

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Ai sensi dell'art. 6, comma 1, lett. A del D. Lgs. 8 giugno 2001, n. 231

Versione approvata dal Consiglio di Amministrazione di Reply SpA
13 marzo 2025



INDICE

PARTE GENERALE	7
1. Il Decreto Legislativo 231/2001	8
1.1. Premessa	8
1.2. Normativa.....	8
1.2.1 I reati.....	8
1.2.2. I soggetti destinatari del Decreto	12
1.2.3. La condizione esimente	13
1.3. Le Linee Guida di Confindustria	13
2. Adozione del Modello nell'ambito del Gruppo Reply	14
2.1. Modello e Codice Etico	14
2.2. Struttura del Modello.....	15
2.3. Principi generali per l'adozione del Modello	15
2.4. Approvazione del Modello e suo recepimento nell'ambito del Gruppo.....	16
2.5. Modifiche e integrazioni del Modello	17
2.6. Coordinamento sui sistemi di controllo e verifica sul piano generale dell'efficacia del Modello	17
2.7. L'adozione del Modello Organizzativo nell'ambito del Gruppo.....	18
3. Metodologia seguita per l'individuazione delle attività sensibili e dei processi di supporto	18
3.1. Individuazione delle attività a rischio reato.....	19
4. Organismo di Vigilanza	19
4.1. Modalità di nomina e di revoca dell'Organismo di Vigilanza.....	20
4.2. Compiti dell'Organismo di Vigilanza	21
4.3. Requisiti e poteri dell'Organismo di Vigilanza	22
4.4. Flussi informativi nei confronti dell'Organismo di Vigilanza.....	23
4.5. Funzioni di coordinamento dell'Organismo di Vigilanza di Reply SpA con gli Organismi di Vigilanza delle altre società del Gruppo	25
5. Il Sistema di segnalazione Whistleblowing	25
6. La formazione delle risorse e la diffusione del Modello	27
6.1. Formazione ed informazione dei Dipendenti	27
6.2. Consulenti, partner e fornitori	27
7. Sistema disciplinare	28
7.1. Misure nei confronti di quadri e impiegati.....	28
7.2. Misure nei confronti dei dirigenti	29



7.3.	Misure nei confronti degli amministratori	29
7.4.	Misure nei confronti dei sindaci	29
7.5.	Misure nei confronti dei consulenti e dei partner	30
8.	Aggiornamento ed adeguamento del Modello	30
PARTE SPECIALE.....		31
9.	Reati rilevanti	32
9.1.	Principi di comportamento	33
9.2.	Approccio metodologico	33
10.	Parte Speciale “A”: Reati nei Rapporti con la Pubblica Amministrazione e di Corruzione tra privati.....	35
10.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	35
10.2.	Le fattispecie di reato applicabili	36
10.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati nei Rapporti con la Pubblica Amministrazione e alla Corruzione tra privati.....	36
10.3.1.	Rapporti con la PA	36
10.3.2.	Corruzione tra privati	38
10.4.	Gli standard di controllo specifici.....	39
10.5.	Compiti dell’Organismo di Vigilanza	41
11.	Parte Speciale “B”: Reati informatici e trattamento illecito di dati	42
11.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	42
11.2.	Le fattispecie di reato applicabili	43
11.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati informatici.....	43
11.4.	Gli standard di controllo specifici.....	44
11.5.	Compiti dell’Organismo di Vigilanza	45
12.	Parte Speciale “C”: Delitti contro l’industria e il commercio.....	46
12.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	46
12.2.	Le fattispecie di reato applicabili	46
12.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Delitti contro l’industria e il commercio.....	46
12.4.	Gli standard di controllo specifici.....	47
12.5.	Compiti dell’Organismo di Vigilanza	47
13.	Parte Speciale “D”: Reati Societari.....	48
13.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	48
13.2.	Le fattispecie di reato applicabili	48
13.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati Societari.....	49



13.4.	Gli standard di controllo specifici.....	50
13.5.	Compiti dell'Organismo di Vigilanza	53
14.	Parte Speciale "E": Reati con finalità di terrorismo o di eversione dell'ordine democratico; Delitti di criminalità organizzata; Reato di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare; Reati transnazionali; Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.....	54
14.1.	Reati con finalità di terrorismo o di eversione dell'ordine democratico	54
14.1.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	54
14.1.2.	Le fattispecie di reato applicabili	54
14.1.3.	I Principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati con finalità di terrorismo o di eversione dell'ordine democratico.....	55
14.1.4.	Gli standard di controllo specifici.....	55
14.1.5.	Compiti dell'Organismo di Vigilanza	56
14.2.	Delitti di criminalità organizzata.....	57
14.2.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	57
14.2.2.	Le fattispecie di reato applicabili	57
14.2.3.	I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti di criminalità organizzata	58
14.2.4.	Gli standard di controllo specifici.....	58
14.2.5.	Compiti dell'Organismo di Vigilanza	60
14.3.	Reati di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare	61
14.3.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	61
14.3.2.	Le fattispecie di reato applicabili	61
14.3.3.	I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative al Reato di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare	62
14.3.4.	Gli standard di controllo specifici.....	62
14.3.5.	Compiti dell'Organismo di Vigilanza	63
14.4.	Reati transnazionali.....	64
14.4.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	64
14.4.2.	Le fattispecie di reato applicabili	64
14.4.3.	I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati transnazionali.....	64
14.4.4.	Gli standard di controllo specifici.....	65
14.4.5.	Compiti dell'Organismo di Vigilanza	67
14.5.	Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.....	67
14.5.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	67
14.5.2.	Le fattispecie di reato applicabili	68
14.5.3.	I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.....	68
14.5.4.	Gli standard di controllo specifici.....	71
14.5.5.	Compiti dell'Organismo di Vigilanza	72
15.	Parte Speciale "F": Reati di abuso di mercato.....	74



15.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	76
15.2.	Le fattispecie di reato applicabili	76
15.3.	I Principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati di abuso di mercato	76
15.4.	Gli standard di controllo specifici.....	77
15.5.	Compiti dell’Organismo di Vigilanza	78
16.	Parte Speciale “G”: Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro	80
16.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	82
16.2.	Le fattispecie di reato applicabili	82
16.3.	Principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro	82
16.4.	Gli standard di controllo specifici.....	84
16.5.	Compiti dell’Organismo di Vigilanza	85
17.	Parte Speciale “H”: Delitti in materia di violazione del Diritto d’Autore	87
17.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	87
17.2.	Le fattispecie di reato applicabili	87
17.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Delitti in materia di violazione del Diritto d’Autore	88
17.4.	Gli standard di controllo specifici.....	88
17.5.	Compiti dell’Organismo di Vigilanza	89
18.	Parte Speciale “I”: Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria.....	90
18.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	90
18.2.	Le fattispecie di reato applicabili	90
18.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative all’Induzione a non rendere Dichiarazioni o a rendere Dichiarazioni mendaci all’Autorità Giudiziaria	90
18.4.	Gli standard di controllo specifici.....	90
18.5.	Compiti dell’Organismo di Vigilanza	91
19.	Parte speciale “L”: Reati tributari	92
19.1.	Le “Aree Sensibili” ai fini del D.Lgs. 231/2001	92
19.2.	Le fattispecie di reato applicabili	92
19.3.	I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati Tributari	92
19.4.	Gli standard di controllo specifici.....	94



19.5.	Compiti dell'Organismo di Vigilanza	96
20.	Parte Speciale "M": Delitti contro la personalità individuale e di Razzismo e Xenofobia.....	97
20.1.	Delitti contro la personalità individuale.....	97
20.2.	Reati di Razzismo e Xenofobia.....	100
21.	Parte Speciale "N": Reati Ambientali.....	103
21.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001	103
21.2.	Le fattispecie di reato applicabili	103
21.3.	I principi generali di comportamento da tenere nell'ambito delle attività di rischio relative ai Reati Ambientali.....	103
21.4.	Gli standard di controllo specifici.....	103
21.5.	Compiti dell'Organismo di Vigilanza	104
22.	Parte Speciale "O": Delitti contro il patrimonio culturale e paesaggistico	105
22.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001	105
22.2.	Le fattispecie di reato applicabili	105
22.3.	I principi generali di comportamento da tenere nell'ambito delle attività di rischio relative ai Delitti contro il patrimonio culturale	105
22.4.	Gli standard di controllo specifici.....	105
22.5.	Compiti dell'Organismo di Vigilanza	106
23.	Parte Speciale "P": Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.....	107
23.1.	Le "Aree Sensibili" ai fini del D.Lgs. 231/2001.....	107
23.2.	Le fattispecie di reato applicabili	107
23.3.	I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.....	108
23.4.	Gli standard di controllo specifici.....	109
23.5.	Compiti dell'Organismo di Vigilanza	112



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi dell'art. 6, comma 1, lett. a)
del D. Lgs. 8 giugno 2001, n. 231

PARTE GENERALE



1. Il Decreto Legislativo 231/2001

1.1. Premessa

La società Reply SpA (di seguito anche “**Capogruppo**”), le società da essa controllate e i Consorzi costituiti dalla Capogruppo e dalle società controllate (di seguito “**Reply**”, “**Gruppo Reply**” o “**Gruppo**”) sono da sempre sensibili all’esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della propria posizione ed immagine, delle aspettative dei propri azionisti e del lavoro dei propri dipendenti.

In tale contesto, Reply SpA ha ritenuto conforme alla propria politica procedere all’adozione del Modello di organizzazione, gestione e controllo (di seguito “**Modello Organizzativo**” o “**Modello**”) previsto dal Decreto Legislativo 231/2001 (di seguito anche “**Decreto**” o “**D. Lgs. 231/2001**”) nell’ambito del proprio Gruppo.

A tal fine, il Gruppo Reply ha avviato e monitorato nel tempo un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure adottate con le finalità previste dal Decreto.

Il presente Modello ed i principi in esso contenuti si applicano agli organi societari (intendendosi per tali, tra gli altri, il Consiglio di Amministrazione, di seguito anche “**Organo Amministrativo**”, e il Collegio Sindacale di Reply SpA e i relativi componenti), ai dipendenti, ai collaboratori, ai consulenti, ai fornitori, ai partner e, più in generale, a tutti coloro che, a qualunque titolo, operano nell’ambito delle attività “sensibili” per conto o nell’interesse del Gruppo (di seguito “**Destinatari**”).

1.2. Normativa

Il Decreto Legislativo 8 giugno 2001, n. 231, recante “*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’art. 11 della legge 29 settembre 2000, n. 300*” ha introdotto per la prima volta nel nostro ordinamento la responsabilità in “sede penale” degli enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito.

1.2.1 I reati

La responsabilità degli enti non è riferibile a qualsiasi reato, ma è circoscritta alle fattispecie criminose richiamate nel D. Lgs. 231/01 (così come modificato dalla sua entrata in vigore ad oggi) e, più precisamente:

- (i) **reati contro la Pubblica Amministrazione**¹, richiamati dagli artt. 24 e 25 del Decreto;

¹ L’articolo 24 è stato modificato dalla Legge n. 161/2017, dal D. Lgs. n. 75/2020, dalla Legge n. 137/2023 e dalla Legge 90/2024.

L’articolo 25 è stato modificato dalla Legge n. 190/2012, dalla Legge n. 3/2019, dal D. Lgs. 75/2020 e dalla Legge n. 112/2024.



- (ii) **falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento**, richiamati dall'art. 25-*bis*², introdotto nel Decreto dal D. Lgs. del 25 settembre 2001, n. 350;
- (iii) **delitti contro l'industria e il commercio**, richiamati dall'art. 25-*bis*.1, introdotto nel Decreto dalla Legge del 23 luglio 2009, n. 99³;
- (iv) **reati societari**, richiamati dall'art. 25-*ter*, introdotto nel Decreto dal D. Lgs. del 11 aprile 2002, n. 61 e s.m.i.⁴;
- (v) **reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali**, richiamati dall'art. 25-*quater*, introdotto nel Decreto dalla Legge n. 7/2003⁵;

² I reati di cui all'art 25-*bis* comprendono: falsificazione in monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.); alterazione di monete (art. 454 c.p.); spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.); spendita di monete falsificate ricevute in buona fede (art. 457 c.p.); falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.); contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.); fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.); uso di valori di bollo contraffatti o alterati (art. 464 c.p.); 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.).

L'articolo 25-*bis* è stato aggiunto dal D. Lgs. 350/2001; convertito con modificazioni dalla Legge n. 409/2001; modificato dalla Legge n. 99/2009; modificato dal D. Lgs. 125/2016.

³ Detti reati comprendono: 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., delitto introdotto *ex novo*); contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p., delitto introdotto *ex novo*).

⁴ Così come modificati dalla Legge 190/2012, dalla Legge 69/2015, dal D. Lgs. 38/2017 e dal D. Lgs. 19/2023.

⁵ Si tratta dei *"delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali"*, nonché dei delitti, diversi da quelli sopra indicati, *"che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999"*. Tale Convenzione punisce chiunque, illegalmente e dolosamente, fornisce o raccoglie fondi sapendo che gli stessi saranno, anche parzialmente, utilizzati per compiere: (i) atti diretti a causare la morte - o gravi lesioni - di civili, quando l'azione sia finalizzata ad intimidire una popolazione, o coartare un governo o un'organizzazione internazionale; (ii) atti costituenti reato ai sensi delle convenzioni in materia di: sicurezza del volo e della navigazione, tutela del materiale nucleare, protezione di agenti diplomatici, repressione di attentati mediante uso di esplosivi. La categoria dei *"delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali"* è menzionata dal Legislatore in modo generico, senza indicare le norme specifiche la cui violazione comporterebbe l'applicazione del presente articolo.

Si possono, in ogni caso, individuare quali principali reati presupposti: associazioni sovversive (art. 270 c.p.), associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis* c.p.) e assistenza agli associati (art. 270-*ter* c.p.), arruolamento con finalità di terrorismo anche internazionale (art. 270-*quater* c.p.), addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-*quinquies* c.p.), finanziamento di condotte con finalità di terrorismo (Legge n. 151/2016, art. 270-*quinquies*.1 c.p.), sottrazione di beni o denaro sottoposti a sequestro (art. 270-*quinquies*.2 c.p.), condotte con finalità di terrorismo (art. 270-*sexies* c.p.), attentato per finalità terroristiche o eversione (art. 280 c.p.), atto di terrorismo con ordigni micidiali o esplosivi (art. 280-*bis* c.p.), atti di terrorismo nucleare (art. 280-*ter* c.p.), sequestro di persona a scopo di terrorismo o di eversione (art. 289-*bis* c.p.), istigazione a commettere alcuno dei delitti previsti dai Capi primo e secondo (art. 302 c.p.), cospirazione politica mediante accordo (art. 304 c.p.), cospirazione politica mediante associazione (art. 305 c.p.), banda armata: formazione e partecipazione (art. 306 c.p.), assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.), impossessamento, dirottamento e distruzione di un aereo (Legge n. 342/1976, art. 1), danneggiamento delle installazioni a terra (Legge n. 342/1976, art. 2), sanzioni (Legge n. 422/1989, art. 3), pentimento operoso (D. Lgs. n. 625/1979, art. 5).



- (vi) **delitti in materia di pratiche di mutilazione degli organi genitali femminili**, richiamati dall'art. 25-*quater*.1, introdotto nel Decreto dalla Legge del 9 gennaio 2006, n. 7⁶;
- (vii) **delitti contro la personalità individuale**, richiamati dall'art. 25-*quinquies*, introdotto nel Decreto dalla Legge dell'11 agosto 2003, n. 228⁷;
- (viii) **reati di abuso di mercato**, richiamati dall'art. 25-*sexies*, introdotto nel D. Lgs. 231/2001 dall'art. 9 della Legge del 18 aprile 2005, n. 62⁸;
- (ix) **altre fattispecie in materia di abusi di mercato**, richiamati dall'art. 187-*quinquies* TUF⁹;
- (x) **reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro**, richiamati dall'art. 25-*septies*, introdotto nel Decreto dall'art. 9 della Legge del 3 agosto 2007, n. 123 e s.m.i.¹⁰;
- (xi) **reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio**, richiamati dall'art. 25-*octies*, introdotti nel Decreto dall'art. 72 del D. Lgs. del 21 novembre 2007, n. 231¹¹;
- (xii) **delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori**, richiamati dall'art. 25-*octies*.1, introdotti nel Decreto dall'art. 3 del D. Lgs. dell'8 novembre 2021, n. 184¹²;
- (xiii) **altre fattispecie in materia di strumenti di pagamento diversi dai contanti**, richiamati dall'art. 25-*octies*.1, comma 213, introdotto nel Decreto dall'art. 3 dell'8 novembre 2021, n. 184;

⁶ Si riferisce ai delitti di pratiche di mutilazione degli organi genitali femminili di cui all'art. 583-*bis* c.p.

⁷ Come da ultimo modificati dalla Legge 23 dicembre 2021, n. 238, recante “*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*”.

⁸ Come da ultimo modificati dalla Legge 23 dicembre 2021, n. 238, recante “*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*”.

⁹ I reati di cui all'art. 187-*quinquies* TUF comprendono: divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE n. 596/2014); divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014).

L'articolo è stato modificato dal D. Lgs. 107/2018.

¹⁰ L'art. 25-*septies* è stato successivamente sostituito dall'art. 300, co.1, n. D. Lgs. 21/2008 e poi modificato dalla Legge n.3/2018.

¹¹ Detti reati comprendono: 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.) introdotto dalla Legge 186/2014. Sul punto, si segnala l'entrata in vigore, a far data dal 15 dicembre 2021, del D. Lgs. 195/2021 – in attuazione della Direttiva (UE) 2018/1673 in materia di lotta al riciclaggio mediante il diritto penale – il quale è intervenuto sulle fattispecie di reato appena richiamate, introducendo un'importante novità in tema di responsabilità degli enti. Segnatamente, dette categorie di reato non saranno più limitate alle condotte di natura dolosa ma ricomprenderanno altresì i delitti puniti a titolo di colpa e addirittura i casi in cui il fatto riguardi denaro o cose provenienti da contravvenzione (purché punita con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi).

¹² Il citato D. Lgs. 184/2021 ha operato alcune modifiche al Codice Penale e, segnatamente, ha: introdotto il nuovo art. 493-*quater*, ai sensi del quale viene sanzionata (con la reclusione fino a 2 anni e la multa fino ad Euro 1.000) la detenzione e la diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dal denaro contante; integrato il reato di frode informatica di cui all'art. 640-*ter*, introducendo una nuova circostanza aggravante che si concretizza ogni qualvolta l'alterazione di un sistema informatico determini un trasferimento di denaro, di valore monetario o di valuta virtuale; operato una modifica nella formulazione dell'art. 493-*ter*, relativo all'indebito utilizzo e falsificazione di carte di credito e di pagamento (le parole “*carte di credito o di pagamento ovvero qualsiasi altro documento*” sono state sostituite da “*strumenti di pagamento immateriali, carte di credito o di pagamento, ovvero qualsiasi altro strumento o documento*”). L'articolo 25-*octies*.1 è stato successivamente modificato dalla Legge 137/2023.

¹³ L'articolo 25-*octies*.1 comma 2 è stato aggiunto dal D. Lgs. 184/2021, modificato dalla Legge 137/2023.



- (xiv) **delitti in materia di violazione del diritto d'autore**, richiamati dall'art. 25-*novies*, introdotti nel Decreto dalla Legge del 23 luglio 2009, n. 99¹⁴;
- (xv) **delitti informatici e trattamento illecito di dati**, richiamati dall'art. 24-*bis*, introdotti nel Decreto dalla Legge del 18 marzo 2008, n. 48¹⁵;
- (xvi) **delitti di criminalità organizzata**, richiamati dall'art. 24-*ter*, introdotto nel Decreto dalla Legge del 15 luglio 2009, n. 94¹⁶;
- (xvii) **reati transnazionali**; l'art. 10 della Legge del 16 marzo 2006 n. 146 prevede la responsabilità amministrativa degli Enti anche con riferimento ai reati specificati dalla stessa legge che presentino la caratteristica della transnazionalità¹⁷;
- (xviii) **delitto consistente nel non rendere dichiarazioni o rendere dichiarazioni mendaci all'autorità giudiziaria**, richiamato dall'art. 25-*decies*, introdotto nel Decreto dalla Legge del 3 agosto 2009, n. 116, come sostituito dall'art. 2, comma 1, D. Lgs. 7 luglio 2011, n. 121;
- (xix) **reati ambientali**, richiamati dall'art. 25-*undecies*, introdotto nel Decreto dall'art. 4, comma 2, L. 3 agosto 2009, n. 116, come sostituito dall'art. 2, comma 1, D. Lgs. 7 luglio 2011, n. 121 e s.m.i.¹⁸;
- (xx) **reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare**, richiamato dall'art. 25-*duodecies*, introdotto nel Decreto dal D. Lgs. 109/2012¹⁹;

¹⁴ La citata Legge 99/2009 punisce: la messa a disposizione del pubblico non autorizzata in un sistema di reti telematiche, di un'opera dell'ingegno protetta, o parte di essa; l'utilizzo non autorizzato di un'opera altrui non destinata alla pubblicazione; la duplicazione di programmi per elaboratore o la distribuzione, vendita ecc. di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE); la duplicazione, riproduzione, ecc. di opere dell'ingegno destinate al circuito televisivo, cinematografico, ecc.; i produttori o importatori dei supporti non soggetti al contrassegno "SIAE"; la produzione, installazione ecc. di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato.

L'articolo 25-*novies* è stato successivamente modificato dalla Legge n. 93/2023.

¹⁵ Come da ultimo modificati dalla Legge 23 dicembre 2021, n. 238, recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*" e dalla Legge 90/2024.

¹⁶ Detti reati comprendono: associazione per delinquere (art. 416 c.p.); associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.); scambio elettorale politico-mafioso (art. 416-*ter* c.p.). Si segnala che l'art 1 della Legge 21 maggio 2019, n. 43 ha da ultimo modificato il testo di detto articolo che così recita: "*Chiunque accetta, direttamente o a mezzo di intermediari, la promessa di procurare voti da parte di soggetti appartenenti alle associazioni di cui all'art. 416-bis o mediante le modalità di cui al terzo comma dell'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di qualunque altra utilità o in cambio della disponibilità a soddisfare gli interessi o le esigenze dell'associazione mafiosa è punito con la pena stabilita nel primo comma dell'art. 416-bis. La stessa pena si applica a chi promette, direttamente o a mezzo di intermediari, di procurare voti nei casi di cui al primo comma. Se colui che ha accettato la promessa di voti, a seguito dell'accordo di cui al primo comma, è risultato eletto nella relativa consultazione elettorale, si applica la pena prevista dal primo comma dell'art. 416-bis aumentata della metà. In caso di condanna per i reati di cui al presente articolo, consegue sempre l'interdizione perpetua dai pubblici uffici.*"; sequestro di persona a scopo di rapina o estorsione (art. 630 c.p.); associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990); termini di durata massima delle indagini preliminari (art. 407, comma 2, lettera a), numero 5) c.p.p.

¹⁷ In questo caso non sono state inserite ulteriori disposizioni nel corpo del D. Lgs. n. 231/2001. La responsabilità degli Enti deriva da un'autonoma previsione contenuta nel predetto art. 10 della Legge n. 146/2006, il quale stabilisce le specifiche sanzioni amministrative applicabili ai reati, disponendo - in via di richiamo - nell'ultimo comma che "*agli illeciti amministrativi previsti dal presente articolo si applicano le disposizioni di cui al D. Lgs. 8 giugno 2001, n. 231*".

¹⁸ Successivamente modificato dalla Legge 68/2015, D. Lgs. 21/2018 e dalla Legge n.137/2023.

¹⁹ L'art. 25-*duodecies* è stato modificato dalla Legge 161/2017 che ha aggiunto i seguenti commi: "*1 – ter. In relazione alla commissione dei delitti di cui all'articolo 12, comma 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni, si applica all'ente la sanzione pecuniaria da cento a duecento quote. 1 – quarter. Nei casi di condanna per i delitti di cui ai commi 1- bis e 1 – ter del presente articolo, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore ad un anno*". Da ultimo, l'articolo è stato modificato dal D.L. n. 20/2023.



- (xxi) **reato di corruzione tra privati**, richiamato dall'art. 25-ter, comma 1, lett. s-bis, introdotto nel Decreto dalla Legge del 6 novembre 2012, n. 190²⁰;
- (xxii) **reato di razzismo e xenofobia**, richiamato dall'art. 25-ter-decies, introdotto dalla Legge del 20 novembre 2017, n. 167;
- (xxiii) **frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati**, richiamato dall'art. 25-quater-decies, introdotto dalla Legge del 3 maggio 2019, n. 39;
- (xxiv) **reati tributari**, richiamati dall'art. 25-quinquies-decies, introdotto dall'art. 39, comma 2 del Decreto Legge del 26 ottobre 2019, n. 124²¹ e **contrabbando**, richiamato dall'art. 25-sexies-decies, introdotto dall'art. 5, comma 1, lettera d) del D. Lgs. 75/2020²²;
- (xxv) **delitti contro il patrimonio culturale**, richiamato dall'art. 25-septies-decies, introdotto dalla Legge del 9 marzo 2022, n. 22²³;
- (xxvi) **riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici**, richiamato dall'art. 25-duodevices, introdotto dalla Legge del 9 marzo 2022, n. 22.

I reati rilevanti nel contesto di Reply SpA sono indicati nelle Parti Speciali del presente Modello. Reply SpA (anche nella sua qualifica di Capogruppo) si impegna a monitorare costantemente sia le nuove fattispecie di reato introdotte nel perimetro del Decreto, sia quelle già contemplate per verificare l'impatto e la rilevanza delle stesse nel contesto aziendale ed operare gli eventuali adeguamenti e/o integrazioni del caso alle citate Parti Speciali.

1.2.2. I soggetti destinatari del Decreto

Sotto il profilo dei soggetti destinatari, il Decreto indica *“gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica”* (art. 1, co. 2). Il quadro descrittivo è completato dall'indicazione, a carattere negativo, dei soggetti a cui non si applica la legge, vale a dire *“lo Stato, gli enti*

²⁰ Come modificato dal D. Lgs. 15 marzo 2017, n. 38 e in ultimo dalla Legge 3/2019.

²¹ Successivamente modificato dalla Legge di conversione 19 dicembre 2019, n. 157. L'articolo 25-quinquiesdecies richiama i delitti previsti dal D. Lgs. 74/2000 e ovvero: il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (di cui all'art. 2, comma 1 e comma 2-bis) per il quale sono previste sanzioni pecuniarie diverse qualora l'ammontare degli elementi passivi fittizi sia superiore o inferiore ad Euro 100.000; il delitto di dichiarazione fraudolenta mediante altri artifici (di cui all'art. 3); il delitto di emissione di fatture o altri documenti per operazioni inesistenti (di cui all'art. 8, comma 1 e comma 2-bis), per il quale sono previste sanzioni pecuniarie diverse qualora l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo di imposta, sia superiore o inferiore ad Euro 100.000; il delitto di occultamento o distruzione di documenti contabili (di cui all'art. 10) e il delitto di sottrazione fraudolenta al pagamento di imposte (di cui all'art. 11). L'art. 25-quinquiesdecies è stato successivamente modificato dall'art. 5, comma 1 lett. c) del D. Lgs. 75/2020, denominato “Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale”, avente ad oggetto il recepimento della c.d. Direttiva PIF. Tale modifica ha introdotto all'interno del perimetro dei reati rilevanti ai sensi del Decreto le fattispecie di cui all'art. 4 del D. Lgs. 74/2000, dichiarazione infedele, all'art. 5 del D. Lgs. 74/2000, omessa dichiarazione e all'art. 10-quater del D. Lgs. 74/2000, indebita compensazione; la rilevanza di tali reati ai sensi del Decreto è inoltre subordinata alla loro commissione “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”. L'art. 10-quater D.Lgs. 74/2000 richiamato dall'art. 25-quinquiesdecies è stato da ultimo modificato con il D. Lgs. 87/2024.

²² L'articolo 25-sexiesdecies introduce nel novero dei reati presupposto del Decreto alcuni dei reati di cui al D.P.R. 23 gennaio 1973, n. 43 (Testo Unico delle disposizioni legislative in materia doganale). L'articolo 25-sexiesdecies è stato aggiunto dal D.lgs. 75/2020 e modificato dal D.lgs. n. 141 del 26 settembre 2024.

²³ L' articolo 25-septiesdecies è stato aggiunto dalla Legge n. 22/2022 e modificato dalla Legge n. 6/2024.



pubblici territoriali nonché gli enti che svolgono funzioni di rilievo costituzionale” (art. 1, co. 3). Come si vede, la platea dei destinatari è molto ampia e non sempre è identificabile con certezza la linea di confine, specialmente per gli enti che operano nel settore pubblico. È indubbia, in proposito, la soggezione alla disciplina in argomento delle società di diritto privato che esercitino un pubblico servizio (in base a concessione, ecc.). Nei loro riguardi – come, del resto, nei confronti degli enti pubblici economici – la problematica della responsabilità riguarda, tra le altre comuni a tutti i destinatari del Decreto, anche le ipotesi di corruzione sia attiva che passiva.

La responsabilità sorge soltanto in occasione della realizzazione di determinati tipi di reati da parte di soggetti legati a vario titolo all’ente e solo nelle ipotesi in cui la condotta illecita sia stata realizzata nell’*interesse* o a *vantaggio* di esso. Dunque, non soltanto allorché il comportamento illecito abbia determinato un vantaggio, patrimoniale o meno, per l’ente, ma anche nell’ipotesi in cui, pur in assenza di tale concreto risultato, il fatto-reato trovi ragione nell’*interesse* dell’ente.

1.2.3. La condizione esimente

L’art. 6 del Decreto contempla l’esonero da responsabilità dell’ente se lo stesso dimostra, in occasione di un procedimento penale per uno dei reati rilevanti, di aver adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati. Il sistema prevede l’istituzione di un organo di controllo interno all’ente (“**Organismo di Vigilanza**” o “**OdV**”) con il compito di vigilare sull’efficacia reale del citato modello.

Di conseguenza una forma specifica di esonero della responsabilità si ottiene qualora la società dimostri che:

- (i) l’Organo Dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire i reati e gli illeciti della specie di quello verificatosi;
- (ii) il compito di vigilare sul funzionamento e sull’osservanza del Modello, nonché di curare il suo aggiornamento è stato affidato all’Organismo di Vigilanza, a cui sono attribuiti autonomi poteri di iniziativa e controllo;
- (iii) le persone che hanno commesso i reati e gli illeciti hanno agito eludendo fraudolentemente il suddetto Modello;
- (iv) non vi sia stata omessa o insufficiente vigilanza da parte dell’organismo di cui al precedente punto (ii).

L’esonero dalle responsabilità di Reply SpA e del Gruppo passa attraverso il giudizio d’idoneità del sistema interno di organizzazione e controllo, che il giudice penale è chiamato a formulare in occasione del procedimento penale a carico dell’autore materiale del fatto illecito. Dunque, la formulazione del Modello e l’organizzazione dell’attività dell’Organismo di Vigilanza devono porsi come obiettivo l’esito positivo di tale giudizio d’idoneità. Questa particolare prospettiva finalistica impone agli enti di valutare l’adeguatezza delle proprie procedure alle esigenze sopra citate.

1.3. Le Linee Guida di Confindustria

Allo scopo di offrire un aiuto concreto alle imprese ed associazioni nella elaborazione dei modelli e nella individuazione di un Organismo di Vigilanza, le Linee Guida predisposte da Confindustria contengono una serie di indicazioni e misure, essenzialmente tratte dalla pratica aziendale, ritenute in astratto idonee a rispondere alle esigenze delineate dal D. Lgs.



n. 231/2001, e quindi tali da rivestire un importante ruolo ispiratore nella costruzione del Modello e nella nomina del citato Organismo con i relativi compiti da parte del singolo ente.

Nella predisposizione del presente Modello, si sono tenute in massima considerazione le Linee Guida emanate da Confindustria (ultimo aggiornamento di giugno 2021), le cui caratteristiche essenziali per la costruzione del Modello sono individuate nelle seguenti fasi:

1. identificazione dei rischi, ossia l'analisi delle strutture aziendali al fine di evidenziare dove (in quale area/settore di attività) e secondo quali modalità si può verificare la commissione dei reati previsti dal D. Lgs. 231/2001;
2. progettazione del sistema di controllo (c.d. protocolli), ossia la valutazione del sistema di controllo esistente nell'ambito aziendale ed il suo eventuale adeguamento, al fine di contrastare efficacemente i rischi identificati.
Le componenti di un sistema di controllo preventivo dai **reati (dolosi)** che devono essere attuate a livello aziendale per garantire l'efficacia del Modello sono così individuate da Confindustria:
 - adozione di un codice etico;
 - adozione di un sistema organizzativo sufficientemente formalizzato e chiaro soprattutto per quanto concerne l'attribuzione di responsabilità;
 - adozione di procedure cartacee e informatiche;
 - adozione di un sistema di poteri autorizzativi e di firma;
 - adozione di un sistema di adeguato controllo interno;
 - adozione di un sistema di comunicazione e formazione del personale.

Le componenti sopra evidenziate devono ispirarsi ai seguenti principi:

- ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua;
 - nessuno può gestire in autonomia un intero processo;
- il sistema di controllo interno deve essere sottoposto periodicamente ad apposite verifiche circa la sua adeguatezza ed effettività.
3. la nomina dell'Organismo di Vigilanza, ossia dell'organo al quale affidare il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
 4. la previsione di un sistema disciplinare o di meccanismi sanzionatori per le violazioni delle norme del codice etico e delle procedure previste dal Modello.

Si segnala che il presente Modello è stato redatto tenendo in considerazione la realtà concreta di Reply SpA, la sua struttura organizzativa, nonché la specifica attività prestata.

Pertanto, pur facendo riferimento alle Linee Guida di Confindustria, il presente Modello può, tenuto conto di quanto sopra evidenziato, discostarsi dalle suddette indicazioni che per loro natura hanno comunque carattere generale.

2. Adozione del Modello nell'ambito del Gruppo Reply

2.1. Modello e Codice Etico

Il Gruppo intende operare secondo principi etici diretti ad improntare lo svolgimento dell'attività, il perseguimento dello scopo sociale e la crescita delle società nel rispetto delle leggi vigenti. A tale fine, il Gruppo si è dotato di un proprio codice etico (di seguito "**Codice**



Etico” che costituisce un Allegato del Modello) volto a definire una serie di principi di “deontologia aziendale” che le società del Gruppo riconoscono come propri e dei quali esigono l’osservanza da parte degli organi societari, dei propri dipendenti e di tutti coloro che cooperano a qualunque titolo al perseguimento dei fini aziendali.

Il Codice Etico ha pertanto una portata di carattere generale e rappresenta uno strumento adottabile anche in via autonoma da parte del Gruppo. Il Modello, invece, risponde a specifiche prescrizioni contenute nel D. Lgs. 231/2001, finalizzate a prevenire la commissione di particolari tipologie di reati (per fatti che, commessi a vantaggio di Reply SpA, possono far sorgere a carico della stessa una responsabilità amministrativa da reato in base alle disposizioni del Decreto medesimo).

Tuttavia, in considerazione del fatto che il Codice Etico richiama principi di comportamento idonei anche a prevenire i comportamenti illeciti di cui al D. Lgs. 231/2001, esso acquisisce rilevanza ai fini del Modello e costituisce, pertanto, elemento rilevante del Modello medesimo.

2.2. Struttura del Modello

Il presente Modello è costituito da una **Parte Generale** e da una **Parte Speciale**.

La **Parte Generale** ha la funzione di definire i principi di carattere generale che il Gruppo pone come riferimento per la gestione del proprio business e che sono validi per la realtà aziendale in senso lato e non soltanto per prevenire il compimento delle attività potenzialmente a rischio.

La **Parte Speciale** ha la funzione di:

- individuare i reati potenzialmente commissibili in azienda e le relative misure preventive;
- individuare i principi comportamentali da porre in essere;
- ripercorrere l’approccio metodologico utilizzato alla fine della predisposizione del Modello;
- definire i compiti dell’Organismo di Vigilanza.

Nella Parte Speciale sono previste le fattispecie delittuose contemplate dal D. Lgs. 231/2001 ritenute rilevanti nel contesto del Gruppo. Con riferimento al novero delle aree/attività sensibili, l’analisi è stata circoscritta alle fattispecie ritenute esposte al rischio di reato, secondo un criterio probabilistico.

2.3. Principi generali per l’adozione del Modello

L’adozione del Modello Organizzativo è attuata secondo i seguenti criteri generali:

- Predisposizione e aggiornamento del Modello
È rimessa alla società Reply SpA la predisposizione del Modello Organizzativo che poi è soggetto al recepimento anche da parte delle altre società del Gruppo in relazione alle attività a rischio da esse svolte con le modalità indicate ai successivi paragrafi. È rimesso alla responsabilità delle singole società del Gruppo l’aggiornamento del Modello medesimo in relazione alle esigenze di adeguamento che per esso si verranno nel tempo a determinare.
- Applicazione del Modello e controlli sulla sua attuazione



È rimessa alla responsabilità delle singole società del Gruppo l'applicazione del Modello in relazione alle attività dalle stesse in concreto poste in essere. A tal fine l'Organo Dirigente della società può decidere se nominare un proprio Organismo di Vigilanza dotato di autonomi poteri oppure assumersi l'incarico, avvalendosi dell'Organismo di Vigilanza della Capogruppo quale supporto per l'espletamento dei propri compiti di controllo e vigilanza.

- Coordinamento sulle funzioni di controllo e verifica della efficacia del Modello

Nel caso in cui l'Organo Dirigente assuma il ruolo di Organismo di Vigilanza, è affidato all'Organismo di Vigilanza di Reply SpA, quale società Capogruppo, il compito di coordinare sul piano generale, anche mediante contatti sulla rete informatica, le attività di controllo sull'applicazione del Modello nell'ambito di tutte le società del Gruppo per assicurare al Modello stesso una corretta e omogenea attuazione, nonché di effettuare, in casi particolari, specifiche azioni di controllo sulle singole società del Gruppo stesso.

In conformità ai criteri sopra indicati, il Modello trova attuazione come esplicitato nei paragrafi successivi.

- Pubblicazione del Modello

Il presente documento è reperibile sul sito aziendale www.reply.com.

Reply SpA si impegna ad individuare gli strumenti e ad attuare gli interventi più efficaci ed idonei a garantire la diffusione, la conoscenza e l'applicazione del Modello e del Codice Etico, prevedendo adeguati interventi formativi e informativi.

Reply SpA fornisce inoltre ogni chiarimento necessario per l'interpretazione e l'attuazione dei principi contenuti nel presente documento.

2.4. Approvazione del Modello e suo recepimento nell'ambito del Gruppo

Il presente Modello, costituito dalla Parte Generale e dalla Parte Speciale e dai relativi Allegati, è stato approvato dal Consiglio di Amministrazione di Reply SpA con delibera del 28 marzo 2008 e successivamente aggiornato con delibere del Consiglio di Amministrazione di Reply SpA del 4 agosto 2011, del 1° agosto 2013, del 14 maggio 2019, del 31 luglio 2020, del 14 novembre 2022, del 14 novembre 2024 e da ultimo del 13 marzo 2025.

Il Modello, nei limiti previsti nei prossimi paragrafi, è soggetto al recepimento anche da parte delle altre società del Gruppo che rientrano nel perimetro di consolidamento di Reply SpA, in relazione alle attività a rischio da esse svolte.

In particolare, è demandato ai Consigli di Amministrazione delle singole società del Gruppo di provvedere mediante apposita delibera al recepimento del presente Modello, in funzione dei profili di rischio configurabili nelle attività svolte dalle società stesse.

Nel recepire il Modello, i Consigli di Amministrazione delle singole società del Gruppo, nei limiti previsti nei prossimi paragrafi, hanno la possibilità di:

- (i) istituire un proprio Organismo di Vigilanza ex art. 6, co. 1, lett. b), D. Lgs. n. 231/2001 con tutte le relative attribuzioni di competenze e responsabilità. Per le società di piccole dimensioni (definite in questa sede, più che in funzione dei parametri quantitativi, nella essenzialità della struttura interna gerarchica e funzionale) è fatta salva la possibilità di attribuire questa funzione direttamente all'Organo Dirigente della controllata (così come previsto dall'art. 6, co. 4, D. Lgs. n. 231/2001);



- (ii) far sì che l'Organismo di Vigilanza/Organo Dirigente della controllata possa avvalersi, nell'espletamento del compito di vigilare sul funzionamento e l'osservanza del Modello, delle risorse allocate presso l'analogo Organismo della Capogruppo, sulla base di un predefinito rapporto contrattuale con la stessa. In tale contesto, l'Organismo di Vigilanza della Capogruppo, nella effettuazione di controlli presso le società del Gruppo, assume nella sostanza la veste di professionista esterno che svolge la sua attività nell'interesse della controllata stessa, riportando all'Organismo di Vigilanza/Organo Dirigente di quest'ultima, con i vincoli di riservatezza propri del consulente esterno.

Per l'essenzialità della struttura funzionale e gerarchica delle società controllate e in considerazione del fatto che i processi di amministrazione, controllo di gestione, gestione del personale, tesoreria, adempimenti societari e fiscali sono accentrati sulla Capogruppo, la funzione di Organismo di Vigilanza, quando non già presente un Organismo di Vigilanza autonomo in seno alla singola controllata, è assegnata dai Consigli di Amministrazione delle società del Gruppo agli stessi Organi Dirigenti. L'Organo Dirigente della controllata, nell'espletamento del compito di vigilare sul funzionamento e l'osservanza del Modello, si avvale delle risorse allocate presso l'Organismo di Vigilanza della Capogruppo.

2.5. Modifiche e integrazioni del Modello

Essendo il Modello un "atto di emanazione dell'Organo Dirigente" (in conformità alle prescrizioni dell'art. 6, primo comma, lettera a del Decreto) le modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse all'approvazione rispettivamente del Consiglio di Amministrazione di Reply SpA e delle società del Gruppo.

È peraltro riconosciuta al Presidente e/o ai Consiglieri Delegati la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale.

Reply SpA comunica tempestivamente alle società controllate ogni modifica apportata al Modello ai fini del loro recepimento.

2.6. Coordinamento sui sistemi di controllo e verifica sul piano generale dell'efficacia del Modello

Ferma restando l'attribuzione delle responsabilità in capo alle singole società del Gruppo riguardo l'attuazione del Modello in relazione alle attività dalle stesse in concreto poste in essere nelle aree a rischio, qualora le funzioni di Organismo di Vigilanza vengano assunte dall'Organo Dirigente, è attribuito all'Organismo di Vigilanza di Reply SpA il compito di supportare le attività di vigilanza e controllo sull'effettiva attuazione del Modello stesso nell'ambito delle società del Gruppo per assicurarne una corretta e omogenea applicazione nell'ambito del Gruppo stesso.

In particolare, sono riconosciute all'Organismo di Vigilanza di Reply SpA, nel rispetto dell'autonomia delle diverse società del Gruppo e dei limiti imposti da disposizioni di legge (ad esempio, per quanto concerne la segretezza aziendale, la tutela della privacy, ecc.), le seguenti attribuzioni nei confronti delle controllate:

- supportare le attività di verifica e controllo nonché di applicazione del Modello;
- proporre, sulla base delle verifiche di cui sopra, l'aggiornamento del Modello laddove si riscontrino esigenze di adeguamento dello stesso;



- effettuare, singolarmente o congiuntamente all'Organo Dirigente, particolari azioni di controllo sulle singole controllate del Gruppo nelle aree di attività a rischio, con facoltà di accedere alla documentazione rilevante di tutte le società del Gruppo, senza alcuna forma di intermediazione.

Le società estere del Gruppo Reply, che non svolgono attività nel territorio italiano, non sono tenute all'adeguamento ai dettami del Decreto, fermo restando il rispetto del Codice Etico anche per dette società.

2.7. L'adozione del Modello Organizzativo nell'ambito del Gruppo

Il presente Modello Organizzativo è adottato dalle società del Gruppo che rientrano nel perimetro di consolidamento di Reply SpA e, se del caso, rivisto in alcune parti e adattato alle differenti peculiarità organizzative, alla diversa rischiosità e alle strutture che risultano più snelle.

Al fine di evitare appesantimenti burocratici e una moltiplicazione dei costi connessi ai controlli da effettuare, si potranno stabilire per le società controllate, nel rispetto dei diritti degli altri azionisti, criteri specifici per l'adozione del rispettivo Modello Organizzativo, relativi:

- alla nomina di un Organismo di Vigilanza *ad hoc* o in alternativa alla identificazione dell'Organo Dirigente per l'assunzione di tale ruolo, nel rispetto delle previsioni del Decreto;
- alla significatività del controllo da parte della Capogruppo;
- alla mappatura delle attività a rischio;
- alle modalità attraverso le quali garantire le attività di controllo.

Tali criteri dovranno trovare enunciazione nella comunicazione di diffusione del Modello e/o, a seconda dei casi, nel regolamento dell'Organismo di Vigilanza.

3. Metodologia seguita per l'individuazione delle attività sensibili e dei processi di supporto

L'art. 6.2 lett. a) del D. Lgs. 231/2001 indica, come uno dei requisiti del Modello, l'individuazione delle cosiddette "aree sensibili" o "a rischio", cioè di quei processi e di quelle aree di attività aziendali in cui potrebbe determinarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001.

Si è, pertanto, analizzata la realtà operativa aziendale nelle aree/settori aziendali in cui è possibile la commissione dei reati previsti dal D. Lgs. 231/2001, evidenziando i processi maggiormente rilevanti.

Parallelamente, è stata condotta un'indagine sugli elementi costitutivi dei reati in questione, allo scopo di identificare le condotte concrete che, nel contesto aziendale, potrebbero realizzare le fattispecie delittuose.

L'iter metodologico seguito dalla società Reply SpA per la realizzazione del Modello è scomponibile nelle seguenti fasi:



- Fase di Scoping: definizione dettagliata del perimetro oggetto di valutazione e individuazione, attraverso questionari specifici rivolti ai soggetti apicali, dei corretti processi aziendali e dei relativi referenti;
- Fase di Analisi: valutazione del sistema di controllo interno in essere, raccolta, mediante interviste ed analisi documentale, delle informazioni necessarie a costruire la mappa delle principali attività a rischio reato e l'elenco delle possibili modalità di realizzazione dei comportamenti configurati come reati e per i quali sia prevista una responsabilità di Reply SpA ai sensi del Decreto, analisi e valutazione dei punti di debolezza individuati, determinazione dei possibili rimedi.

3.1. Individuazione delle attività a rischio reato

Al fine di individuare specificatamente e in concreto le aree di attività a rischio di commissione di reato (di seguito “**attività a rischio**” o “**sensibili**”) si è proceduto ad un'analisi della struttura societaria ed organizzativa di Reply SpA (e del Gruppo).

Con riferimento alle fattispecie di reati suscettibili di configurare la responsabilità amministrativa di Reply SpA, sono state identificate le aree di “attività a rischio” (dettagliatamente analizzate nella Parte Speciale) che sono state distinte tra quelle che fanno riferimento a:

- Gestione dei rapporti con la Pubblica Amministrazione;
- Gestione delle attività commerciali a rischio reati in materia di corruzione tra privati;
- Gestione dei sistemi informatici e dei documenti informatici;
- Gestione delle attività commerciali a rischio reati contro l'industria e il commercio;
- Gestione degli adempimenti societari;
- Gestione delle attività a rischio reati con finalità di terrorismo o di eversione dell'ordine democratico, di criminalità organizzata, di impiego di cittadini di paesi terzi il cui soggiorno è irregolare e transnazionali;
- Gestione delle attività commerciali e finanziarie a rischio reati in materia di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- Gestione delle informazioni privilegiate e price sensitive;
- Gestione delle attività relative alla salute e alla sicurezza sul lavoro;
- Gestione delle attività a rischio in materia di violazione del diritto d'autore;
- Gestione del contenzioso a rischio reati in materia di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria;
- Gestione degli adempimenti fiscali/tributari e contributivi;
- Gestione delle attività a rischio reati contro la personalità individuale e in materia di razzismo e xenofobia;
- Gestione delle attività legate all'ambiente e alla gestione dei rifiuti;
- Gestione delle attività legate a siti e a immobili a rischio reato contro il patrimonio culturale e paesaggistico;
- Gestione delle attività a rischio reato in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.

4. Organismo di Vigilanza

Affinché Reply SpA e il Gruppo possano usufruire dell'esonero dalla responsabilità, il D. Lgs. 231/2001 (art. 6) prevede che l'Organo Dirigente abbia, tra l'altro:



- adottato un modello di organizzazione, gestione e controllo idoneo a prevenire il compimento di “reati rilevanti” (il presente Modello è stato adottato per la prima volta dal Consiglio di Amministrazione di Reply SpA con delibera del 28 marzo 2008);
- affidato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento all'Organismo di Vigilanza. Il Consiglio di Amministrazione di Reply SpA ha affidato l'incarico all'Organismo di Vigilanza per la prima volta in data 28 marzo 2008.

L'affidamento di detti compiti all'Organismo di Vigilanza ed il corretto ed efficace svolgimento degli stessi sono presupposti indispensabili per l'esonero dalla responsabilità, sia che il reato sia stato commesso dai soggetti “apicali” (espressamente contemplati dall'art. 6 del D. Lgs. 231/2001), che dai soggetti sottoposti all'altrui direzione (di cui all'art. 7 del D. Lgs. 231/2001).

L'art. 7, co. 4, del D. Lgs. 231/2001 ribadisce, infine, che l'efficace attuazione del Modello richiede, oltre all'istituzione di un sistema disciplinare, una sua verifica periodica da parte dell'Organismo di Vigilanza.

4.1. Modalità di nomina e di revoca dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere nominato con delibera del Consiglio di Amministrazione. Nella dichiarazione formale di incarico devono essere obbligatoriamente indicati:

- il soggetto / i soggetti chiamato/i ad assumere il ruolo di Organismo di Vigilanza e le relative responsabilità;
- la durata in carica, se è previsto un termine, e in ogni caso le modalità di revoca.

La revoca, così come la nomina, deve essere deliberata dal Consiglio di Amministrazione, che definisce altresì:

- i principali compiti cui l'Organismo di Vigilanza è chiamato nell'ambito dell'espletamento delle attività di controllo sull'efficienza ed efficacia del Modello Organizzativo (l'indicazione dei compiti ha carattere generale, essendo rimessa all'Organismo stesso la formulazione di un regolamento interno delle proprie attività – calendarizzazione dei controlli, individuazione dei criteri e delle procedure di analisi, disciplina dei flussi informativi, etc.);
- i poteri di cui l'Organismo di Vigilanza deve necessariamente essere dotato per assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello Organizzativo;
- le tempistiche e gli organi destinatari dell'attività di reporting dell'Organismo di Vigilanza.

La società Reply SpA ha ritenuto opportuno affidare l'incarico ad un organismo composto da tre membri effettivi, di cui almeno uno esterno (che riveste il ruolo di Presidente dell'Organismo di Vigilanza) e almeno uno interno, che devono avere le qualità richieste per svolgere i loro compiti assicurando professionalità e competenza. La scelta è determinata dall'esigenza di garantire all'Organismo di Vigilanza i requisiti di autonomia, indipendenza, professionalità e continuità d'azione che si richiedono per tale funzione.

In conformità ai principi di cui al D. Lgs. 231/2001 è consentita all'Organismo di Vigilanza la possibilità di affidare all'esterno (a soggetti terzi che posseggano le specifiche competenze necessarie per la migliore esecuzione dell'incarico) compiti di natura tecnica, rimanendo la



responsabilità complessiva per la vigilanza sul Modello in capo all'Organismo di Vigilanza stesso.

4.2. Compiti dell'Organismo di Vigilanza

Il Modello costituisce, in sostanza, un'estrinsecazione, con un oggetto ben circostanziato (identificabile con la prevenzione di comportamenti criminosi riguardanti alcune specifiche fattispecie di reato), del più ampio "Sistema di Controllo Interno" implementato da Reply SpA.

Le attività che l'Organismo di Vigilanza è chiamato ad assolvere, anche sulla base delle indicazioni contenute negli artt. 6 e 7 del D. Lgs. n. 231/2001, possono così schematizzarsi:

- vigilanza sull'**effettività** del Modello, che si sostanzia nella verifica della coerenza tra i comportamenti posti in essere e le previsioni del Modello;
- disamina in merito all'**adeguatezza** del Modello, ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;
- analisi circa il **mantenimento** nel tempo dei requisiti di solidità e funzionalità del Modello;
- cura dell'**aggiornamento** in senso dinamico del Modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti.

In particolare, all'Organismo di Vigilanza sono affidati i seguenti compiti:

- vigilare sul funzionamento e l'osservanza del Modello;
- verificare l'effettiva idoneità del Modello a prevenire la commissione dei reati richiamati dal D. Lgs. 231/2001;
- analizzare la persistenza nel tempo dei requisiti di solidità e funzionalità del Modello;
- curare, sviluppare e promuovere, in collaborazione con le unità organizzative interessate, il costante aggiornamento del Modello e del sistema di vigilanza sull'attuazione dello stesso, suggerendo, ove necessario, all'organo amministrativo le correzioni e gli opportuni adeguamenti;
- mantenere un collegamento costante con la società di revisione;
- mantenere i rapporti e assicurare i flussi informativi di competenza verso il Consiglio di Amministrazione, il Comitato Controllo e Rischi ed il Collegio Sindacale;
- richiedere e acquisire informazioni e documentazione di ogni tipo da e verso ogni livello e funzione di Reply SpA;
- compiere verifiche ed ispezioni al fine di accertare eventuali violazioni del Modello;
- elaborare un programma di vigilanza, in coerenza con i principi contenuti nel Modello, nell'ambito dei vari settori di attività;
- assicurare l'attuazione del programma di vigilanza anche attraverso la calendarizzazione delle attività;
- assicurare l'elaborazione della reportistica sulle risultanze degli interventi effettuati;
- assicurare il costante aggiornamento del sistema di identificazione, mappatura e classificazione delle aree di rischio ai fini dell'attività di vigilanza propria dell'Organismo stesso;
- definire e promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché della formazione del personale e della sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- fornire chiarimenti in merito al significato ed all'applicazione delle previsioni contenute nel Modello;



- predisporre un efficace sistema di comunicazione interna per consentire la trasmissione e raccolta di notizie rilevanti ai fini del D. Lgs. 231/2001, garantendo la tutela e riservatezza del segnalante;
- formulare la previsione di spesa per lo svolgimento della propria attività da sottoporre all'approvazione del Consiglio di Amministrazione; eventuali spese straordinarie, non contemplate nel documento previsionale, dovranno essere parimenti sottoposte alla preventiva approvazione del Consiglio di Amministrazione;
- segnalare le violazioni accertate all'organo competente per l'apertura del procedimento disciplinare;
- promuovere l'attivazione di eventuali procedimenti disciplinari;
- verificare che le violazioni del Modello siano effettivamente e adeguatamente sanzionate.

È opportuno precisare sin da ora che il massimo vertice societario (es. Consiglio di Amministrazione o Amministratore Delegato), pur con l'istituzione dell'Organismo di Vigilanza ex D. Lgs. 231/2001, mantiene invariate tutte le attribuzioni e le responsabilità previste dal Codice Civile²⁴, alle quali si aggiunge quella relativa all'adozione ed all'efficacia del Modello, nonché all'istituzione dell'Organismo (art. 6, co. 1, lett. a) e b) del D. Lgs. 231/2001).

Il Collegio Sindacale, essendo investito della responsabilità di valutare l'adeguatezza dei sistemi di controllo interno, è informato dall'Organismo di Vigilanza dell'eventuale commissione dei reati rilevanti ex D. Lgs. 231/2001, così come di eventuali carenze del Modello.

4.3. Requisiti e poteri dell'Organismo di Vigilanza

I principali requisiti che l'Organismo di Vigilanza deve possedere sono:

- Autonomia ed indipendenza²⁵
La posizione dell'Organismo di Vigilanza nell'ambito di Reply SpA e del Gruppo deve garantire l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e/o di condizionamento da parte di qualunque componente della società (e in particolare dell'Organo Dirigente). Tali requisiti sono assicurati dall'inserimento dell'Organismo di Vigilanza come unità di staff in posizione gerarchica la più elevata possibile e prevedendo il riporto diretto al Consiglio di Amministrazione nel suo complesso.

²⁴ Cfr. il nuovo art. 2392 cod. civ. "(Responsabilità verso la società). Gli amministratori devono adempiere i doveri ad essi imposti dalla Legge e dallo statuto con la diligenza richiesta dalla natura dell'incarico e dalle loro specifiche competenze. Essi sono solidalmente responsabili verso la società dei danni derivanti dall'inosservanza di tali doveri, a meno che si tratti di attribuzioni proprie del comitato esecutivo o di funzioni in concreto attribuite ad uno o più amministratori.

In ogni caso gli amministratori, fermo quanto disposto dal comma terzo dell'articolo 2381, sono solidalmente responsabili se, essendo a conoscenza di fatti pregiudizievoli, non hanno fatto quanto potevano per impedirne il compimento o eliminarne o attenuarne le conseguenze dannose.

La responsabilità per gli atti o le omissioni degli amministratori non si estende a quello tra essi che, essendo immune da colpa, abbia fatto annotare senza ritardo il suo dissenso nel libro delle adunanze e delle deliberazioni del consiglio, dandone immediata notizia per iscritto al presidente del collegio sindacale."

²⁵ Si ritiene opportuno richiamare quanto recita effettivamente il D. Lgs. n. 231/2001 in ordine alla citata esigenza di autonomia o indipendenza (quest'ultimo termine in particolare sta ad indicare l'indipendenza di giudizio dell'Organismo rispetto ai soggetti controllati): "art.6, comma 1, lett. b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controlli".

Un minimo di riflessione ci conduce ad escludere la necessaria sovrapposibilità tra "soggetto autonomo ed indipendente" e l'esercizio "di autonomi poteri d'iniziativa e controllo".



All'Organismo di Vigilanza non sono attribuiti compiti operativi che, rendendolo partecipe di decisioni ed attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

I componenti dell'Organismo di Vigilanza della società Reply SpA, oltre alle competenze professionali di seguito descritte, sono in possesso di requisiti soggettivi di onorabilità, assenza di conflitti di interessi e di relazioni di parentela con i componenti degli organi sociali; tali requisiti garantiscono ulteriormente l'autonomia e l'indipendenza richiesta dal compito affidato a detti componenti.

- Professionalità

L'Organismo di Vigilanza deve possedere un bagaglio di strumenti e tecniche tale da poter svolgere efficacemente l'attività assegnata. Si tratta di tecniche specialistiche proprie di chi svolge attività "ispettiva", ma anche consulenziale di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico. È dunque essenziale la conoscenza della struttura e delle modalità realizzative dei reati, che potrà essere assicurata mediante l'utilizzo delle risorse aziendali ovvero della consulenza esterna. Per quanto concerne le tematiche di tutela della salute e sicurezza sul lavoro, l'Organismo di Vigilanza dovrà avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti comprese quelle previste dalle normative di settore.

- Continuità di azione

La definizione degli aspetti attinenti alla continuità di azione dell'Organismo di Vigilanza, quali la programmazione dell'attività di verifica, le modalità di effettuazione della stessa, la verbalizzazione delle riunioni, le modalità ed il contenuto specifico dei flussi informativi relativi alle aree a rischio reato, nonché le specifiche modalità operative e di funzionamento interno, sono rimesse ad un piano di lavoro *ad hoc* predisposto dall'Organismo di Vigilanza stesso.

- Altri requisiti

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che l'Organo Dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto la responsabilità ultima del funzionamento e dell'efficacia del Modello Organizzativo è in capo all'Organo Dirigente stesso.

Inoltre, l'Organismo di Vigilanza ha libero accesso presso tutte le funzioni di Reply SpA - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D. Lgs. 231/2001.

L'Organismo di Vigilanza, qualora lo ritenesse opportuno, può avvalersi - sotto la sua diretta sorveglianza e responsabilità - dell'ausilio di tutte le strutture di Reply SpA ovvero di consulenti esterni.

Infine, l'Organo Dirigente dovrà approvare una dotazione adeguata di risorse finanziarie, proposta dall'Organismo di Vigilanza della quale l'Organismo stesso potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte, ecc.).

4.4. Flussi informativi nei confronti dell'Organismo di Vigilanza



All'Organismo di Vigilanza dovranno pervenire, oltre alle informazioni e alla documentazione richiesta dalla Parte Speciale trattata nei capitoli successivi e alle indicazioni che si renderanno necessarie durante l'espletamento delle attività di monitoraggio, le segnalazioni relative alla mancata attuazione del Modello, alla commissione di reati previsti dal Decreto o comunque a comportamenti non in linea con le regole di condotta adottate dal Gruppo.

L'Organismo di Vigilanza di Reply SpA valuterà le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali decisioni di non procedere a una indagine interna.

L'Organismo di Vigilanza di Reply SpA agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone accusate con colpa grave o in mala fede.

In ambito aziendale, tutte le strutture operative e manageriali del Gruppo devono comunicare all'Organismo di Vigilanza:

- su base periodica, le informazioni identificate dall'Organismo e da questi richieste alle singole strutture organizzative e manageriali del Gruppo. Tali informazioni devono essere trasmesse nei tempi e nei modi che saranno definiti dall'Organismo medesimo;
- su base occasionale, ogni altra informazione, di qualsivoglia genere, proveniente anche da terzi ed attinente alla mancata attuazione del Modello nelle aree di attività "a rischio" ed al rispetto delle previsioni del Decreto, che possano essere ritenute utili ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza.

In particolare, dovranno essere obbligatoriamente trasmesse all'Organismo di Vigilanza informazioni circa:

- eventuali provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, su persone, società, terzi che intrattengono rapporti con le società del Gruppo Reply per i reati rilevanti di cui al D. Lgs. 231/2001;
- eventuali richieste di assistenza legale inoltrate da amministratori, dirigenti e/o dipendenti in caso di avvio di un procedimento giudiziario per i reati rilevanti di cui al D. Lgs. 231/2001;
- eventuali relazioni predisposte dai responsabili delle diverse funzioni aziendali dalle quali possano emergere fatti, comportamenti, eventi od omissioni con profili di criticità e responsabilità rispetto ai reati rilevanti ex D. Lgs. 231/2001;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Tali segnalazioni potranno pervenire sia da parte di esponenti aziendali sia da parte di terzi e potranno avere ad oggetto ogni violazione o sospetto di violazione del presente Modello e delle procedure allo stesso collegate, comportamenti difforni dai principi etici e dal Codice Etico del Gruppo, anomalie o atipicità riscontrate nell'espletamento dell'attività. Le segnalazioni pervenute saranno valutate dall'Organismo di Vigilanza a sua ragionevole discrezione e responsabilità.

All'Organismo di Vigilanza deve essere comunicato il sistema delle deleghe adottato da ciascuna società del Gruppo.



L'Organismo di Vigilanza riporterà al Consiglio di Amministrazione e, nei casi più gravi aventi attinenza con il Sistema di Controllo Interno, anche al Comitato Controllo e Rischi e al Collegio Sindacale, le violazioni del Modello Organizzativo emerse con riferimento alle segnalazioni suddette.

Nel contesto sopra descritto, il Gruppo Reply ha già provveduto ad implementare un sistema di comunicazione delle segnalazioni valido per tutte le società facenti parte del Gruppo stesso, come descritto nella *Whistleblowing Policy* pubblicata sul sito del Gruppo.

Le segnalazioni possono essere presentate attraverso uno dei seguenti canali:

- via e-mail, all'indirizzo di posta elettronica: odv@reply.com - accessibile solo ai membri dell'Organismo di Vigilanza di Reply S.p.A.;
- per posta, a: Reply S.p.A. - Via Nizza n.250 - 10126 Torino - Italia, all'attenzione dell'Organismo di Vigilanza di Reply S.p.A.;
- linea telefonica, al numero: +39 011 7711594, chiedendo di conferire con l'Organismo di Vigilanza.

4.5. Funzioni di coordinamento dell'Organismo di Vigilanza di Reply SpA con gli Organismi di Vigilanza delle altre società del Gruppo

È assegnato all'Organismo di Vigilanza di Reply SpA il compito di coordinare, anche mediante contatti sulla rete informatica, le attività dell'OdV delle altre società del Gruppo ai fini della realizzazione di un coerente sistema dei controlli nell'ambito del Gruppo stesso.

In tal caso, è data facoltà all'Organismo di Vigilanza di Reply SpA di acquisire documentazione e informazioni e di effettuare controlli periodici e verifiche sulle attività a rischio delle diverse società del Gruppo.

5. Il Sistema di segnalazione Whistleblowing

Il Consiglio dei Ministri, nella seduta del 10 marzo 2023, ha approvato il D. Lgs. 24/2023 per il recepimento della Direttiva UE 2019/1937 in materia di "protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali".

In forza del nuovo dettato normativo, facendo seguito alla modifica di cui al comma 2-bis dell'art. 6 ex D. Lgs. 231/2001, il Gruppo ha adottato un proprio sistema di segnalazione degli illeciti e delle irregolarità, prevedendo:

- l'istituzione di un canale di segnalazione interno che garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione nonché del contenuto della segnalazione e della relativa documentazione (ex art. D. Lgs. 24/2023 e art. 6 comma 2-bis D. Lgs. 231/2001);
- la previsione di canali di segnalazione alternativi (es. un contatto telefonico con l'Organo individuato per la gestione delle segnalazioni);
- la gestione del canale di segnalazione affidata ad un Organo gestorio dedicato e con personale specificatamente formato;
- la previsione di tempistiche precise in termini di riscontro delle segnalazioni (avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione della stessa, riscontro alla segnalazione entro 3 mesi dalla data dell'avviso di ricevimento della segnalazione);



- la previsione di tutele contro ogni atto ritorsivo e/o discriminatorio nei confronti della persona che effettua la segnalazione;
- l'estensione delle misure di protezione a soggetti diversi dal segnalante quali: i facilitatori, le persone del medesimo contesto lavorativo che hanno un rapporto di parentela e/o un legame affettivo o rapporti abituali e che hanno supportato il Whistleblower, agli enti di proprietà – in via esclusiva o in compartecipazione maggioritaria di terzi – del segnalante nonché gli enti presso i quali il segnalante lavora, compresi i sub-fornitori;
- la possibilità di effettuare la segnalazione per gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso il Gruppo; i lavoratori autonomi che svolgono la propria attività lavorativa presso il Gruppo; i lavoratori o i collaboratori che svolgono la propria attività lavorativa presso il Gruppo, che forniscono beni o servizi o che realizzano opere in favore di terzi; i lavoratori dipendenti del Gruppo; i liberi professionisti e i consulenti che prestano la propria attività presso il Gruppo; i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso il Gruppo; i candidati durante la fase di selezione se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali, i neoassunti nel periodo di prova, gli ex dipendenti se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso;
- la previsione di tempi di conservazione (5 anni a decorrere dalla data di ricezione della segnalazione e della documentazione ad essa correlata ai sensi dell'art. 14 ex D. Lgs. 24/2023);
- l'adeguamento alle disposizioni in tema di tutela dei dati personali ai sensi e per gli effetti dell'art. 13 ex D. Lgs. 24/2023.

A tal fine, il Gruppo Reply ha adottato la “**Whistleblowing Policy e Informativa Privacy**” (https://www.reply.com/contents/Reply-Whistleblowing-Policy_ITA.pdf), dove sono previsti i seguenti canali alternativi di segnalazione:

- **piattaforma web** accessibile su: <https://reply-whistleblowing.integrityline.com/?lang=it>;
- **posta ordinaria**, a: Reply S.p.A. - Via Nizza n.250 - 10126 Torino - Italia, all'attenzione dell'Organismo di Vigilanza di Reply S.p.A.;
- **linea telefonica**, al numero: +39 011 7711594, chiedendo di conferire con l'Organismo di Vigilanza.

La tutela del segnalante sarà supportata anche da un'efficace attività di sensibilizzazione e comunicazione per i dipendenti sui diritti e gli obblighi relativi alla divulgazione delle azioni illecite.

Nel rispetto della normativa nazionale e sovranazionale relativa alle misure di protezione da adottare per assicurare la tutela del segnalante, Reply SpA garantisce, nel corso di tutto il processo di gestione delle segnalazioni, confidenzialità e riservatezza circa l'identità del segnalante e le informazioni oggetto delle stesse. Fatte salve le ulteriori responsabilità previste per legge, Reply SpA prevede responsabilità disciplinari nei confronti di chiunque violi gli obblighi di riservatezza o per chiunque diffami o calunni con dolo o colpa grave.

L'Organismo di Vigilanza di Reply SpA ha il compito di verificare la veridicità delle segnalazioni per conto delle Società del Gruppo Reply e, in conformità con quanto previsto dalla normativa di riferimento, di svolgere tutte le azioni necessarie ai fini della gestione delle segnalazioni stesse.



6. La formazione delle risorse e la diffusione del Modello

6.1. Formazione ed informazione dei Dipendenti

Ai fini dell'attuazione del presente Modello, è obiettivo di Reply SpA garantire una corretta conoscenza, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei processi sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con il responsabile della Funzione Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione del Modello.

La comunicazione iniziale: L'adozione del presente Modello è comunicata a tutte le risorse presenti in azienda al momento dell'adozione stessa e inserita sul portale aziendale. Tutte le modifiche intervenute successivamente e le informazioni concernenti il Modello verranno comunicate attraverso i medesimi canali informativi. Per i neo assunti sono predisposti incontri in cui sono formati sulle policy in materia di *compliance* (Codice Etico, Modello Organizzativo, procedura per le informazioni riservate, lettera insider dealing, ...).

La formazione: L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società. In particolare, il Gruppo prevede livelli diversi di informazione e formazione attraverso strumenti di divulgazione quali, a titolo esemplificativo, corsi online, post di aggiornamento sulla intranet aziendale, occasionali e-mail di aggiornamento, note informative interne.

6.2. Consulenti, partner e fornitori

Su proposta dell'Organismo di Vigilanza di Reply SpA potranno essere istituiti nell'ambito del Gruppo, ulteriori sistemi di valutazione per la selezione di consulenti, partner e fornitori, in aggiunta a quelli già previsti dal Gruppo.

Inoltre, saranno fornite a soggetti esterni al Gruppo (consulenti, partner e fornitori) apposite informative sulle politiche e le procedure adottate dal Gruppo anche in forza del presente Modello.

I soggetti esterni devono essere informati del contenuto del Modello e dell'esigenza delle società del Gruppo Reply che il loro comportamento sia conforme ai disposti del D. Lgs. 231/2001.

Nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano con la Pubblica Amministrazione o coinvolte nello svolgimento di attività a rischio rispetto ai reati societari (incluso il reato di corruzione tra privati) e reati di *market abuse* per conto o nell'interesse del Gruppo, i relativi contratti devono:

- essere definiti per iscritto, in tutte le loro condizioni e termini;
- contenere clausole standard, condivise con la Funzione Legale di Reply SpA, al fine del rispetto del D. Lgs. 231/2001;



- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (es. clausole risolutive espresse, penali).

7. Sistema disciplinare

La predisposizione di un efficace sistema sanzionatorio costituisce, ai sensi dell'art. 6 primo comma lettera e) del D. Lgs. 231/2001, un requisito essenziale del Modello ai fini dell'esimente rispetto alla responsabilità dell'ente.

Il Modello adottato da Reply SpA prevede un adeguato sistema disciplinare applicabile in caso di violazioni o di comportamenti non coerenti con le previsioni del Modello stesso e/o del Codice Etico.

La previsione di un sistema sanzionatorio rende efficiente l'azione dell'Organismo di Vigilanza e ha lo scopo di garantire l'effettività del Modello stesso.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D. Lgs. 231/2001.

7.1. Misure nei confronti di quadri e impiegati

La violazione da parte dei dipendenti soggetti al CCNL delle regole comportamentali di cui al presente Modello costituisce illecito disciplinare. Con riferimento alle sanzioni irrogabili nei riguardi di detti lavoratori dipendenti, il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente e cioè le norme pattizie di cui al CCNL applicabili.

Tali categorie 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.

L'inosservanza, da parte del lavoratore, delle disposizioni contenute nel contratto di lavoro e/o nel presente Modello può dar luogo, secondo la gravità della infrazione, all'applicazione dei seguenti provvedimenti:

- richiamo verbale nel caso in cui siano violate le procedure richiamate e/o previste dal presente Modello (ad esempio, che si ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, si ometta di svolgere controlli, ecc.) o sia adottato un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una non osservanza delle disposizioni portate a conoscenza da Reply SpA con ordini di servizio o altro mezzo idoneo;
- ammonizione scritta per le mancanze di minor rilievo;
- multa non superiore a tre ore di paga base e contingenza o minimo di stipendio e contingenza;



- sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni; la multa e la sospensione sono previste per le mancanze di maggior rilievo. L'importo delle multe che non costituiscono risarcimento di danni è devoluto alle esistenti istituzioni assistenziali e previdenziali di carattere aziendale o, in mancanza di queste, alla Cassa mutua malattia;
- licenziamento per mancanze con preavviso nel caso in cui il lavoratore adotti un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento la determinazione di un danno notevole o di una situazione di notevole pregiudizio;
- licenziamento per mancanze senza preavviso nel caso in cui il lavoratore adotti un comportamento palesemente in violazione alle prescrizioni del presente Modello e tale da determinare la concreta applicazione a carico della società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento il compimento di "*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 per l'azienda.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate saranno applicate, ai sensi di quanto previsto dal codice disciplinare vigente in Reply SpA, in relazione:

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

7.2. Misure nei confronti dei dirigenti

In caso di violazione, da parte di dirigenti, delle procedure richiamate e/o previste dal presente Modello o di adozione di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali, tra cui la risoluzione del rapporto di lavoro.

7.3. Misure nei confronti degli amministratori

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea degli azionisti al fine di adottare le misure più idonee previste dalla legge; resta fermo che tali violazioni costituiscono inadempimento dell'obbligo di diligenza posto a carico degli Amministratori ai sensi dell'art. 2392 del Codice Civile.

7.4. Misure nei confronti dei sindaci

In caso di violazione del Modello da parte di uno o più sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli



opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea degli azionisti al fine di adottare le misure più idonee previste dalla legge resta fermo che tali violazioni costituiscono inadempimento dell'obbligo di diligenza posto a carico dei sindaci ai sensi dell'art. 2407 del Codice Civile.

7.5. Misure nei confronti dei consulenti e dei partner

Ogni violazione da parte dei consulenti o dei partner delle regole di cui al Modello adottato da Reply SpA agli stessi applicabili o di commissione dei reati di cui al D. Lgs. 231/2001 è sanzionata secondo quanto previsto nelle specifiche clausole inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal D. Lgs. 231/2001.

8. Aggiornamento ed adeguamento del Modello

Ai fini del relativo aggiornamento e/o adeguamento, il presente Modello sarà oggetto da parte dell'Organismo di Vigilanza a verifiche periodiche sugli aggiornamenti normativi, sugli atti e sulle procedure del Gruppo, nonché sulle segnalazioni ricevute nel corso dell'anno, al fine di verificare la rispondenza dei presidi di controllo corrispondenti.

Per quanto concerne le società controllate, tale verifica verrà effettuata sotto la supervisione dell'Organismo di Vigilanza di Reply SpA, salvo i casi in cui sia nominato un Organismo di Vigilanza (non coincidente con l'Organo Dirigente), secondo modalità che verranno definite da quest'ultimo.



PARTE SPECIALE



9. Reati rilevanti

La presente Parte Speciale riporta le fattispecie delittuose contemplate dal D. Lgs. 231/2001 ritenute rilevanti ed illustra e definisce le attività che i Destinatari devono porre in essere affinché adottino regole di comportamento conformi a quanto prescritto nel Decreto Legislativo 231/2001 al fine di prevenire il verificarsi dei reati ivi considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- a) indicare le norme/protocolli che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

I Destinatari, nello svolgimento delle rispettive attività, si attengono:

- (i) alle disposizioni legislative e regolamentari, italiane o straniere, applicabili alla fattispecie;
- (ii) alle previsioni dello Statuto sociale;
- (iii) al Codice Etico;
- (iv) alle previsioni del Modello;
- (v) alle deliberazioni del Consiglio di Amministrazione e degli altri Comitati Consiliari;
- (vi) alle risoluzioni degli Amministratori Delegati;
- (vii) alle policy e alle disposizioni di servizio emanate dalle unità organizzative competenti e dai relativi responsabili.

Di seguito si riportano le Parti Speciali applicabili:

- Parte Speciale "A": Reati nei rapporti con la Pubblica Amministrazione e Corruzione tra privati.
- Parte Speciale "B": Reati informatici e trattamento illecito di dati.
- Parte Speciale "C": Delitti contro l'industria e il commercio.
- Parte Speciale "D": Reati societari.
- Parte Speciale "E": Reati con finalità di terrorismo o di eversione dell'ordine democratico; Delitti di criminalità organizzata; Reato di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare; Reati transnazionali; Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.
- Parte Speciale "F": Reati di abuso di mercato.
- Parte Speciale "G": Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
- Parte Speciale "H": Delitti in materia di violazione del Diritto d'Autore.
- Parte Speciale "I": Induzione a non rendere Dichiarazioni o a rendere Dichiarazioni mendaci all'Autorità Giudiziaria.
- Parte Speciale "L": Reati tributari.
- Parte Speciale "M": Delitti contro la personalità individuale e di Razzismo e Xenofobia
- Parte Speciale "N": Reati ambientali.
- Parte Speciale "O": Delitti contro il patrimonio culturale e paesaggistico.
- Parte Speciale "P": Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori.



Si ritiene opportuno precisare che seppur astrattamente rilevanti, si ritengono di remota applicazione, stante la realtà di Reply, i seguenti “reati presupposto” richiamati dal Decreto:

- falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- pratiche di mutilazione degli organi genitali femminili;
- frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;
- contrabbando.

9.1. Principi di comportamento

Tutti i Destinatari si astengono dal:

- (i) porre in essere comportamenti tali da integrare le fattispecie di reato considerate dal D. Lgs. 231/2001;
- (ii) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle differenti ipotesi di reato.

9.2. Approccio metodologico

Il processo che ha consentito di pervenire ad una mappa documentata delle potenziali modalità attuative degli illeciti di cui al D. Lgs. 231/2001 e dei relativi presidi di controllo, al fine della valutazione del rischio potenziale di compimento di reati rilevanti, della corretta progettazione delle misure preventive e della valutazione del rischio residuo, è descritto nei capitoli che seguono.

Tale metodologia è stata applicata per la valutazione dei rischi relativamente alle aree di attività a rischio reato che fanno capo al Gruppo Reply.

In fase di estensione dell'analisi dei rischi alle altre società del Gruppo è stato deciso di adottare la stessa metodologia di valutazione della “rischiosità”, in relazione sia all'omogeneità del business, sia alla loro operatività e alle loro peculiarità organizzative.

Tale metodologia costituirà inoltre base di riferimento per tutti i successivi aggiornamenti degli schemi di analisi della “rischiosità” a seguito di cambiamenti organizzativi e/o di variazioni nell'operatività aziendale e/o aggiornamenti legislativi.

L'analisi che ha condotto all'identificazione delle attività sensibili ai fini della commissione degli illeciti previsti dal D. Lgs. 231/2001 si è svolta secondo un approccio basato sui rischi, ovvero sull'analisi per processi.

Il lavoro è iniziato con l'analisi della struttura organizzativa di Reply SpA acquisendo la seguente documentazione:

- Statuto;
- Poteri e procure;
- Disposizioni organizzative e organigramma;
- Policy;
- Comunicazioni interne;
- Procedure operative;
- Manuale delle procedure contabili;
- Manuale e procedure del Sistema Qualità.



Per ognuna delle aree di attività a rischio reato si è provveduto ad identificare gli ambiti di rischio e le conseguenti attività in cui si estrinseca ciascun processo aziendale.



10. Parte Speciale “A”: Reati nei Rapporti con la Pubblica Amministrazione e di Corruzione tra privati

I reati commessi nei confronti della Pubblica Amministrazione (artt. 24 e 25 D.Lgs. 231/2001) trovano come presupposto l'instaurazione di rapporti (anche di natura commerciale) con la Pubblica Amministrazione stessa (intesa in senso lato).

Per completezza espositiva, essendo strettamente collegati ai reati di corruzione contro la PA, per modalità e rischi operativi, si riportano in questa sezione anche i reati di Corruzione tra privati ed Istigazione alla Corruzione tra privati di cui all'art. 25-ter del Decreto (Reati Societari).

10.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione dei rapporti con la Pubblica Amministrazione**
 - Gestione dei rapporti con esponenti pubblici per adempimenti normativi ed in occasione di verifiche e ispezioni sul rispetto della normativa medesima
 - Gestione dei rapporti di profilo istituzionale con esponenti della PA
 - Gestione dei rapporti con le authorities
 - Gestione dei finanziamenti ricevuti da enti pubblici
- **Partecipazione a gare e trattative**
- **Fornitura dei servizi nel settore pubblico e privato**
 - Acquisizione di contratti con clienti (gestione dei rapporti commerciali per l'acquisizione di commesse)
 - Gestione delle attività progettuali nell'ambito di servizi resi a clienti (sviluppo software e gestione delle licenze di terzi, trattamento dei dati e accesso ai sistemi informativi)
- **Gestione del contenzioso**
 - Gestione del contenzioso giudiziale, stragiudiziale e procedimenti arbitrali

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione degli acquisti di beni e servizi
- Gestione del personale (dipendenti e collaboratori)
- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni
- Rapporti infragruppo
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione degli adempimenti fiscali/tributari e contributivi
- Gestione della Tesoreria
- Amministrazione, finanza e controllo
- Gestione dei sistemi informativi
- Gestione degli adempimenti societari
- Gestione della salute e sicurezza
- Ambiente e gestione dei rifiuti.



10.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie di Reato nei Rapporti con la PA e la Corruzione tra privati richiamate dal D.Lgs. 231/2001 rispettivamente agli artt. 24, 25 e 25-ter, rilevanti per la Società.

- **Reati contro la Pubblica amministrazione (art. 24 e 25 D.lgs. 231/2001)**
 - Malversazione di erogazioni pubbliche (art. 316-bis c.p.)
 - Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.)
 - Truffa in danno dello Stato o di altro ente pubblico o delle Comunità Europee (art. 640, comma 2, n.1, c.p.)
 - Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.)
 - Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)
 - Frode nelle pubbliche forniture (art. 356 c.p.)
 - Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898)
 - Turbata libertà degli incanti (art. 353 c.p.)
 - Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.)
 - Concussione (art. 317 c.p.)
 - Corruzione per l'esercizio della funzione, corruzione per un atto contrario ai doveri d'ufficio e circostanze aggravanti (artt. 318, 319 e 319-bis c.p.)
 - Corruzione in atti giudiziari (art. 319-ter c.p.)
 - Induzione indebita a dare o promettere utilità (art. 319-quater c.p.)
 - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
 - Pene per il corruttore (art. 321 c.p.)
 - Istigazione alla corruzione (art. 322 c.p.)
 - Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso di ufficio di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali e di funzionari delle Comunità europee e degli Stati esteri (art. 322-bis c.p.)
 - Traffico di influenze illecite (art. 346 bis c.p.)
 - Peculato (limitatamente al primo comma) (art. 314 c.p.)
 - Peculato mediante profitto dell'errore altrui (art. 316 c.p.)
 - Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.)
- **Reati di corruzione tra Privati (da Reati Societari, art. 25-ter D.lgs. 231/2001)**
 - Corruzione tra privati (art. 2635 c.c.)
 - Istigazione alla corruzione tra privati (art. 2635-bis c.c.)

10.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati nei Rapporti con la Pubblica Amministrazione e alla Corruzione tra privati

10.3.1. Rapporti con la PA

I presidi procedurali necessitano della maggiore trasparenza possibile relativamente ai processi decisionali che riguardano i rapporti con pubblici ufficiali o incaricati di pubblico



servizio. In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dagli artt. 24 e 25 del D. Lgs. 231/2001. È, altresì, proibito porre in essere comportamenti che determinino situazioni di conflitto di interessi nei confronti di esponenti della Pubblica Amministrazione.

A tal riguardo, Reply SpA divulga la conoscenza delle disposizioni del Codice Etico del Gruppo in relazione al quale viene periodicamente svolta un'attività di aggiornamento.

In particolare, coerentemente con i principi deontologici aziendali è fatto divieto di:

- promettere, effettuare, assecondare il comportamento induitivo alla dazione di denaro o altra utilità a esponenti della Pubblica Amministrazione, per finalità diverse da quelle istituzionali e di servizio;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione) in favore di esponenti della Pubblica Amministrazione, italiana o straniera;
- effettuare prestazioni o pagamenti in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operino per conto di Reply SpA o altre Società del Gruppo, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- riconoscere compensi in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operino per conto di Reply SpA o altre Società del Gruppo, che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere;
- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati da esponenti della Pubblica Amministrazione, come condizione per lo svolgimento di successive attività;
- erogare omaggi a esponenti pubblici o loro familiari;
- fornire o promettere di rilasciare informazioni e/o documenti riservati;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione in errore di valutazione tecnico-economica della documentazione presentata;
- esibire documenti e dati falsi o alterati;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;
- destinare contributi, sovvenzioni, finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti.

È, inoltre, fatto obbligo ai Destinatari di attenersi alle seguenti prescrizioni:

- in caso di tentata concussione da parte di un pubblico esponente, il soggetto interessato deve: (i) non dare seguito alla richiesta; (ii) fornire tempestivamente informativa al proprio responsabile (in caso di dipendente) o al referente interno (in caso di soggetti terzi) ed attivare formale informativa verso l'Organismo di Vigilanza.
- In caso di conflitti di interesse che sorgano nell'ambito dei rapporti con la Pubblica Amministrazione, il soggetto interessato deve fornire tempestivamente informativa al proprio responsabile (in caso di dipendente) o al referente interno (in caso di soggetto terzo) ed attivare formale informativa verso l'Organismo di Vigilanza.
- In caso di dubbi circa la corretta attuazione dei principi etico-comportamentali di cui sopra nel corso dello svolgimento delle attività operative, il soggetto interessato deve interpellare senza ritardo il proprio responsabile (in caso di dipendente) o il referente interno (in caso di soggetto terzo) ed inoltrare formale richiesta di parere all'Organismo di Vigilanza.



Riveste una particolare importanza l'attività di monitoraggio e di rispetto delle procedure di Gruppo in relazione ai seguenti aspetti:

- gestione e erogazione di omaggi;
- gestione delle erogazioni liberali;
- modalità di ricorso all'attività di professionisti esterni e consulenti allo scopo di garantire che le prestazioni richieste al consulente siano effettivamente determinate da una esigenza aziendale;
- gestione delle carte di credito aziendali.

Inoltre, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.) che operano con la Pubblica Amministrazione per conto o nell'interesse di Reply SpA, i relativi contratti:

- definiscono per iscritto in tutte le loro condizioni e termini;
- contengono clausole standard al fine del rispetto del D. Lgs. 231/2001;
- contengono apposita dichiarazione dei medesimi con cui affermano di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contengono apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (es. clausole risolutive espresse, penali).

10.3.2. Corruzione tra privati

Reply SpA ha individuato presidi e misure di contenimento, che possono riassumersi di seguito:

- osservanza della procedura in tema di selezione e qualificazione dei fornitori;
- tracciabilità di tutte le fatture emesse dai fornitori a Reply SpA, tramite archiviazione nel sistema gestionale;
- presenza di una procedura di pricing per cui le eventuali variazioni in diminuzione, in caso di richiesta di sconto da parte del cliente, devono essere oggetto di necessaria approvazione da parte delle Funzioni interessate. Qualora detta richiesta di sconto risulti particolarmente significativa o comunque eccedenti le normali prassi in materia adottate da Reply SpA, la tematica viene rimessa ai Partners meeting.

In aggiunta, Reply SpA definisce i seguenti divieti, quali principi generali di comportamento che i Destinatari devono rispettare in relazione al reato in esame:

- divieto di intrattenere rapporti con soggetti qualificati di altre società, anche tramite interposta persona, nonché con soggetti terzi, operanti in ambiti a rischio strumentale o diretto rispetto alla commissione del reato in esame, se non da parte di quanti siano a ciò deputati secondo il sistema di deleghe e procure adottato da Reply;
- divieto di offrire o effettuare, direttamente e indirettamente, pagamenti indebiti e promesse di vantaggi personali di qualsiasi natura (compresa la gratuita disponibilità di servizi, finalizzata ad influenzare decisioni e transazioni), a soggetti qualificati di altre società, se non nel rispetto delle regole definite da Reply SpA nella policy Omaggi, spese di rappresentanza, sponsorizzazioni e erogazioni liberali;
- divieto di ricorrere a qualsivoglia forma di pressione, inganno e/o suggestione di soggetti qualificati appartenenti ad altra società, tali da influenzare i reciproci rapporti, con effetto distorsivo della concorrenza;
- divieto di effettuare pagamenti in contanti, salvo che di modico valore, nonché di effettuare pagamenti, versamenti o depositi su conti correnti diversi da quelli contrattualmente indicati e riferiti alle controparti negoziali;



- divieto di pagamento delle parcelle relative alle prestazioni ricevute dai consulenti, in mancanza di previa autorizzazione della funzione aziendale competente, nonché della previa attestazione dell'effettività della prestazione e valutazione della relativa congruità;
- divieto di erogazione di compensi o benefit a consulenti, collaboratori, partner commerciali di Reply SpA che non trovino giustificazione nelle attività effettivamente prestate.

Si rileva che Reply Spa, il Consorzio Public Sector e tutte le società consorziate sono dotate di un Sistema di Gestione Anticorruzione certificato secondo la norma ISO:37001.

10.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili alla Parte Speciale in esame, rispettivamente alle Aree sensibili rilevate.

Gestione dei rapporti con la Pubblica Amministrazione

- Esistenza di direttive aziendali che sanciscono l'obbligo alla massima collaborazione e trasparenza nei rapporti con Soggetti Pubblici/Autorità di Vigilanza.
- Monitoraggio dei procedimenti di richiesta di erogazioni, contributi o finanziamenti pubblici e il rispetto della corretta destinazione degli stessi.
- Formale segregazione tra chi decide e svolge l'attività sensibile in oggetto e chi è investito del potere di destinare le necessarie risorse economiche e finanziarie.
- Tracciabilità delle risorse economiche e finanziarie utilizzate nell'ambito dell'attività sensibile.
- Archiviazione della documentazione prodotta e inviata ai soggetti coinvolti nell'ambito della gestione dei rapporti istituzionali.
- Esistenza della policy per la gestione dei contatti con esponenti della Pubblica Amministrazione che identifica i soggetti responsabili per la gestione dei rapporti con i soggetti pubblici in caso di ispezioni, appositamente delegati dai vertici aziendali. La policy disciplina anche le modalità di archiviazione e conservazione delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di report sulla chiusura delle attività, indicante i nominativi dei soggetti coinvolti nell'ispezione, l'oggetto dell'ispezione e le eventuali decisioni che ne sono seguite. Inoltre, nell'ambito delle visite ispettive, si assicura la presenza di almeno due soggetti appartenenti alla Funzione interessata dall'ispezione e, se diversa, comunque sempre alla presenza del responsabile aziendale dei rapporti con l'Ufficio della Pubblica Amministrazione (o suoi delegati).

Partecipazione a gare e trattative

- Individuazione della Funzione competente a identificare le opportunità di business e le modalità/strumenti utilizzati (tramite analisi dei bollettini delle Pubbliche Amministrazioni Pubbliche o con altre fonti esterne o con contatti diretti).
- Identificazione delle Funzioni competenti per la valutazione tecnica ed economica dell'iniziativa.
- Approvazione dell'iniziativa dai soggetti titolari di specifica delega.
- Modalità di raccolta e verifica delle informazioni per la predisposizione della documentazione necessaria per la partecipazione alla procedura competitiva o trattativa diretta.



- Criteri per l'approvazione da parte di adeguati livelli autorizzativi della documentazione da trasmettere per la partecipazione alla procedura competitiva o trattativa diretta.
- Rispetto della normativa sulla privacy e delle norme di sicurezza.
- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.
- In caso di contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarano di conoscere e si obbligano a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

Fornitura dei servizi nel settore pubblico e privato

- Identificazione dei soggetti responsabili della predisposizione dell'offerta.
- Definizione delle attività svolte dalla Funzione incaricata nella fase di predisposizione dell'offerta.
- Identificazione dei soggetti autorizzati ad intrattenere rapporti con i clienti.
- Definizione delle attività svolte dalle Funzioni incaricate relative alla negoziazione dei contratti.
- Condivisione della documentazione predisposta dalle Funzioni competenti nella fase di formulazione dell'offerta.
- Verifica della documentazione di offerta (tecnica e commerciale) da inviare al cliente da parte delle Funzioni competenti.
- Definizione delle modalità di approvazione del contratto di vendita.
- Identificazione dei ruoli aziendali responsabili dell'approvazione del contratto di vendita.
- Definizione delle attività svolte dalla Funzione incaricata ai fini dell'elaborazione della richiesta di modifica contrattuale.
- Definizione delle modalità di approvazione delle richieste di modifica contrattuale.
- Definizione della documentazione necessaria a supporto della richiesta di modifica contrattuale.
- Definizione di contratti standard in coordinamento con le Funzioni competenti, volti a garantire il rispetto della normativa vigente.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione dell'offerta.
- Verifica circa la raccolta delle informazioni economico/professionali necessarie al fine di controllare il possesso dei requisiti di attendibilità e solidità della controparte.
- Esistenza di un'anagrafica clienti.
- Verifica della correttezza degli ordini di vendita inseriti a sistema.
- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.



Gestione del contenzioso

- Laddove esponenti aziendali siano stati destinatari di richieste di rendere o produrre davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni, è fatto divieto di indurre o favorire i medesimi esponenti a rendere dichiarazioni mendaci.
- I rapporti con l'Autorità Giudiziaria e con la Pubblica Amministrazione nell'ambito del contenzioso giudiziale e stragiudiziale devono essere improntati ai principi di correttezza, trasparenza e tracciabilità, anche quando gestiti per il tramite di un legale esterno.

Si segnala che Reply è certificata ISO:9001 per il sistema di gestione della qualità a livello di Gruppo.

10.5. Compiti dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza concernenti la valutazione sull'efficacia delle procedure e l'osservanza delle prescrizioni del Modello in materia di prevenzione dei reati contro la Pubblica Amministrazione sono i seguenti:

- verifica periodica, del sistema di deleghe vigente e del rispetto della procedura di comunicazione delle variazioni agli enti interessati;
- raccolta ed armonizzazione delle procedure interne poste a presidio delle attività individuate come rischiose;
- raccolta ed esame di eventuali segnalazioni riguardanti irregolarità riscontrate o situazioni di particolare criticità ricevute dai responsabili delle diverse funzioni o da qualsiasi dipendente, nonché da terzi;
- effettuazione delle attività di controllo secondo quanto disposto nel piano di audit e disposizione degli accertamenti ritenuti necessari e opportuni a seguito delle segnalazioni ricevute;
- monitoraggio sull'efficacia dei presidi e proposta di eventuali modifiche/integrazioni.

Qualora, nell'espletamento dei compiti di cui sopra, l'Organismo di Vigilanza riscontri violazioni delle regole e dei principi contenuti nella presente Parte Speciale del Modello da parte di Amministratori Delegati, dirigenti e/o dipendenti ne deve dare immediata informazione al Consiglio di Amministrazione e, nei casi più gravi aventi attinenza con il Sistema di Controllo Interno, anche al Comitato Controllo e Rischi e al Collegio Sindacale.



11. Parte Speciale “B”: Reati informatici e trattamento illecito di dati

Mediante la promulgazione della Legge n.48 del 18 marzo 2008, con il cui art. 7 è stata prevista l'introduzione dell'art. 24-*bis* nell'impianto normativo del D. Lgs. n. 231/2001, il legislatore ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001.

L'introduzione dell'articolo 24-*bis* nel D. Lgs. 231/2001 risponde all'esigenza di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi.

L'area di attività a rischio che presenta profili di maggiore criticità potenziale risulta essere, ai fini della presente Parte Speciale del Modello, la gestione dei sistemi informativi e dei documenti informatici ed in particolare le seguenti attività:

- *Maintenance* dell'hardware e del software aziendale;
- Gestione delle misure di sicurezza a protezione dei sistemi informatici e/o telematici;
- Gestione del processo di assegnazione dei codici di accesso ai sistemi informatici e/o telematici.

Reply ha implementato un sistema procedurale in materia di gestione dei sistemi informativi e dei documenti informatici che si compone delle seguenti policy:

- ICT Security Policy: dettaglia i requisiti per la sicurezza delle informazioni, da rispettare nelle attività svolte internamente o presso i Clienti, sulla base delle best practice internazionali;
- GDPR Compliance Program: descrive le pratiche di protezione dei dati e di tutela della privacy per tutte le società del Gruppo;
- Employees' Privacy Policy: stabilisce i principi per la protezione dei dati personali durante lo svolgimento dell'operatività quotidiana per i Clienti e/o per Reply;
- Regole di comportamento per la gestione sicura degli asset aziendali e delle informazioni: elenca le norme che devono essere rispettate da tutto il personale per
- garantire il corretto e sicuro utilizzo delle risorse messe a disposizione dalle società del Gruppo Reply per lo svolgimento dell'attività lavorativa, nelle attività interne e presso i Clienti;
- Policy per lo svolgimento servizi per conto del Cliente: descrive le linee guida di comportamento da osservare per garantire che il servizio fornito sia conforme alla normativa vigente, al fine di prevenire la commissione di reati informatici.
- Policy AI: delinea le responsabilità e le azioni raccomandate per garantire un uso etico e lecito dell'AI nel lavoro svolto dai dipendenti Reply per Reply e i suoi Clienti.

Tali policy a tutela dei rischi di commissione dei reati informatici di cui all'art. 24-*bis* del D. Lgs. 231/2001, definiscono:

- ruolo e responsabilità dei soggetti coinvolti nelle singole fasi del processo;
- flussi informativi e documentali;
- flussi autorizzativi;
- attività di controllo e monitoraggio;
- modalità di gestione delle eccezioni;
- modalità di archiviazione della documentazione.

11.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.



- **Gestione dei sistemi informativi**

- Maintenance dell'hardware e del software aziendale
- Gestione delle misure di sicurezza a protezione dei sistemi informatici e/o telematici
- Gestione del processo di assegnazione dei codici di accesso ai sistemi informatici e/o telematici
- Gestione delle licenze software

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Fornitura dei servizi nel settore pubblico e privato

11.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati informatici richiamate all'art. 24-*bis* (Reati Informatici e trattamento illecito di dati) del D.Lgs. 231/2001, rilevanti per la Società.

- Documenti informatici (art. 491-*bis* c.p.)
- Accesso abusivo a un sistema informatico o telematico (art. 615-*ter* c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o 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 interesse pubblico (art. 635-*ter* c.p.)
- Danneggiamento di sistemi informatici e telematici (art. 635-*quater* c.p.)
- Danneggiamento di sistemi informatici e telematici di pubblico interesse (art. 635-*quinquies* c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.)
- Art. 1 comma 11 D.L. 105/2019 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica²⁶
- Estorsione informatica (art. 629, comma 3, c.p.)

11.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati informatici

I presidi procedurali necessitano la maggiore trasparenza e tracciabilità possibile nei processi di gestione dei sistemi informatici. A tal fine, i Destinatari devono assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle

²⁶ La valutazione completa circa l'applicabilità di tale fattispecie di reato sarà subordinata alla pubblicazione, con Decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), dell'elenco delle amministrazioni pubbliche, degli enti e degli operatori nazionali, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal D.L. n.105.



procedure aziendali, in tutte le attività che prevedono l'utilizzo dei sistemi informatici di Reply SpA.

In via generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 24-*bis* del D.Lgs. 231/2001.

A tal riguardo è stato completato il processo di divulgazione e conoscenza delle disposizioni previste nelle policy emanate. In particolare, coerentemente con i principi deontologici aziendali è fatto divieto di:

- acquisire, copiare e utilizzare, senza autorizzazione, o danneggiare software del Gruppo Reply o di terze parti;
- effettuare e/o distribuire copie del software o della documentazione da utilizzare all'interno del Gruppo Reply o per altri fini né per uso personale o altrui, inclusi clienti e membri delle rispettive famiglie;
- introdurre e/o utilizzare nel Gruppo Reply software proveniente da fonti non autorizzate, incluso quello scaricato da Internet o che non prevede l'acquisto di licenze;
- utilizzare i sistemi informativi del Gruppo Reply o quello personale in modo da intercettare abusivamente, interrompere o danneggiare l'attività del Gruppo Reply o l'attività di soggetti terzi o in modo da violare le norme o le leggi in merito;
- falsificare documenti informatici aventi efficacia probatoria;
- detenere e utilizzare le password di accesso alle caselle e-mail dei dipendenti, allo scopo di controllare le attività svolte nell'interesse della Società, anche in violazione delle norme sulla privacy;
- porre in essere o in qualsiasi modo contribuire alla realizzazione delle fattispecie di cui all'art. 24-*bis* del D. Lgs. 231/2001 ovvero alla violazione dei principi e delle procedure aziendali descritte nel presente Modello.

11.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione dei sistemi informativi

- Esistenza della ICT Security Policy in materia di sicurezza dei sistemi informativi che definisce, fra l'altro:
 - o gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda;
 - o la gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
 - o modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
 - o ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica;
 - o implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;
 - o identificazione dei requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;



- gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
 - Confidenzialità, autenticità e integrità delle informazioni;
 - sicurezza nel processo di sviluppo dei sistemi informativi
- Formazione specifica sul tema del Ricatto Informatico, in particolare, al fine di evitare, nell'ambito del procacciamento di affari e dei servizi svolti, situazioni di minacce di sospensione dei servizi e/o pubblicazione di dati del cliente.
- Svolgimento di riunioni periodiche con il Data Protection Officer sulle modalità di trattamento dei dati personali da parte del Titolare, anche con riguardo al profilo delle misure di sicurezza adeguate al livello di rischio adottato.

11.5. Compiti dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati e gli illeciti in materia di delitti informatici e trattamento illecito dei dati sono i seguenti:

- emanare o proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- svolgere verifiche periodiche sull'efficacia e il rispetto delle procedure e/o policy interne inerenti la tutela della proprietà intellettuale e la gestione dei sistemi informatici e altre attività volte a prevenire la commissione dei reati;
- esaminare le eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.



12. Parte Speciale “C”: Delitti contro l’industria e il commercio

12.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Fornitura dei servizi nel settore pubblico e privato**
 - Acquisizione di contratti con clienti (gestione dei rapporti commerciali per l'acquisizione di commesse)
 - Gestione delle attività progettuali nell'ambito di servizi resi a clienti (sviluppo software e gestione delle licenze di terzi, trattamento dei dati e accesso ai sistemi informativi)

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Partecipazione a gare e trattative
- Gestione degli acquisti di beni e servizi

12.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti contro l’industria e il commercio richiamate dal D.Lgs. 231/2001 dall’art. 25-*bis*.1 (Delitti contro l’industria e il commercio), rilevanti per la Società.

- 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.)
- 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.)

12.3. I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Delitti contro l’industria e il commercio

I Destinatari del Modello sono tenuti a osservare i seguenti principi generali di comportamento:

- assicurare il regolare funzionamento delle attività di competenza;
- rispettare i principi etici e i valori del Gruppo Reply nei rapporti commerciali con le imprese;
- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione.

In generale, è fatto dunque divieto ai Destinatari del Modello di porre in essere comportamenti che possano rientrare, anche potenzialmente, nelle fattispecie di reato richiamate dall’art. 25-*bis*.1. D.Lgs. 231/2001, ovvero di collaborare o dare causa alla relativa realizzazione.



12.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Fornitura dei servizi nel settore pubblico e privato

- Identificazione dei soggetti responsabili della predisposizione dell'offerta.
- Definizione delle attività svolte dalla Funzione incaricata nella fase di predisposizione dell'offerta.
- Identificazione dei soggetti autorizzati ad intrattenere rapporti con i clienti.
- Definizione delle attività svolte dalle Funzioni incaricate relative alla negoziazione dei contratti.
- Condivisione della documentazione predisposta dalle Funzioni competenti nella fase di formulazione dell'offerta.
- Verifica della documentazione di offerta (tecnica e commerciale) da inviare al cliente da parte delle Funzioni competenti.
- Definizione delle modalità di approvazione del contratto di vendita.
- Identificazione dei ruoli aziendali responsabili dell'approvazione del contratto di vendita.
- Definizione delle attività svolte dalla Funzione incaricata ai fini dell'elaborazione della richiesta di modifica contrattuale.
- Definizione delle modalità di approvazione delle richieste di modifica contrattuale.
- Definizione della documentazione necessaria a supporto della richiesta di modifica contrattuale.
- Definizione di contratti standard in coordinamento con le Funzioni competenti, volti a garantire il rispetto della normativa vigente.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione dell'offerta.
- Verifica circa la raccolta delle informazioni economico/professionali necessarie al fine di controllare il possesso dei requisiti di attendibilità e solidità della controparte.
- Esistenza di un'anagrafica clienti.
- Verifica della correttezza degli ordini di vendita inseriti a sistema.
- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.

12.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



13. Parte Speciale “D”: Reati Societari

13.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Rapporti Infragruppo**
 - Gestione dei rapporti fra le Società del Gruppo
- **Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)**
 - Investimenti e disinvestimenti
 - Operazioni straordinarie (es. fusioni, scissioni e operazione su azione/partecipazioni)
 - Operazioni sul capitale e destinazione dell'utile
- **Amministrazione, finanza e controllo**
 - Gestione della contabilità generale e redazione del Bilancio civilistico
 - Gestione delle operazioni di redazione del Bilancio consolidato
 - Controllo di gestione (gestione delle attività di pianificazione e controllo)
 - Rapporti con Organi di Vigilanza e Controllo
- **Gestione degli adempimenti societari**
 - Gestione dei rapporti con gli Organi Societari e con i Soci
 - Gestione degli atti del Consiglio di Amministrazione

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione degli adempimenti fiscali/tributari e contributivi
- Gestione delle informazioni privilegiate e price sensitive
- Gestione della tesoreria
- Gestione dei sistemi informativi
- Gestione del personale (dipendenti e collaboratori)

13.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati Societari richiamate dal D.Lgs. 231/2001 all'art. 25-ter (Reati societari) del D.Lgs. 231/2001, rilevanti per la Società.

- False comunicazioni sociali (art. 2621 c.c.)
- Fatti di lieve entità (art. 2621-bis c.c.)
- False comunicazioni sociali delle società quotate (art. 2622 c.c.)
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione dei conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili o 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 d'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.)
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza (art. 2638, commi 1 e 2, c.c.)
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023)

13.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati Societari

I principi generali di comportamento prevedono che i Destinatari del Modello:

- si astengono dal porre in essere o in qualsiasi modo contribuire alla realizzazione delle fattispecie di reato di cui all'art. 25-*ter* del D. Lgs. 231/2001 ovvero alla violazione dei principi richiamati nel Modello e delle procedure aziendali;
- assumono un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio;
- i preposti alla formazione del bilancio e delle altre comunicazioni sociali si adoperano al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria di Reply SpA e del Gruppo;
- assumono un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, al fine di garantire la tutela del patrimonio degli investitori, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative ai prodotti finanziari ed agli emittenti, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria dell'emittente e sull'evoluzione della sua attività, nonché sui prodotti finanziari e relativi diritti;
- osservano le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agiscono sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori, dei soci e dei terzi in genere;
- non agiscono ponendo in atto comportamenti corruttivi verso amministratori, direttori generali, dirigenti preposti, liquidatori o persone sottoposte alla loro direzione e vigilanza di società terze, ed in primo luogo dei clienti e/o dei potenziali clienti, al fine di ottenere un vantaggio per la conduzione delle attività del Gruppo Reply;
- assicurano il regolare funzionamento della società e degli organi sociali, garantendo ogni forma di controllo sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà degli organi sociali;
- si astengono dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari;
- effettuano con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese;
- assumono un comportamento corretto e veritiero con gli organi di stampa, di informazione e con gli analisti finanziari.



I Destinatari consentono al Collegio Sindacale ed alle società di revisione l'esercizio dei poteri che la legge loro affida. In particolare, è garantita al Collegio Sindacale ed ai sindaci individualmente la possibilità di procedere, in qualsiasi momento, ad atti di ispezione e controllo.

I Destinatari che abbiano conoscenza della richiesta di un socio di consultare la documentazione societaria segnalano il fatto all'unità organizzativa competente per i rapporti con gli azionisti.

Le aree di riferimento sono state oggetto di analisi dettagliate volte all'adeguamento del Sistema di Controllo Interno, nell'ambito amministrativo-contabile, ai requisiti della Legge 262/2005. La valutazione del suddetto Sistema è finalizzata a limitare i rischi connessi alla non attendibilità o rappresentazione non veritiera e corretta dell'informativa economico-finanziaria di Reply SpA.

Nello specifico, con riferimento ai postulati di bilancio (esistenza e accadimento, completezza, valutazione e misurazione, diritti ed obblighi, presentazione ed informativa) e all'adeguatezza della segregazione dei compiti e ruoli, sono stati analizzati i seguenti processi aziendali:

- Gestione della Tesoreria;
- Amministrazione, Finanza e Controllo;
- Adempimenti fiscali/tributari e contributivi;
- Gestione del personale (dipendenti e collaboratori);
- Gestione degli Adempimenti societari;
- Gestione dei Sistemi informativi.

Pertanto, per quanto riguarda tutti gli aspetti legati alla gestione della contabilità generale e predisposizione dei progetti di bilancio civilistico ed altri adempimenti in materia societaria della società Reply SpA e del Gruppo Reply, si rimanda alla documentazione predisposta per l'adeguamento della società ai dettami della Legge 262/2005 e al "Manuale delle procedure amministrativo-contabili".

Il sistema di controllo così definito e utilizzato dalla società Reply SpA fornisce anche una tutela rispetto al rischio di commissione dei reati societari previsti dal Decreto Legislativo 231/2001.

13.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Rapporti infragruppo

- Identificazione di ruoli aziendali responsabili della stesura/verifica dei contratti infragruppo.
- Esistenza di appositi template per la predisposizione dei contratti per l'identificazione dei servizi da erogare.
- Formale definizione degli obblighi e delle responsabilità della società mandante e della società mandataria.
- Monitoraggio e aggiornamento dei corrispettivi previsti nei contratti.
- Operazioni di acquisizione/cessione di asset tra Società del Gruppo e con controparti esterne sono condotte nel rispetto delle normative fiscali vigenti.



Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)

- Le operazioni straordinarie/sul capitale sono approvate dal Consiglio di Amministrazione sulla base di adeguata informativa messa a disposizione dei membri nel rispetto di quanto previsto dalle normative.
- Le riunioni del Consiglio di Amministrazione sono verbalizzate e archiviate (i verbali riportanti le deliberazioni, sono redatti e trascritti su apposito Libro tenuto a norma di legge).
- L'Assemblea approva le operazioni nel rispetto di quanto previsto dalla legge e dallo Statuto.
- Vengono individuate le Funzioni aziendali responsabili delle attività finalizzate ad ottenere il "certificato preliminare" di cui all'art. 29 del D.Lgs. 19/2023, nell'ambito delle fusioni transfrontaliere.

Amministrazione, finanza e controllo

- Monitoraggio costante dell'evoluzione del quadro normativo di riferimento e verifica della corretta applicazione del quadro normativo di riferimento.
- Apposita formazione al personale delle Funzioni di contabilità e fiscale per quanto concerne le tematiche contabili e fiscali in vigore.
- Profilazione delle utenze per l'accesso al sistema informativo aziendale dedicato alla gestione della contabilità.
- Formale definizione delle modalità e dei criteri per la registrazione e la validazione delle scritture contabili.
- Esecuzione delle verifiche circa la completa e corretta registrazione delle scritture contabili nel sistema informativo aziendale dedicato alla gestione della contabilità.
- Esecuzione di verifiche circa la correttezza del trattamento contabile degli asset (ammortamenti, svalutazioni, rivalutazioni, manutenzioni e dismissioni).
- Formale controllo circa la corrispondenza tra la documentazione a supporto ed il calcolo di ratei e risconti.
- Esecuzione di verifiche su scritture di rettifica, ratei e risconti con andamenti anomali.
- Controllo sul trattamento contabile del personale: il calcolo delle imposte sul personale è verificato mediante supporto di terzi adeguatamente qualificati.
- Controllo sul corretto inserimento all'interno del sistema informativo aziendale dedicato alla gestione della contabilità del tax coding e codice IVA.
- Identificazione dei ruoli aziendali responsabili del monitoraggio e della gestione dell'anagrafica dei conti a sistema.
- Formale definizione delle modalità operative della gestione dell'anagrafica dei conti a sistema.
- Formale definizione delle modalità con le quali viene tracciato il processo di formazione dei dati contabili.
- Esecuzione di verifiche circa la precisione e la veridicità dei registri contabili.
- Esecuzione di verifiche mensili su registrazioni contabili inserite manualmente superiori importi prestabiliti dalle procedure interne e relative verifiche della documentazione a supporto della registrazione.
- Utilizzo di mezzi idonei a garantire la documentabilità e la riservatezza dei flussi informativi relativi alla gestione della contabilità.
- Archiviazione della documentazione prodotta nel corso della gestione della contabilità.



- Utilizzo di strumenti idonei a garantire un adeguato processo di custodia di tutta la documentazione con valenza fiscale prevista dalla normativa vigente.
- Formale definizione delle modalità di conservazione dei documenti rilevanti ai fini fiscali.
- Monitoraggio periodico volto a verificare eventuali aggiornamenti normativi in materia di predisposizione e approvazione del bilancio.
- Identificazione dei ruoli aziendali responsabili della predisposizione della bozza di bilancio e della sua approvazione.
- Verifica del rispetto dei vincoli normativi in materia di predisposizione del bilancio.
- Formalizzazione delle variazioni apportate ai criteri di valutazione adottati per la redazione dei documenti contabili.
- Formale definizione e verifica del rispetto delle tempistiche di trasmissione delle informazioni finalizzate alla predisposizione del bilancio (calendario di chiusura).
- Esecuzione di verifiche circa la completezza e la correttezza delle informazioni contenute nel fascicolo di bilancio, in ottemperanza a quanto previsto dalle norme vigenti.
- Formale attestazione da parte delle Funzioni coinvolte in merito alla completezza e veridicità dei dati di bilancio forniti.
- Verifica della precisione e veridicità dei registri contabili e divulgazione, a chi di competenza, di errori, delle omissioni e/o delle falsificazioni degli stessi.
- Formale approvazione del bilancio della Società.
- Archiviazione della documentazione prodotta nel corso della predisposizione del bilancio.
- Monitoraggio costante dell'evoluzione normativa.
- Osservanza dei principi di redazione del bilancio consolidato.
- Profilazione delle utenze per l'accesso al sistema informativo aziendale dedicato alla gestione della contabilità.
- Utilizzo di mezzi idonei a garantire la documentabilità e la riservatezza dei flussi informativi relativi alla predisposizione del bilancio consolidato e alla redazione delle relazioni finanziarie intermedie.
- Esecuzione di verifiche circa la completezza e la correttezza delle informazioni contenute nel reporting package, in ottemperanza a quanto previsto dalle norme vigenti.
- Formale approvazione del bilancio consolidato e delle relazioni finanziarie intermedie della Società.
- Archiviazione della documentazione prodotta nel corso della predisposizione del bilancio consolidato e della redazione delle relazioni finanziarie intermedie.

Gestione degli adempimenti societari

- Svolgimento di riunioni periodiche tra: la Società di Revisione e il Collegio Sindacale; la Società di Revisione e la Funzione competente per l'esame e condivisione dei documenti contabili societari da sottoporre all'approvazione del Consiglio di Amministrazione e dell'Assemblea, nonché ai fini della valutazione di possibili criticità emerse nello svolgimento delle attività di revisione.
- Gestione delle richieste di informazioni, di dati e di documenti (consegnati o resi disponibili) ricevute da Soci, Società di Revisione, Collegio Sindacale e che le stesse siano improntate ai principi di trasparenza e collaborazione.
- Pianificazione di incontri periodici tra la Società di Revisione, il Collegio Sindacale e l'Organismo di Vigilanza.



- Utilizzo di mezzi idonei a garantire la documentabilità e la riservatezza dei flussi informativi relativi alla gestione dei rapporti con la Società di Revisione ed il Collegio Sindacale.
- Formale definizione delle modalità di convocazione e svolgimento del Consiglio di Amministrazione in osservanza dei principi normativi e statutari adottati.
- Formale definizione delle modalità di trasmissione degli argomenti da trattare all'interno del Consiglio di Amministrazione e verifica della completezza, accuratezza e veridicità dei dati e delle informazioni riportate all'interno.
- Formale predisposizione e approvazione del verbale e trascrizione dello stesso all'interno del libro delle adunanze e delle deliberazioni delle assemblee.

13.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività connesse ai processi sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello (esistenza e adeguatezza della relativa procura, limiti di spesa, effettuato reporting verso gli organi deputati, ecc.).

Specificatamente, all'Organismo di Vigilanza vengono assegnati i seguenti compiti:

- emanare o proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- con riferimento al bilancio, alle relazioni ed alle altre comunicazioni sociali previste dalla legge, in ragione della circostanza che il bilancio di esercizio ed il bilancio consolidato è sottoposto a verifica di una società di revisione, l'Organismo di Vigilanza provvede all'espletamento dei seguenti compiti:
 - monitoraggio sull'efficacia delle procedure interne per la prevenzione del reato di false comunicazioni sociali;
 - esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
 - vigilanza sull'effettiva sussistenza delle condizioni per garantire alla società di revisione una concreta autonomia nelle sue funzioni di controllo delle attività aziendali.
- con riferimento alle altre attività a rischio:
 - svolgere verifiche periodiche sul rispetto delle procedure interne;
 - svolgere verifiche periodiche sull'effettuazione delle comunicazioni alle Autorità Pubbliche di Vigilanza e sull'osservanza delle procedure adottate nel corso di eventuali ispezioni compiute dagli esponenti di queste ultime;
 - valutare periodicamente l'efficacia delle procedure volte a prevenire la commissione dei reati;
esaminare le 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.



14. Parte Speciale “E”: Reati con finalità di terrorismo o di eversione dell’ordine democratico; Delitti di criminalità organizzata; Reato di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare; Reati transnazionali; Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

14.1. Reati con finalità di terrorismo o di eversione dell’ordine democratico

14.1.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Fornitura dei servizi nel settore pubblico e privato**
- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Partecipazione a gare e trattative
- Fornitura dei servizi nel settore pubblico e privato
- Gestione degli omaggi, eventi spese di rappresentanza e sponsorizzazioni
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione della Tesoreria
- Rapporti infragruppo

14.1.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati con finalità di terrorismo o di eversione dell’ordine democratico richiamati all’art. 25-*quater* del D.Lgs. 231/2001, rilevanti per la Società.

- Associazioni con finalità di terrorismo anche internazionale o di eversione dell’ordine democratico (art. 270-*bis* c.p.)
- Assistenza agli associati (art. 270-*ter* c.p.)
- Istigazione a commettere alcuno dei delitti previsti dai capi primo e secondo (art. 302 c.p.)
- Convenzione di New York del 9 dicembre 1999, art. 2



14.1.3. I Principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati con finalità di terrorismo o di eversione dell'ordine democratico

È fatto divieto a tutti i Destinatari del Modello di:

- intrattenere rapporti, negoziare e/o stipulare e/o porre in esecuzione contratti o atti con persone "a rischio";
- concedere utilità a persone "a rischio";
- assumere persone "a rischio".

Per persone "a rischio" si intendono le persone fisiche e giuridiche presenti nelle Liste di Riferimento predisposte dall'Unione Europea per la prevenzione dei reati con finalità di terrorismo e come misura per evitare che risorse economiche o servizi di qualsiasi tipo possano essere utilizzate per commettere atti terroristici. Tali Liste: (a) sono contenute in Regolamenti dell'Unione Europea, pubblicati nel Bollettino Ufficiale della Unione Europea, e (b) sono diffuse dall'Unità di Informazione Finanziaria - UIF - istituita presso la Banca d'Italia.

Conseguentemente, è vietato:

- 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;
- violare le regole contenute nelle procedure, nel Modello, nel Codice Etico di Reply e nella documentazione adottata in attuazione dei principi di riferimento previsti nella presente Parte Speciale.

14.1.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione degli acquisti di beni e servizi

- Qualificazione dei fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Previsione delle tipologie di beni e/o importi per i quali si possa procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti a identificare eventuali condizioni di incompatibilità e conflitto di interessi.
- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello e Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- In caso di contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e



sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obblighino a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria. L'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
 - applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;
 - assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;
 - non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte della Funzione preposta che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.
- Verifiche da parte delle Funzioni competenti in materia di anticorruzione sulle precedenti esperienze professionali indicate dal candidato e, inoltre, sono richieste informazioni riguardanti, ove possibile, eventuali precedenti penali, procedimenti penali in corso; L'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Evidenza dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.
- Divieto di impiegare lavoratori stranieri privi di permesso di soggiorno o con un permesso revocato o scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo.

14.1.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



14.2. Delitti di criminalità organizzata

14.2.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta
- **Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni**
 - Gestione degli omaggi
 - Organizzazione di eventi
 - Erogazione di sponsorizzazioni
 - Erogazione di donazioni
 - Gestione delle spese di rappresentanza

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Partecipazione a gare e trattative
- Fornitura dei servizi nel settore pubblico e privato
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione degli adempimenti fiscali/tributari e contributivi
- Gestione della Tesoreria
- Rapporti infragruppo
- Amministrazione, finanza e controllo

14.2.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti di criminalità organizzata, richiamate dal D.Lgs. 231/2001 all'art. 24-ter, rilevanti per la Società.

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309)



- Tutti i delitti se commessi avvalendosi delle condizioni previste dall'art. 416-*bis* c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo (L. 203/91)
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), numero 5), c.p.p.)

14.2.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti di criminalità organizzata

È fatto divieto a tutti i Destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reati di criminalità organizzata;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

È, inoltre, necessario:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- che sia rispettato il principio di separazione di ruoli e responsabilità nelle fasi dei processi;
- che sia assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività "sensibili" nell'aree "a rischio reato".

14.2.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Fornitura dei servizi nel settore pubblico e privato

- Identificazione dei soggetti responsabili della predisposizione dell'offerta.
- Definizione delle attività svolte dalla Funzione incaricata nella fase di predisposizione dell'offerta.
- Identificazione dei soggetti autorizzati ad intrattenere rapporti con i clienti.
- Definizione delle attività svolte dalle Funzioni incaricate relative alla negoziazione dei contratti.
- Condivisione della documentazione predisposta dalle Funzioni competenti nella fase di formulazione dell'offerta.
- Verifica della documentazione di offerta (tecnica e commerciale) da inviare al cliente da parte delle Funzioni competenti.
- Definizione delle modalità di approvazione del contratto di vendita.
- Identificazione dei ruoli aziendali responsabili dell'approvazione del contratto di vendita.
- Definizione delle attività svolte dalla Funzione incaricata ai fini dell'elaborazione della richiesta di modifica contrattuale.
- Definizione delle modalità di approvazione delle richieste di modifica contrattuale.



- Definizione della documentazione necessaria a supporto della richiesta di modifica contrattuale.
- Definizione di contratti standard in coordinamento con le Funzioni competenti, volti a garantire il rispetto della normativa vigente.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione dell'offerta.
- Verifica circa la raccolta delle informazioni economico/professionali necessarie al fine di controllare il possesso dei requisiti di attendibilità e solidità della controparte.
- Esistenza di un'anagrafica clienti.
- Verifica della correttezza degli ordini di vendita inseriti a sistema.
- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.

Gestione degli acquisti di beni e servizi

- Qualificazione dei fornitori e previsione dell'Albo Fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Tipologie di beni e/o importi per i quali si può procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti a identificare eventuali condizioni di incompatibilità e conflitto di interessi.
- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello e Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- In caso di contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obbligano a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

In particolare, l'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
- applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;
- assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;



- non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte delle Funzioni preposte che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.
- Verifica da parte delle Funzioni competenti in materia di anticorruzione, sulle precedenti esperienze professionali indicate dal candidato e sono richieste informazioni riguardanti, ove possibile, eventuali precedenti penali, procedimenti penali in corso. L'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Evidenza dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.
- Divieto di impiegare lavoratori stranieri privi di permesso di soggiorno o con un permesso revocato o scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo.

Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni

- Qualsiasi omaggio, vantaggio economico, ospitalità o altra utilità (di seguito "omaggio") ricevuto/effettuato dal personale, si prevede che sia, da un punto di vista oggettivo, ragionevole e in buona fede.
- Iter autorizzativo specifico per la corresponsione e/o ricezione di omaggi che superano la soglia prevista nelle policy o che siano nei confronti o da parte di pubblici ufficiali.
- Redazione in forma scritta dei contratti di sponsorizzazione e degli accordi di donazione.
- Impegno del beneficiario/erogante a rispettare le leggi applicabili e a effettuare le dovute registrazioni contabili/fiscali in modo corretto e trasparente.
- Divieto di effettuare pagamenti per importi superiori ai valori indicati nella documentazione di riferimento (es: contratto).
- Documentazione delle donazioni/sponsorizzazioni in modo preciso ed accurato, in conformità con la legge vigente.
- In caso di donazioni/sponsorizzazioni collegate a Enti Pubblici, Funzionari pubblici o Incaricati di pubblico servizio, valutazione dei potenziali rischi conseguenti.
- Raccolta da parte degli Enti Richiedenti delle evidenze a conferma che le donazioni/sponsorizzazioni hanno avuto luogo in accordo con i piani proposti e/o con gli accordi contrattuali e sono disponibili su richiesta delle Funzione/Organismi di controllo.

14.2.5. Compiti dell'Organismo di Vigilanza



L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

14.3. Reati di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare

Il D.Lgs. 16 luglio 2012, n. 109, mediante l'introduzione dell'art. 25-*duo-decies* nel D.Lgs. 231/2001, ha ampliato i reati presupposto per la responsabilità amministrativa delle persone giuridiche anche alle fattispecie disciplinate dall'articolo 22, comma 12, del D.Lgs. 286/1998 (c.d. Testo unico dell'immigrazione), sanzionando i datori di lavoro che impiegano lavoratori stranieri privi del permesso di soggiorno o lavoratori il cui permesso sia scaduto, revocato o annullato; la sanzione si applica nel caso in cui i lavoratori occupati siano più di tre, oppure minori in età non lavorativa o ancora esposti a situazioni di grave pericolo in ragione alle prestazioni da svolgere e alle condizioni di lavoro.

Lo scopo della norma è quello di sanzionare l'ente-datore di lavoro che ricorra alla pratica, considerata particolarmente grave, di sfruttamento di personale straniero irregolare con abuso della posizione di inferiorità proprio di quest'ultimo. La sanzione in capo all'ente ai sensi del D. Lgs. 231/2001 ricorre peraltro solo nei casi più gravi di ripetitività del comportamento illecito (i lavoratori irregolari siano tre o più) ovvero di particolare riprovevolezza dello stesso (i lavoratori siano minori in età non lavorativa o esposti a situazioni di grave pericolo in ragione alle prestazioni da svolgere e alle condizioni di lavoro).

14.3.1. Le "Aree Sensibili" ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta

14.3.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie di Reato di impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare, richiamate dal D.Lgs. 231/2001 all'art. 25-*duo-decies*, rilevanti per la Società.



- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, *3bis*, *3ter*, 5 D.Lgs. 286/1998)
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12-*bis*, D.Lgs. 286)

14.3.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative al Reato di Impiego di cittadini di Paesi Terzi il cui soggiorno è irregolare

In via generale, ai Destinatari del Modello è richiesto di:

- osservare e garantire l'osservanza, all'interno di Reply SpA di tutte le norme a tutela del lavoratore ed in materia di immigrazione;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di cui all'art. 25-*duo-decies* del D. Lgs. 231/2001.

È, inoltre, previsto, a carico dei Destinatari, l'espresso divieto di:

- favorire e/o promuovere l'impiego, alle dipendenze di Reply SpA, di lavoratori stranieri privi del permesso di soggiorno o con permesso scaduto rispetto al quale non sia stato chiesto, entro i termini di legge, il rinnovo oppure con permesso revocato o annullato;
- ridurre o mantenere i lavoratori in stato di soggezione continuativa;
- sottoporre i lavoratori a condizioni di sfruttamento, ad esempio esponendoli a situazioni di grave pericolo, in considerazione della prestazione da svolgere e del contesto lavorativo.

È fatto, inoltre, divieto di assegnare incarichi di fornitura o di prestazione di servizi a terzi nei casi in cui si abbia notizia, o anche solo il fondato sospetto, dell'utilizzo di lavoro straniero irregolare da parte del fornitore o del mancato rispetto delle norme a tutela del lavoratore e in materia di immigrazione.

14.3.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione degli acquisti di beni e servizi

- Qualificazione dei fornitori e previsione dell'Albo Fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Definizione delle tipologie di beni e/o importi per i quali si possa procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti ad identificare eventuali condizioni di incompatibilità e conflitto di interessi.



- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello 231 e del Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- Per i contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obblighino a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

In particolare, l'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
 - applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;
 - assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;
 - non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte delle Funzioni preposte che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.
- Verifica da parte delle Funzioni competenti in materia di anticorruzione, sulle precedenti esperienze professionali indicate dal candidato e sono richieste informazioni riguardanti, ove possibile, eventuali precedenti penali, procedimenti penali in corso; L'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Evidenza dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.

14.3.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla



presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

14.4. Reati transnazionali

14.4.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Partecipazione a gare e trattative
- Fornitura dei servizi nel settore pubblico e privato
- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni
- Rapporti infragruppo
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione degli adempimenti fiscali/tributari e contributivi
- Gestione della Tesoreria
- Amministrazione, finanza e controllo

14.4.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie di cui alla L. n. 146/2006 (Reati transnazionali) del D.Lgs. 231/2001, rilevanti per la Società.

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter, 5 D.Lgs. 286/98)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 *bis* c.p.)
- Favoreggiamento personale (art. 378 c.p.)

14.4.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati transnazionali



È fatto divieto a tutti i Destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di Reati transnazionali;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti, i quali, sebbene risultino tali da non costituire di per sé reato, possano potenzialmente diventarlo.

È, inoltre, necessario:

- che tutte le attività e le operazioni svolte per conto della Società siano improntate al massimo rispetto delle leggi vigenti, nonché dei principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- che sia rispettato il principio di separazione di ruoli e responsabilità nelle fasi dei processi;
- che sia assicurata la massima rispondenza tra i comportamenti effettivi e quelli richiesti dalle procedure interne, prestando una particolare attenzione per ciò che concerne lo svolgimento delle attività “sensibili” nell’aree “a rischio reato”.

14.4.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Fornitura dei servizi nel settore pubblico e privato

- Identificazione dei soggetti responsabili della predisposizione dell’offerta.
- Definizione delle attività svolte dalla Funzione incaricata nella fase di predisposizione dell’offerta.
- Identificazione dei soggetti autorizzati ad intrattenere rapporti con i clienti.
- Definizione delle attività svolte dalle Funzioni incaricate relative alla negoziazione dei contratti.
- Condivisione della documentazione predisposta dalle Funzioni competenti nella fase di formulazione dell’offerta.
- Verifica della documentazione di offerta (tecnica e commerciale) da inviare al cliente da parte delle Funzioni competenti.
- Definizione delle modalità di approvazione del contratto di vendita.
- Identificazione dei ruoli aziendali responsabili dell’approvazione del contratto di vendita.
- Definizione delle attività svolte dalla Funzione incaricata ai fini dell’elaborazione della richiesta di modifica contrattuale.
- Definizione delle modalità di approvazione delle richieste di modifica contrattuale.
- Definizione della documentazione necessaria a supporto della richiesta di modifica contrattuale.
- Definizione di contratti standard in coordinamento con le Funzioni competenti, volti a garantire il rispetto della normativa vigente.
- Archiviazione della documentazione prodotta nel corso dell’attività di gestione dell’offerta.
- Verifica circa la raccolta delle informazioni economico/professionali necessarie al fine di controllare il possesso dei requisiti di attendibilità e solidità della controparte.
- Esistenza di un’anagrafica clienti.
- Verifica della correttezza degli ordini di vendita inseriti a sistema.
- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici



della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.

Gestione degli acquisti di beni e servizi

- Qualificazione dei fornitori e previsione dell'Albo Fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Definizione delle tipologie di beni e/o importi per i quali si possa procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti ad identificare eventuali condizioni di incompatibilità e conflitto di interessi.
- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello 231 e del Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- Per i contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obblighino a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

In particolare, l'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
 - applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;
 - assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;
 - non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte delle Funzioni preposte che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel



rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.

- Verifica da parte delle Funzioni competenti in materia di anticorruzione, sulle precedenti esperienze professionali indicate dal candidato e sono richieste informazioni riguardanti, ove possibile, eventuali precedenti penali, procedimenti penali in corso; L'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Evidenza dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.
- Divieto di impiegare lavoratori stranieri privi di permesso di soggiorno o con un permesso revocato o scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo.

14.4.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

14.5. Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Le attività aziendali da prendere in considerazione ai fini della prevenzione dei reati di cui all'art. 25-*octies* del D. Lgs. 231/2001 possono essere suddivise in due macrocategorie:

- attività con soggetti terzi, intendendosi per tali le attività relative ai rapporti instaurati tra Reply SpA e soggetti terzi;
- attività infragruppo, poste in essere nell'ambito dei rapporti intercorrenti fra società appartenenti allo stesso gruppo.

Reply SpA ha implementato un sistema procedurale in materia di attività a rischio di riciclaggio che garantisce il rispetto dei seguenti obiettivi di controllo ex D. Lgs. 231/2001 costituito dalle seguenti attività:

- verifica dell'attendibilità commerciale e professionale dei fornitori, dei clienti e partner tramite, ad esempio, acquisizione di informazioni commerciali sulla azienda, sui soci e sugli amministratori avvalendosi di società specializzate;
- verifica della regolarità dei pagamenti;
- definizione di controlli formali e sostanziali dei flussi finanziari aziendali;
- monitoraggio sulle verifiche della Tesoreria (in merito a: rispetto delle soglie per i pagamenti per contanti, eventuale utilizzo di libretti o altri strumenti anonimi per la gestione della liquidità, ecc.).

14.5.1. Le "Aree Sensibili" ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.



- **Gestione della Tesoreria**
 - Gestione degli incassi e dei pagamenti
 - Gestione dei conti correnti
 - Utilizzo e gestione delle carte di credito
 - Gestione della piccola cassa
- **Rapporti infragruppo**
 - Gestione dei rapporti fra le Società del Gruppo

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Partecipazione a gare e trattative
- Fornitura dei servizi nel settore pubblico e privato
- Gestione del personale (dipendenti e collaboratori)
- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni
- Gestione del contenzioso
- Gestione degli adempimenti fiscali/tributari e contributivi
- Amministrazione, finanza e controllo
- Gestione degli adempimenti societari

14.5.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio richiamate dal D.Lgs. 231/2001 all'art. 25-*octies*, rilevanti per la Società.

- 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.)

14.5.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

I Destinatari del Modello:

- si astengono dal porre in essere o in qualsiasi modo contribuire alla realizzazione delle fattispecie di cui all'art. 25-*octies* del D.Lgs. 231/2001 ovvero alla violazione dei principi del presente Modello;
- assicurano il regolare funzionamento di Reply SpA e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge;
- forniscono all'Organismo di Vigilanza, e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti operativi necessari al fine di esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

Ai Destinatari del Modello è fatto divieto di:

- instaurare rapporti con consulenti, fornitori, intermediari o partner commerciali qualora tali soggetti:
 - esercitino la propria attività professionale o imprenditoriale attraverso strutture o enti "di comodo", privi di una effettiva struttura operativa (ad es. senza alcun



- dipendente o sede fisica determinata, etc.);
- richiedano pagamenti, rimborsi, omaggi o altre utilità destinati ad essere rigirati al cliente o a terzi tramite fatture false o operazioni simulate (es. commissioni per operazioni inesistenti, etc.);
- richiedano o abbiano richiesto che la propria identità rimanga nascosta.
- Procedere all'erogazione di finanziamenti/donazioni/sponsorizzazioni a favore di soggetti terzi e in particolare a favore della Pubblica Amministrazione qualora vi sia il ragionevole sospetto che gli importi erogati siano in realtà utilizzati per finalità diverse da quelle espressamente dichiarate;
- effettuare pagamenti in favore di soggetti diversi dalle controparti contrattuali o in un paese terzo diverso da quello delle parti o di esecuzione del contratto, salvo adeguata motivazione risultante per iscritto.

I principi di comportamento di seguito riportati, comuni a tutte le funzioni aziendali, dovranno essere applicati e rispettati dalle funzioni di volta in volta interessate dal singolo adempimento.

Gestione dei conti correnti bancari

I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei flussi monetari e dei pagamenti devono:

- informare immediatamente il Chief Financial Officer, il Direttore Amministrativo e l'Organismo di Vigilanza, quando ritengano di aver individuato somme di denaro di provenienza illecita;
- non effettuare pagamenti non debitamente autorizzati a imprese/professionisti/terzi in genere non chiaramente identificabili;
- evitare di aprire conti correnti bancari se non ove muniti dei relativi poteri.

Gestione dei pagamenti

I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei flussi monetari e dei pagamenti devono:

- operare nel rispetto delle disposizioni aziendali, e più precisamente non effettuare pagamenti non autorizzati, non documentati o a persone non identificabili;
- evitare o ridurre al minimo pagamenti in contanti, comunque non superiori ai limiti di legge in vigore.

È fatto divieto ai Destinatari di:

- emettere assegni bancari e postali per importi pari o superiori ai limiti di legge che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare pagamenti non adeguatamente documentati e autorizzati;
- effettuare pagamenti a fornitori in contanti;
- effettuare pagamenti per cassa eccetto per limitate tipologie di acquisto (beni di uso comune, ad esempio cancelleria) e comunque per importi non superiori ai limiti di legge applicabili;
- promettere o versare somme di denaro, anche attraverso soggetti terzi, a esponenti della Pubblica Amministrazione a titolo personale, con la finalità di promuovere o favorire interessi di Reply SpA o del Gruppo, anche a seguito di illecite pressioni;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi che operino per conto di Reply SpA o del Gruppo, che non trovino adeguata giustificazione in relazione al tipo di incarico svolto. In merito, si veda anche quanto esposto in relazione al reato di "Corruzione tra privati" trattato nella Parte Speciale A.



Gestione degli incassi

I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione dei flussi monetari, finanziari e degli incassi, devono:

- operare nel rispetto di leggi, normative nazionali ed internazionali vigenti, principi di lealtà, correttezza, eticità e trasparenza, ed in generale del Codice Etico;
- operare in coerenza con il sistema di deleghe e procure in vigore presso Reply SpA;
- limitare al minimo indispensabile l'utilizzo di denaro contante, privilegiando il canale bancario nell'effettuazione delle operazioni di incasso e pagamento derivanti da rapporti di acquisto o vendita di beni, servizi, consulenze;
- utilizzare la clausola di non trasferibilità per le operazioni a mezzo assegno bancario;
- consentire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte, archiviando tutta la documentazione.

È fatto divieto ai Destinatari di:

- aprire conti o libretti di risparmio in forma anonima o con intestazione fittizia e utilizzare conti aperti presso filiali in paesi esteri, ove ciò non sia giustificato dalla sottostante attività economica/commerciale;
- creare fondi a fronte di pagamenti non giustificati (in tutto o in parte);
- detenere/trasferire denaro contante (superiore ai limiti di legge in vigore) o libretti di deposito bancari o postali al portatore o titoli al portatore in euro o in valuta estera per importi, anche frazionati, complessivamente pari o superiori ai limiti di legge;
- richiedere il rilascio e l'utilizzo di moduli di assegni bancari e postali in forma libera, in luogo di quelli con clausola di non trasferibilità;
- accettare pagamenti frazionati se non supportati da accordi contrattuali in tal senso (quali anticipo e saldo alla consegna e pagamenti rateizzati);
- ricevere incassi, trasferimenti di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in euro o in valuta estera, quando il valore dell'operazione, anche frazionata, sia complessivamente pari o superiore ai limiti di legge.

Contanti

Non può essere accettato denaro contante per importi superiori ai limiti di legge di volta in volta in vigore. Nel caso sia accettato è necessario identificare il soggetto persona fisica che effettua l'operazione (riportando i dati del documento d'identità) e se l'operazione è ripetuta deve essere inoltrata segnalazione alla Funzione di Amministrazione e all'Organismo di Vigilanza.

Sponsorizzazioni e liberalità

La policy Omaggi, spese di rappresentanza, sponsorizzazioni e erogazioni liberali regola definisce le regole comportamentali da osservare in materia, prevedendo l'autorizzazione del Top Management di Gruppo.

I Destinatari hanno l'esplicito divieto di:

- negoziare, conseguire il possesso o nascondere denaro o beni di provenienza non chiaramente esplicita o illecita;
- sostituire, trasferire denaro o beni o compiere altre operazioni per ostacolare l'identificazione della loro provenienza delittuosa;
- impiegare, utilizzare e/o investire in qualsiasi modo e forma, in attività economiche e finanziarie denaro o beni di provenienza non chiaramente esplicita o illecita;



- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di denaro o altra utilità.

14.5.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione della Tesoreria

- Definizione dei ruoli aziendali e delle modalità operative per la gestione degli incassi.
- Attività di profilazione delle utenze, che consente l'accesso al sistema di gestione degli incassi e dei crediti alle sole risorse autorizzate.
- Monitoraggio degli incassi accreditati dagli istituti bancari.
- Monitoraggio dei crediti scaduti/in scadenza.
- Esecuzione di verifiche circa:
 - o la coerenza dei dati presenti nella fattura attiva e l'incasso;
 - o gli accantonamenti/utilizzi del fondo svalutazione crediti.
- Riconciliazione periodica, fisico-contabile, dei saldi banca/cassa.
- Divieto di ricevere pagamenti su conti cifrati.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione degli incassi e del recupero crediti.
- Attività di profilazione delle utenze che consente l'accesso al sistema di gestione dei pagamenti alle sole risorse autorizzate.
- Definizione di limiti all'autonomo impiego delle risorse finanziarie, anche attraverso la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative.
- Riconciliazione periodica, fisico-contabile, dei saldi banca/cassa.
- Monitoraggio dei pagamenti addebitati dagli istituti bancari.
- Esecuzione di verifiche circa la coerenza dei dati presenti:
 - o nella fattura passiva e nell'ordine di acquisto a sistema/contratto;
 - o nella fattura passiva e la bolla di entrata merci;
 - o la coerenza delle informazioni contenute nelle fatture passive e nelle disposizioni/lettere di pagamento.
- Ruoli aziendali responsabili e formale definizione delle modalità operative per la predisposizione dello scadenziario di pagamento delle fatture.
- Formale approvazione, nel rispetto delle deleghe e delle procure in essere, delle disposizioni/lettere di pagamento in relazione ai livelli autorizzativi definiti.
- Ruoli aziendali responsabili e formale definizione delle modalità operative per la predisposizione e l'autorizzazione delle disposizioni di pagamento.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione dei pagamenti.
- Predisposizione di pagamenti nei confronti dei soli soggetti presenti in anagrafica.
- I pagamenti tramite bonifici sono sempre processati dalla Funzione Tesoreria mediante appositi sistemi di autenticazione e gli importi oggetto di bonifico sono opportunamente autorizzati, mediante sistemi informativi e condivisi mediante flussi di comunicazione protetti.
- Attività di profilazione delle utenze, che consenta l'accesso al sistema di gestione delle anagrafiche dei conti correnti alle sole risorse autorizzate.
- Definizione dei ruoli aziendali responsabili e formale definizione delle modalità operative per l'apertura/chiusura dei conti correnti.



- Esecuzione di verifiche circa i termini, le clausole e le condizioni contrattuali inserite nel contratto di apertura di un conto corrente.
- Verifica che tutti i conti correnti siano detenuti in nome della Società e presso istituti bancari precedentemente autorizzati.
- Riconciliazione periodica, fisico-contabile, dei saldi bancari.
- Archiviazione della documentazione prodotta nel corso dell'attività di apertura, chiusura o modifica di un conto corrente.
- Definizione dei ruoli aziendali responsabili e definizione delle modalità operative per la predisposizione del report di riconciliazione e per la gestione di eventuali anomalie emerse.
- Policy per l'utilizzo delle carte di credito.
- Effettuazione di controlli sugli estratti conto per verificare il corretto utilizzo di tali carte nel rispetto delle regole vigenti.
- Formale identificazione del responsabile/i della Tesoreria.
- Esecuzione di verifiche sul corretto utilizzo e corretta gestione della cassa contante.

Rapporti infragruppo

- Identificazione di ruoli aziendali responsabili della stesura/verifica dei contratti infragruppo.
- Esecuzione di verifiche formali e sostanziali sui flussi finanziari aziendali, con riferimento a pagamenti/operazioni infragruppo.
- Esistenza di appositi template per la predisposizione dei contratti per l'identificazione dei servizi da erogare.
- Formale definizione degli obblighi e delle responsabilità della società mandante e della società mandataria.
- Monitoraggio e aggiornamento dei corrispettivi previsti nei contratti.
- Operazioni di acquisizione/cessione di asset tra Società del Gruppo e con controparti esterne sono condotte nel rispetto delle normative fiscali vigenti.

14.5.5. Compiti dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati e gli illeciti di riciclaggio, ricettazione e impiego di denaro, beni o utilità di provenienza illecita sono i seguenti:

- emanare o proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- verificare se siano fissati/determinati, da parte delle Funzioni competenti, i requisiti minimi in possesso dei soggetti offerenti per poter intraprendere rapporti commerciali con la Società;
- verificare l'implementazione, da parte delle Funzioni competenti, di una corretta procedura per la verifica della correttezza dei pagamenti con riferimento alla piena coincidenza tra Destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nella transazione;
- verificare la sussistenza di controlli formali e sostanziali dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo;
- verificare l'adozione, da parte delle Funzioni competenti, di corrette modalità di valutazione circa l'analisi della congruità economica degli investimenti effettuati;



- verificare l'adozione, da parte delle Funzioni competenti, di programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.



15. Parte Speciale "F": Reati di abuso di mercato

La nozione di informazione privilegiata rappresenta il fulcro attorno al quale ruota l'intera disciplina dell'*insider trading*.

Secondo l'art. 180 TUF, per "informazione privilegiata" si intende quanto contemplato dall'art. 7, comma 1, lettere da a) a d), del Regolamento (UE) n. 596/2014 e ovvero una informazione:

- "avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati";
- "in relazione agli strumenti derivati su merci, un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più di tali strumenti derivati o concernente direttamente il contratto a pronti su merci collegato, e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti derivati o sui contratti a pronti su merci collegati e qualora si tratti di un'informazione che si possa ragionevolmente attendere sia comunicata o che debba essere obbligatoriamente comunicata conformemente alle disposizioni legislative o regolamentari dell'Unione o nazionali, alle regole di mercato, ai contratti, alle prassi o alle consuetudini, convenzionali sui pertinenti mercati degli strumenti derivati su merci o a pronti";
- "in relazione alle quote di emissioni o ai prodotti oggetto d'asta correlati, un'informazione avente un carattere preciso, che non è stata resa pubblica, concernente, direttamente o indirettamente, uno o più di tali strumenti e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti o sui prezzi di strumenti finanziari derivati collegati";
- "nel caso di persone incaricate dell'esecuzione di ordini relativi a strumenti finanziari, s'intende anche l'informazione trasmessa da un cliente e connessa agli ordini pendenti in strumenti finanziari del cliente, avente un carattere preciso e concernente, direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti finanziari, sul prezzo dei contratti a pronti su merci collegati o sul prezzo di strumenti finanziari derivati collegati".

In aggiunta a quanto precede, i paragrafi 2, 3 e 4 dell'art. 7 del summenzionato Regolamento (UE), stabiliscono quanto segue:

- si considera che un'informazione ha un carattere preciso se essa fa riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se tale informazione è sufficientemente specifica da permettere di trarre conclusioni sul possibile effetto di detto complesso di circostanze o di detto evento sui prezzi degli strumenti finanziari o del relativo strumento finanziario derivato, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base delle quote di emissioni. A tal riguardo, nel caso di un processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, tale futura circostanza o futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della circostanza o dell'evento futuri, possono essere considerati come informazioni aventi carattere preciso;



- una tappa intermedia in un processo prolungato è considerata un'informazione privilegiata se, di per sé, risponde ai criteri fissati nel presente articolo riguardo alle informazioni privilegiate;
- informazione che, se comunicata al pubblico, avrebbe probabilmente un effetto significativo sui prezzi degli strumenti finanziari, degli strumenti finanziari derivati, dei contratti a pronti su merci collegati o dei prodotti oggetto d'asta sulla base di quote di emissioni, s'intende un'informazione che un investitore ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni di investimento.

Relativamente alla nozione di strumenti finanziari, si segnala che, ai sensi dell'art. 180 TUF, per essi si intendono gli strumenti finanziari:

- 1) di cui all'articolo 1, comma 2, ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
- 2) di cui all'articolo 1, comma 2, ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un sistema multilaterale di negoziazione italiano o di altro Paese dell'Unione europea;
- 2-bis) negoziati su un sistema organizzato di negoziazione italiano o di altro Paese dell'Unione europea;
- 2-ter) non contemplati dai precedenti numeri, il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario ivi menzionato, ovvero ha un effetto su tale prezzo o valore, compresi, non in via esclusiva, i *credit default swap* e i contratti differenziali.

A tal riguardo, si evidenzia che gli strumenti di cui all'art. 1, comma 2, del TUF sono i seguenti:

- 1) valori mobiliari;
- 2) strumenti del mercato monetario;
- 3) quote di un organismo di investimento collettivo;
- 4) contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», accordi per scambi futuri di tassi di interesse e altri contratti derivati connessi a valori mobiliari, valute, tassi di interesse o rendimenti, quote di emissione o altri strumenti finanziari derivati, indici finanziari o misure finanziarie che possono essere regolati con consegna fisica del sottostante o attraverso il pagamento di differenziali in contanti;
- 5) contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», contratti a termine («*forward*»), e altri contratti su strumenti derivati connessi a merci quando l'esecuzione deve avvenire attraverso il pagamento di differenziali in contanti o può avvenire in contanti a discrezione di una delle parti, con esclusione dei casi in cui tale facoltà consegue a inadempimento o ad altro evento che determina la risoluzione del contratto;
- 6) contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*» ed altri contratti su strumenti derivati connessi a merci che possono essere regolati con consegna fisica purché negoziati su un mercato regolamentato, un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione, eccettuati i prodotti energetici all'ingrosso negoziati in un sistema organizzato di negoziazione che devono essere regolati con consegna fisica;
- 7) contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», contratti a termine («*forward*») e altri contratti su strumenti derivati connessi a merci che non possono essere eseguiti in modi diversi da quelli indicati al numero 6, che non hanno scopi commerciali, e aventi le caratteristiche di altri strumenti finanziari derivati;



- 8) strumenti finanziari derivati per il trasferimento del rischio di credito;
- 9) contratti finanziari differenziali;
- 10) contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», contratti a termine sui tassi d'interesse e altri contratti su strumenti derivati connessi a variabili climatiche, tariffe di trasporto, tassi di inflazione o altre statistiche economiche ufficiali, quando l'esecuzione avviene attraverso il pagamento di differenziali in contanti o può avvenire in tal modo a discrezione di una delle parti, con esclusione dei casi in cui tale facoltà consegue a inadempimento o ad altro evento che determina la risoluzione del contratto, nonché altri contratti su strumenti derivati connessi a beni, diritti, obblighi, indici e misure, non altrimenti indicati nella presente sezione, aventi le caratteristiche di altri strumenti finanziari derivati, considerando, tra l'altro, se sono negoziati su un mercato regolamentato, un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione;
- 11) quote di emissioni che consistono di qualsiasi unità riconosciuta conforme ai requisiti della direttiva 2003/87/CE (sistema per lo scambio di emissioni).

15.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione delle Informazioni Privilegiate e price sensitive**
 - Gestione del Registro dei soggetti rilevanti e dell'archivio comunicazioni al mercato
 - Gestione delle informazioni "price sensitive" atta a provocare una sensibile alterazione del prezzo degli strumenti finanziari emessi
 - Utilizzo delle informazioni "price sensitive" nello svolgimento dell'attività aziendale

15.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati di abuso di mercato, richiamate dal D.Lgs. 231/2001 all'art. 25-sexies del D.Lgs. 231/2001, e altre fattispecie in materia di abuso di mercato richiamate dall'art. 187-*quinquies* TUF, rilevanti per la Società.

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998)
- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE n. 596/2014)
- Divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014)
- Manipolazione del mercato (ex artt. 185 e 187-*ter* del T.U.F.)

15.3. I Principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati di abuso di mercato

Obiettivo della presente Parte Speciale è che i Destinatari del Modello, nella misura in cui gli stessi possano essere coinvolti nello svolgimento di attività nelle aree a rischio, e in considerazione della diversa posizione e dei diversi obblighi che ciascuno assume nei confronti del Gruppo, si attengano a regole di condotta aventi il fine di prevenire ed impedire il verificarsi degli illeciti in materia di abusi di mercato.

In particolare, la presente Parte Speciale ha la funzione di:



- indicare i principi di comportamento cui i Destinatari, in relazione al tipo di rapporto in essere con il Gruppo, sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti operativi necessari al fine di esercitare le attività di controllo, monitoraggio e verifica allo stesso demandate.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli esponenti aziendali sono tenuti in generale a conoscere e rispettare tutte le regole ed i principi contenuti nei seguenti documenti:

- Codice Etico;
- disciplina dell'internal dealing;
- Regolamento interno per la gestione ed il trattamento delle informazioni riservate e per la comunicazione all'esterno di documenti e di informazioni (approvato con delibera del Consiglio di Amministrazione di Reply SpA del 2 agosto 2018 e 14 marzo 2019);
- procedura interna in materia di "Tenuta ed aggiornamento del Registro delle persone che hanno accesso alle informazioni privilegiate" (approvata con delibera del Consiglio di Amministrazione di Reply SpA del 31 marzo 2006, come successivamente aggiornata).

Relativamente alle operazioni di acquisto di azioni proprie e alle attività di stabilizzazione le stesse dovranno essere effettuate nel rispetto delle normative di legge ed in conformità delle prassi di mercato ammesse dalla Consob.

Reply SpA, al fine di prevenire la commissione di abusi di mercato, predispone programmi di formazione-informazione periodica dei Destinatari della presente Parte Speciale sui reati e gli illeciti amministrativi di abuso di mercato e sulle relative procedure aziendali in essere.

Reply SpA, inoltre, in conformità alle prescrizioni di legge, ha provveduto ad istituire un Registro unico di Gruppo nel quale sono iscritte tutte le persone (fisiche o giuridiche) che hanno accesso in modo regolare od occasionale ad informazioni privilegiate concernenti il Gruppo Reply.

Le procedure aziendali che possono risultare rilevanti ai fini della prevenzione dei reati e degli illeciti di cui alla presente Parte Speciale possono essere aggiornate dai competenti organi aziendali, anche su proposta o segnalazione dell'Organismo di Vigilanza.

Sono ammesse, sotto la responsabilità di chi le attua, eventuali deroghe ai principi comportamentali qui descritti, nei soli casi di particolare urgenza nella formazione o nell'attuazione della decisione o in caso di impossibilità temporanea del rispetto delle procedure. In questi casi, è inviata immediata informazione anche all'OdV ed è sempre richiesta la successiva ratifica da parte del soggetto/organo competente in merito.

15.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione delle Informazioni Privilegiate e price sensitive



- Definizione di compiti e ruoli dei soggetti responsabili della gestione delle Informazioni Privilegiate.
- Esistenza di norme che regolano la diffusione delle medesime e le modalità che i Responsabili sono tenuti ad utilizzare per il loro trattamento e la loro pubblicazione.
- Definizione di criteri idonei a qualificare le informazioni come privilegiate o destinate a divenire tali.
- Definizione di misure per proteggere, conservare e aggiornare le Informazioni ed evitare la comunicazione impropria e non autorizzata all'interno o all'esterno del Gruppo delle stesse.
- Definizione delle persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, hanno accesso alle Informazioni Privilegiate o destinate a divenire privilegiate.
- Esistenza di un registro delle persone che, in ragione dell'attività lavorativa o professionale ovvero in ragione delle funzioni svolte, gestiscono e hanno accesso alle specifiche Informazioni Privilegiate o destinate a divenire tali. In particolare, sono stabiliti i criteri di aggiornamento del registro e i vincoli all'accesso dello stesso.
- Monitoraggio periodico volto a verificare eventuali aggiornamenti normativi in materia di acquisto di titoli e strumenti finanziari.
- Verifiche formalizzate, con il supporto delle Funzioni competenti, atte ad accertare il rispetto dei vincoli normativi in materia di acquisto di titoli e strumenti finanziari.
- Verifica formalizzata dei rischi di particolare rilevanza in riferimento ad operazioni di acquisto di titoli e strumenti finanziari.
- Definizione di criteri formalizzati che presiedono alla corretta formazione del prezzo degli strumenti finanziari.
- Formale negoziazione e registrazione delle operazioni di compravendita titoli.

15.5. Compiti dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati e gli illeciti di abuso di mercato sono i seguenti:

- emanare o proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- con riferimento al trattamento delle Informazioni Privilegiate, l'Organismo di Vigilanza provvede all'espletamento dei seguenti compiti:
 - monitoraggio sull'efficacia delle procedure interne per la prevenzione degli illeciti di abuso di mercato;
 - esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in conseguenza delle segnalazioni ricevute;
 - vigilanza sull'effettiva sussistenza delle condizioni per garantire alla società di revisione una concreta autonomia nelle sue funzioni di controllo delle attività aziendali.
- con riferimento alle altre attività a rischio l'Organismo di Vigilanza provvede all'espletamento dei seguenti compiti:
 - svolgimento delle verifiche periodiche sul rispetto delle procedure interne;
 - svolgimento delle verifiche periodiche sull'effettuazione delle comunicazioni alle Autorità pubbliche di Vigilanza;
 - valutazione periodica dell'efficacia delle procedure volte a prevenire la commissione dei reati;



- esame delle eventuali segnalazioni di presunte violazioni del Modello ed effettuazione degli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.



16. Parte Speciale “G”: Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro

L’art. 9 della Legge n. 123/2007 ha introdotto nel D. Lgs. n. 231/2001 l’art. 25-*septies*, che estende la responsabilità amministrativa delle società ai reati di omicidio colposo e lesioni personali colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro.

Nelle ipotesi di commissione dei reati contemplati dall’art. 25-*septies*, la responsabilità prevista dal D. Lgs. n. 231/2001 è configurabile solo se dal fatto illecito ne sia derivato un vantaggio per la società, che, nel caso di specie, potrebbe essere rinvenuto in un risparmio di costi o di tempi.

I presupposti per definire il fatto colposo sono:

- le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell’inosservanza di norme antinfortunistiche;
- soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare le norme di prevenzione e protezione. Tale soggetto può quindi individuarsi, ai sensi del D. Lgs. n. 81/2008, nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori;
- nella previsione del codice penale, le fattispecie delittuose contemplate dagli artt. 589 e 590 sono caratterizzate dall’aggravante della negligente inosservanza delle norme antinfortunistiche. L’elemento soggettivo, dunque, consiste nella c.d. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte a impedire gli eventi dannosi previsti dalla norma incriminatrice;
- il concetto di colpa specifica rimanda all’art. 43 c.p., nella parte in cui si prevede che il delitto è colposo quando l’evento, anche se preveduto ma in ogni caso non voluto dall’agente, si verifica a causa dell’inosservanza di norme di leggi, regolamenti, ordini o discipline;
- le norme antinfortunistiche di cui agli artt. 589, co. 2, e 590, co. 3, c.p., ricomprendono anche l’art. 2087 c.c., che impone al datore di lavoro di adottare tutte quelle misure che, secondo la particolarità del lavoro, l’esperienza e la tecnica, sono necessarie a tutelare l’integrità fisica dei lavoratori.

Il Gruppo Reply è assoggettato ai principi normativi previsti dal D. Lgs. 81/08 in materia di sicurezza sul posto di lavoro e, in merito, ha provveduto a definire il seguente organigramma:

- il datore di lavoro che ha il potere di spesa;
- il responsabile del servizio di prevenzione e protezione (RSPP);
- l’addetto al servizio di prevenzione e protezione (ASPP);
- il preposto per la sicurezza;
- il medico del lavoro competente (medico del lavoro esterno);
- il rappresentante dei lavoratori per la sicurezza (RLS) per le società del Gruppo rispetto alle quali si ponga il relativo obbligo normativo di nomina;
- addetti primo soccorso;
- addetti emergenze in caso d’incendio.

Con riferimento alle attività che possono presentare un rischio di commissione dei reati di



cui all'art. 25 *septies* del Decreto, è necessario distinguere le attività che possono comportare un rischio per la salute e la sicurezza del lavoratore (e dalle quali, pertanto, può derivare la morte o la lesione di un lavoratore a seguito di infortunio o malattia professionale) dalle attività che possono comportare il rischio di commissione di uno dei reati qui considerati ed alle quali è specificatamente rivolto il Modello.

La valutazione delle attività che possono comportare un rischio di infortunio o malattia professionale, infatti, è oggetto del relativo Documento di Valutazione dei Rischi (“**DVR**”) adottato e periodicamente aggiornato da Reply SpA in rapporto all'evoluzione dei fattori di rischio, delle misure adottate per eliminare o ridurre i rischi individuati o ad eventuali evoluzioni della normativa in conformità al presente Modello.

Le attività sensibili in relazione al rischio di commissione dei reati in esame sono, invece, costituite dalle attività necessarie ad assicurare un'efficiente gestione della sicurezza ed il corretto adempimento degli obblighi giuridici previsti dalla vigente normativa e principalmente relative ai seguenti profili:

- valutazione dei rischi;
- gestione emergenze;
- sorveglianza sanitaria;
- formazione e addestramento.

Esclusione della responsabilità amministrativa della Società

Il D.Lgs. 81/2008, all'art. 30, ha indicato le caratteristiche e i requisiti che deve possedere un Modello di Organizzazione e di Gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto Legislativo 8 giugno 2001, n. 231.

Secondo l'art. 30 del D.Lgs. 81/2008, il Modello di Organizzazione e di Gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche ex D.Lgs. 231/2001 deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi a:

- rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- attività di sorveglianza sanitaria;
- attività di informazione e formazione dei lavoratori;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documentazioni e certificazioni obbligatorie di legge;
- verifiche periodiche dell'applicazione e dell'efficacia delle procedure adottate.

Inoltre, il Modello Organizzativo e Gestionale deve prevedere:

- idonei sistemi di registrazione dell'avvenuta effettuazione delle suddette attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nello stesso;
- un autonomo sistema di supervisione e controllo sullo svolgimento delle suddette attività.

Infine, il comma 5 del medesimo art. 30 dispone che: “In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al



British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui ai commi precedenti per le parti corrispondenti”.

Si specifica che Reply ha ottenuto la certificazione ISO:45001 (Requisiti per il Sistema di Salute e Sicurezza sul lavoro), che ha sostituito il British Standard OHSAS 18001:2007.

16.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione della salute e sicurezza**

16.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro, richiamate dal D.Lgs. 231/2001 all’art. 25-septies rilevanti per la Società.

- Omicidio colposo (art. 589 c.p.)
- Lesioni personali colpose (art. 590 c.p.)

16.3. Principi generali di comportamento da tenere nell’ambito delle attività a rischio relative ai Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro

È fatto obbligo per tutti i Destinatari del Modello di rispettare ogni cautela possibile (anche non espressamente nominata) volta ad evitare la causazione di infortuni sul luogo di lavoro e quindi di danni al personale (anche di terze parti operanti in azienda). Reply SpA ha implementato gli opportuni standard di sicurezza in relazione alle attività dalla stessa svolte.

Secondo la migliore dottrina e la più recente giurisprudenza l’obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza (forme di protezione oggettiva) ma deve intendersi anche in maniera dinamica implicando l’obbligo di informare e formare i lavoratori sui rischi propri dell’attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

Il datore di lavoro che abbia, secondo i criteri sopra esposti, adempiuto agli obblighi in materia di salute e sicurezza sul luogo di lavoro (sia generali ex art. 2087 c.c., sia speciali ex D. Lgs. n. 81/2008), è responsabile del solo evento di danno che si sia verificato in occasione dell’attività di lavoro e abbia un nesso di derivazione effettiva con lo svolgimento dell’attività lavorativa.

In tale contesto, il Modello non intende sostituirsi alle prerogative e responsabilità di legge disciplinate in capo ai soggetti individuati dal D. Lgs. 81/2008 e dalla normativa ulteriormente applicabile nei casi di specie. Costituisce, invece, un presidio ulteriore di controllo e verifica dell’esistenza, efficacia ed adeguatezza della struttura e organizzazione posta in essere in ossequio alla normativa speciale vigente in materia di antinfortunistica e tutela della sicurezza e della salute nei luoghi di lavoro.



In particolare, costituiscono presupposto e parte integrante dei protocolli di prevenzione i principi di comportamento individuati nel Codice Etico, che qui s'intende integralmente richiamato, la documentazione relativa alla tutela ed alla sicurezza dei luoghi di lavoro (ivi compresi il DVR nonché le procedure di gestione delle emergenze) attraverso cui si individuano le situazioni ove ragionevolmente è possibile si manifestino degli eventi lesivi riconducibili all'attività lavorativa in Reply SpA (e nel Gruppo).

Presupposti essenziali del Modello al fine della prevenzione degli infortuni sui luoghi di lavoro sono il rispetto di alcuni principi e la tenuta di determinati comportamenti da parte dei dipendenti di Reply SpA, nonché dagli eventuali soggetti esterni che si trovino legittimamente presso i locali della stessa. In particolare, ciascun dipendente e più in generale ogni Destinatario del Modello che si trovi legittimamente presso Reply SpA ovvero la cui attività ricada sotto la responsabilità della stessa dovrà:

- conformemente alla propria formazione ed esperienza, nonché alle istruzioni e ai mezzi forniti ovvero predisposti dal datore di lavoro, non adottare comportamenti imprudenti quanto alla salvaguardia della propria salute e della propria sicurezza;
- rispettare la normativa e le procedure aziendali interne al fine della protezione collettiva ed individuale, esercitando in particolare ogni opportuno controllo ed attività idonei a salvaguardare la salute e la sicurezza dei collaboratori esterni e/o di persone estranee, eventualmente presenti sul luogo di lavoro;
- utilizzare in modo appropriato i dispositivi di protezione ove messi a disposizione;
- segnalare immediatamente alle competenti funzioni le anomalie dei mezzi e dei dispositivi di cui ai punti precedenti, nonché le altre eventuali condizioni di pericolo di cui viene a conoscenza;
- intervenire direttamente a fronte di un pericolo rilevato e nei soli casi di urgenza, compatibilmente con le proprie competenze e possibilità;
- sottoporsi ai controlli sanitari previsti;
- partecipare agli interventi formativi;
- contribuire all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

A questi fini è fatto divieto di:

- rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- compiere di propria iniziativa operazioni o manovre che non siano di propria competenza ovvero che possano compromettere la sicurezza propria o di altri dipendenti o terzi;
- accedere ad aree di lavoro alle quali non si è autorizzati;
- in generale, porre in essere, collaborare o dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato previste dalla presente Parte Speciale.

I Destinatari che venissero a conoscenza di eventuali omissioni, inefficienze o trascuratezze nella gestione della sicurezza sul lavoro sono tenuti a riferirne tempestivamente al proprio responsabile e all'Organismo di Vigilanza.

Reply si impegna a rispettare e ad operare nel rispetto delle leggi di tempo in tempo vigenti.

È, infine, necessario che la Società preveda la conduzione di una periodica attività di monitoraggio sulla funzionalità del sistema preventivo adottato. Detto monitoraggio



dovrebbe consentire l'adozione delle decisioni più opportune ed essere condotto da personale competente che assicuri l'obiettività e l'imparzialità, nonché l'indipendenza dal settore di lavoro sottoposto a verifica ispettiva.

16.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione della salute e sicurezza

- Le parti coinvolte nella gestione della sicurezza e salute sul luogo di lavoro si attengono a quanto disciplinato dal Testo Unico sulla Sicurezza, la normativa vigente in materia di salute e sicurezza sul lavoro e alle regole di condotta conformi a quanto prescritto di seguito. In particolare: il Datore di Lavoro e tutti i soggetti aventi compiti e responsabilità nella gestione degli adempimenti previsti dalle norme sulla tutela della salute e della sicurezza sul lavoro, quali, a titolo esemplificativo, Responsabile del Servizio di Prevenzione e Protezione (RSPP), Rappresentante dei Lavoratori per la Sicurezza (RLS), Medico Competente (MC), addetti primo soccorso, addetti emergenze in caso d'incendio, si impegnano a rispettare, ognuno per la propria competenza: gli obblighi previsti dalla vigente normativa, gli standard tecnico-strutturali di legge relativi ad attrezzature, luoghi di lavoro, agenti chimici, fisici e biologici anche attraverso un processo continuo di manutenzione (ordinaria e straordinaria) degli strumenti, degli impianti, dei macchinari e, in generale, delle strutture aziendali.
- Tutti i soggetti, inoltre, operano nel rispetto delle leggi e della normativa vigente in materia di salute e sicurezza sul lavoro, ciascuno con riferimento alle proprie competenze ed attribuzioni, al fine di prevenire ed impedire il verificarsi dei reati e degli illeciti amministrativi commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
- Esistenza di disposizioni organizzative (organigramma o deleghe) per l'individuazione della figura datoriale che tengono conto della struttura organizzativa della Società e del settore di attività produttiva.
- Esistenza di disposizioni organizzative (conferimenti di incarico) relative alla designazione del Responsabile del Servizio di Prevenzione e Protezione (RSPP), degli addetti del servizio di prevenzione e protezione (ASPP), del Medico Competente e dei lavoratori incaricati di attuare le misure di emergenza, prevenzione incendi e primo soccorso.
- Esistenza di una relazione sulla Valutazione dei Rischi redatta secondo le disposizioni definite dalla normativa vigente.
- Esistenza di una procedura aziendale che individua i criteri e le modalità definite per l'affidamento delle mansioni ai lavoratori da parte del DDL.
- Esistenza di una procedura per la gestione, distribuzione ed il mantenimento in efficienza dei Dispositivi di Protezione Individuale (DPI).
- Esistenza di un piano aziendale per la gestione delle emergenze, ove richiesto dalla vigente normativa, atto a mitigare le conseguenze di una possibile emergenza.
- Esistenza di una procedura aziendale che definisce le misure necessarie per la prevenzione incendi e dettaglia gli obblighi conseguenti.
- Esistenza di un calendario che prevede riunioni periodiche delle figure previste per la verifica dell'andamento nella gestione delle tematiche riguardanti salute e sicurezza.



- Esistenza di una procedura aziendale che disciplina la consultazione e la partecipazione dei lavoratori per il tramite del loro rappresentante e la diffusione delle informazioni relative alla salute e sicurezza.
- Esistenza di una procedura aziendale che regola il processo di informazione, formazione e addestramento (ove previsto) del personale sulle tematiche di salute e sicurezza e sui rischi presenti nei luoghi di lavoro.
- Esistenza di una procedura aziendale che definisce modalità e contenuti dell'informazione fornita alle imprese appaltatrici e responsabilità per le attività di coordinamento volta all'eliminazione dei rischi di interferenza.
- Esistenza di una procedura aziendale che definisce modalità di qualifica dei fornitori sulla base requisiti tecnico-professionali degli appaltatori e della rispondenza di quanto fornito con le specifiche di acquisto in tema di tutela della salute e della sicurezza.
- Esistenza di clausole contrattuali standard riguardanti i costi della sicurezza nei contratti di somministrazione, di appalto e di subappalto.
- Esistenza di procedure aziendali che disciplinano le attività di manutenzione/ispezione degli asset aziendali garantendone integrità e adeguatezza.
- Esistenza di una procedura aziendale che indica le modalità di rilevazione, registrazione ed investigazione degli infortuni, degli incidenti e dei quasi incidenti.
- Esistenza di una procedura che definisce ruoli, responsabilità e modalità di registrazione e monitoraggio dei dati relativi a: sorveglianza sanitaria; sicurezza degli impianti; esposizione a sostanze e preparati pericolosi; ecc.
- Attività monitoraggio continuo circa le/i controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro al fine di identificare le aree a maggior rischio infortuni.
- Esistenza di una procedura che disciplini l'attività di predisposizione del Documento Unico di Valutazione dei Rischi da Interferenza (c.d. "DUVRI") nel caso in cui Reply SpA, in qualità di Committente, appalti a terzi lo svolgimento di attività – erogazione servizi o esecuzione di lavori. Il DUVRI deve elencare tutti i possibili rischi di interferenza che possano insorgere in relazione alle attività proprie di Reply e di quelle dell'Appaltatore. In particolare, in caso di affidamento dei lavori all'impresa appaltatrice o a lavoratori autonomi all'interno della propria azienda, Reply verifica l'idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi acquisendo l'iscrizione alla camera di commercio, industria e artigianato, e fornisce agli stessi soggetti dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività. Il DUVRI deve essere allegato al contratto di appalto o d'opera.
- Esistenza di una procedura che disciplini il rispetto degli obblighi in capo al Committente di cui al titolo IV del D.Lgs. 81/08 nel caso di lavori o interventi effettuati su cantieri temporanei o mobili, come definiti dall'allegato X del medesimo decreto.

16.5. Compiti dell'Organismo di Vigilanza

È innanzitutto importante sottolineare che l'estensione dell'applicazione del Decreto ai delitti colposi (come i reati in esame) non pone un problema di rapporti tra il piano della sicurezza e quello del Modello, nonché tra le attività dei soggetti responsabili dei controlli in materia di salute e sicurezza sul lavoro e l'Organismo di Vigilanza. L'autonomia di funzioni proprie di detti soggetti non consente di ravvisare una sovrapposizione dei compiti di controllo; i diversi soggetti deputati al controllo svolgono infatti i propri compiti su piani differenti.



Per quanto concerne le tematiche di tutela della salute e sicurezza sul lavoro, l'Organismo di Vigilanza si avvale di tutte le risorse attivate per la gestione dei relativi aspetti (RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC - Medico Competente, addetti primo soccorso, addetti emergenze in caso d'incendio).

All'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante e dovrà ricevere copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

L'Organismo di Vigilanza può anche intervenire a seguito di segnalazioni ricevute.



17. Parte Speciale “H”: Delitti in materia di violazione del Diritto d’Autore

17.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Fornitura dei servizi nel settore pubblico e privato**
 - Acquisizione di contratti con clienti (gestione dei rapporti commerciali per l'acquisizione di commesse)
 - Gestione delle attività progettuali nell'ambito di servizi resi a clienti (sviluppo software, gestione delle licenze di terzi, trattamento dei dati e accesso ai sistemi informativi)
- **Gestione dei sistemi informativi**
 - Maintenance dell'hardware e del software aziendale
 - Gestione delle misure di sicurezza a protezione dei sistemi informatici e/o telematici
 - Gestione del processo di assegnazione dei codici di accesso ai sistemi informatici e/o telematici
 - Gestione delle licenze software

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni

17.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti in materia di violazione del Diritto d’Autore, richiamate dal D.Lgs. 231/2001 all’art. 25-*novies*, rilevanti per la Società.

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, l. 633/1941 comma 1 lett. a) *bis*).
- Reati previsti dall’art. 171, comma 1 commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l’onore o la reputazione (art. 171, l. 633/1941 comma 3).
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-*bis*, c. 1, l. 633/1941).
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-*bis*, c. 2, l. 633/1941).
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico di opere dell'ingegno (art. 171-*ter*, L. 633/1941).
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-*septies*, L. 633/1941).



- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-*octies*, L. 633/1941).

17.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti in materia di violazione del Diritto d'Autore

Reply SpA nello svolgimento della propria attività e *mission* aziendale garantisce il costante e puntuale rispetto delle norme a tutela della proprietà industriale e intellettuale, e pertanto del software, delle banche dati elettroniche e/o telematiche, dei programmi per elaboratore e di ogni attività che possa esplicarsi tramite l'utilizzo di computer e l'accesso ad Internet. Reply SpA si è quindi dotata di apposite policy aziendali, valide per tutte le Società del Gruppo, volte alla repressione delle potenziali attività illegali connesse con la copia e l'uso dei software aziendali.

In particolare, coerentemente con i principi deontologici aziendali è fatto divieto di:

- effettuare copie non autorizzate del software aziendale;
- effettuare download/upload di software illegali (privi di regolare licenza);
- utilizzare o anche solo installare software illegali sugli elaboratori di proprietà di Reply SpA, che siano per uso individuale o che forniscano servizi ad utenti interni a Reply o esterni.

I processi di gestione dei software asset sviluppano le policy menzionate indicando le responsabilità, le attività, gli strumenti e gli output necessari. Nello specifico, essi si articolano nelle seguenti fasi:

- responsabilizzazione del personale;
- monitoraggio delle attività per verificare la conformità alle policy;
- esecuzione di eventuali azioni correttive e, se necessario, disciplinari;
- predisposizione della documentazione necessaria per attestare l'attuazione degli adempimenti agli Organismi pubblici preposti ai controlli.

17.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Fornitura dei servizi nel settore pubblico e privato

- Informativa verso i Team di progetto sui vincoli attinenti alla proprietà intellettuale del progetto in cui sono coinvolti.
- Informativa verso i dipendenti sui vincoli legali associati all'utilizzo di codici open source nei diversi tipi di licenze esistenti.
- Informativa verso i dipendenti sui rischi associati all'utilizzo di pezzi di codice ottenuti da motori di intelligenza artificiale.
- Inserimento nel sistema di *Asset Library* di tutti i progetti più sensibili al rischio di un'errata gestione dell'*Intellectual Property*.
- Controllo a campione "four eyes" che consista in una review del codice da parte del personale esperto.
- Previsione all'interno dei contratti di clausole riferite all'osservanza delle norme in materia di proprietà intellettuale nei rapporti con i Terzi contraenti.



- In caso di accessi ai sistemi informatici della PA, sono rispettate tutte le misure di sicurezza del caso affinché non vengano alterati, ad esempio, i registri informatici della PA stessa e/o i dati contenuti nella documentazione procurando in tal modo un qualsivoglia danno alla Pubblica Amministrazione.

Gestione dei sistemi informativi

- Esistenza della ICT Security Policy in materia di sicurezza dei sistemi informativi che definisce, fra l'altro:
 - o gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda;
 - o la gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
 - o modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
 - o ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica;
 - o implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;
 - o identificazione dei requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
 - o gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
 - o Confidenzialità, autenticità e integrità delle informazioni;
 - o sicurezza nel processo di sviluppo dei sistemi informativi
- Formazione specifica sul tema del Ricatto Informatico, in particolare, al fine di evitare, nell'ambito del procacciamento di affari e dei servizi svolti, situazioni di minacce di sospensione dei servizi e/o pubblicazione di dati del cliente.
- Svolgimento di riunioni periodiche con il Data Protection Officer sulle modalità di trattamento dei dati personali da parte del Titolare, anche con riguardo al profilo delle misure di sicurezza adeguate al livello di rischio adottato.

17.5. Compiti dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati e gli illeciti in materia di violazione del diritto d'autore sono i seguenti:

- emanare o proporre che vengano emanate ed aggiornate le istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle aree a rischio, come individuate nella presente Parte Speciale. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- svolgere verifiche periodiche sull'efficacia e il rispetto delle procedure e/o policy interne inerenti la tutela della proprietà intellettuale e la gestione dei sistemi informatici e altre attività volte a prevenire la commissione dei reati;
- esaminare le eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.



18. Parte Speciale “I”: Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria

La Legge 3 agosto 2009, n. 116 (recante "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale.") ha introdotto il reato presupposto di induzione a non rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis*, c.p.), inserendo l'art. 25--decies nel D. Lgs. 231/2001.

18.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione del contenzioso**
 - Gestione del contenzioso giudiziale, stragiudiziale e procedimenti arbitrali

18.2. Le fattispecie di reato applicabili

Di seguito si riporta la fattispecie di Induzione a non rendere Dichiarazioni o a rendere Dichiarazioni mendaci all’Autorità Giudiziaria, richiamata all’art. 25--decies del D.Lgs. 231/2001, rilevante per la Società.

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria (art. 377-*bis* c.p.)

18.3. I principi generali di comportamento da tenere nell’ambito delle attività a rischio relative all’Induzione a non rendere Dichiarazioni o a rendere Dichiarazioni mendaci all’Autorità Giudiziaria

Ai Destinatari del Modello è vietato:

- porre in essere condotte che possano integrare le fattispecie di reato previste dall’art. 25-*decies* ex D. Lgs. 231/01 o che, nonostante non costituisca di per sé reato, possa potenzialmente diventarlo;
- usare violenza o minaccia al fine di indurre un soggetto chiamato a rendere dichiarazioni avanti l'autorità giudiziaria a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci;
- compiere atti intimidatori al fine di indurre un soggetto chiamato a rendere dichiarazioni avanti l'autorità giudiziaria a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci;
- offrire o promettere denaro o altra utilità al fine di indurre un soggetto chiamato a rendere dichiarazioni avanti l'autorità giudiziaria a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci.

18.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.



Gestione del contenzioso

- Individuazione dei soggetti coinvolti nella gestione del contenzioso.
- Individuazione di legali esterni per la gestione dei contenziosi.
- Condivisione della strategia difensiva in sede processuale da parte della Funzione legale, con i legali esterni ed il Vertice Aziendale.
- Predisposizione di uno scadenziario che permetta di controllare l'intera attività esecutiva, con particolare riferimento al rispetto dei termini processuali previsti.
- Tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate.
- Formalizzazione di documenti giustificativi degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvati dal superiore gerarchico e archiviati.
- Conduzione dell'eventuale transazione e/o conciliazione da parte della persona titolare di un'apposita procura e delega ad litem, che contempli il potere di conciliare o transigere la controversia e che sia approvata dalle competenti Funzioni/Organi.
- Laddove esponenti aziendali siano stati destinatari di richieste di rendere o produrre, davanti all'Autorità Giudiziaria, dichiarazioni utilizzabili in un procedimento penale relative all'esercizio delle proprie funzioni, il divieto di indurre o favorire i medesimi esponenti a non rendere / produrre le suddette dichiarazioni, ovvero a renderle mendaci.
- I rapporti con l'Autorità Giudiziaria e con la Pubblica Amministrazione nell'ambito del contenzioso giudiziale e stragiudiziale sono improntati ai principi di correttezza, trasparenza e tracciabilità anche quando gestiti per il tramite di un legale esterno.

18.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



19. Parte speciale “L”: Reati tributari

19.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli adempimenti fiscali/tributari e contributivi**
 - Adempimenti fiscali/tributari
 - Adempimenti contributivi

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Partecipazione a gare e trattative
- Fornitura dei servizi nel settore pubblico e privato
- Gestione del personale (dipendenti e collaboratori)
- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni
- Gestione del contenzioso
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione della Tesoreria
- Amministrazione, finanza e controllo
- Gestione degli adempimenti societari

19.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati Tributari, richiamate dal D.Lgs. 231/2001 all'art. 25-*quinques-decies*, rilevanti per la Società.

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/2000)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000)
- Dichiarazione infedele (art. 4 del D.Lgs. 74/2000)
- Omessa dichiarazione (art. 5 del D.Lgs. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000)
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000)
- Indebita compensazione (art.10-*quater* del D.Lgs. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000)

19.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Reati Tributari

Le attività e i processi che presentano profili di criticità potenziale sono mappate all'interno del “Manuale delle procedure amministrativo-contabili” che definiscono anche gli iter approvativi tracciati dal sistema informativo contabile mediante apposito workflow.

Il sistema di controllo così definito e utilizzato dalla società Reply SpA fornisce una tutela rispetto al rischio di commissione di reati tributari previsti dal Decreto.



Fermo quanto precede, nell'esercizio delle attività e delle mansioni ad essi affidate, i Destinatari devono astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti che possano integrare o comunque agevolare la commissione delle fattispecie di reato di cui alla presente Parte Speciale.

I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nelle attività di gestione della contabilità generale e predisposizione del bilancio devono:

- rispettare le regole e i principi contenuti nel Codice etico e ogni altra documentazione relativa al sistema di controllo interno;
- osservare, nello svolgimento delle attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, un comportamento corretto, trasparente e pienamente conforme alle norme di legge e regolamentari, al fine di fornire ai soci e al pubblico in generale informazioni veritiere e complete sulla situazione economica, patrimoniale e finanziaria della società e sull'evoluzione delle relative attività;
- assicurare il regolare funzionamento della società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare e mantenere traccia di tutta la documentazione richiesta e consegnata agli organi di controllo nonché di quella utilizzata nell'ambito delle attività assembleari;
- effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate; assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- assicurare che per ogni operazione vi sia un adeguato supporto documentale al fine di poter procedere, in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato e verificato l'operazione stessa;
- attuare un sistema di controllo sui clienti e fornitori al fine di evitare che la società entri in contatto con enti fittizi, ad esempio le società cd. "cartiere";
- riferire prontamente all'Organismo di Vigilanza eventuali situazioni di irregolarità;
- astenersi dall'effettuare prestazioni, pagamenti e/o elargizioni di qualsiasi natura in favore di terzi che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e/o in relazione al tipo di incarico da svolgere, o che potrebbero essere effettuate per assicurarsi condizioni di favore non pattuite o non dovute.

I Destinatari hanno, inoltre, l'esplicito divieto di:

- trasferire denaro o beni o altre utilità o compiere altre operazioni al fine di sottrarli all'azione coattiva dell'Amministrazione Finanziaria;
- utilizzare strumenti non istituzionali per il compimento di operazioni di trasferimento di denaro o altra utilità.

Al fine di ridurre, per quanto possibile, il rischio di commissione dei reati menzionati nella presente Parte Speciale, Reply SpA:

- ha implementato procedure che disciplinano i processi di acquisto, al fine di garantire la separazione di ruoli tra chi richiede l'acquisto e chi lo autorizza (nel rispetto delle soglie di autorizzazione di spesa predefinite), la tracciabilità delle operazioni svolte e l'identificazione delle responsabilità relative alle funzioni coinvolte;



- utilizza, ove possibile, sistemi gestionali che verifichino la coerenza delle informazioni relative agli acquisti e ai fornitori, e che – se possibile – blocchino i processi di acquisto qualora le informazioni inserite non siano coerenti con quelle preimpostate nel sistema, ad esempio qualora il prezzo di acquisto di un prodotto/bene/servizio/consulenza non sia coerente con i corrispettivi concordati con il fornitore oppure qualora l'autorizzazione alla spesa provenga da un soggetto non autorizzato;
- utilizza, ove possibile, sistemi gestionali che verifichino la coerenza delle informazioni relative alle vendite e ai clienti, e che blocchino i processi di vendita qualora le informazioni inserite non siano coerenti con quelle preimpostate nel sistema;
- conserva la documentazione relativa all'operazione in un apposito archivio, al fine di permettere la tracciabilità dell'intero processo e di agevolare eventuali controlli successivi;
- sottopone i fornitori ad un processo di selezione che non si basa unicamente sulla valutazione economica della prestazione, ma altresì su ulteriori criteri aggiuntivi tra cui, ad esempio, la capacità degli stessi di fornire i prodotti/beni/servizi/consulenze richiesti, nei tempi e con le modalità concordate;
- monitora le prestazioni dei consulenti, degli appaltatori o dei fornitori con documentazione da conservare al fine di permettere controlli successivi e il tracciamento dell'attività;
- inserisce nei contratti clausole che contemplino il rispetto da parte del consulente, appaltatore o fornitore dei principi di cui al D. Lgs. 231/2001 e del Codice Etico, nonché la dichiarazione di loro ottemperanza agli adempimenti indicati nel Modello e nel Codice Etico stesso;
- garantisce che i rapporti con i clienti siano gestiti esclusivamente dai soggetti muniti di idonei poteri e nell'ambito delle proprie competenze;
- garantisce che eventuali sconti siano stati preventivamente approvati coerentemente con le procedure aziendali;
- garantisce la tracciabilità di tutte le operazioni compiute.

Inoltre, nei processi implementati da Reply SpA relativi alle attività sensibili richiamate nella presente Parte Speciale, è necessario che:

- vi sia distinzione tra i soggetti che si occupano del calcolo delle imposte e della predisposizione delle dichiarazioni fiscali ed i soggetti che si occupano di verificare le informazioni e sottoscrivere le dichiarazioni;
- le dichiarazioni fiscali siano sottoscritte da esponenti di Reply SpA muniti di idonei poteri;
- le attività di elaborazione delle imposte siano svolte anche con il supporto di un consulente esterno;
- vi sia distinzione tra i soggetti richiedenti i pagamenti ed i soggetti che li autorizzano.

Si rimanda, altresì, a quanto esposto al capitolo sui Reati Societari.

19.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione degli adempimenti fiscali/tributari e contributivi

- Svolgimento delle attività attinenti al processo fiscale, incluse le modalità operative per la fruizione di servizi prestati da professionisti esterni, con diligenza,



professionalità, trasparenza, correttezza e nel rispetto di tutte le leggi ed i regolamenti applicabili, del Codice Etico e del Modello 231.

- Monitoraggio costante dell'evoluzione del quadro normativo di riferimento.
- Apposita formazione al personale delle Funzioni di contabilità e fiscale per quanto concerne le tematiche contabili e fiscali in vigore.
- Definizione dei ruoli aziendali responsabili del monitoraggio dell'evoluzione della normativa di riferimento e del rispetto dei relativi adempimenti.
- Formale definizione delle scadenze per la predisposizione della documentazione richiesta dalla normativa e/o di eventuali comunicazioni specifiche e definizione delle relative responsabilità.
- Formale definizione delle modalità e dei criteri per la determinazione delle imposte dirette e indirette.
- Formale identificazione dei flussi di comunicazione tra i soggetti/Funzioni coinvolti nelle attività in cui è articolato il processo di cui sopra e definizione delle modalità operative di trasferimento delle informazioni.
- Tempestiva e corretta registrazione delle rettifiche in bilancio risultati da verifiche o controversie fiscali.
- Tenuta dei registri contabili e amministrativi nel rispetto dei criteri di ordine, sistematicità e tempestività.
- Archiviazione della documentazione prodotta nel corso dell'attività di determinazione delle imposte e di tenuta e aggiornamento dei registri fiscali.
- Verifica del processo di archiviazione della documentazione a supporto prodotta.
- Conservazione dei documenti rilevanti ai fini fiscali e relativa segnalazione delle violazioni (i.e. controllo degli accessi sia fisici che digitali alle aree in cui sono conservati i documenti rilevanti).
- Esecuzione di verifiche circa la completezza, correttezza e veridicità dei dati necessari al calcolo delle imposte da parte della Funzione aziendale preposta alle registrazioni amministrativo-contabili.
- Revisione del calcolo delle imposte correnti e differite da parte della Funzione aziendale competente prima della registrazione in contabilità per verificare accuratezza e completezza.
- Verifica della corretta determinazione degli importi da parte della Società di Revisione come comprova della sua accuratezza e completezza.
- Documentazione accurata del processo di calcolo delle imposte e archiviazione della stessa in formato elettronico o cartaceo.
- Identificazione dei ruoli aziendali responsabili della predisposizione dei modelli dichiarativi e di versamento delle imposte.
- Formale elaborazione dei dati necessari alla predisposizione delle dichiarazioni fiscali ed alla liquidazione dei relativi tributi.
- Formale approvazione, nel rispetto delle deleghe e delle procure in essere, dei modelli dichiarativi e di versamento delle imposte.
- Monitoraggio e rispetto delle tempistiche per la presentazione delle dichiarazioni annuali e per il versamento delle imposte.
- Analisi dell'andamento dell'IVA e delle imposte sul reddito, in linea con l'andamento degli acquisti e delle vendite nel periodo.
- Analisi dell'andamento dei crediti e dei debiti tributari, con evidenza degli eventuali andamenti anomali.
- Controllo della corretta identificazione del trattamento delle poste indetraibili/indeducibili e della corretta deduzione/detrazione delle poste di bilancio (i.e. donazioni).
- Controllo delle perdite pregresse e delle imposte anticipate/differite.



- Archiviazione della documentazione prodotta nel corso delle attività di predisposizione ed approvazione dei modelli di versamento/dichiarativi.
- Controllo sul corretto pagamento e sulla liquidazione delle imposte nel rispetto dei tempi previsti dalla normativa.
- Riconciliazione degli importi derivanti dalle liquidazioni IVA mensili con la dichiarazione annuale.
- Utilizzo di mezzi idonei a garantire la documentabilità dei flussi informativi verso l'Amministrazione Finanziaria.
- Formale identificazione dei soggetti deputati a rappresentare la Società nei confronti dell'Amministrazione Finanziaria.
- Formalizzazione dei rapporti intrattenuti con esponenti dell'Amministrazione Finanziaria.
- Archiviazione della documentazione prodotta nel corso delle attività di gestione dei rapporti con l'Amministrazione Finanziaria.

19.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza:

- monitora l'efficacia delle procedure interne per la prevenzione dei reati tributari, attraverso incontri periodici con il Dirigente Preposto;
- acquisisce le relazioni della società di revisione al Comitato Controllo e Rischi, vigilando sull'effettiva sussistenza delle condizioni per garantire alla società di revisione una concreta autonomia nelle sue funzioni di controllo delle attività aziendali;
- esamina eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettua gli accertamenti ritenuti necessari in conseguenza delle segnalazioni ricevute;
- monitora l'esito delle ispezioni svolte dall'Amministrazione Finanziaria.

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



20. Parte Speciale “M”: Delitti contro la personalità individuale e di Razzismo e Xenofobia

20.1. Delitti contro la personalità individuale

In relazione alla fattispecie del reato di cui all'art. 603-bis c.p. “*Intermediazione illecita e sfruttamento del lavoro*” (richiamato dall'art. 25-*quiquies* del Decreto), la legge n. 199/2016 ha introdotto importanti novità in materia di contrasto al fenomeno del cosiddetto “caporalato” e ha apportato un ampliamento della platea dei soggetti attivi del reato con l'estensione della punibilità non solo al “caporale”, ma anche al “datore di lavoro”.

Con l'espressione “caporalato” si definisce un sistema informale di reclutamento e sfruttamento di manodopera, in base al quale un “caporale”, dietro corrispettivo, ingaggia, per conto del proprietario di un'azienda, dei lavoratori, sfruttando lo “stato di bisogno” in cui essi si trovano.

Il reato, pur essendo maggiormente diffuso nei settori dell'agricoltura e dell'edilizia, può riguardare anche altri settori come la cura familiare, le attività commerciali e quelle dei servizi.

In tale contesto, assumono particolare rilievo il processo di gestione del personale e di gestione degli acquisti di beni e servizi.

Pertanto, l'attività di valutazione dei rischi svolta da Reply ha tenuto conto non solo del personale interno, ma anche dei lavori e dei servizi appaltati a terzi.

20.1.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta

20.1.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti contro la personalità individuale, richiamate dal D.Lgs. 231/2001 all'art. 25-*quiquies*, rilevanti per la Società.

- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)

20.1.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti contro la personalità individuale



Ai fini della presente Parte Speciale e con riferimento al reato in esame, sono stati individuati i seguenti principi di comportamento cui i Destinatari a qualsiasi titolo coinvolti nelle attività a rischio devono attenersi.

Pertanto, i Destinatari nell'ambito dell'attività di controllo loro attribuita, devono:

- svolgere tutte le attività a rischio conformandosi alle leggi vigenti, ai principi di governance di Reply, alle norme del Codice Etico e ai principi generali di comportamento enucleati nel presente Modello;
- attenersi a quanto disciplinato dalle procedure implementate da Reply;
- operare in coerenza con il sistema di deleghe e procure in vigore;
- procedere all'identificazione delle controparti in operazioni di acquisto di beni, servizi e prestazioni;
- garantire lo svolgimento di una valutazione dell'integrità, onestà ed affidabilità delle controparti contrattuali, attraverso una specifica analisi di *background* che consideri eticità, competenze di natura tecnica, solidità patrimoniale e finanziaria delle stesse;
- mirare all'accertamento dell'identità delle controparti e dei soggetti per conto dei quali esse eventualmente agiscono (attraverso, ad esempio, la raccolta di dati e documentazione quali denominazione, sede legale e codice e/o domicilio fiscale, atto costitutivo e statuto, poteri di rappresentanza e dei dati identificativi degli amministratori delle controparti);
- consentire la tracciabilità delle attività di controllo svolte.

È fatto esplicito divieto ai Destinatari di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato prevista;
- porre in essere e adottare comportamenti che, sebbene non integrino, di per sé, la fattispecie di reato qui prevista, possano potenzialmente diventare idonei alla realizzazione del reato medesimo;
- occupare presso Reply e/o le Società del Gruppo lavoratori minorenni, in violazione delle disposizioni di legge che regolano la materia;
- sottoporre i lavoratori a condizioni lavorative di particolare sfruttamento, quali, a titolo esemplificativo: offrire ai lavoratori una retribuzione palesemente difforme dai contratti collettivi nazionali o comunque sproporzionata rispetto alla quantità e qualità del lavoro prestato, ovvero imporre ai lavoratori condizioni di lavoro in violazione sistematica della normativa relativa all'orario di lavoro, al riposo settimanale, all'aspettativa obbligatoria, alle ferie, o ancora esporre i lavoratori a pericolo per la salute, la sicurezza o l'incolumità personale a causa della violazione della normativa in materia di sicurezza e igiene nei luoghi di lavoro, infine esporre i lavoratori a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro;
- selezionare fornitori, partner e consulenti non ispirandosi ai principi di obiettività, competenza, economicità, trasparenza e correttezza e sulla base di criteri oggettivi quali la qualità, il prezzo e la capacità di fornire e garantire beni o servizi di livello adeguato.

20.1.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione degli acquisti di beni e servizi



- Qualificazione dei fornitori e previsione dell'Albo Fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Definizione delle tipologie di beni e/o importi per i quali si possa procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti ad identificare eventuali condizioni di incompatibilità e conflitto di interessi.
- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello 231 e del Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- Per i contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obblighino a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

In particolare, l'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
 - applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;
 - assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;
 - non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte delle Funzioni preposte che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Divieto di impiegare lavoratori stranieri privi di permesso di soggiorno o con un permesso revocato o scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo.
- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni,



uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.

- Verifiche da parte delle Funzioni competenti su eventuali precedenti penali, procedimenti penali in corso: l'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Richiesta dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.

20.1.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

20.2. Reati di Razzismo e Xenofobia

20.2.1. Le "Aree Sensibili" ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione degli acquisti di beni e servizi**
 - Qualifica e selezione dei Fornitori
 - Stipula dei contratti di acquisto
 - Gestione dei pagamenti
 - Verifica delle forniture
- **Gestione del personale (dipendenti e collaboratori)**
 - Ricerca, selezione e assunzione del personale
 - Gestione e sviluppo delle risorse umane
 - Gestione amministrativa del personale
 - Gestione delle spese di trasferta

20.2.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie di Razzismo e Xenofobia, richiamate dal D.Lgs. 231/2001 all'art. 25-ter-decies rilevanti per la Società.

- Razzismo e xenofobia (L. 167/2017, art. 5, comma)

20.2.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative al reato di Razzismo e Xenofobia

Al fine di prevenire i reati sopra enunciati, tutti i Destinatari del Modello devono rispettare, oltre i principi di comportamento già previsti ed espressi nel Codice Etico, anche quelli riportati nei documenti organizzativi adottati dalla Società, nonché tenere comportamenti conformi a quanto previsto dalle vigenti norme di legge. In particolare, devono:



- prestare la massima attenzione per prevenire e nel caso sopprimere episodi di razzismo o xenofobia che potrebbero essere consumati sia da figure apicali che sottoposti;
- astenersi dall'approvare e/o diffondere policy, comunicazioni esterne ed interne che istighino o incitino al razzismo e xenofobia e da cui possa derivare un concreto pericolo di diffusione di tali gravi forme di intolleranza;
- 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;
- assicurarsi che le società terze di recruiting o di somministrazione rispettino i principi e di protocolli previsti nella presente Parte Speciale.

20.2.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione degli acquisti di beni e servizi

- Qualificazione dei fornitori e previsione dell'Albo Fornitori.
- Richiesta, in fase di selezione e scelta delle offerte di fornitura, di una pluralità di preventivi a fornitori, individuati all'interno dell'Albo Fornitori.
- Esecuzione di una valutazione tecnico-economica delle offerte ricevute dai potenziali fornitori.
- Definizione delle tipologie di beni e/o importi per i quali si possa procedere all'assegnazione della fornitura direttamente ad un fornitore.
- Accertamento preliminare dei requisiti professionali, di onorabilità, economici ed organizzativi a garanzia degli standard qualitativi richiesti e meccanismi di valutazione complessiva del servizio reso, nonché controlli atti ad identificare eventuali condizioni di incompatibilità e conflitto di interessi.
- Inserimento di specifiche clausole nei contratti con cui il fornitore si impegna ad approvare e a conformare i propri comportamenti ai principi del Modello 231 e del Codice Etico applicabili all'attività svolta in favore della Società.
- Possibilità per la Società di risolvere il contratto con il fornitore in caso di violazione dei summenzionati principi.
- Per i contratti di appalto sono formalizzate clausole che prevedono: la disciplina del subappalto, che in ogni caso deve essere preventivamente approvato dalla Società; i costi della sicurezza e il rispetto delle norme in materia di salute e sicurezza; la dichiarazione in cui gli appaltatori dichiarino di conoscere e si obblighino a rispettare le norme vigenti in materia di lavoro (es. versamento contributi, adempimenti in materia di sicurezza), di tutela del lavoro minorile e delle donne, delle condizioni igienico-sanitarie e di sicurezza, di diritti sindacali o comunque di associazione e rappresentanza richiesti dalla normativa del Paese in cui essi operano, della tracciabilità finanziaria.

In particolare, l'appaltatore dichiara e garantisce che:

- il proprio personale riceve retribuzioni conformi al contratto collettivo nazionale e/o territoriale applicabile e, comunque, proporzionate rispetto alla quantità e qualità del lavoro prestato;
- applica correttamente a tutto il personale la normativa che regola l'orario di lavoro, il periodo di riposo, il riposo settimanale, l'aspettativa obbligatoria e le ferie;



- assicura al proprio personale tutte le misure atte a garantire la sua salute e sicurezza sul luogo di lavoro;
 - non sottopone il proprio personale a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
 - l'eventuale personale di paesi terzi impiegato nell'esecuzione delle attività di cui al contratto è in regola con il permesso di soggiorno.
- Verifica da parte delle Funzioni preposte che il corrispettivo corrisposto alla Terza Parte sia equo rispetto al valore di mercato e coerente con i beni/servizi forniti.

Gestione del personale (dipendenti e collaboratori)

- Previsione di criteri trasparenti di selezione dei professionisti e la documentabilità delle attività svolte. La scelta dei Dipendenti, dei consulenti e dei collaboratori avviene, a cura e su indicazione dei Responsabili delle Funzioni della Società, nel rispetto delle direttive, anche di carattere generale, formulate dalla medesima, sulla base di requisiti di professionalità specifica rispetto all'incarico o alle mansioni, uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, la scelta deve essere motivata e tracciabile.
- Verifiche da parte delle Funzioni competenti su eventuali precedenti penali, procedimenti penali in corso: l'effettuazione e le risultanze di tali verifiche sono valutate in relazione al ruolo e alle mansioni che il candidato andrà a svolgere.
- Richiesta dell'accettazione del Codice Etico e del Modello di Organizzazione e Controllo da parte del dipendente al momento dell'assunzione.

20.2.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



21. Parte Speciale “N”: Reati Ambientali

21.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Ambiente e gestione dei rifiuti**

21.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Reati Ambientali, richiamate dal D.Lgs. 231/2001 all'art. 25-*undecies*, rilevanti per la Società.

- Inquinamento ambientale (art. 452-*bis* c.p.)
- Attività di gestione di rifiuti non autorizzata (D.Lgs. 152/2006, art. 256)
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.Lgs. 152/2006, art. 257)
- Traffico illecito di rifiuti (D.Lgs. 152/2006, art. 259)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs. 152/2006, art. 258)
- Attività organizzate per il traffico illecito di rifiuti (art. 452-*quater-decies* c.p.)
- Sanzioni (D.Lgs. 152/2006, art. 279)
- Cessazione e riduzione dell'impiego delle sostanze lesive (L. n. 549/1993 art. 3)

21.3. I principi generali di comportamento da tenere nell'ambito delle attività di rischio relative ai Reati Ambientali

In generale, è fatto divieto ai Destinatari del Modello di porre in essere comportamenti che possano rientrare, anche potenzialmente, nella fattispecie di reato sopra richiamata, ovvero di collaborare o dare causa alla relativa realizzazione. Nell'ambito dei citati comportamenti è dunque fatto divieto, in particolare, di:

- effettuare attività di gestione dei rifiuti o conferire analogo incarico a soggetti terzi, in assenza delle necessarie autorizzazioni previste dalle norme di legge vigenti;
- raccogliere o trasportare i rifiuti senza il Formulario di identificazione del rifiuto;
- non effettuare gli obblighi di comunicazione previsti dalle norme di legge vigenti nei tempi e nei modi normativamente definiti;
- gestire erroneamente i rifiuti, cagionando inquinamento all'ambiente e/o alle persone fisiche;
- non rispettare gli obblighi imposti dalla normativa ambientale.

21.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Ambiente e gestione dei rifiuti

- Adozione della Policy Ambientale dove sono delineate le linee di indirizzo per il monitoraggio e la riduzione degli impatti che le attività aziendali generano sull'ambiente, includendo anche gli aspetti legati ai consumi e alle emissioni; la policy



è costantemente aggiornata e diffusa ai dipendenti e alle persone che lavorano per conto dell'organizzazione.

- Esistenza di una normativa aziendale che definisce ruoli, responsabilità e modalità da adottarsi per: l'identificazione delle prescrizioni normative vigenti in materia ambientale e delle prescrizioni autorizzative, anche attraverso la predisposizione di scadenziari e registri normativi; l'individuazione delle aree aziendali che rientrano nell'ambito di applicabilità delle prescrizioni e delle azioni che sono eventualmente messe in atto; l'individuazione dei soggetti responsabili del rispetto delle prescrizioni; la diffusione e l'accessibilità alle prescrizioni; l'attività di verifica periodica degli aggiornamenti normativi.
- Esistenza di normative aziendali che disciplinano ruoli, responsabilità e modalità relative alla gestione ed archiviazione della documentazione rilevante in materia ambientale. In particolare, tali normative riportano le modalità di gestione (es.: approvazione, diffusione, aggiornamento e controllo) e conservazione/archiviazione della documentazione stessa.
- Esistenza di regole interne che disciplinano le attività di gestione dei rifiuti prodotti dall'organizzazione affinché le stesse siano svolte in conformità ai requisiti normativi e autorizzativi vigenti.
- Esistenza di regole interne che disciplinano la gestione degli impianti e delle attività che generano emissioni in atmosfera al fine di garantire il rispetto dei limiti di emissione applicabili.
- Esistenza di regole interne che disciplinano la selezione di recuperatori / smaltitori / intermediari / trasportatori di rifiuti al fine della verifica dell'esistenza e della validità delle iscrizioni/comunicazioni/autorizzazioni previste dalla normativa per le attività di gestione dei rifiuti e che disciplinano l'affidamento dei contratti.
- Esistenza di regole interne per il monitoraggio delle prestazioni dei fornitori in materia ambientale affinché le attività siano svolte in conformità a quanto previsto dalle norme ambientali vigenti e ai requisiti specifici stabiliti dall'organizzazione.
- Esistenza di regole interne che disciplinano le modalità di rilevazione delle non conformità ambientali e di individuazione, registrazione e attuazione delle azioni correttive e preventive.

Reply SpA, il Consorzio Reply Public Sector e tutte le società consorziate hanno conseguito la certificazione del sistema di gestione ambientale secondo la norma ISO:14001 e la certificazione ISO 14064 (Carbon footprint di Organizzazione).

21.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



22. Parte Speciale “O”: Delitti contro il patrimonio culturale e paesaggistico

22.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Gestione dei siti e degli immobili**
 - Compravendita di terreni e immobili civili
 - Locazioni attive/passive di terreni e immobili civili
 - Gestione degli immobili di interesse culturale/con vincolo paesaggistico
- **Gestione degli eventi**
 - Organizzazione di eventi

22.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti contro il patrimonio culturale e paesaggistico e di Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici richiamate dal D.Lgs. 231/2001 agli artt. 25-*septies-decies* e 25-*duodevicies* del D.Lgs. 231/2001, rilevanti per la Società.

- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-*duo-decies* c.p.)
- Riciclaggio di beni culturali (art. 518-*sexies* c.p.)
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-*ter-decies* c.p.)

22.3. I principi generali di comportamento da tenere nell’ambito delle attività di rischio relative ai Delitti contro il patrimonio culturale

I Destinatari del Modello sono tenuti a osservare i seguenti principi generali di comportamento:

- rispettare la normativa italiana applicabile (Codice dei beni culturali; disposizioni del codice civile, del codice penale, leggi e regolamenti speciali in materia, etc.);
- astenersi dal porre in essere o partecipare alla realizzazione di condotte che, considerate individualmente o collettivamente, possano integrare le fattispecie di reato sopra riportate;
- astenersi dal porre in essere e adottare comportamenti che, sebbene non integrino, di per sé, alcuna delle fattispecie dei reati sopra riportati, possano potenzialmente diventare idonei alla realizzazione dei reati medesimi.

22.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Gestione dei siti e degli immobili

- Attività di due diligence, finalizzata a verificare eventuali prescrizioni di carattere culturale e/o paesaggistico dei siti ove effettuare gli scavi ed aprire un cantiere.
- Richiesta delle autorizzazioni previste dalle norme e regolamenti nazionali e/o locali alle autorità/istituzioni competenti, anche in materia di beni culturali e paesaggistici.



- In caso di ritrovamenti di potenziali reperti archeologici, beni culturali, interrompere le attività di scavo e/o di manutenzione, e richiedere il coinvolgimento delle autorità competenti.
- In caso di ritrovamenti di potenziali reperti archeologici, conservare e custodire i beni scoperti e farne denuncia alle autorità competenti.
- Richiesta di assistenza e consulenza di legali, esperti in materia di codice dei beni culturali e del paesaggio, previo accertamento dei relativi curricula.
- Il contratto di locazione/compravendita prevede l'inserimento di specifiche clausole a tutela dei rischi 231.

Gestione degli eventi

- Selezione dei fornitori e contrattualizzazione degli stessi nel rispetto delle policy aziendali vigenti in materia di acquisti.
- Verifiche, anche "on site" sull'effettivo e corretto svolgimento dell'evento.
- Nel caso di eventi svolti in siti ed immobili sottoposti a vincolo di interesse culturale/paesaggistico, la Società si avvale di agenzie accreditate per verificare la presenza di eventuali vincoli connessi all'organizzazione dell'evento.
- Nei contratti stipulati con le agenzie che si occupano dell'organizzazione degli eventi, previsione di apposite clausole e tutele contrattuali volte a preservare la Società da qualsiasi responsabilità eventualmente derivante da violazione di vincoli normativi.
- Stipula di apposite tutele assicurative.

22.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.



23. Parte Speciale “P”: Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

23.1. Le “Aree Sensibili” ai fini del D.Lgs. 231/2001

Di seguito sono elencate le Aree Sensibili identificate e le relative Attività Sensibili, suddivise per macrocategoria.

- **Fornitura dei servizi nel settore pubblico e privato**
 - Acquisizione di contratti con clienti (gestione dei rapporti commerciali per l'acquisizione di commesse)
 - Gestione delle attività progettuali nell'ambito di servizi resi a clienti (sviluppo software e gestione delle licenze di terzi, trattamento dei dati e accesso ai sistemi informativi)
- **Rapporti infragruppo**
 - Gestione dei rapporti fra le Società del Gruppo
- **Gestione della Tesoreria**
 - Gestione degli incassi e dei pagamenti
 - Gestione dei conti correnti
 - Utilizzo e gestione delle carte di credito
 - Gestione della piccola cassa
- **Gestione dei sistemi informativi**
 - Maintenance dell'hardware e del software aziendale
 - Gestione delle misure di sicurezza a protezione dei sistemi informatici e/o telematici
 - Gestione del processo di assegnazione dei codici di accesso ai sistemi informatici e/o telematici
 - Gestione delle licenze software

Di seguito si riportano le Aree sensibili strumentali alla commissione dei reati richiamati nella presente Parte Speciale:

- Gestione dei rapporti con la Pubblica Amministrazione
- Partecipazione a gare e trattative
- Gestione degli acquisti di beni e servizi
- Gestione del personale (dipendenti e collaboratori)
- Gestione degli omaggi, eventi, spese di rappresentanza e sponsorizzazioni
- Investimenti e operazioni straordinarie (comprese le operazioni sul capitale sociale, la restituzione dei conferimenti e la ripartizione degli utili/riserve)
- Gestione degli adempimenti fiscali/tributari e contributivi
- Amministrazione, finanza e controllo.

23.2. Le fattispecie di reato applicabili

Di seguito si riportano le fattispecie dei Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, richiamate dal D.Lgs. 231/2001 all'art. 25-octies.1, rilevanti per la Società.



- 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 aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)
- Trasferimento fraudolento di valori (art. 512-bis c.p.)

23.3. I principi generali di comportamento da tenere nell'ambito delle attività a rischio relative ai Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

I Destinatari del Modello sono tenuti a osservare i seguenti principi generali di comportamento:

- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
- garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
- garantire la piena collaborazione agli organi di controllo e alla Funzione Internal audit nell'ambito degli audit/controlli, oltre che nell'ambito di eventuali indagini/accertamenti da parte di organi esterni.

Con particolare riguardo alle attività di gestione dei pagamenti:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori (attraverso l'amministrazione, l'aggiornamento e il monitoraggio del relativo elenco storico);
- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;
- assicurare, in caso di pagamenti a favore di soggetti terzi tramite bonifico bancario, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta;
- operare nel rispetto delle rispettive procedure per quanto concerne i pagamenti con carta di credito, oltre che nel rispetto dei limiti delle deleghe e delle procure conferite in tale ambito;
- in caso di pagamento a carico della Società a mezzo di carta di credito, impiegare esclusivamente la carta di credito aziendale o altro strumento comunque intestato alla Società o a persona fisica in sua rappresentanza;
- assicurare che tutti i pagamenti riferiti ad acquisti realizzati dalla Società vengano effettuati a fronte dell'inserimento a sistema della fattura corrispondente;
- operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;
- segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;



- non 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 (i.e. a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura).

Con riguardo all'utilizzo delle apparecchiature informatiche/software:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della Funzione competente alla gestione dei relativi sistemi informatici;
- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società o delle Pubbliche Amministrazioni coinvolte, informare tempestivamente il responsabile della Funzione competente alla gestione dei relativi sistemi/dispositivi informatici;
- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle Funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- impiegare sulle apparecchiature della Società soltanto prodotti ufficialmente acquisiti dalla Società;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software.

La Società al momento non svolge un ruolo attivo all'interno del mercato dei servizi VAS. Tuttavia, qualora la Società decidesse di rivalutare tale posizione, sarebbe necessario rivedere il quadro normativo presente su tali servizi alla data della decisione e porre in essere un apparato di monitoraggio dei KPI che permetta di rilevare tempestivamente ed efficacemente la presenza di eventuali anomalie.

23.4. Gli standard di controllo specifici

Di seguito si riportano gli standard di controllo specifici applicabili a questa Parte Speciale.

Fornitura dei servizi nel settore pubblico e privato

- Implementazione da parte della Società di una lista contenente l'elenco delle applicazioni che gestiscono:
 - o il trattamento di dati finalizzati ai pagamenti;
 - o i calcoli di importi dovuti;
 - o le informazioni di pagamento quali IBAN e numeri di carta di credito anche in maniera transitoria.
- Per ciascuna delle suddette applicazioni, sono mappate le seguenti informazioni:
 - o nome dell'applicativo;
 - o stato attuale dell'applicativo (in produzione, in fase di test, ecc.);
 - o descrizione della funzionalità di pagamento, ossia se:
 1. l'applicativo gestisce pagamenti diretti (ad es.: transazioni, incassi), o
 2. l'applicativo tratta esclusivamente informazioni relative ai pagamenti (ad es.: visualizzazione storico, estratti conto).
 - o Tipologia di dati di pagamento trattati (IBAN, numero di carta di credito, ecc.);



- misure di sicurezza e compliance adottate per proteggere i dati di pagamento (es. PCI DSS per la protezione dei dati delle carte di credito);
 - clienti per i quali l'applicativo è stato sviluppato;
 - eventuali incidenti di sicurezza passati relativi all'applicativo.
- Attività di Risk Assessment sulla base di suddette informazioni, e analisi mirata sugli applicativi che risultano maggiormente rischiosi.

Rapporti infragruppo

- Identificazione di ruoli aziendali responsabili della stesura/verifica dei contratti infragruppo.
- Esecuzione di verifiche formali e sostanziali sui flussi finanziari aziendali, con riferimento a pagamenti/operazioni infragruppo.
- Esistenza di appositi template per la predisposizione dei contratti per l'identificazione dei servizi da erogare.
- Formale definizione degli obblighi e delle responsabilità della società mandante e della società mandataria.
- Monitoraggio e aggiornamento dei corrispettivi previsti nei contratti.
- Operazioni di acquisizione/cessione di asset tra Società del Gruppo e con controparti esterne sono condotte nel rispetto delle normative fiscali vigenti.

Gestione della Tesoreria

- Definizione dei ruoli aziendali e delle modalità operative per la gestione degli incassi.
- Attività di profilazione delle utenze, che consente l'accesso al sistema di gestione degli incassi e dei crediti alle sole risorse autorizzate.
- Monitoraggio degli incassi accreditati dagli istituti bancari.
- Monitoraggio dei crediti scaduti/in scadenza.
- Esecuzione di verifiche circa:
 - la coerenza dei dati presenti nella fattura attiva e l'incasso;
 - gli accantonamenti/utilizzi del fondo svalutazione crediti.
- Riconciliazione periodica, fisico-contabile, dei saldi banca/cassa.
- Divieto di ricevere pagamenti su conti cifrati.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione degli incassi e del recupero crediti.
- Attività di profilazione delle utenze che consente l'accesso al sistema di gestione dei pagamenti alle sole risorse autorizzate.
- Definizione di limiti all'autonomo impiego delle risorse finanziarie, anche attraverso la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative.
- Riconciliazione periodica, fisico-contabile, dei saldi banca/cassa.
- Monitoraggio dei pagamenti addebitati dagli istituti bancari.
- Esecuzione di verifiche circa la coerenza dei dati presenti:
 - nella fattura passiva e nell'ordine di acquisto a sistema/contratto;
 - nella fattura passiva e la bolla di entrata merci;
 - la coerenza delle informazioni contenute nelle fatture passive e nelle disposizioni/lettere di pagamento.
- Ruoli aziendali responsabili e formale definizione delle modalità operative per la predisposizione dello scadenziario di pagamento delle fatture.
- Formale approvazione, nel rispetto delle deleghe e delle procure in essere, delle disposizioni/lettere di pagamento in relazione ai livelli autorizzativi definiti.



- Ruoli aziendali responsabili e formale definizione delle modalità operative per la predisposizione e l'autorizzazione delle disposizioni di pagamento.
- Archiviazione della documentazione prodotta nel corso dell'attività di gestione dei pagamenti.
- Predisposizione di pagamenti nei confronti dei soli soggetti presenti in anagrafica.
- I pagamenti tramite bonifici sono sempre processati dalla Funzione Tesoreria mediante appositi sistemi di autenticazione e gli importi oggetto di bonifico sono opportunamente autorizzati, mediante sistemi informativi e condivisi mediante flussi di comunicazione protetti.
- Attività di profilazione delle utenze, che consenta l'accesso al sistema di gestione delle anagrafiche dei conti correnti alle sole risorse autorizzate.
- Definizione dei ruoli aziendali responsabili e formale definizione delle modalità operative per l'apertura/chiusura dei conti correnti.
- Esecuzione di verifiche circa i termini, le clausole e le condizioni contrattuali inserite nel contratto di apertura di un conto corrente.
- Verifica che tutti i conti correnti siano detenuti in nome della Società e presso istituti bancari precedentemente autorizzati.
- Riconciliazione periodica, fisico-contabile, dei saldi bancari.
- Archiviazione della documentazione prodotta nel corso dell'attività di apertura, chiusura o modifica di un conto corrente.
- Definizione dei ruoli aziendali responsabili e definizione delle modalità operative per la predisposizione del report di riconciliazione e per la gestione di eventuali anomalie emerse.
- Policy per l'utilizzo delle carte di credito.
- Effettuazione di controlli sugli estratti conto per verificare il corretto utilizzo di tali carte nel rispetto delle regole vigenti.
- Formale identificazione del responsabile/i della Tesoreria.
- Esecuzione di verifiche sul corretto utilizzo e corretta gestione della cassa contante.

Gestione dei sistemi informativi

- Esistenza della ICT Security Policy in materia di sicurezza dei sistemi informativi che definisce, fra l'altro:
 - o gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni, i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda;
 - o la gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.
 - o modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
 - o ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica;
 - o implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche;
 - o identificazione dei requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
 - o gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
 - o Confidenzialità, autenticità e integrità delle informazioni;



- sicurezza nel processo di sviluppo dei sistemi informativi
- Formazione specifica sul tema del Ricatto Informatico, in particolare, al fine di evitare, nell'ambito del procacciamento di affari e dei servizi svolti, situazioni di minacce di sospensione dei servizi e/o pubblicazione di dati del cliente.

23.5. Compiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza effettua periodicamente controlli a campione diretti a verificare il corretto svolgimento delle attività connesse alle attività a rischio relative ai reati previsti dalla presente Parte Speciale, fermo restando il potere discrezionale dell'Organismo di Vigilanza di attivarsi con specifici controlli a seguito delle segnalazioni ricevute. A tal fine all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.