornamento del Modello, indicando al CDA le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

7.28 Regole di comportamento e Protocolli operativi con riferimento ai delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1 del Decreto).

Il D. Lgs. 184/2021 ha dato attuazione alla Direttiva UE 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e con la sua entrata in vigore il 14

dicembre 2021 ha comportato sia modifiche al codice penale che l'introduzione del nuovo articolo 25-octies.1 nel D. Lgs. 231/01.

Con il d.lgs. 184/2021 è stata innanzitutto introdotta una nozione di valuta virtuale valida «agli effetti della legge penale».

Alla luce della norma del 2021, pertanto, si intende per valuta virtuale «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente». La nozione viene fatta rientrare all'interno della più ampia categoria di «strumento di pagamento diverso dal contante», intendendosi per tale «un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali»

Per quanto concerne il codice penale gli interventi riguardano modifiche agli artt. 493-ter e 640-ter e l'introduzione del nuovo art. 493-quater.

Il d.lgs. 184/2021 ha modificato anche l'art. 640 ter c.p., comma 2, c.p., prevedendo una aggravante nel caso in cui il fatto produca un «trasferimento di denaro, di valore monetario o di valuta virtuale».

È opportuno soffermarsi sui termini e sul raggio di azione della duplice modifica normativa apportata dal Decreto Legislativo 8 novembre 2021, n. 184.

Attraverso tale provvedimento normativo, rubricato "Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti", il Legislatore è voluto intervenire sul noto e sempre più allarmante fenomeno delle azioni/attività a carattere manipolativo riguardanti gli strumenti di pagamento e i flussi monetari digitali (bancomat, carte di credito, carte ricaricabili, POS, internet banking, etc.).

Detta operazione di politica legislativa ha reso necessaria la modifica del codice penale, attraverso:

a) l'ampliamento per integrazione dell'art. 493 ter c.p. con la conseguente precisazione che la falsificazione punibile riguarda non solo le "carte di credito" ma anche qualsiasi strumento di pagamento lato sensu "digitale" e diverso dal contante;

b) l'introduzione del nuovo reato di cui all'art. 493 quater c.p., finalizzato alla punizione di chi, in chiave di evidente sfruttamento economico, produce e/o commercializza i sofisticati strumenti e programmi finalizzati a questo tipo di falsificazione;

c) l'estensione del reato di frode informatica di cui all'art. 640 ter, attraverso la previsione di una ulteriore aggravante nel caso in cui il fatto illecito produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

In questa sede, deve essere focalizzata l'attenzione sulle conseguenze applicative dell'altra (pur richiamata) importante disposizione del D.Lgs. 184/2021, ovvero l'introduzione dell'art. 25 octies.1 nel Decreto Legislativo 231/2001

Reati presupposti dall'art. 25 octies.1 e relativa collocazione nei Modelli 231.

Nello specifico caso dell'art. 25 octes.1 introdotto dal D.Lgs. 184/2021, i reati presupposto richiamati sono:

- *Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti* (art. 493 ter c.p.);
- *Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti* (art. 493 quater c.p.);
- *Frode informatica* (art. 640 ter c.p.)

Delle tre fattispecie delittuose, va considerato che:

- *due (artt. 493 ter e 493 quater c.p.) sono totalmente "nuove" rispetto al corredo di tutti i reati presupposto, ossia quelli menzionati dal Decreto 231 agli articoli: dal 24 al 25- duodevices, cui si aggiunge il neo art. 25 octies.1;*
- *la frode informatica ex art. 640 ter invece, pur in termini parziali e nella versione prescrittrice antecedente alla modifica del D.Lgs. 184/2021, era già presupposta dall'art. 24.*

Il dato di estrema importanza nell'ottica della comprensione applicativa del neo art. 25 octies.1. è che i tre richiamati *reati presupposto*, sebbene siano giuridicamente appartenenti a due diverse "famiglie" del codice penale (gli artt. 493 ter e 494 quater ai "Delitti contro la fede pubblica", l'art. 640 ter ai "Delitti contro il patrimonio"):

A) sono stati inseriti nello stesso art. 25 octies.1 del D.lgs. 231/2001;

B) sono stati allocati in posizione di immediata contiguità e prosecuzione funzionale all'art. 25, che sostanzialmente si occupa dei delitti afferenti alla prevenzione e al controllo dei flussi patrimoniali e finanziari.

Ciò non sembra affatto casuale perchè, implicitamente, indica le aree organizzative e i processi di lavoro maggiormente sensibili ed idealmente a "rischio" di commissione degli stessi reati.

La conferma di tale chiave di lettura è data dal fatto che l'art. 25 octies.1 introdotto nel Decreto 231 porta la rubrica *"Delitti in materia di strumenti di pagamento diversi dai contanti"*; dunque, è lo stesso Legislatore ad indirizzare verso quelle aree organizzative dell'ente (e processi di lavoro e specifiche funzioni aziendali) che si occupano di gestire, controllare e monitorare gli strumenti di pagamento diversi dal contante.

Non è, insomma, involontaria l'allocazione della nuova disposizione in contiguità con l'art. 25 octies, considerato che anche questa norma è sostanzialmente rivolta alla gestione, controllo e monitoraggio, dei flussi patrimoniali e finanziari, previa definizione degli opportuni presidi preventivi (protocolli, procedure, istruzioni operative e azioni analoghe) che afferiscono alla gestione, diretta o indiretta, degli strumenti di pagamento (in entrata o in uscita) e dei movimenti monetari.

Infine, il D.L. 10 agosto 2023 n. 105 coordinato con la Legge di conversione n. 137 del 9 ottobre 2023 (c.d. "Decreto Giustizia") ha modificato la rubrica dell'art. 25 octies.1 aggiungendo *"e trasferimento fraudolento di valori"* ed ha inserito all'interno di tale norma, al comma 2-bis, la fattispecie del reato di trasferimento fraudolento di valori di cui all'art. 512-bis c.p. (n vigore dal 10.10.2023)

Art. 25-octies.1.

Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

1. In relazione alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie

a) per il delitto di cui all'art. 493-ter, la sanzione pecuniaria da 300 a 800 quote;

b) per il delitto di cui all'art. 493-quater e per il delitto di cui all'art. 640-ter, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria sino a 500 quote.

2. Salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente, in relazione alla commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, si applicano all'ente le seguenti sanzioni pecuniarie:

a) se il delitto è punito con la pena della reclusione inferiore ai dieci anni, la sanzione pecuniaria sino a 500 quote;

b) se il delitto è punito con la pena non inferiore ai dieci anni di reclusione, la sanzione pecuniaria da 300 a 800 quote.

2-bis. In relazione alla commissione del delitto di cui all'articolo 512-bis del codice penale, si applica all'ente la sanzione pecuniaria da 250 a 600 quote.

3. Nei casi di condanna per uno dei delitti di cui ai commi 1, 2 e 2-bis si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2.

Come si evince da quanto precede, in relazione agli artt. 493 quater e 640 ter c.p., tali delitti vengono in rilievo ai fini della responsabilità dell'ente, solo ove commessi nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale.

Al comma secondo, invece, l'art. 25 octies-1 apre le porte, quali fattispecie presupposto della responsabilità dell'ente derivante da reato, ad una serie vasta e non analiticamente individuata di delitti, con la previsione di una clausola di riserva, assumendo *prima facie* il carattere di norma di chiusura.

Difatti, ai sensi della nuova disposizione, costituisce reato presupposto, ove il fatto non integri altro illecito amministrativo sanzionato più gravemente, ogni delitto previsto dal codice penale "contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio", esclusivamente ove il fatto, però, abbia ad oggetto strumenti di pagamento diversi dai contanti.

Tenuto conto che l'art. 25 bis, D. Lgs. 231/01 già annovera quali reati presupposto alcuni delitti contro la fede pubblica, assumono, astrattamente, rilievo, anche ai fini della responsabilità da reato dell'ente ex art. 25 octies-1, sicuramente, i delitti previsti e puniti dal Titolo VII, Capo I del codice penale, dall'art. 453 all'art. 458, riguardanti la falsità in monete ed in carte di pubblico credito, a condizione che l'oggetto materiale della condotta sia uno strumento di pagamento diverso dal contante. Considerato il riferimento generico alla fede pubblica, in ragione della ratio della modifica legislativa e del suo contenuto, appaiono astrattamente privi di una potenziale rilevanza, i delitti

previsti nei Capi II, III e IV del Titolo VII (restando, peraltro verso, fattispecie presupposte, ai sensi degli artt. 24 bis e 25 bis, gli artt. 473, 474 e 491 bis c.p.).

Medesima considerazione deve svolgersi per i reati previsti al Titolo XIII, osservato, parimenti, il generico richiamo ai delitti contro il patrimonio operato dal comma secondo dell'art. 25 octies-1. Ed invero, di assoluta irrilevanza appaiono quelli commessi con violenza alle cose. Rispetto ai delitti contro il patrimonio commessi con violenza alla persona, occorrerà, invece, verificare, avuto riguardo della ratio della modifica legislativa, la compatibilità tra condotta incriminata e lo specifico oggetto di rilievo della responsabilità dell'ente, come detto, individuato negli strumenti di pagamento diversi dal contante.

Pertanto, l'offesa al patrimonio arrecata mediante violenza alla persona appare di dubbia rilevanza ai fini della responsabilità ex art. 25 octies-1, D. Lgs. 231/01, a meno che non si voglia estendere tale responsabilità nel caso di furto, rapina o estorsione avente oggetto, quale res illecitamente appresa nell'interesse o a vantaggio dell'ente, uno strumento di pagamento diverso dal denaro, a prescindere dal suo tentato o realizzato illegale utilizzo.

Analoghe considerazioni possono essere svolte in ordine ai delitti in danno del patrimonio commessi mediante frode diversi da quelli già previsti dall'art. 25 octies e dalle altre disposizioni del D. Lgs. 231/01.

7.29. La tipologia dei delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.

Le nuove fattispecie di delitti in materia di strumenti di pagamento diversi dai contanti introdotte nell'elenco dei reati suscettibili di rilevare secondo il Decreto 231, sono dunque le seguenti:

Con il decreto legislativo 8 novembre 2021 n. 184 è stato modificato anche l'**art. 493 ter c.p. («Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti»)**.

Nella sua formulazione originaria la disposizione prevedeva tre diverse ipotesi di reato: (i) l'indebito utilizzo, al fine di trarne profitto per sé o per altri, di carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, da parte del soggetto non titolare; (ii) la falsificazione o alterazione delle carte di credito e di pagamento; (iii) il possesso, la cessione o acquisizione di carte di credito o di pagamento che abbiano provenienza illecita o che siano stati alterati o falsificati.

Il decreto del 2021 non introduce sostanziali modifiche. Viene solo ampliato l'oggetto materiale della condotta, estendendosi il campo d'applicazione della fattispecie a tutti gli strumenti di

pagamento diversi dai contanti. È infatti punito «l'utilizzo indebito» – oltre che delle carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi - anche di «ogni altro strumento di pagamento diverso dai contanti». Lo stesso vale in caso di «falsificazione o alterazione» oppure in ipotesi di «possesso, cessione o acquisto» dei beni di cui in precedenza se di «provenienza illecita o comunque falsificati o alterati».

Il decreto legislativo 8 novembre 2021 n. 184 ha introdotto, nell'ambito dei delitti contro la fede pubblica, **l'art 493 quater c.p. («Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti»)**. Ai sensi della nuova disposizione, è punito con «la reclusione fino a 2 anni e la multa fino a 1.000 euro» chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, «produce», «importa», «esporta», «vende», «trasporta», «distribuisce», «mette a disposizione» o in qualsiasi modo «procura» a sé o ad altri «apparecchiature, dispositivi o programmi informatici» che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti, o sono specificamente adattati al medesimo scopo. È prevista una clausola di riserva «salvo che il fatto costituisca più grave reato» e una forma di confisca obbligatoria delle apparecchiature, dei dispositivi e dei programmi informatici - nonché del profitto o del prodotto del reato ovvero, laddove non sia possibile, di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto - in caso di condanna o patteggiamento della pena.

Il D. Lgs. 184/2021 ha anche modificato **l'art. 640-ter c.p. (Frode Informatica)**.

La norma estende il reato di frode informatica di cui all'art. 640-ter, attraverso la previsione di una ulteriore aggravante nel caso in cui il fatto illecito produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

La condotta consiste nell'alterazione, comunque realizzata, del sistema informatico e dell'intervento, senza averne diritto, con qualsiasi modalità, su dati, informazioni, programmi di un sistema informatico.

Il D.L. 10 agosto 2023 n. 106 coordinato con la Legge di conversione n. 137 del 9 ottobre 2023 ha inserito all'interno dell'art. 25 octies.1, al comma 2bis , **l'art. 512 bis c.p.** che prevede il reato di **Trasferimento fraudolento di valori** ai sensi del quale, *“Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di*

contrabbandando ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648 bis e 648 ter, è punito con la reclusione da due a sei anni”.

7.30 Sanzioni nei confronti dell'Ente.

Il nuovo articolo 25-octies.1 prevede sanzioni diverse a seconda che il reato presupposto commesso sia quello previsto da art. 493-ter c.p. o art. 493-quater c.p. o art. 640-ter c.p. (per tale ultimo reato nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale) oppure, come previsto al comma 2, sia un delitto contro la fede pubblica, il patrimonio o che comunque offende il patrimonio quando ha ad oggetto strumenti di pagamento diversi dai contanti o, infine, se sia quello previsto dall'articolo 512-bis del codice penale.

In particolare possono essere comminate le seguenti sanzioni:

- sanzione pecuniaria da 300 a 800 quote per il delitto di cui all'art. 493-ter;
- sanzione pecuniaria sino a 500 quote per i delitti di cui all'art. 493-quater o all'art. 640-ter sempre nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valore virtuale. Per inciso giova ricordare che l'art. 640-ter risulta già essere reato presupposto con la previsione delle relative sanzioni amministrative quando la frode informatica sia commessa, se commessa ai danni dello Stato o di altro Ente pubblico.

Nell'ipotesi invece in cui il delitto commesso sia un reato contro la fede pubblica o il patrimonio o che comunque offende il patrimonio può essere ravvisata una responsabilità in capo all'ente solo qualora il fatto non integri un altro illecito amministrativo sanzionato più gravemente. Le sanzioni amministrative previste in questo caso sono:

- sanzione pecuniaria fino a 500 quote, se il delitto è punito con la pena della reclusione inferiore a dieci anni;
- sanzione pecuniaria da 300 a 800 quote, se il delitto è punito con la pena della reclusione non inferiore a dieci anni.
- sanzione pecuniaria da 250 a 600 quote per il delitto di cui all'art. 512 bis c.p..

Per tutte le fattispecie di reato presupposto in caso di condanna si applicano le sanzioni interdittive previste dall'art. 9, co. 2 D. Lgs. 231/01.

7.31 Area a rischio reato e processi sensibili

In relazione alle tipologie di reato di cui sopra è possibile delineare una specifica **area astrattamente a rischio** per le ipotesi di cui al comma 1. In particolare, l'area ritenuta più a rischio in relazione a tali reati presupposto è:

a) l'utilizzo di carte di credito.

Le tipologie di reati presupposto che potrebbero essere realizzate nell'utilizzo delle carte di credito sono: Art. 25 *octies*.1 Decreto 231, Delitti in materia di strumenti di pagamento diversi dai contanti.

In questo ambito si può ipotizzare la condotta di falsificazione o alterazione di una carta di credito, di cui all'art. 493 *ter* c.p., al fine di far trarre profitto alla Società effettuando con essa pagamenti e/o acquisti a vantaggio di HS..

Con riferimento al reato di trasferimento fraudolento di valori di cui al comma 2bis, si potrebbero ipotizzare trasferimenti fraudolenti o intestazioni fittizie finalizzate ad evitare la sottrazione di patrimonio della società anche soltanto potenzialmente assoggettabile a misure di prevenzione.

7.32 Regole di comportamento

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-*octies*.1 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame..

7.33 Compiti dell'Organismo di Vigilanza

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-*octies*.1 del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di delitti in materia di strumenti di pagamento diversi dai contanti, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante..

8 SEZIONE H – DIREZIONE MARKETING E COMMERCIALE (R. MKTG).

Questa sezione si occuperà di analizzare l'area di rischio relativa al Settore Marketing e Commerciale sotto la cui direzione vi sono le seguenti unità operative:

- Unità Marketing e vendite estero – Terapie Ablative;
- Ufficio Servizi Marketing, Congressi e Pubblicità;
- Customer Care estero;
- Customer Care Italia;
- Unità Clinica Biomedica;
- Product Manager;
- Ufficio Gare;
- Divisioni Vendite (Divisione Italia Linea Interventistica, Divisione Italia Terapie Ablative, Divisione Italia Critical Care/Civco, Informatori Scientifici, Vendite Estero-Biopsy & Critical Care).

Le potenziali aree sensibili che HS ha individuato in relazione alle attività svolte in questo settore dal Responsabile e dalle unità sottoposte, nell'ambito dei reati di cui al Decreto, sono quelle descritte nella tabella che segue:

DIREZIONE MARKETING E COMMERCIALE	
REATI EX D.LGS. 231/01	AREE SENSIBILI
Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)	• Rapporti anche istituzionali con la Pubblica Amministrazione; • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.); • Gestione delle gare e dei bandi pubblici; • Scelta di fornitori e consulenti; • Richiesta e ottenimento di finanziamenti pubblici; • Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi; • Spese di rappresentanza; • Assunzione del personale; • Accesso ai sistemi informatici della Pubblica Amministrazione; • Gestione dei contenziosi.
Delitti informatici (art. 24-bis del Decreto)	Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali, falsità in documenti informatici pubblici o aventi efficacia probatoria, frode informatica, indebito utilizzo, falsificazione o alterazione di carte di credito o di pagamento o di qualsiasi altro documento analogo, trattamento illecito di dati, falsità nelle dichiarazioni e notificazioni al Garante della

	privacy, inosservanza delle misure minime di sicurezza e di protezione dei dati personali.
Delitti contro l'industria e il commercio (art. 25-bis 1 del Decreto), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto)	Contraffazione, alterazione o uso di marchi.
Reati societari (art. 25-ter)	• Tenuta delle scritture contabili e dei Libri Sociali; • Creazione di fondi extracontabili; • Gestione degli ordini e delle fatture; • Gestione della liquidità; • Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale; • Scelta consulenti/fornitori/partner commerciali.
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies)	• Scelta consulenti/fornitori/partner commerciali; • Gestione dei flussi finanziari/creazione di fondi extracontabili; • Gestione della liquidità e cassa.
Delitti in materia di violazione del diritto d'autore (art. 25-novies)	Gestione delle licenze e dei software per elaboratore.
Reati tributari (art. 25-quinquiesdecies del Decreto)	• Gestione della contabilità • Acquisto di beni e servizi • Adempimenti fiscali e tributari in genere • Tenuta e custodia delle scritture contabili e fiscali • Gestione di eventuali operazioni straordinarie
Reati di contrabbando (art. 25-sexiesdecies)	• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine; Scarico e deposito delle merci oltre confine.

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza che le sottoporrà al Consiglio di Amministrazione nei modi che di seguito verranno descritti.

8.1 I reati contro la Pubblica Amministrazione.

Il d.lgs. 231/2001 elenca tassativamente i reati contro la Pubblica Amministrazione che comportano responsabilità a carico degli Enti. Essi sono:

- ✓ **malversazione a danno dello Stato**, (art. 316-bis c.p.): *"Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità Europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **indebita percezione di erogazioni a danno dello Stato**, (art. 316-ter c.p.): *"(Comma 1) Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante*

*l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità o dei suoi poteri. **La pena è della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.**²³ (Comma 2). Quando la somma indebitamente percepita è pari o inferiore a lire sette milioni settecentoquarantacinquemila si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da dieci a cinquanta milioni di lire. Tale sanzione non può comunque superare il triplo del beneficio conseguito" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*

- ✓ **Truffa** (art. 640, comma 2, n. 1 c.p.): "(Comma 1). Chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire cinquecento a diecimila. 2. La pena è della reclusione da uno a cinque anni e della multa da lire tremila a quindicimila:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o **dell'Unione europea**²⁴ o col pretesto di far esonerare taluno dal servizio militare;

2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità;

2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

(Comma 3). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

- ✓ **truffa aggravata per il conseguimento di erogazioni pubbliche** (art. 640-bis c.p.), "La pena è della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;

²³ Aggiornamento del D.Lgs. 74/2020.

²⁴ Aggiornamento del D.Lgs. 74/2020.

- ✓ **Frode informatica** (art. 640-ter c.p.): *“(Comma 1). Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. (Comma 2). La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. (Comma 3). La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- ✓ **Frode nelle pubbliche forniture** (art. 356 c.p.)²⁵: *“Chiunque commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni e con la multa non inferiore ad euro 1.032. La pena è aumentata nei casi preveduti dal primo capoverso dell'articolo precedente” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*
- ✓ **Frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale** (art. 2 L. 898/1986): *“(Comma 1). 1. Ove il fatto non configuri il più grave reato previsto dall'articolo 640-bis del codice penale, chiunque, mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni quando il danno o il profitto sono superiori a euro 100.000. Quando la somma indebitamente percepita è pari od inferiore a 5.000 euro si applica soltanto la sanzione amministrativa di cui agli articoli seguenti. (Comma 2). Agli effetti della disposizione del precedente comma 1 e di quella del comma 1 dell'articolo 3, alle erogazioni a carico del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale sono assimilate le quote nazionali previste dalla normativa comunitaria a complemento delle somme a carico di detti Fondi, nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa comunitaria. (Comma 3). Con la sentenza il giudice determina altresì l'importo indebitamente percepito e condanna il colpevole alla restituzione di esso all'amministrazione che ha disposto la erogazione di cui al comma 1” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote.*

²⁵ Fattispecie inserita dal D.Lgs. 75/2020.

L'art. 25²⁶ rubricato "Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio", elenca le seguenti fattispecie criminose quali reati suscettibili di far scattare la responsabilità dell'Ente ex Decreto:

- ✓ **Peculato** (art. 314, co. 1, c.p.): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro [c.p. 458] o di altra cosa mobile altrui [c.c. 812, 814] , se ne appropria, è punito con la reclusione da quattro anni a dieci anni e sei mesi."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Peculato mediante profitto dell'errore altrui** (art. 316): *"Il pubblico ufficiale [c.p. 357] o l'incaricato di un pubblico servizio [c.p. 358], il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni. (Comma 2) La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000²⁷"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Concussione** (art. 317 c.p.), *"Il pubblico ufficiale o l'incaricato di un pubblico servizio che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità, è punito con la reclusione da sei a dodici anni."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;
- ✓ **Corruzione per l'esercizio della funzione** (art. 318 c.p.), *"Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da tre a otto anni"* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;
- ✓ **Corruzione per un atto contrario ai doveri d'ufficio** (art. 319 c.p.), *"Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da sei a dieci anni."* - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;
- ✓ **Circostanze aggravanti** (art. 319 bis c.p.), *"La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene"*

²⁶ AGGIORNAMENTO: Il D.lgs. n. 75/2020 modifica l'art. 25 D.Lgs. 231/2001, ampliando il catalogo dei reati con le fattispecie di peculato ex artt. 314 e 316 c.p. e di abuso d'ufficio ex art. 323 c.p.

²⁷ Comma aggiunto dall'art. 1, comma 1, lett. a), D.Lgs. n. 75/2020.

nonché il pagamento o il rimborso di tributi" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;

- ✓ **Corruzione in atti giudiziari** (art. 319-ter c.p.): *"(Comma 1) Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da sei a dodici anni. (Comma 2) Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote per il comma 1 e fino 800 quote per il comma 2;*
- ✓ **Induzione indebita a dare o promettere utilità** (art. 319-quater c.p.), *"(Comma 1) Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei anni a dieci anni e sei mesi. (Comma 2) Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;*
- ✓ **Corruzione di persona incaricata di pubblico servizio** (art. 320 c.p.), *"(Comma 1) Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. (Comma 2) In ogni caso, le pene sono ridotte in misura non superiore a un terzo" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote nel caso di commissione art. 318 c.p. e fino a 600 quote in caso di commissione art. 319 c.p.;*
- ✓ **Pene per il corruttore** (art. 321 c.p.), *"Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 800 quote;*
- ✓ **Istigazione alla corruzione** (art. 322 commi 1 e 3 c.p.): *"(Comma 1) Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo [...]. (Comma 3) La pena di cui al primo comma si applica al pubblico ufficiale o*

all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote;

- ✓ **Istigazione alla corruzione** (art. 322 commi 2 e 4 c.p.): *"(Comma 2) Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo [...]. (Comma 4) La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319" - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 600 quote;*

- ✓ **Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri** (art. 322-bis c.p.): *"Le disposizioni degli articoli 314, 316, da 317 a 320 e 322, terzo e quarto comma, si applicano anche:*

1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;

3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;

4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;

5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;

5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale;

5-ter) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di organizzazioni pubbliche internazionali;

5-quater) ai membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e ai giudici e funzionari delle corti internazionali;

5-quinquies) alle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione²⁸.

Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso (5):

1) alle persone indicate nel primo comma del presente articolo;

2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi” - Sono previste in capo all'Ente le medesime sanzioni pecuniarie previste per gli artt. 314, 316, da 317 a 320 e 322 terzo e quarto comma c.p;

- ✓ **Traffico di influenze illecite** (art. 346 bis c.p.): tale ipotesi delittuosa punisce chi, sfruttando o vantando relazioni esistenti o asserite con un pubblico ufficiale o un incaricato di un pubblico servizio indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità, come prezzo della propria mediazione illecita verso un pubblico ufficiale o un incaricato di un pubblico servizio. Tale fattispecie può concretizzarsi in attività che pongono in relazione due soggetti privati, (uno dei quali funge da intermediario “illecito” verso un pubblico ufficiale o incaricato di pubblico servizio in cambio di un interesse o vantaggio) - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.
- ✓ **Abuso d'ufficio** (art. 323 c.p.), “*Salvo che il fatto non costituisca un più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto è punito con la reclusione da uno a quattro anni²⁹. La pena è*

²⁸ Numero aggiunto dall'art. 1, comma 1, lett. d), D.Lgs. 14 luglio 2020, n. 75, a decorrere dal 30 luglio 2020.

²⁹ Comma così modificato, a decorrere dal 17 luglio 2020, dall'art. 23, comma 1, D.L. 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120.

aumentata nei casi in cui il vantaggio o il danno hanno un carattere di rilevante gravità” - È prevista nei confronti dell'Ente una sanzione pecuniaria fino a 200 quote.

8.2 Definizione di Pubblica Amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio.

– Pubblica Amministrazione (di seguito “PA”) s'intende, in estrema sintesi, qualsiasi ente o soggetto pubblico (ma talvolta anche privato) che svolga in qualche modo la funzione pubblica, nell'interesse della collettività, e quindi nell'interesse pubblico.

A titolo esemplificativo, si possono indicare, quali soggetti della PA, i seguenti enti o categorie di enti:

- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, Ente Dogane, ecc.);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAL, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di reati nei rapporti con la PA. In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei “Pubblici Ufficiali” e degli “Incaricati di Pubblico Servizio”.

- **Pubblici ufficiali e incaricati di un pubblico servizio** Ai sensi dell'art. 357, primo comma, del codice penale, è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".

La norma chiarisce solo la nozione di "pubblica funzione amministrativa" (poiché le altre due non hanno suscitato dubbi interpretativi) precisando che, agli effetti della legge penale "è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

In altre parole, è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.

Diversamente, l'art. 358 c.p. definisce i "soggetti incaricati di un pubblico servizio" come quei soggetti "i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il servizio, affinché possa definirsi pubblico, deve essere disciplinato, al pari della "pubblica funzione", da norme di diritto pubblico, ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

È pertanto un incaricato di pubblico servizio colui il quale svolge una pubblica funzione non riconducibile ai poteri di cui è dotato un pubblico ufficiale (potere legislativo, giudiziario e amministrativo) e non concernente semplici mansioni d'ordine e/o la prestazione d'opera meramente materiale, in quanto tali prive di alcun apporto intellettuale e discrezionale.

8.3 Regole di comportamento e protocolli operativi in materia di reati contro la P.A. (artt. 24 e 25 D.Lgs. 231/2001).

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale in relazione ai reati contro la P.A. prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati in esame;
- ✓ porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. in relazione a quanto previsto dalle predette ipotesi di reato;
- ✓ comunicare alla P.A. dati non rispondenti al vero, predisporre e fornire documenti falsi, omettere le informazioni dovute;
- ✓ violare i sistemi informativi della P.A. al fine di ottenere o manipolare informazioni a vantaggio della Società.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a diffondere i principi di HS previsti dal Codice Etico; a promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati; a rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con la P.A.; ad assicurarsi che ciascun dipendente partecipi e concluda l'attività di formazione in tema di anticorruzione; a rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con la P.A., deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che effettuano pagamenti o, in generale, transazioni con la P.A. e/o pubblici funzionari, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per fronteggiare i tentativi di corruzione;
- ✓ tutti i partner commerciali di HS devono essere informati circa le linee guida contro la corruzione predisposte dalla Società;
- ✓ qualunque criticità o conflitto d'interesse sorga nell'ambito del rapporto con la P.A. deve essere comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;

- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

Protocollo 1	
• Rapporti anche istituzionali con la Pubblica Amministrazione. • Gestione dei rapporti con le Autorità e gli organi di controllo anche in occasione di verifiche e ispezioni (es. ASL, ARPA, VV. FF., Guardia di Finanza, INAIL ecc.). • Gestione delle gare e dei bandi pubblici • Accesso a sistemi informatici della Pubblica Amministrazione	
Definizione dei ruoli e responsabilità	• Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare alla P.A. (ad es., nel caso di richiesta e conseguente sottoscrizione di contratto di fornitura con un nuovo cliente appartenente alla P.A. [es. strutture ospedaliere], deve essere ben chiara la segregazione delle funzioni tra (a) chi propone la richiesta (b) chi valuta detta richiesta, anche attraverso una verifica sul cliente, sulle modalità di ingaggio dello stesso nonché sulla possibilità di eseguire la fornitura senza necessità di gara (c) chi raccoglie e dispone la documentazione necessaria e (d) chi approva e sottoscrive la richiesta). • Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione operativa	È fatto divieto di: • proporre opportunità commerciali che possano avvantaggiare dipendenti della P.A. a titolo personale o accordare altri vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A., o comunque di soggetti agli stessi collegati; • porre in essere artifici o raggiri tali da indurre la P.A. a valutare in modo errato le caratteristiche tecniche ed economiche dei prodotti o dei servizi offerti o forniti; • distrarre, anche solo parzialmente, i contributi, le sovvenzioni ed i finanziamenti pubblici dalle finalità per le quali sono stati ottenuti; • presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati; • presentare false dichiarazioni ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati o rendicontare in modo non veritiero l'attività per la quale sono già state effettuate delle erogazioni pubbliche; Inoltre, è necessario che: • sia prevista una verifica dell'esistenza di eventuali conflitti di interesse con riferimento anche alla possibilità di entrare in trattativa con la P.A.; • ogni eventuale accordo preso con la P.A. sia documentato. • sia implementato un sistema di verifica (c.d. <i>Activity Check</i>) sulle attività svolte in concreto dai venditori e/o informatori scientifici, nonché sui rapporti da questi

	intrattenuti con soggetti, potenziali clienti e/o fornitori e/o distributori, appartenenti alla P.A. o con essa collegati, attraverso scambio continuo di documentazione telematica e/o cartacea da parte degli stessi venditori e/o informatori scientifici alla Società, contenente la descrizione delle attività svolte e l'identificazione dei soggetti con i quali vengono intrattenuti rapporti commerciali a nome della Società.
Gestione operativa: Venditori Informatori Scientifici	In caso di proposizione di nuove opportunità commerciali (es. nuovo cliente appartenente alla P.A.) e comunque in caso di rapporti con la P.A. in genere, è necessario che: a) vi sia una verifica sull'esistenza di eventuali conflitti di interesse con riferimento alla possibilità di entrare in trattativa con la P.A. o con soggetti ad essa collegati, b) vi sia un controllo sulle modalità di ingaggio del nuovo cliente/fornitore/distributore, c) vi sia una verifica sul cliente in termini di casellario giudiziale, d) sia previsto <u>un doppio controllo mensile</u> (c.d. <i>Activity Check</i>) sull'attività svolta da venditori e/o informatori scientifici, oltre la possibilità di effettuare dei <i>random check</i> (ovvero controlli casuali) sull'attività di questi ultimi. A tal fine è obbligo dei venditori e/o degli informatori scientifici: documentare le proprie attività (appuntamenti giornalieri, identità del cliente, attività in concreto svolta con il cliente, ecc.) in formato telematico e/o cartaceo; • inoltrare alla Società due volte al mese l'<i>activity check</i> per via telematica; • informare immediatamente la Società di eventuali proposte o fatti illeciti commessi dal cliente, che possano integrare ipotesi di reato ai danni della Società, come sopra descritte. È, inoltre, fatto divieto di: • intrattenere qualsiasi forma di rapporto (commerciale e non) di cui la Società non sia stata previamente messa a conoscenza
Ispezioni	• Durante eventuali ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e quelle poste in essere dalle Autorità di Vigilanza di settore ivi comprese anche le autorità preposte alla verifica del rispetto del d.lgs. 81/2008, alle verifiche tributarie e alle verifiche INPS da parte dell'Ispettorato del lavoro <u>devono partecipare i soggetti a ciò espressamente delegati (almeno due)</u>; • di tutto il procedimento concernente l'ispezione devono essere redatti e conservati gli appositi verbali interni. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'Organismo di Vigilanza ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta; • devono essere osservate specifiche procedure che disciplinino le modalità di partecipazione, da parte dei soggetti incaricati da HS sia per la società stessa che per conto di terzi, alle ispezioni giudiziarie, fiscali, amministrative e/o di vigilanza e le modalità di gestione dei rapporti con i soggetti pubblici anche preposte alla sicurezza dei luoghi di lavoro, alla tutela ambientale, alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
Autorizzazioni e Licenze	Tale attività deve prevedere: • la segregazione delle funzioni responsabili delle attività di presa di contatto con il soggetto pubblico per la richiesta di informazioni, di redazione della domanda e di gestione della licenza e/o delle autorizzazioni, prevedendo specifici sistemi di controllo (ad esempio la compilazione di schede formative, anche da parte del consulente esterno, l'indizione di apposite riunioni, la verbalizzazione delle principali statuizioni) al fine di garantire il rispetto dei canoni di integrità, trasparenza e correttezza del processo; • specifici protocolli di controllo e verifica della veridicità e correttezza dei

	documenti la cui produzione è necessaria per ottenere la licenza e/o autorizzazione.
--	--

Protocollo 2 – Scelta di fornitori e consulenti	
Deleghe, Procure e poteri	Qualora dipendenti, collaboratori, consulenti e partner dovessero intrattenere materialmente rapporti con soggetti pubblici per conto di HS deve essere formalmente conferito potere in tal senso (con apposita delega per i dipendenti ovvero con clausola <i>ad hoc</i> per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri definiti.
Gestione operativa	• I collaboratori esterni devono essere scelti in modo trasparente. Sarà cura di ogni singola funzione interna controllare che essi non versino in conflitto di interessi. • I contratti tra HS e i collaboratori, consulenti e partner devono essere definiti per iscritto in tutte le loro condizioni e termini; devono contenere clausole standard che impegnino al rispetto del d.lgs. 231/2001. • Sarà, altresì, cura di ogni singola funzione interna controllare, ove sia ragionevolmente possibile, le attività commerciali dei terzi intermediari coinvolti in un pagamento a funzionari pubblici italiani e/o stranieri. Potranno così essere raccolte informazioni - tramite questionari, interviste, indagini - su un futuro possibile intermediario, prestando attenzione all'esperienza, alle referenze, ai legami con pubblici funzionari nazionali e/o stranieri e alla sua affidabilità finanziaria. • Inoltre, è fatto divieto di riconoscere compensi, o effettuare prestazioni, in favore dei collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al compenso ricevuto, alle caratteristiche del rapporto di <i>partnership</i> ed alle prassi vigenti.

Protocollo 3 – Richiesta e ottenimento di finanziamenti pubblici	
Transazioni finanziarie	• Nessun pagamento può essere effettuato in contanti, salvo espressa autorizzazione da parte della direzione amministrazione e finanza che potrà concederla solo nei casi in cui sia espressamente richiesto dalla normativa regolante l'attività dell'ente pubblico e comunque con regolare imputazione nelle prescritte voci di bilancio. • In caso di ottenimento di erogazioni, contributi o finanziamenti, deve essere predisposto un apposito rendiconto sull'effettiva utilizzazione dei fondi ottenuti; • Le transazioni fatte con la P.A. devono essere tracciabili e verificabili <i>ex post</i> tramite adeguati supporti documentali/informativi, nel rispetto anche di quanto previsto dall'art. 3 della legge n. 136/12010, che impone tra l'altro l'utilizzo di un conto corrente dedicato; • è necessario verificare la corrispondenza tra accordi, ordini di acquisto, fatturazioni, pagamenti relativi anche alle somme da versare al fisco, agli enti previdenziali con una forte attenzione alle autorizzazioni siglate dalle persone delegate a tale compito; • è necessario verificare la corrispondenza tra i pagamenti effettuati ai collaboratori e ai membri degli organi sociali, e l'effettiva attività svolta che

	dovrà essere necessariamente corredata da idonea documentazione giustificativa.
Irregolarità anomalie	o Coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle seguenti attività: • pagamento di fatture; • pagamento relativo alle somme da versare al fisco e agli enti previdenziali; • corrispondenza tra accordi, ordini di acquisti e fatturazioni; • destinazione di finanziamenti ottenuti dagli organismi comunitari o nazionali o regionali, devono porre particolare attenzione sull'attuazione degli adempimenti stessi e riferire immediatamente all'Organismo di Vigilanza, eventuali situazioni di

Protocollo 4 – Assunzione del personale	
Assunzione, gestione, formazione incentivazione dei dipendenti e collaboratori	La regolamentazione di detta attività deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • Il monitoraggio di ogni eventuale conflitto di interessi nei confronti della P.A. da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato. Il personale che si occupa di transazioni con funzionari pubblici nazionali o stranieri ha l'obbligo di eseguire una certificazione periodica di non aver violato la Parte Speciale del presente Modello.

Protocollo 5 – Gestione dei contenziosi giudiziali e stragiudiziali	
Contenziosi/Contestazioni	• Devono essere osservate specifiche procedure che definiscano modalità e termini di gestione delle contestazioni della P.A., individuando le funzioni responsabili della ricezione delle contestazioni e della verifica sulla materia oggetto del contendere. • Eventuali contenziosi/contestazioni o altre problematiche devono essere comunque portati a conoscenza del Consiglio di Amministrazione e all'attenzione dell'Organismo di Vigilanza.

Protocollo 6	
• Gestione di liberalità (donazioni e sponsorizzazioni) e omaggi • Spese di rappresentanza	
Omaggi/Donazioni	Non devono essere effettuate elargizioni in denaro e/o regali a pubblici funzionari o riceverle al di fuori di quanto previsto dalle prassi generalmente accettate (ovvero,

	ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività della Società) in ottemperanza a quanto previsto nel Codice Etico. A tal fine si prevede la creazione di una procedura sulle liberalità che: • indichi i soggetti che possono da un lato autorizzarle e dall'altro riceverle; • definisca il valore massimo per ogni omaggio ed i casi in cui le liberalità possono essere eseguite; È, inoltre, fatto obbligo che qualora gli omaggi vengano elargiti a soggetti appartenenti la P.A., questo sia comunicato immediatamente al C.d.A. In ogni caso, nessun omaggio e/o donazione potrà essere effettuato se non quelli espressamente approvati dal C.d.A.
--	---

8.4 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui agli artt. 24-25 del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- c. esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- d. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- e. curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

8.5 Regole di comportamento e protocolli operativi in materia di delitti informatici (art. 24-bis D.Lgs. 231/2001).

Il Decreto Legislativo n. 48 del 4 aprile 2008, di ratifica ed esecuzione della Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, introduce nell'ambito di applicazione del d.lgs. 231/01 le seguenti fattispecie di reato:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);

- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies c.p.).

I delitti informatici trovano come presupposto l'utilizzo della rete informatica aziendale intesa come struttura integrata di apparati, collegamenti, infrastrutture e servizi e composta da:

- l'infrastruttura di rete, che è costituita dalle apparecchiature e dal relativo software che consentono i collegamenti all'interno delle sedi aziendali e la connessione da e verso l'esterno dell'azienda;
- i servizi di rete, che sono le *utilities* di carattere generale a disposizione di tutti i dipendenti, distribuite o messe a disposizione centralmente quali servizi di posta elettronica, accesso a internet, anagrafiche centralizzate, ecc.;
- le applicazioni ed i servizi di rete aziendali, che sono resi disponibili agli utenti attraverso i server, mentre i punti di accesso alla rete aziendale sono le postazioni di lavoro fisse e mobili assegnate agli utenti stessi.

Il Sistema informativo aziendale della Società (c.d. Servizi IT) è gestito con il supporto tecnico della Ditta DESIDERIO TAGLIENTI, la quale stanno implementando un sistema per la sicurezza e la gestione dei dati aziendali, anche nell'ottica di un adeguamento al Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 2016/679, c.d. GDPR).

A tale ultimo proposito la Società implementando le proprie procedure interne in materia di protezione dei dati personali, attraverso l'adozione un software che permette:

- l'identificazione univoca degli utenti, attraverso un ID, un Identity Provider utilizzabile per eseguire l'accesso e l'autenticazione a norma a tutti gli applicativi e servizi in cloud;
- la crittazione dei dati sensibili, (ad es. dichiarazioni di appartenenza ad organizzazioni sindacali, dati relativi allo stato di salute, ecc.), attraverso cifratura delle informazioni per rendere i dati inaccessibili al di fuori dell'applicazione software, tenendo conto anche del contesto e delle finalità del trattamento, nonché del rischio per i diritti degli interessati;
- il log delle attività per l'archiviazione e la consultazione dei log delle attività previsti dalla nuova normativa.

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello. In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 24-bis del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In particolare, sarà opportuno:

- non divulgare informazioni relative ai sistemi informatici aziendali;
- non utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico.

La Società pone in essere i seguenti adempimenti:

- a. fornisce ai Destinatari un'adeguata informazione relativamente al corretto utilizzo delle risorse informatiche aziendali ed al rischio della commissione di reati informatici;
- b. limita per quanto possibile l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;
- c. effettua, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;
- d. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;

- e. predisporre e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali.

Protocollo 1 - Utilizzo dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali

Applicazione di misure idonee a garantire la riservatezza e la sicurezza informatica	In aggiunta ai presidi aziendali già esistenti, si dispone che è assolutamente vietato: • introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del Reparto IT e in qualunque modo, modificare la configurazione rilasciata dalla funzione IT di postazioni di lavoro fisse o mobili; • acquisire, possedere o utilizzare strumenti <i>software e/o hardware</i> che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (quali ad esempio sistemi per individuare le <i>password</i>, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.); • ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti con metodi o procedure differenti da quelle a tale scopo autorizzate dalla Società; • divulgare, cedere o condividere con personale interno o esterno alla società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti e terze parti; • distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità; • manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi; • effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti col cliente (<i>vulnerability test, penetration test</i>) e previsto nei propri compiti lavorativi; • sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi; • comunicare a persone non autorizzate, interne o esterne all'azienda, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati; Inoltre: • l'utilizzo del servizio aziendale di posta elettronica che deve essere effettuato nel rispetto del Codice Etico aziendale, impiegando esclusivamente il proprio account; • i dati e le informazioni non pubbliche relative a clienti e terze parti (commerciali, organizzative, tecniche) incluse le modalità di connessione da remoto devono essere gestite come dati riservati; • ogni titolare di <i>account</i> è responsabile delle azioni condotte tramite il proprio <i>account</i> sui sistemi e sulla rete aziendale;
--	---

	• ogni titolare di <i>account</i> deve curare l'effettuazione/giornaliera/settimanale bisettimanale delle copie di sicurezza delle banche dati trattati, in collaborazione con l'operatore o gli operatori incaricati della gestione e della manutenzione degli strumenti elettronici, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita; distorcere, oscurare, sostituire la propria identità, e inviare e-mail anonime o riportanti false generalità. La Società deve, a sua volta, porre in essere i seguenti adempimenti: • informare adeguatamente i Destinatari dell'importanza di mantenere i propri codici di accesso (<i>username e password</i>) confidenziali, di non divulgare gli stessi a soggetti terzi e di usare correttamente le risorse informatiche aziendali; • informare i Destinatari della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso; • impostare i sistemi informatici stessi in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente; • fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei destinatari che ne abbiano necessità ai fini lavorativi o connessi all'amministrazione societaria; • dotare il centro di elaborazione dati di porta con chiusura a chiave; • proteggere, per quanto possibile, ogni sistema informatico della Società al fine di prevenire l'illecita installazione di dispositivi <i>hardware</i> in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle (<i>keylogger, backdoor, malicious software</i>, ecc.); • fornire ogni sistema informatico di adeguato <i>software firewall e antivirus</i> e far sì che, ove possibile, questi non possano venir disattivati; • impedire l'installazione e l'utilizzo di <i>software</i> non approvati dalla Società o non correlati con l'attività professionale espletata per la stessa; • limitare l'accesso alle aree ed ai siti <i>internet</i> particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "<i>virus</i>") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e files); • qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna <i>WiFi</i>), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete internet tramite i <i>routers</i> della stessa e compiere illeciti ascrivibili ai dipendenti della Società; • prevedere, ove possibile, un procedimento di autenticazione mediante <i>username e password</i> al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ogni destinatario o categoria di Destinatari; • limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Destinatari.
--	--

8.6 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art. 24-bis del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine all'Organismo di Vigilanza è garantito libero accesso a tutta la documentazione aziendale rilevante.

8.7 Regole di comportamento e Protocolli operativi in materia di delitti contro l'industria e il commercio (art. 25-bis 1, D.Lgs. 231/2001), in materia di contraffazione (art. 25-bis, lett. f-bis del Decreto) e di Violazione del Diritto d'Autore (art. 25-novies del Decreto).

L'art. 15 della L. 99/2009, dal titolo *Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia*. (GU n.176 del 31-7-2009 - Suppl. Ordinario n. 136) ha ampliato le ipotesi di responsabilità amministrativa degli Enti in materia di contraffazione, violazione del diritto d'autore e condotte illecite contro l'industria e il commercio, introducendo nel d.lgs. 231/2001 nuove fattispecie di reati-presupposto.

In considerazione della convergenza, da un punto di vista logico/sistematico, dell'incidenza di tali reati su aspetti particolari dell'attività della Società, si è preferito ricomprendere tali fonti di responsabilità amministrativa in un'unica Sezione del Modello di Organizzazione, Gestione e Controllo di HS.

I delitti in materia di contraffazione che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis, lett. f-bis) del d.lgs. 231/2001 sono i seguenti:

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

I delitti contro l'industria e il commercio che possono dare origine ad una responsabilità amministrativa dell'ente ex art. 25-bis.1 del d.lgs. 231/2001 sono i seguenti:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.).

I delitti in violazione del diritto d'autore di cui all'art. 25-novies del d.lgs. 231/2001, introdotti dalla Legge 99/2009, sono i seguenti:

- Abusiva immissione in reti telematiche di opere protette (art. 171, comma 1 lettera a-bis, L. n. 633/1941);
- Abusivo utilizzo aggravato di opere protette (art. 171, comma 3, L. n. 633/1941);
- Abusi concernenti il software e le banche dati (art. 171-bis L. n. 633/1941);
- Abusi concernenti le opere audiovisive o letterarie (art. 171-ter L. n. 633/1941);
- Omesse o false comunicazioni alla SIAE (art. 171-septies L. n. 633/1941);
- Fraudolenta decodificazione di trasmissioni ad accesso condizionato (art. 171-octies L. n. 633/1941).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative di riferimento e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

In ogni caso, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare, in esecuzione di contratti con la clientela, gli impegni e le condizioni risultanti dai contratti medesimi, ivi compresa la consegna di prodotti e servizi con specifiche tecniche, nomi, autori, diritti di utilizzo, marchi o altri segni distintivi conformi alle pattuizioni contrattuali, salvo che contrattualmente, con

apposita clausola sottoscritta dal cliente, la Società non si riserva, in sede di esecuzione del contratto, di consegnare prodotti o servizi con nomi, marchi, altri segni distintivi o specifiche tecniche diversi, purché tale variazione non induca in errore il cliente o incida in maniera sostanziale sul prodotto/servizio o sull'utilizzo al quale era preordinato l'acquisto e sia comunque idonea a soddisfare pienamente le esigenze del cliente medesimo.

Protocollo 1 – Commercializzazione di prototipi e/o nuovi prodotti

Gestione dello sviluppo dei prototipi e del lancio di nuovi prodotti

La regolamentazione dell'attività descritta deve prevedere che:

- i Destinatari si accertino che i dipartimenti di *patent e trademark* internazionali, incaricati di verificare l'eventuale esistenza di marchi o brevetti identici o l'eventuale esistenza di marchi e brevetti simili che possano potenzialmente entrare in conflitto con quello che si intende registrare, non abbiano espresso parere negativo al deposito e al conseguente utilizzo sul mercato italiano di un marchio o brevetto;
- in fase di messa in commercio di un nuovo prodotto, i Destinatari si attengano alle procedure adottate dalla Società che attribuiscono ai dipartimenti di *patent e trademark* internazionali l'incarico di rilevare qualsiasi criticità del marchio o del brevetto.
- I Destinatari dovranno predisporre contratti (e non meri preventivi) con le società di consulenza esterna che gestiscono marchi e brevetti.

Inoltre, è fatto espressamente divieto di:

- contraffare o alterare marchi o segni distintivi, nazionali o esteri, di prodotti industriali, potendo conoscere dell'esistenza del titolo di proprietà industriale o fare uso di marchi o segni distintivi contraffatti o alterati;
- contraffare o alterare brevetti, disegni o modelli industriali, nazionali o esteri, o fare uso di tali brevetti, disegni o modelli contraffatti o alterati;
- introdurre nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati;
- detenere per la vendita, porre in vendita o mettere altrimenti in circolazione, al fine di trarne profitto, prodotti industriali che sono contrassegnati con marchi contraffatti o alterati che potrebbero indurre l'acquirente a scambiargli con altri noti, creando una possibile confusione nella clientela e tale da arrecare un danno rilevante al proprietario del marchio contraffatto;
- consegnare all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita;
- porre in vendita o metter altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri, atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto;
- adoperare industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, potendo conoscere dell'esistenza del titolo di proprietà industriale;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con offerta diretta ai consumatori o mettere comunque in circolazione oggetti o altri beni realizzati usurpando un titolo di proprietà industriale o in violazione dello stesso, al fine di trarne profitto;
- contraffare o comunque alterare indicazioni geografiche o denominazioni di origine di prodotti agroalimentari;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita con

	offerta diretta ai consumatori o mettere comunque in circolazione prodotti agroalimentari con le indicazioni o denominazioni contraffatte;
--	--

Protocollo 2 – Gestione dei rapporti con la clientela, con particolare riguardo ad attività di pubbliche relazioni, comunicazione istituzionale (siti internet), sponsorizzazioni ed eventi volti alla commercializzazione o pubblicizzazione dei prodotti e dei marchi legati alla Società

Gestione dei rapporti con la clientela	È fatto espressamente divieto di: - abusivamente rimuovere o alterare le informazioni elettroniche di cui all'articolo 102 quinquies della legge n. 633/1941, ovvero distribuire, importare a fini di distribuzione, diffondere per radio o per televisione, comunicare o mettere a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse; - riprodurre, duplicare, trasmettere o diffondere abusivamente, vendere o porre altrimenti in commercio, cedere a qualsiasi titolo o importare abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; - in violazione dell'art. 16 della legge n. 633/1941, mettere a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa, oppure un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore; - detenere per la vendita o la distribuzione, porre in commercio, vendere, noleggiare, cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (SIAE), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato; - duplicare abusivamente, riprodurre, trasmettere o diffondere in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; - riprodurre abusivamente, trasmettere o diffondere in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; - pur non avendo concorso alla duplicazione o riproduzione, introdurre nel territorio dello Stato, detenere per la vendita o la distribuzione, o distribuire, porre in commercio, concedere in noleggio o comunque cedere a qualsiasi titolo, proiettare in pubblico, trasmettere a mezzo della televisione con qualsiasi procedimento, trasmettere a mezzo della radio, far ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b) dell'art. 171-ter L. 633/1941; - importare, distribuire, vendere, noleggiare, cedere a qualsiasi titolo, pubblicizzare per la vendita o il noleggio, o detenere per scopi commerciali, attrezzature, prodotti o componenti ovvero prestare servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater della legge n. 633/1941 ovvero siano principalmente progettati, prodotti, adattati o
---	--

	realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure.
--	---

Protocollo 3 – Approvvigionamento, installazione e/o configurazione di prodotti software, banche dati ed altre opere dell'ingegno strumentali all'attività della Società con particolare riguardo alla presenza e validità di licenze d'uso e dei bollini SIAE

Utilizzo del software	La regolamentazione dell'attività descritta deve prevedere che: • l'installazione di programmi, che non sono già stati acquisiti a livello centralizzato, debba essere autorizzata da ogni singolo Direttore di reparto; • tutti i supporti informatici alienati (PC, floppy disk, CD o DVD) debbano essere preventivamente e opportunamente resi illeggibili onde evitare l'involontaria diffusione di programmi e/o banche dati protetti; Inoltre, è fatto espressamente divieto di: • duplicare, abusivamente e per trarne profitto, programmi per elaboratore o, ai medesimi fini, importare, distribuire, vendere, detenere a scopo commerciale o imprenditoriale o concedere in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); • riprodurre, al fine di trarne profitto, su supporti non contrassegnati SIAE, oppure trasferire su altro supporto, distribuire, comunicare, presentare o dimostrare in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies della legge n. 633/1941, ovvero eseguire l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter della medesima legge, ovvero distribuire, vendere o concedere in locazione una banca di dati.
------------------------------	--

8.8 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-bis, lett. f-bis, 25-bis 1 e 25-novies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio dei delitti in materia di contraffazione, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

- d. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale;
- e. esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

8.9 Regole di comportamento e Protocolli operativi in materia di reati societari (art. 25-ter, D.Lgs. 231/2001).

Nell'ambito della riforma del diritto societario, il Decreto Legislativo 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-ter del Decreto, estendendo il regime della responsabilità amministrativa degli Enti ai c.d. "reati societari".

I reati societari sono reati propri e, in quanto tali, possono essere commessi direttamente da:

- Consiglio di Amministrazione;
- Amministratori;
- Direttori Generali;
- Sindaci;
- Liquidatori;
- Sottoposti alla direzione e alla vigilanza dei soggetti sopra elencati nel caso di corruzione tra privati;
- nonché, a titolo di concorso, anche dalle strutture preposte alla gestione di attività amministrativo-contabili, finanziarie o relative all'implementazione del sistema informativo contabile.

Le fattispecie di reati societari considerate sono:

- false comunicazioni sociali (art. 2621 c.c.);
- false comunicazioni sociali in danno dei soci o dei creditori (art. 2622, commi 1 e 3, c.c.);
- falso in prospetto (art. 173-bis, T.U.F.);
- impedito controllo (art. 2625, comma 2, c.c.);
- indebita restituzione dei conferimenti (art. 2626 c.c.);
- illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- operazioni in pregiudizio dei creditori (art. 2629 c.c.);

- omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.);
- formazione fittizia del capitale (art. 2632 c.c.);
- indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- corruzione tra privati (art. 2635, comma 3 c.c.); [modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019];
- istigazione alla corruzione tra privati (art. 2635-bis c.c.) [introdotto dal D.Lgs. n. 38/2017];
- illecita influenza sull'assemblea (art. 2636 c.c.);
- aggioaggio (art. 2637 c.c.);
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, dalle procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (ex art. 25-ter del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame.

Conseguentemente la presente Parte Speciale prevede l'obbligo, a carico dei Destinatari, di:

- a. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle eventuali procedure interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società. A questo proposito, è fatto espresso divieto di:
 - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà riguardo alla situazione economica, patrimoniale e finanziaria della Società;
 - omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- b. attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione del bilancio e della rendicontazione periodica disciplinata dalla legge;

- c. osservare tutte le norme poste in essere dalla legge a tutela dell'integrità ed effettività del patrimonio della Società, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- d. perseguire l'obiettivo dell'interesse sociale nella gestione e nell'esercizio dell'attività aziendale, fino alle fasi eventuali di liquidazione o cessazione della Società;
- e. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- f. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge non frapponendo alcun ostacolo ai controlli delle Autorità di Vigilanza. A questo proposito è fatto espresso divieto di:
 - ✓ omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile;
 - ✓ esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti alla realtà, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
 - ✓ porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza, anche in sede di ispezione, da parte dell'Autorità Amministrativa (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- g. predisporre procedure per la preparazione del bilancio e la gestione delle risorse finanziarie; inoltre,
 - ✓ il presente Modello deve essere portato adeguatamente a conoscenza di tutto il personale, non solo dirigente, e appositi meccanismi di comunicazione (ad esempio tramite poster nelle sale comuni o pubblicazioni periodiche) devono essere predisposti in modo da permettere la conoscenza di modifiche e/o aggiornamenti del Modello stesso e deve essere attivato un programma di informazione/formazione a favore del personale addetto atto a prevenire la commissione di reati societari;
 - ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità o di conflitto di interesse, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili, le attività finalizzate alla formazione del bilancio e le altre comunicazioni sociali siano accurati e trasparenti.

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente contabile esterno non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1 • Predisposizione del bilancio; • Tenuta delle scritture contabili e dei Libri Sociali; • Gestione degli ordini e delle fatture.	
Definizione dei ruoli e responsabilità	Devono essere osservate specifiche procedure che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione della contabilità, predisposizione dei bilanci, dei rendiconti, prevedendo controlli in ordine alla completezza e veridicità delle informazioni contenute nei singoli documenti finali; • individuino la funzione e il soggetto deputato a gestire per conto di HS la contabilità ed il processo di formazione dei documenti contabili, cui conferire apposita delega e procura scritta. Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione Operativa	In aggiunta ai presidi aziendali già esistenti, si dispone: • la trasmissione agli amministratori e al collegio sindacale di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o del consiglio di amministrazione o sui quali esso debba esprimere un parere ai sensi di legge; • la previsione di riunioni periodiche tra il collegio sindacale e l'Organismo di Vigilanza per verificare l'osservanza della disciplina in tema di normativa societaria e di <i>Corporate Governance</i>. Inoltre, per la predisposizione delle comunicazioni ai Soci relative alla situazione economica, patrimoniale e finanziaria della Società, si dispone che la redazione delle

	stesse sia effettuata determinando in maniera chiara e completa: • i dati e le informazioni che ciascuna funzione deve fornire; • i criteri contabili per l'elaborazione dei dati; • la tempistica per la loro consegna alle aree aziendali responsabili. Infine, in caso di comunicati stampa e ogniqualvolta vengano diffuse all'esterno notizie aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società, si dispone che chi diffonde tali informazioni, oltre ad osservare i principi suindicati, deve attenersi esclusivamente alle informazioni desumibili da documenti già approvati e resi pubblici.
--	--

Protocollo 2

- **Gestione delle operazioni societarie (aumento o riduzione del capitale, conferimenti, ripartizione di utili, fusioni e scissioni);**
- **Creazione di fondi extracontabili.**

Gestione operativa	• Le modalità di gestione delle operazioni societarie devono essere condotte in maniera veritiera e corretta, coerentemente e nel rispetto dei principi di <i>Corporate Governance</i> adottati dal Consiglio di Amministrazione. • Deve esistere una segregazione di ruoli e responsabilità tra chi evidenzia la necessità di un'operazione, chi la esegue e chi effettua il relativo controllo. • Per ogni documentazione predisposta deve essere assicurata la tracciabilità delle relative fonti e degli elementi informativi. • Tutta la documentazione deve contenere elementi assolutamente veritieri e devono essere coerenti all'oggetto per cui sono stati richiesti. A tal fine tutta la documentazione relativa alle operazioni societarie deve essere archiviata in un apposito fascicolo con sottoscrizione del responsabile della funzione. • E' inoltre necessario che sia previsto quanto segue: – un programma di formazione – informazione del personale impiegato nella predisposizione della documentazione attinente le operazioni societarie; – un monitoraggio dei poteri anche con riferimento alla verifica delle firme dei documenti inerenti le operazioni societarie; – la documentazione redatta ed in genere ogni altra informazione formalizzata deve contenere solo elementi assolutamente veritieri.
---------------------------	---

Protocollo 3 – Rapporti con il Collegio Sindacale relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e con i Soci nell'attività di verifica della gestione aziendale

Identificazione dei soggetti responsabili	Nella gestione dei rapporti con il collegio sindacale, società di revisione e soci devono essere osservate le seguenti disposizioni: • identificazione del personale all'interno di HS preposto ad interloquire con il collegio sindacale e alla trasmissione della relativa documentazione; • possibilità per il Collegio Sindacale e della società di revisione di prendere contatto con l'Organismo di Vigilanza per verificare congiuntamente situazioni che possono presentare aspetti di criticità in relazione ai reati societari.
--	---

Protocollo 4

- **Scelta consulenti/fornitori/partner commerciali e rapporti con i clienti;**
- **Gestione della liquidità.**

Gestione del processo di acquisizione di nuova clientela e di gestione della clientela acquisita	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con clienti o altre controparti contrattuali; • garantire una segregazione di funzioni e responsabilità e una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione delle vendite, in particolare tra responsabilità nei rapporti con il cliente (cd. <i>account manager</i>), responsabilità nella definizione del prezzo di offerta e delle condizioni/tempi di pagamento (e relative penali), responsabilità nella definizione di eventuali risoluzioni transattive in caso di controversie; • individuare criteri generali e trasparenti per la determinazione di un prezzo massimo di offerta per singolo prodotto o servizio, di modo che qualunque anomalia possa essere agevolmente rilevata. In caso di qualsivoglia criticità sorta nell'ambito dei rapporti sopra descritti, deve essere informato l'Organismo di Vigilanza con nota scritta. In particolare, vi è l'obbligo di comunicare: • le operazioni di vendita superiori ad un dato importo che potrà rappresentare la soglia di rischio; • le operazioni di vendita superiori di una data percentuale rispetto al prezzo medio del prodotto, come risultante dai criteri generali suddetti; • tutte le operazioni di incasso al di sotto dei termini standard di pagamento (ad esempio, fatture pagate a vista).
Assegnazione/gestione degli incarichi e delle consulenze esterne	In aggiunta ai presidi aziendali già esistenti, si dispongono le seguenti regole di comportamento: • agire rigorosamente sui controlli necessari a garantire trasparenza nei rapporti con fornitori o altre controparti contrattuali; • garantire una netta ripartizione dei compiti tra le varie funzioni nell'ambito dell'organizzazione degli acquisti, in particolare tra funzione che individua e seleziona il fornitore, il consulente o il prestatore di servizi, funzione che ratifica la c.d. entrata merci, funzione che autorizza il pagamento e funzione che effettua il controllo di gestione e la tracciabilità delle operazioni; • effettuare una pianificazione dell'attività di <i>benchmarking</i> (raffronto con i valori economici di mercato); • predisporre adeguati protocolli aziendali per acquisti di beni e servizi, affidamento di consulenza ed altre prestazioni professionali e gestione del magazzino.
Selezione e gestione del personale	La regolamentazione dell'attività descritta deve prevedere: • una definizione chiara dei ruoli e compiti dei soggetti responsabili della selezione e della gestione dei dipendenti e collaboratori; • un sistema strutturato di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione del candidato; • l'individuazione del soggetto responsabile della gestione dell'attività in oggetto e l'attribuzione delle relative responsabilità; • la gestione dell'incentivazione dei dipendenti e collaboratori; • la definizione di metodologie di archiviazione della documentazione relativa alle attività in oggetto, al fine di garantire la pronta reperibilità dei documenti in caso di richiesta e la tracciabilità del processo; • il monitoraggio di ogni eventuale conflitto di interessi da parte dei dipendenti e collaboratori in relazione a quanto previsto dalle predette ipotesi di reato.

Gestione del marketing eventuale omaggistica clienti comprese le organizzazioni no profit	Con riguardo alla formazione del personale dipendente e amministrativo, sono prescritte le seguenti e ulteriori regole di comportamento: • divieto di offrire, sollecitare, istigare o ricevere da terzi, direttamente o indirettamente, o di accettare la promessa di ricevere omaggi, benefici o altre utilità, a meno che questi omaggi, benefici e utilità abbiano "modico valore" e rientrino nei limiti della normale cortesia e non abbiano lo scopo di influenzare decisioni aziendali o creare obblighi nei confronti di terzi o di compiere o omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà. In particolare: – le spese di rappresentanza devono essere limitate a pranzi o cene di lavoro; – i c.d. omaggi a clienti sono da limitare alla gadgettistica o ad oggetti di puro valore simbolico, meglio ancora se riportanti il marchio dell'azienda per collegarli a finalità pur sempre commerciali, con la previsione di un listino; • proibire liberalità che non siano inquadrate in programmi generali di <i>social responsibility</i>, come sponsorizzazioni sportive di club, associazioni, ecc. riconducibili ad un ente/cliente o a suoi singoli manager; • prevedere una chiara casistica ed un flusso di comunicazioni verso l'Organismo di Vigilanza affinché si possa vigilare su eventuali abusi, attraverso l'analisi incrociata con altri dati, ad esempio quelli relativi alle commesse acquisite; • prevedere che chiunque riceva tali richieste o offerte, eccezione fatta per omaggi di modico valore, debba informarne "il responsabile della funzione aziendale competente"; • prevedere, nell'informativa comunicata ai clienti/fornitori, che ogni violazione dei principi contenuti nel Codice Etico rappresenta una violazione contrattuale; • prevedere l'obbligo per i clienti/fornitori di conformarsi al Codice Etico prima di poter avere rapporti commerciali con la società.
Partecipazione a gare indette da soggetti privati e gestione dei rapporti con il cliente in caso di vittoria di una gara	È necessario che sia previsto quanto segue: • una corretta applicazione della procedura di partecipazione ai bandi privati sia con riferimento alla fase di ricezione (fonte interna e/o fonte esterna) dell'informazione circa la natura del bando cui si vorrà partecipare anche in forma associata (ovvero il modo con cui su è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, che alla predisposizione e spedizione della documentazione all'Ente (o alla capofila) che indica il relativo bando; • una verifica dell'esistenza di eventuali conflitti di interessi con riferimento anche alla possibilità di partecipare o meno al bando. Inoltre, devono essere previste regole di comportamento che: • definiscano con chiarezza ruoli e compiti delle unità responsabili della gestione delle varie fasi dei rapporti con partner/terze parti ed altri soggetti privati in genere, prevedendo controlli in ordine alla regolarità dei requisiti di ammissione degli stessi ad eventuali bandi di gara privati o all'ottenimento di contributi, sovvenzioni e finanziamenti privati; • individuino la funzione e la persona fisica deputata a rappresentare l'azienda nei confronti dei terzi privati, cui conferire apposita delega e procura e stabiliscano forme di riporto periodico dell'attività svolta verso il responsabile della funzione competente a gestire tali rapporti; Infine, il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.

8.10 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. verificare, attraverso controlli campione sulle aree a rischio reato, l'osservanza, l'attuazione e l'adeguatezza del Modello e la corretta esplicazione delle attività contenute nelle aree a rischio in relazione alle regole di cui al Modello stesso (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato *reporting* verso gli organi deputati, ecc.);
- b. monitorare l'efficacia delle eventuali procedure interne per la prevenzione dei reati considerati nella presente Parte Speciale;
- c. verificare annualmente i principali atti societari ed in particolare la relazione del Collegio Sindacale e della Società di Revisione nonché il rispetto delle procedure per la diffusione delle comunicazioni rivolte ai Soci, dei comunicati stampa e delle notizie scritte rivolte all'esterno aventi ad oggetto informazioni potenzialmente idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari della Società al fine di verificare l'osservanza della presente Parte Speciale nonché la sua idoneità a prevenire i reati ivi elencati;
- d. esaminare eventuali segnalazioni specifiche provenienti dagli organi societari, da terzi o da qualsiasi esponente aziendale, effettuando gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;
- e. comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- f. curare l'aggiornamento del Modello, indicando al consiglio di amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

8.11 Regole di comportamento e Protocolli operativi in materia di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25-octies).

I reati di cui all'art. 25-octies del d.lgs. 231/2001 sono i seguenti:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).
- Autoriciclaggio (art. 648-ter 1 c.p.)

Nell'espletamento delle rispettive attività/funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di Corporate Governance, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di:

- a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-octies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente diventarlo;
- b) intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo, persone legate all'ambiente del riciclaggio, del terrorismo, al traffico di droga, all'usura, ecc.;
- c) utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti;
- d) accettare rapporti contrattuali con clienti o altre controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI;
- e) effettuare elargizioni in denaro ad individui, società od organizzazioni condannate per aver svolto attività illecite, in particolare attività terroristiche o sovversive dell'ordine pubblico;
- f) avere contatti con individui inseriti nelle *black list* antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea.

Inoltre è previsto, a carico dei Destinatari, l'espresso obbligo di:

- g) richiedere tutte le informazioni necessarie al fine di valutare l'affidabilità, la solidità economica e l'attendibilità commerciale/ professionale dei fornitori e del partner;
- h) assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme;
- i) tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti;
- j) prestare particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti esteri.

Protocollo 1 - Scelta consulenti, fornitori, partner commerciali	
Selezione dei partner e dei fornitori	Si riportano di seguito specifiche regole di comportamento da tenere in osservanza del Decreto: la Società procede alla selezione dei Partner commerciali secondo modalità che consentano una comparazione obiettiva e trasparente delle offerte, basata su criteri

	oggettivi e documentabili, verificandone l'attendibilità commerciale attraverso: – verifica ex ante, conservando evidenza dei dati raccolti, che i soggetti con cui intrattiene rapporti contrattuali, anche lavorativi, abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati come non cooperativi dal GAFI e non siano inseriti nelle <i>black list</i> antiterrorismo consultabili all'indirizzo http://europa.eu/rapid/press-release_IP-19-781_it.pdf, della Commissione Europea. – visure ordinarie presso la Camera di Commercio o certificato equivalente di giurisdizioni estere; – referenze da parte di altri soggetti già in rapporti con la Società o pubbliche istituzioni o associazioni professionali o studi professionali di alta reputazione; – ove possibile, certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti di giurisdizioni estere; • la Società inserisce nei contratti con i Partner commerciali una specifica clausola con la quale gli stessi si dichiarano a conoscenza dei principi etici e comportamentali di HS e dei principi contenuti nel Modello e si impegnano al rispetto degli stessi; il mancato rispetto dei comportamenti etici o false dichiarazioni relative alla situazione del Partner comporteranno l'applicazione di una penale o, a seconda della gravità, la risoluzione del contratto; • la Società verifica l'attendibilità commerciale e professionale dei Fornitori, perlomeno di una certa rilevanza (da concordare un limite di importo di fornitura superato il quale procedere alle verifiche) attraverso: – visure ordinarie presso la Camera di Commercio o certificati equivalenti per Fornitori stranieri; – certificato antimafia o certificato carichi pendenti degli amministratori o certificati equivalenti per fornitori stranieri; – analisi del Fornitore per verificarne la coerenza con le prestazioni richieste dalla Società. Inoltre, è previsto, a carico dei Destinatari, l'espresso obbligo di tenere un comportamento corretto, trasparente, di buona fede e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori e clienti. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 2 – Gestione dei flussi finanziari/creazione di fondi extracontabili e gestione della liquidità e cassa	
Gestione di investimenti	Si prevede l'espresso divieto di: • utilizzare strumenti che non siano proceduralizzati per il compimento di operazioni di trasferimento di importi rilevanti; • effettuare elargizioni in denaro, in particolare ad individui, società od organizzazioni condannate per aver svolto attività illecite. Inoltre, è previsto l'obbligo di assicurarsi che tutti i pagamenti siano avvenuti con precisa regolarità: in particolare, bisognerà verificare che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
Monitoraggio flussi finanziari	La Società effettua un costante monitoraggio dei flussi finanziari aziendali, con particolare riferimento all'origine dei pagamenti; tali controlli devono tener conto della sede legale della controparte contrattuale (es. paradisi fiscali, paesi a rischio terrorismo),

	degli istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni) e di eventuali strutture fiduciarie utilizzate per transazioni o operazioni straordinarie. Inoltre, si prevede che: • nel caso di elargizioni di danaro ad individui, società o organizzazioni è necessario controllare la serietà e la professionalità del destinatario del denaro. Inoltre deve essere redatto un piano d'investimento a giustificazione dell'investimento, comprensivo di controlli periodici dell'avanzamento del piano; • in caso di <i>Joint Venture</i>, la Società proceda alla verifica della congruità economica dell'investimento, avendo riguardo, nello specifico, al rispetto dei prezzi medi di mercato, all'utilizzo di professionisti di fiducia per l'effettuazione della <i>due diligence</i>; • la Società presti particolare attenzione ai pagamenti ricevuti da istituti di credito/clienti/partner/fornitori esteri. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 3 – Negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio

Gestione organizzativa ed operativa	L'eventuale coinvolgimento di consulenti, intermediari, agenti, promotori finanziari e <i>broker</i> a supporto della prestazione dei servizi della Società presuppone un'adeguata conoscenza degli stessi e la verifica, anche mediante attestazione degli interessati, della sussistenza dei requisiti di onorabilità previsti dalla legge e dell'assenza di situazioni di conflitto di interesse in capo ad essi. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	---

Protocollo 4 – Realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà

Gestione organizzativa ed operativa	La Società deve definire e rispettare i criteri che regolano la scelta delle associazioni/fondazioni in favore delle quali effettuare donazioni od erogazioni liberali di qualsiasi tipo, in modo che sia possibile accertare l'effettiva finalizzazione dell'iniziativa a scopi umanitari che non dissimolino attività di riciclaggio o terrorismo. In particolare: • donazioni e/o erogazioni liberali di qualsiasi tipo sono effettuate sulla base di una lista di associazioni/fondazioni accreditate quali potenziali beneficiarie. Le modalità d'inserimento, mantenimento ed eliminazione delle associazioni/ fondazioni da tale lista sono debitamente formalizzate; • donazioni ed erogazioni liberali di qualsiasi tipo sono operate solo ove adeguatamente autorizzate, formalizzate e rendicontate; • la Società non effettua donazioni né erogazioni liberali di qualsiasi tipo tramite versamenti in contanti o su conti correnti cifrati. Tutte le criticità riscontrate devono essere immediatamente segnalate all'Organismo di Vigilanza.
--	--

8.12 Compiti dell'Organismo di Vigilanza.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- a. svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente la sua efficacia a prevenire la commissione dei reati di cui all'art. 25-octies del Decreto. A tal fine, l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di reati di riciclaggio, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;
- b. proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle aree a rischio individuate nella presente Parte Speciale.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

8.13 Regole di comportamento e Protocolli operativi in materia di reati tributari (art. 25-quinquiesdecies del Decreto)

Il Decreto Legge n. 124 del 26 ottobre 2019, convertito con modificazioni nella Legge n. 157 del 19 dicembre 2019, ha introdotto i reati tributari nell'elenco dei reati presupposto della responsabilità amministrativa degli enti. Con l'inserimento nel Decreto 231 dell'art. 25-quinquiesdecies viene prevista, dunque, una nuova responsabilità nei confronti dell'ente in caso di commissione, nel suo interesse o a suo vantaggio, di alcuni dei reati tributari contemplati nel D.Lgs. 10 marzo 2000, n. 74 "Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della Legge 25 giugno 1999, n. 205".

Successivamente, il 30 luglio 2020, il D.Lgs. 75/2020 (in adempimento alla Direttiva UE/2017/1371 c.d. "PIF") ha esteso ulteriormente il catalogo dei reati tributari presupposto per la responsabilità dell'ente.

Sotto il profilo strettamente fiscale, la Direttiva PIF prevede come soglia minima di tutela la repressione di gravi frodi IVA, ossia di tutte quelle *"azioni od omissioni di carattere intenzionale secondo la definizione di cui all'art. 3, paragrafo 2, lettera d), [che] siano connesse al territorio di due o più Stati membri dell'Unione e comportino un danno complessivo pari ad almeno 10 mln di euro"*, ferma restando la facoltà per la legislazione nazionale di mantenere o adottare norme più rigorose.

Al fine di comprendere cosa possa essere considerato come *"frode che lede gli interessi finanziari dell'Unione"* la menzionata Direttiva, all'art. 3, paragrafo 2, lettera d), precisa che la suddetta frode è l'azione od omissione commessa in sistemi fraudolenti transfrontalieri in relazione:

- "i) all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti relativi all'IVA, cui consegua la diminuzione di risorse del bilancio dell'Unione;*
- ii) alla mancata comunicazione di un'informazione relativa all'IVA in violazione di un obbligo specifico, cui consegua lo stesso effetto;*
- iii) alla presentazione di dichiarazioni esatte relative all'IVA per dissimulare in maniera fraudolenta il mancato pagamento o la costituzione illecita di diritti a rimborsi dell'IVA".*

Si riporta di seguito il testo dell'art. 25-quinquiesdecies del D. Lgs. 231/2001.

Art. 25-quinquiesdecies**Reati tributari**

* * *

"1. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'ente le seguenti sanzioni pecuniarie:

- a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
- d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
- e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
- f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
- g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

1-bis. In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

- e) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
- f) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
- g) per il delitto di indebita compensazione previsto dall'articolo 10 quater, la sanzione pecuniaria fino a quattrocento quote.
- h) Se, in seguito alla commissione dei delitti indicati ai commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

2. Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e) ”.

Ai fini della normativa tributaria di cui al Decreto Legislativo 10 marzo 2000, n. 74 rubricato “Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell’articolo 9 della Legge 25 giugno 1999, n. 205”, si applicano le seguenti definizioni di carattere generale applicabili a tutti i reati tributari:

- per *"fatture o altri documenti per operazioni inesistenti"* si intendono le fatture o gli altri documenti aventi rilievo probatorio analogo in base alle norme tributarie, (i) emessi a fronte di operazioni non realmente effettuate in tutto o in parte o (ii) che indicano i corrispettivi o l'imposta sul valore aggiunto in misura superiore a quella reale, ovvero (iii) che riferiscono l'operazione a soggetti diversi da quelli effettivi;
- per *"elementi attivi o passivi"* si intendono (i) le componenti, espresse in cifra, che concorrono, in senso positivo o negativo, alla determinazione del reddito o delle basi imponibili rilevanti ai fini dell'applicazione delle imposte sui redditi o sul valore aggiunto e (ii) le componenti che incidono sulla determinazione dell'imposta dovuta;
- per *"dichiarazioni"* si intendono anche le dichiarazioni presentate in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche o di sostituto d'imposta, nei casi previsti dalla legge;
- il *"fine di evadere le imposte"* e il *"fine di consentire a terzi l'evasione"* si intendono comprensivi, rispettivamente, anche (i) del fine di conseguire un indebito rimborso o il riconoscimento di un inesistente credito d'imposta, e (ii) del fine di consentirli a terzi;
- riguardo ai fatti commessi da chi agisce in qualità di amministratore, liquidatore o rappresentante di società, enti o persone fisiche, il *"fine di evadere le imposte"* ed il *"fine di sottrarsi al pagamento"* si intendono riferiti alla società, all'ente o alla persona fisica per conto della quale si agisce;
- per *"imposta evasa"* si intende la differenza tra l'imposta effettivamente dovuta e quella indicata nella dichiarazione, ovvero l'intera imposta dovuta nel caso di omessa dichiarazione, al netto delle somme versate dal contribuente o da terzi a titolo di acconto, di ritenuta o comunque in pagamento di detta imposta prima della presentazione della dichiarazione o della scadenza del relativo termine; non si considera imposta evasa quella teorica e non effettivamente dovuta collegata a una rettifica in diminuzione di perdite dell'esercizio o di perdite pregresse spettanti e utilizzabili;

- le soglie di punibilità riferite all'imposta evasa si intendono estese anche all'ammontare dell'indebito rimborso richiesto o dell'inesistente credito di imposta esposto nella dichiarazione;
- per "*operazioni simulate oggettivamente o soggettivamente*" si intendono (i) le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero (ii) le operazioni riferite a soggetti fittiziamente interposti;
- per "*mezzi fraudolenti*" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà.

8.14 La tipologia dei reati tributari (art. 25 quinquiesdecies del Decreto)

Le nuove fattispecie di reati tributari introdotte nell'elenco dei reati suscettibili di rilevare secondo il Decreto 231, sono dunque le seguenti:

- **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti** (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74).

La fattispecie di reato si configura a carico di coloro che, al fine di evadere le imposte sui redditi o sul valore aggiunto, indicano, in una delle dichiarazioni relative a dette imposte, elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.

Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

- **Dichiarazione fraudolenta mediante altri artifici** (art. 3, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si configura allorché, fuori dai casi previsti dall'articolo 2 (di cui sopra), al fine di evadere le imposte sui redditi o sul valore aggiunto, il soggetto autore del reato - (i) compiendo operazioni simulate oggettivamente o soggettivamente ovvero (ii) avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria - indichi in una delle dichiarazioni relative a dette imposte (a) elementi attivi per un ammontare inferiore a quello effettivo o (b) elementi passivi fittizi o (c) crediti e ritenute fittizi, quando, congiuntamente:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;

- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, (i) è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, (ii) è superiore a euro un milione cinquecentomila, ovvero (iii) qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

Ai fini dell'applicazione della norma non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

- **Emissione di fatture o altri documenti per operazioni inesistenti** (art. 8, comma 1 e comma 2-bis, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

Ai fini di quanto sopra indicato, l'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

- **Occultamento o distruzione di documenti contabili** (art. 10, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza allorché un soggetto, (i) al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero (ii) di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

- **Sottrazione fraudolenta al pagamento di imposte** (art. 11, D.Lgs. 10 marzo 2000, n. 74)

La fattispecie di reato si realizza:

a) allorché un soggetto - (i) al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero (ii) di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila - aliena simulatamente o compie altri atti

fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva.

b) allorché un soggetto - al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori - indica nella documentazione presentata ai fini della procedura di transazione fiscale (i) elementi attivi per un ammontare inferiore a quello effettivo o (ii) elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.

- **Dichiarazione infedele ex art. 4 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Si realizza qualora un soggetto, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:

- c. l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila;
- d. l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso ***"nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro"***, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Omessa dichiarazione ex art. 5 D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF)

Tale fattispecie punisce chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila. Punisce, altresì, chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

- **Indebita compensazione ex art. 10-quater D.Lgs. 74/2000** (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).

Tale ipotesi delittuosa si configura qualora un soggetto non versi le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti o crediti inesistenti, per un importo annuo superiore a cinquantamila euro.

Tale illecito è rilevante per la Cooperativa solo nel caso in cui sia commesso “***nell’ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l’imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro***”, in ottemperanza a quanto previsto dalla Direttiva PIF.

8.15 Sanzioni nei confronti dell’ente

In relazione alla commissione dei reati sopra elencati si applicano le seguenti sanzioni pecuniarie:

- art. 2 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 3 - Dichiarazione fraudolenta mediante altri artifici: sanzione pecuniaria fino a 500 quote;
- art. 8 - Emissione di fatture o altri documenti per operazioni inesistenti: sanzioni pecuniarie per il comma 1 fino a 500 quote e per il comma 2bis fino a 400 quote;
- art. 10 - Occultamento o distruzione di documenti contabili: sanzione pecuniaria fino a 400 quote;
- art. 11 - Sottrazione fraudolenta al pagamento di imposte: sanzione pecuniaria fino a 400 quote;
- art. 4 - Dichiarazione infedele: sanzione pecuniaria fino a 300 quote;
- art. 5 - Omessa dichiarazione: sanzione pecuniaria fino a 400 quote;
- art. 10-quater - Indebita compensazione: sanzione pecuniaria fino a 400 quote.

Nei casi previsti dai commi 1 e 2 dell'art. 25-quinquiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

8.16 Aumenti delle sanzioni nei confronti dell'ente

Le sanzioni pecuniarie sono aumentate di un terzo qualora, a seguito alla commissione dei delitti di cui trattasi (indicati nel comma 1 dell'art. 25-quinquiesdecies), l'ente abbia conseguito un profitto di rilevante entità.

8.17 Aree a rischio reato e processi sensibili

I processi sensibili individuati da HS che presentano il rischio di commissione dei reati di cui alla presente sezione riguardano le seguenti attività:

- Gestione della contabilità: con riferimento alla gestione della fatturazione attiva e passiva e all'emissione e contabilizzazione di fatture e altra documentazione afferente alla contabilità;
- Acquisto di beni e servizi - con riferimento all'attività di selezione e gestione dei fornitori esterni e di eventuali subappaltatori;
- Adempimenti fiscali e tributari in genere: con riferimento a i) predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere, ii) calcolo obbligazioni tributarie, iii) gestione adempimenti dichiarativi e contributivi e iv) pagamento delle imposte;
- Tenuta e custodia delle scritture contabili e fiscali: con riferimento alla conservazione, tracciabilità ed archiviazione di tutta la documentazione contabile e fiscale;
- Gestione di eventuali operazioni straordinarie: con riferimento ad eventuali trasformazioni, fusioni, scissioni, cessioni e/o conferimenti d'azienda, vendite di assets aziendali, ecc.

La tabella che segue indica in modo sintetico processi sensibili e relativi possibili reati tributari.

Processi sensibili	Reato
• <u>Gestione della contabilità</u> • <u>Acquisto di beni e servizi</u> • <u>Adempimenti fiscali e tributari in genere</u>	• Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2-bis D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione fraudolenta mediante altri artifici (art. 3, D.Lgs. 10 marzo 2000, n. 74);

• <u>Tenuta e custodia delle scritture contabili e fiscali</u> • <u>Gestione di eventuali operazioni straordinarie</u>	• Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, D.Lgs. 10 marzo 2000, n. 74); • Occultamento o distruzione di documenti contabili (art. 10, D.Lgs. 10 marzo 2000, n. 74); • Sottrazione fraudolenta al pagamento di imposte (art. 11, D.Lgs. 10 marzo 2000, n. 74); • Dichiarazione infedele ex art. 4 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Omessa dichiarazione ex art. 5 D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF); • Indebita compensazione ex art. 10-quater D.Lgs. 74/2000 (introdotto dal D.Lgs. 75/2020 – in vigore dal 30 luglio 2020 – in recepimento la Direttiva PIF).
---	---

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

8.18 Regole di comportamento

8.18.1 Principi generali e standard di controllo

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Sezione prevede l'espresso divieto di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-quinquiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;
- ✓ comunicare all'Agenzia delle Entrate e/o alle Autorità fiscali dati non rispondenti al vero, con il divieto di predisporre e fornire documenti falsi, omettere le informazioni dovute.

Inoltre,

- ✓ il personale dirigente è responsabile per la formazione e l'aggiornamento dei propri dipendenti e collaboratori. In particolare, il personale dirigente è tenuto a:
 - diffondere i principi di HS previsti dal Codice Etico;
 - promuovere i principi di trasparenza e chiarezza organizzativa fra i dipendenti in modo da favorirne la responsabilizzazione e il raggiungimento degli obiettivi programmati;
 - rendere chiare le regole di comportamento e gli standard richiesti dalla società nei rapporti con l'Agenzia delle Entrate e le Autorità fiscali;
 - rivedere annualmente i risultati ottenuti e le metodologie adottate;
- ✓ tutto il personale che ha, gerarchicamente, poteri direttivi e quindi di controllo e vigilanza sui dipendenti che operano con l'Agenzia delle Entrate e le Autorità fiscali, deve seguire con attenzione l'attività dei propri sottoposti e riferire immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità, oltre che instaurare controlli interni, anche a sorpresa, per assicurare che i libri contabili siano accurati e trasparenti;
- ✓ i dipendenti di HS che si occupano della predisposizione di dichiarazioni e comunicazioni concernenti la materia tributaria, dell'emissione di documentazione afferente alla contabilità, del ricevimento di documentazione afferente alla contabilità o del pagamento di imposte, devono prendere conoscenza delle specifiche procedure e linee guida predisposte dalla Società per evitare il rischio di violazioni in materia tributaria;
- ✓ tutti i consulenti in materia fiscale di HS devono essere informati circa le linee guida contro la commissione di reati tributari;
- ✓ qualunque criticità sorga nell'ambito del rapporto con l'Agenzia delle Entrate e le Autorità fiscali, deve essere immediatamente comunicato all'Organismo di Vigilanza con nota scritta, sulla base delle linee guida della Società richiamate nel Codice Etico di HS;
- ✓ su ogni singola attività sensibile è opportuno prevedere un monitoraggio periodico delle procedure (almeno annuale) al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative.

È, inoltre, sancito l'espresso obbligo di:

- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- garantire un corretto e trasparente processo di gestione delle operazioni straordinarie, compresa la vendita di eventuali asset aziendali;
- assicurare la veridicità dei dati predisposti;

- assicurare la trasparente gestione delle forniture, di beni e servizi;
- garantire il flusso informativo tra le funzioni coinvolte nei processi sensibili in materia contabile-fiscale con il Collegio Sindacale e l'Organismo di Vigilanza;
- svolgere un'adeguata attività di selezione dei fornitori;
- acquistare beni di provenienza garantita e servizi e/o qualsiasi altra utilità ad un prezzo che, salvo casi eccezionali e certificati (quali ad esempio acquisti da aste giudiziarie o da fallimenti), sia commisurato alla qualità e quantità dei beni stessi in base al valore di mercato;
- rispettare la normativa fiscale-tributaria;
- garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali.

Gli standard di controllo da considerare ed applicare con riferimento alle attività sensibili di cui alla presente sezione sono:

- **previsione di procedure interne** idonee a fornire i principi di riferimento generali per la regolamentazione dell'attività sensibile;
- **tracciabilità**: tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali/informatici;
- **segregazione dei compiti**: lo standard concerne l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di un sistema di segregazione delle funzioni coerente** con le responsabilità organizzative assegnate: sono previste regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

8.18.2 Principi procedurali specifici

In relazione alle procedure che seguono si segnala come HS abbia in uso il software gestionale GAMMA ENTERPRISE di Team System, il quale, oltre ad essere utilizzato per la maggior parte dei processi aziendali (gestione amministrativa, commerciale, produzione e controllo gestione), consente attraverso una procedura specifica la gestione della contabilità (prima nota, emissione e registrazione di documenti, fatture, archiviazione della documentazione fiscale).

Per quanto concerne la gestione della contabilità come anche la redazione del bilancio è previsto il supporto tecnico e consulenziale di una società di revisione contabile esterna alla Società sulla base di apposito contratto di servizio. L'intervento del consulente esterno prevede accessi settimanali per verifica della contabilità da un punto di vista fiscale (corretta indicazione e calcolo dell'IVA) nonché sostanziale (verifica della correttezza e congruità delle fatture emesse rispetto

all'oggetto), oltre alla redazione del bilancio e dei relativi documenti da presentare all'Assemblea dei Soci e alle dichiarazioni fiscali che vengono eseguite in nome del contribuente.

Il consulente non ha accesso al software GAMMA ENTERPRISE, ma solo al TS Digital di Team System, ovvero la piattaforma in uso alla Società che consente gestire la fatturazione elettronica attiva e passiva facendo da tramite con il cassetto fiscale presso la relativa piattaforma dell'Agenzia delle Entrate.

Protocollo 1 Definizione di ruoli e responsabilità Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti. Tenuta e custodia delle scritture contabili e fiscali Gestione delle operazioni straordinarie	
Definizione di ruoli e responsabilità	- Devono essere osservate specifiche procedure che garantiscano una chiara segregazione di funzioni e responsabilità, ovvero una netta ripartizione dei compiti tra le varie funzioni e quindi tra chi predispone e chi sottoscrive la documentazione da presentare all'Agenzia delle Entrate o alle altre Autorità fiscali [ad es., nel caso di predisposizione della documentazione ai fini di dichiarazioni e comunicazioni concernenti la materia tributaria, deve essere ben chiara la segregazione delle funzioni tra (i) chi è preposto alla elaborazione e raccolta della documentazione da presentare, (ii) chi verifica, approva e sottoscrive la documentazione da presentare. - Il rispetto dei poteri autorizzativi, delle deleghe, delle procure deve essere adeguatamente monitorato dall'Organismo di Vigilanza tramite interventi a campione sulla documentazione siglata.
Gestione contabilità, Approvvigionamenti di beni e servizi, Gestione buste paga e rimborsi spese ai dipendenti	È fatto obbligo di: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni nelle fasi di autorizzazione / esecuzione / controllo per i seguenti ambiti: - gestione della fatturazione e relativa registrazione - gestione dei pagamenti - gestione delle note di credito - gestione degli acquisti, di beni e servizi - gestione buste paga e rimborsi spesa ai dipendenti - tenere tracciate tutte le fasi di gestione dei flussi finanziari e archiviare in maniera completa i relativi documenti giustificativi; - prevedere un sistema di backup dell'archiviazione dei documenti contabili; - verificare l'effettiva e corretta esecuzione della prestazione richiesta (sia verso fornitori di beni che di servizi), nel rispetto del principio di segregazione delle funzioni, prima di autorizzare il pagamento della relativa fattura; - tenere traccia e registrare ogni richiesta di ordine e relativo preventivo inoltrato, sia che sia stato mandato via e-mail che telefonici (in quest'ultimo caso andrà compilato apposito modulo di richiesta ordine); - verificare che gli incassi siano sempre supportati da un contratto o un ordine autorizzato e conseguentemente non accettare beni e/o altre utilità a fronte delle quali non vi sia un contratto o un ordine adeguatamente autorizzato;

- verificare che l'importo effettivamente incassato corrisponda a quello fatturato e che non vi siano anomalie al riguardo;
 - rispettare le procedure adottate che regolano la gestione della contabilità;
 - rispettare il sistema di deleghe e procure adottato che indica i poteri ed i limiti di spesa dei soggetti coinvolti;
 - verificare periodicamente l'aggiornamento dell'anagrafica dei clienti e dei fornitori, al fine di controllarne l'effettiva esistenza ed operatività;
 - svolgere un'attenta attività di selezione dei potenziali fornitori (sia di beni che di servizi), rispettando i criteri tecnico-economici ed espletando un'adeguata attività selettiva e di obiettiva comparazione tra più offerte;
 - a seconda del servizio richiesto, richiedere al fornitore tutta la documentazione o le certificazioni previste dalla legge di riferimento;
 - formalizzare tutti i contratti/accordi con fornitori e/o consulenti, allegando la relativa documentazione;
 - qualora si faccia uso di soggetti terzi intermediari, verificare con attenzione l'esistenza effettiva, la solidità e l'affidabilità del soggetto;
 - monitorare il mantenimento dei requisiti richiesti in capo al fornitore;
 - inserire un'apposita clausola contrattuale che i Consulenti, i Partner ed i Fornitori devono sottoscrivere in cui dichiarano di essere a conoscenza e di impegnarsi a rispettare i principi previsti dal Codice Etico adottato dalla società, nonché dalla normativa di cui al D.Lgs. n. 231/2001. Tale clausola deve regolare anche le eventuali conseguenze in caso di violazione da parte degli stessi delle norme di cui al Codice Etico (es. clausole risolutive espresse, penali);
 - identificare i ruoli e le responsabilità per la gestione dei rimborsi spese ai dipendenti nel rispetto del principio di segregazione di ruoli nelle fasi di autorizzazione / esecuzione / controllo;
 - controllare che ogni richiesta di rimborso spese sia accompagnata dalla relativa documentazione giustificativa e conseguentemente non riconoscere alcuna somma che non sia supportata da relativo giustificativo.
- Inoltre, ai fini preventivi, si ribadisce che:
- è assolutamente vietato:
 - contabilizzare e registrare fatture per operazioni/prestazioni inesistenti;
 - autorizzare pagamenti a fornitori per operazioni inesistenti o privi dell'evidenza dell'effettuazione del servizio reso;
 - autorizzare rimborsi spesa privi della necessaria documentazione giustificativa;
 - predisporre o comunque utilizzare documenti palesemente falsi;
 - ogni pagamento deve corrispondere esattamente a quanto indicato nel contratto e/o nel preventivo formulato al cliente;
 - nessun pagamento e nessun incasso di denaro verso/da Paesi inseriti nelle principali black list internazionali, può avvenire senza adeguata documentazione comprovante la reale e specifica necessità;
 - nessun pagamento può essere effettuato in favore di un soggetto diverso dalla controparte contrattuale. Eventuali eccezioni a tale divieto sono ammesse solo a fronte della presentazione di una regolare documentazione che giustifichi e consente il pagamento nei confronti di un terzo (es. in caso di cessione del credito o pignoramento presso terzi);
 - nessun acquisto deve essere effettuato attraverso il ricorso a mercati non

	consolidati; - nessun contratto di fornitura può essere stipulato in assenza di un'adeguata attività di selezione o in mancanza della relativa documentazione richiesta dalla legge; - tutti gli incassi devono provenire dalla controparte contrattuale. Eventuali eccezioni sono ammesse solo a fronte della presentazione di una regolare documentazione giustificativa (es. pignoramento presso terzi); - ogni importo effettivamente incassato deve corrispondere a quanto fatturato. Qualora sia necessario restituire un pagamento o parte di esso indebitamente ricevuto, questo deve essere disposto esclusivamente verso il conto corrente di provenienza, tenendo traccia dei documenti giustificativi; - occorre tenere l'evidenza scritta di ogni pagamento; - occorre archiviare tutti i documenti contabili nel rispetto dei principi di correttezza, completezza e attenzione della relativa tenuta.
Tenuta e custodia delle scritture contabili e fiscali	In merito alla tenuta delle scritture contabili, è fatto obbligo: - identificare i ruoli e le responsabilità nel rispetto del principio di segregazione delle funzioni per i seguenti ambiti: - gestione degli adempimenti fiscali e tributari; - gestione del calcolo delle obbligazioni tributarie e dei relativi obblighi dichiarativi; - gestione e tenuta delle scritture contabili e fiscali; - tenere tracciate tutte le fasi di gestione dei citati processi e archiviare in maniera completa i relativi documenti; - prevedere un sistema di back up dell'archiviazione dei documenti contabili e fiscali; - prevedere modalità di aggiornamento, anche tramite consulenti esterni, sulle novità in ambito fiscale e tributario; - provvedere al regolare adempimento degli obblighi fiscali-tributari cui la società è tenuta (tributi, contributi, Iva etc.); - prevedere uno scadenziario che preveda i termini entro i quali occorre provvedere ai vari adempimenti fiscali-tributari. È, inoltre, vietato: - occultare o distruggere, in tutto o in parte, documenti contabili, fiscali o di cui è comunque obbligatoria la conservazione; - omettere o fornire dati ed informazioni inesatte o non complete imposte dalla legge sulla situazione economica, patrimoniale e finanziaria della società; - violare, eludere, evadere obblighi di dichiarazione, attestazione, certificazione di natura tributaria previsti dalla legge; - non adempiere le prescrizioni di legge in materia contabile, di informazione societaria, di valutazione di cespiti e di redazione del bilancio; - occultare in contabilità redditi conseguiti soggetti a tassazione, rappresentare falsamente spese non reali, emettere fatture per prestazioni inesistenti, effettuare stime, valutazioni e determinazione di poste di bilancio con modalità e criteri valutativi difforni da quelli richiesti dalla legge; - porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione da

	parte degli organi di controllo; ostacolare, in ogni modo, l'effettuazione di verifiche, accertamenti ed ispezioni da parte dell'Agenzia delle Entrate o delle altre Autorità fiscali o giudiziarie.
Gestione delle operazioni straordinarie	Con riferimento a tale attività è fatto obbligo di: - garantire l'esplicita approvazione, da parte dell'Assemblea dei Soci, di ogni attività relativa ad operazioni straordinarie, comprese le cessioni e dismissioni di assets aziendali, nonché in merito alla effettuazione di conferimenti, alla distribuzione di utili o riserve, a operazioni sul capitale sociale, a fusioni e scissioni, qualora per il compimento delle suddette operazioni si renda necessaria od opportuna l'approvazione dell'Assemblea; - identificare in maniera chiara e precisa i ruoli ed i soggetti competenti alla predisposizione della documentazione destinata agli organi sociali a supporto delle deliberazioni relative ad operazioni straordinarie; - identificare in maniera chiara ruoli e responsabilità in merito alla tenuta ed archiviazione degli atti di delibera e dei relativi documenti predisposti; - garantire una corretta tenuta ed archiviazione della documentazione relativa alle operazioni, prevedendo anche sistemi di back up.; È, inoltre, assolutamente vietato: - alienare simulatamente beni o assets aziendali al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; - compiere qualsiasi altro atto fraudolento al fine di rendere in tutto o in parte inefficace la procedura di riscossione coattiva; - indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila.

8.18.3 Responsabilità specifiche della Direzione Marketing e Commerciale (R. Mktg).

Con riferimento alla prevenzione del rischio di commissione dei reati tributari sarà compito del (R. Mktg):

- il responsabile della presente divisione dovrà supervisionare l'attività delle diverse funzioni a lui sottoposte come da organigramma e mansionario aziendale;
- in generale tutti i soggetti operanti all'interno della Direzione Marketing e Commerciale dovranno individuare potenziali clienti e formulare offerte sulla base dei listini;
- negoziare termini e condizioni di vendita: quantità, tempi, prezzi, modalità di consegna;
- registrare correttamente sul software gestionale in uso all'azienda tutte le condizioni di fornitura contrattate con terze parti che diventeranno oggetto di fatturazione attiva.

8.19 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'esito di eventuali audit effettuati sulla gestione delle attività sensibili sopra indicate, sia da parte di funzioni interne che da parte di soggetti esterni (ad es. consulenti fiscali, commercialisti, ecc.);
- l'avviso di eventuali ispezioni da parte dell'Agenzia delle Entrate o di altre autorità fiscali o giudiziarie con relativo verbale;
- eventuali comunicazioni provenienti dal Collegio Sindacale relativamente a criticità emerse, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-quinquiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- verificare periodicamente - con il supporto delle funzioni competenti - il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- curare l'aggiornamento del Modello, indicando al Consiglio di Amministrazione le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adequatezza e/o l'effettività dello stesso.

L'Organismo di Vigilanza deve riportare i risultati della sua attività di vigilanza e controllo, con cadenza periodica semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale.

Pertanto, nel caso in cui dagli accertamenti svolti dall'Organismo di Vigilanza emergano elementi che facciano risalire la violazione dei principi e protocolli contenuti nella presente Parte Speciale del Modello, la commissione del reato, o il tentativo di commissione del reato, direttamente al Presidente, l'Organismo di Vigilanza dovrà riferire al Consiglio di Amministrazione ed al Collegio

Sindacale, ai quali compete la decisione sull'eventuale applicazione dei meccanismi previsti dalla legge.

8.20 Regole di comportamento e Protocolli operativi in materia di reati di contrabbando (art. 25-sexiesdecies del Decreto)

Il reato di contrabbando, previsto all'art. 25-sexiesdecies del Decreto, è stato introdotto dal D.Lgs. 14 luglio 2020, n. 75 ("Attuazione della direttiva (UE) 2017/1371 c.d. "Direttiva PIF", relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale").

L'art. 25-sexiesdecies del D.Lgs. 231/01 dispone che: *"1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.*

2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.

3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

La Società ha ritenuto di dover mappare il rischio connesso alla commissione di reati di contrabbando stante la ingente attività di import ed export con diversi paesi UE ed extra UE.

A tal fine, si ritiene necessaria una breve premessa con riferimento alla materia doganale.

I dazi doganali rappresentano una risorsa propria dell'Unione europea e confluiscono nel bilancio unitario, ad esclusione di una percentuale del 25% che viene trattenuta dallo Stato di entrata delle merci a copertura delle spese di riscossione (fonte: dossier di documentazione parlamentare).

La normativa doganale è contenuta nel Decreto del Presidente della Repubblica 23 gennaio 1973 n. 43 (Testo Unico Doganale, "TUD").

Si considerano "diritti doganali" tutti quei diritti che la dogana è tenuta a riscuotere in forza di una legge, in relazione alle operazioni doganali. Fra i diritti doganali costituiscono "diritti di confine" (art. 34 del TUD):

- i dazi di importazione e quelli di esportazione;
- i prelievi e le altre imposizioni all'importazione o all'esportazione previsti dai regolamenti comunitari e dalle relative norme di applicazione;
- i diritti di monopolio, le sovrimposte di confine ed ogni altra imposta o sovrimposta di consumo a favore dello Stato (per quanto concerne le merci in importazione).

Per le merci soggette a diritti di confine, il presupposto dell'obbligazione tributaria è costituito, relativamente alle merci estere, dalla loro destinazione al consumo entro il territorio doganale e, relativamente alle merci nazionali e nazionalizzate, dalla loro destinazione al consumo fuori del territorio stesso (art. 36 del TUD).

8.21 Sanzioni nei confronti dell'Ente.

In relazione alla commissione dei reati di cui sopra si applicano all'ente le seguenti sanzioni pecuniarie:

- ✓ fino a 200 quote in relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica n. 43/1973, ovvero ai delitti del Titolo VII Capo I, intendendosi per tali i fatti ivi previsti (ma solo se superano 10mila euro di diritti di confine evasi) ed in particolare:
 - Articolo 282 (Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali)
 - Articolo 283 (Contrabbando nel movimento delle merci nei laghi di confine)
 - Articolo 284 (Contrabbando nel movimento marittimo delle merci)
 - Articolo 285 (Contrabbando nel movimento delle merci per via aerea)
 - Articolo 286 (Contrabbando nelle zone extra-doganali)
 - Articolo 287 (Contrabbando per indebito uso di merci importate con agevolazioni doganali)
 - Articolo 288 (Contrabbando nei depositi doganali)
 - Articolo 289 (Contrabbando nel cabotaggio e nella circolazione)
 - Articolo 290 (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti).
 - Articolo 291 (Contrabbando nell'importazione od esportazione temporanea)
 - Articolo 291-bis (Contrabbando di tabacchi lavorati esteri)
 - Articolo 291-ter (Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri)
 - Articolo 291-quater (Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri)
 - Articolo 292 (Altri casi di contrabbando)
 - Articolo 294 (Pena per il contrabbando in caso di mancato o incompleto accertamento dell'oggetto del reato)
 - alle contravvenzioni del Titolo VII Capo II, cioè ai fatti ivi previsti ma solo se superano i 10mila euro di diritti di confine evasi (articoli 302 e seguenti).

- ✓ fino a 400 quote qualora i diritti di confine dovuti superino i 100.000 Euro.

Nei casi previsti dai commi 1 e 2 dell'art. 25-sexiesdecies si applicano le sanzioni interdittive di cui all'articolo 9, comma 2 lettere c), d) ed e) del Decreto, ovvero del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio, dell'esclusione da agevolazioni finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e del divieto di pubblicizzare beni e servizi.

8.22 Aree a rischio reato e processi sensibili

I processi sensibili che presentano il rischio di commissione dei reati di cui al presente paragrafo riguardano le seguenti attività:

- vendita, acquisto, commercializzazione e scambio di prodotti oltre confine;
- scarico e deposito delle merci oltre confine.

Le potenziali aree a rischio reato che HS ha astrattamente individuato sono quelle relative alle seguenti attività:

Processi sensibili	Reato
• Vendita, acquisto, commercializzazione e scambio di prodotti oltre confine • Scarico e deposito delle merci oltre confine	• Contrabbando (Decreto del Presidente della Repubblica n. 43/1973);

Eventuali modifiche o integrazioni delle suddette aree a rischio reato sono rimesse alla competenza del CDA, anche su proposta dell'Organismo di Vigilanza, il quale potrà procedere con la successiva attività di ratifica secondo quanto indicato nella parte generale del presente Modello.

8.23 Regole di comportamento.

8.23.1 Principi generali e standard di controllo.

Nell'espletamento delle rispettive attività e funzioni, oltre a conoscere e rispettare le regole disciplinate dallo Statuto della Società, e i principi dettati dal Codice Etico, le procedure operative e ogni altra normativa interna relativa al sistema di *Corporate Governance*, i Destinatari dovranno rispettare le regole di comportamento contenute nel presente Modello.

In particolare, la presente Parte Speciale prevede l'espresso divieto di porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-sexiesdecies del Decreto) o comportamenti che, sebbene non costituiscano di per sé fattispecie di reato, possano potenzialmente integrare uno dei reati qui in esame;

Inoltre, è fatto specifico divieto di:

- introdurre merci estere attraverso il confine di terra in violazione delle prescrizioni, divieti e limitazioni;
- introdurre merci estere via mare in violazione delle prescrizioni, divieti e limitazioni;
- scaricare o depositare merci estere nello spazio intermedio tra la frontiera e la più vicina dogana;
- nascondere merci estere sulla persona o nei bagagli o fra merci di altro genere od in qualunque mezzo di trasporto, per sottrarle alla visita doganale;
- asportare merci dagli spazi doganali senza aver pagato i diritti dovuti senza averne garantito il pagamento;
- portare fuori del territorio doganale merci nazionali o nazionalizzate soggette a diritti di confine;
- detenere merci estere, quando ricorrano le circostanze previste nel secondo comma dell'art. 25-sexiesdecies per il delitto di contrabbando (ovvero, *"Quando i diritti di confine dovuti superano centomila euro"*).

8.23.2 Principi procedurali specifici.

Protocollo 1 Controllo interno sull'emissione e la conservazione dei documenti fiscali	
Applicazione di misure idonee ad evitare l'emissione di documentazione contabile non coerente con la prestazione o la distruzione di documenti fiscali al fine di eventuali controlli da parte delle Autorità Doganali	Devono essere osservate specifiche misure che consentano di: ● evitare di introdurre o esportare merci che violino prescrizioni, divieti e limitazioni di cui al Testo unico delle disposizioni legislative in materia doganale; ● conservare la documentazione doganale; ● non sottrarsi alle visite doganali; ● pagare i diritti dovuti o garantire i dovuti pagamenti.

Con riferimento e per l'espletamento delle operazioni doganali di import ed export la HS si affida a società selezionate per la notorietà e l'esperienza nel settore delle spedizioni e della consulenza per logistica e trasporti a livello internazionale nonché per le pratiche doganali in import/export. L'affidamento di tali incarichi viene fatto a mezzo contratti di mandato e consulenza annuali e/o a tempo indeterminato.

Dovrà essere cura dei Destinatari della presente sezione di verificare la validità e la vigenza dei suddetti contratti di mandato.

8.24 Compiti dell'Organismo di Vigilanza.

Attraverso l'utilizzo degli appositi canali di comunicazione, dovranno essere immediatamente trasmesse all'Organismo di Vigilanza le seguenti informazioni:

- l'avviso di eventuali ispezioni da parte delle Autorità doganali o di altre autorità giudiziarie sempre relativamente alla materia doganale;
- eventuali comunicazioni provenienti dalle Autorità doganali o di altre autorità giudiziarie relativamente a criticità emerse in materia doganale, anche qualora risolte.

Fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), è compito dell'Organismo di Vigilanza:

- ✓ svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare la sua efficacia a prevenire la commissione dei reati di cui all'art 25-sexiesdecies del Decreto, attraverso controlli campione sulle citate aree a rischio reato;
- ✓ verificare periodicamente – con il supporto delle funzioni competenti – il sistema di deleghe e procure in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti agli esponenti aziendali;
- ✓ esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo o da terzi, valutandone l'attendibilità e facendo gli accertamenti ritenuti necessari od opportuni;
- ✓ comunicare eventuali violazioni del Modello agli organi competenti in base al sistema disciplinare per l'adozione di provvedimenti sanzionatori;
- ✓ curare l'aggiornamento del Modello, indicando al CDA le opportune integrazioni e le misure ritenute necessarie al fine di preservare l'adeguatezza e/o l'effettività dello stesso.

9 SEZIONE I – FUNZIONI AZIENDALI ESTERNALIZZATE: IL RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE (RSPP).

Al fine di predisporre un efficace sistema di gestione della sicurezza sui luoghi di lavoro è stato istituito all'interno di HS un Servizio di Prevenzione e Protezione dei rischi (di seguito il SPP).

Secondo quanto disposto dal D.Lgs. 81/2008 (Testo Unico sulla Sicurezza sul lavoro), in tale ambito figura aziendale obbligatoria è il Responsabile del Servizio Prevenzione e Protezione (di seguito RSPP).

Questo compito viene svolto in HS da un consulente esterno, in possesso delle capacità e dei requisiti professionali richiesti dalla normativa (ovvero dall'articolo 32, D.Lgs. 81/2008) ed appositamente nominato dal Datore di Lavoro.

Gli obblighi del RSPP vengono indicati nel D.Lgs. 81/2008, in particolare nell'articolo 33 "Compiti del servizio di prevenzione e protezione", e nell'articolo 35 "Riunione periodica".

Nello specifico è previsto che il RSPP, in collaborazione con il Datore di Lavoro, il Medico Competente e il Rappresentante dei Lavoratori provveda:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2 del D.Lgs. 81/2008 (ovvero il Documento Valutazione Rischi - DVR), e i sistemi di controllo di tali misure;
- ad elaborare le procedure di sicurezza per le varie attività aziendali;
- a proporre i programmi di informazione e formazione dei lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35, D.Lgs. 81/2008;
- a fornire ai lavoratori le informazioni sui rischi per la salute e sicurezza sul lavoro connessi alla attività della impresa in generale, sui rischi specifici cui è esposto in relazione all'attività svolta, alle normative di sicurezza e alle disposizioni aziendali in materia, sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro, nonché sulle misure e le attività di protezione e prevenzione adottate (articolo 36, D.Lgs. 81/2008).

Al fine di una corretta gestione del Servizio di Prevenzione e Protezione, è necessario che, le eventuali istanze o problematiche raccolte dai lavoratori, attraverso il loro rappresentante, siano tempestivamente comunicate all'RSPP il quale, coordinandosi con il Datore di Lavoro, valuta ed elabora soluzioni per poi proporle alla dirigenza aziendale.

È, altresì, previsto che il RSPP, congiuntamente al Medico Competente, ispezioni gli ambienti di lavoro almeno due volte l'anno e fornisca con tempestività le valutazioni e i pareri di competenza al fine della programmazione del controllo dell'esposizione dei lavoratori.

In generale:

- è fatto obbligo al RSPP di rispettare rigorosamente il sistema di gestione della sicurezza e di svolgere tutte le attività di verifica e di controllo prescritte nei documenti aziendali in materia di salute e sicurezza nonché nelle disposizioni di legge e regolamentari vigenti;
- le verifiche ed il controllo devono assicurare che le misure di prevenzione e protezione dei rischi siano idonee ed efficaci;
- le attività di verifica e di controllo devono, tra l'altro, riguardare le misure tecniche, organizzative e procedurali attuate da HS;
- le attività di verifica e controllo potranno essere svolte anche con l'ausilio di altre risorse interne od esterne;
- le operazioni di verifica e controllo devono essere documentate;
- le verifiche dovranno essere estese ad eventuali incidenti o quasi incidenti, anche in itinere, in modo da individuare la causa di tali eventi e le possibili azioni correttive e/o preventive da adottarsi, ivi incluse le eventuali misure tecniche e gestionali per evitare il ripetersi di tali eventi o per impedirne l'evoluzione in un possibile incidente rilevante.

9.1 Rapporti tra il RSPP e l'Organismo di Vigilanza.

In relazione al controllo sul rispetto delle disposizioni in materia di salute e sicurezza sul lavoro contenute nel presente Modello, l'Organismo di Vigilanza dovrà avvalersi delle risorse aziendali che gestiscono i relativi aspetti (tra cui, il Responsabile del Servizio di Prevenzione e Protezione, il Rappresentante dei Lavoratori, il Medico Competente, gli Addetti al Primo Soccorso, alle emergenze, ecc.).

In aggiunta agli obblighi informativi di carattere generale previsti nel Modello di Organizzazione, Gestione e Controllo devono essere trasmesse all'Organismo di Vigilanza, a titolo esemplificativo, le informazioni relative:

- ad eventuali infortuni, situazioni di emergenza, di primo soccorso;
- al numero degli infortuni nonché alle circostanze di tempo e di luogo in cui gli stessi si sono verificati;
- ad eventuali anomalie, difformità riscontrate nello svolgimento delle attività di controllo, verifica e monitoraggio;
- ad eventuali omissioni, violazioni delle procedure poste a presidio della sicurezza;

- agli aspetti più significativi emersi nel corso di verifiche ispettive e simili attività di controllo, con particolare riguardo agli esiti di tali verifiche ispettive;
- agli aspetti più significativi connessi con le attività di manutenzione degli impianti, apparecchiature ed attrezzature di lavoro;
- agli aspetti più significativi connessi all'assunzione e qualificazione del personale, organizzazione del lavoro e delle postazioni di lavoro, acquisto di beni e servizi in materia di sicurezza;
- ad eventuali comunicazioni trasmesse per omissioni e/o violazioni in materia di sicurezza;
- ad eventuali provvedimenti disciplinari adottati per omissioni e/o violazioni in materia di sicurezza.

L'Organismo di Vigilanza effettua i controlli ritenuti necessari ed ha la facoltà di chiedere tutte le ulteriori informazioni ritenute necessarie od opportune ai fini dell'attività di vigilanza.

Su base periodica (trimestrale o semestrale o all'occorrenza), l'Organismo di Vigilanza effettua le proprie verifiche sull'efficacia ed effettività del Modello di Organizzazione, Gestione e Controllo, anche tramite controlli a campione.

I risultati dell'attività dell'Organismo di Vigilanza devono essere riportati al Consiglio di Amministrazione ed al Collegio Sindacale, nonché ai responsabili delle funzioni aziendali interessate; in particolare, il flusso informativo nei confronti del Consiglio di Amministrazione e del Collegio Sindacale deve consentire a tali organi di poter tempestivamente intervenire per l'adozione delle eventuali azioni correttive.