UnipolPay S.p.A.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 231/2001)

28 settembre 2026

UnipolPay

Indice

PARTE GENERALE **4**

1 INTRODUZIONE **4**

1.1 Definizioni 4
1.2 Il Decreto Legislativo 231/2001 5
1.3 Sanzioni a carico dell'Ente 12
1.4 Esenzione dalla responsabilità 14

2 I RIFERIMENTI UTILIZZATI PER L'ELABORAZIONE DEL MODELLO **16**

2.1 Le Linee Guida Confindustria 16
2.2 Le Linee Guida ABI 16

3 ADOZIONE DEL MODELLO **18**

3.1 Il ruolo e le attività di UnipolPay 18
3.2 Il sistema di controllo interno e di gestione dei rischi di UnipolPay 18
3.3 Il sistema normativo interno del Gruppo 19
3.4 Principi generali di controllo 19
3.5 Funzione e scopo del Modello 21
3.6 La costruzione del Modello e la sua struttura 22
3.7 Definizione dei Protocolli: individuazione e analisi dei processi sensibili 24
3.8 Definizione dei principi etici 24
3.9 La procedura di adozione del Modello 25

4 I PROCESSI AZIENDALI ESPOSTI ALLA COMMISSIONE DEI REATI INDICATI NEL D. LGS. 231/2001 ... 26

5 L'ORGANISMO DI VIGILANZA **28**

5.1 Individuazione, requisiti e nomina dell'Organismo di Vigilanza 28
5.2 Funzioni e poteri dell'Organismo di Vigilanza 30
5.3 Reporting dell'Organismo di Vigilanza verso il vertice aziendale 31
5.4 Flussi informativi verso l'Organismo di Vigilanza: informazioni di carattere generale e informazioni specifiche obbligatorie 31
5.5 Comunicazioni da parte degli Organismi di Vigilanza delle Società del Gruppo 32
5.6 Obblighi di riservatezza dell'Organismo di Vigilanza 33
5.7 La segnalazione di reati o di violazioni del Modello 33

6 DISPOSIZIONI DISCIPLINARI E SANZIONATORIE **35**

6.1 Principi Generali 35
6.2 Criteri generali di irrogazione delle sanzioni 35
6.3 Ambito di applicazione 35
6.4 Misure nei confronti dei lavoratori dipendenti 36
6.5 Misure nei confronti dei dirigenti 36
6.6 Misure nei confronti degli Amministratori 36
6.7 Misure nei confronti dei Sindaci 36
6.8 Misure nei confronti di collaboratori e fornitori 36
6.9 Misure a tutela del sistema interno di segnalazione delle violazioni 36

7 LA DIFFUSIONE DEL MODELLO TRA I DESTINATARI **37**

7.1 Informativa e formazione per dipendenti e apicali 37
7.2 Informativa per i collaboratori e fornitori 38

PARTE GENERALE

1 INTRODUZIONE

1.1 Definizioni

Banca d'Italia	Banca centrale della Repubblica italiana
Collaboratori	Soggetti che intrattengono con l'ente rapporti di collaborazione a vario titolo (consulenti, professionisti, etc.).
Consob	Commissione Nazionale per le Società e la Borsa.
Decreto o D. Lgs. 231/2001	Decreto Legislativo del 8 giugno 2001, n. 231, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e successive modifiche e integrazioni.
D. Lgs. 231/2007	Il Decreto Legislativo 21 novembre 2007, n. 231, come modificato dal D.lgs. n. 90/2017, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
Destinatari	Soggetti in posizione apicale e soggetti sottoposti alla loro direzione o vigilanza, ivi compresi collaboratori e fornitori.
Dipendenti	Il personale dipendente a libro matricola della Società, nonché il personale in organico alla stessa e distaccato da altre Società del Gruppo ed il personale ivi operante con contratto di somministrazione.
Ente	Persona giuridica e/o associazione anche priva di personalità giuridica.
Gruppo o Gruppo Unipol	Unipol Assicurazioni S.p.A. e le società dalla stessa direttamente o indirettamente controllate ai sensi dell'art. 2359 del codice civile.
Linee Guida ABI	Linee Guida per il settore bancario in materia di responsabilità amministrativa emanate dall'Associazione bancaria Italiana.
Linee Guida Confindustria	Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001 emanate ai sensi dell'art. 6 comma 3 del Decreto.
Modello o MOG	Il presente modello di organizzazione, gestione e controllo, così come previsto dall'art. 6, comma 1, lett. a), del D. Lgs. 231/2001.
OdV o Organismo di Vigilanza	Organismo previsto all'art. 6, comma 1, lettera b) del D. Lgs. 231/2001, cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento.
Reati	I reati (delitti e contravvenzioni) di cui agli artt. 24 e ss. del D. Lgs. 231/2001 e successive modifiche e integrazioni.
Soggetti in posizione apicale	Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione e il controllo della stessa.

Soggetti sottoposti all'altrui direzione o vigilanza	Persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale.
T.U.B.	D. Lgs. n. 385/1993, "Testo unico delle leggi in materia bancaria e creditizia", e successive modifiche e integrazioni.
T.U.F.	D. Lgs. n. 58 del 24 febbraio 1998, "Testo unico delle disposizioni in materia di intermediazione finanziaria", e successive modifiche e integrazioni.
U.I.F.	Unità di Informazione Finanziaria istituita presso la Banca d'Italia.
Unipol Assicurazioni (anche Unipol, controllante o Capogruppo)	Unipol Assicurazioni S.p.A.
UnipolPay o Società	UnipolPay S.p.A.

1.2 Il Decreto Legislativo 231/2001

Il D. Lgs. 231/2001, emanato in esecuzione della delega di cui all'art. 11 della legge n. 300/2000 al fine di adeguare la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia aveva già da tempo aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione del 26 maggio 1997, anch'essa firmata a Bruxelles, sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione dei pubblici ufficiali stranieri nelle operazioni economiche e internazionali, ha introdotto nel nostro ordinamento "la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" per specifiche tipologie di reato (c.d. "reati presupposto") commesse da propri amministratori e dipendenti.

Il D. Lgs. 231/2001 può essere pertanto inteso come una "norma di sistema" che nel corso degli anni si è implementata con la previsione di nuove fattispecie di reati presupposto, successivamente elencati in modo dettagliato (Allegato 2).

La normativa in parola è frutto di una tecnica legislativa che, mutuando i principi propri dell'illecito penale e dell'illecito amministrativo, ha introdotto nell'ordinamento italiano un sistema punitivo a carico dell'impresa che va ad aggiungersi ed integrarsi con gli apparati sanzionatori preesistenti.

Il giudice penale competente a giudicare l'autore del fatto di reato è, altresì, chiamato a giudicare, anche la responsabilità amministrativa dell'Ente e ad applicare, in caso di condanna, le sanzioni previste.

In tema di abusi di mercato, va tuttavia precisato che, in base a quanto previsto dall'art. 187 – *quinquies* del T.U.F., la responsabilità amministrativa dell'ente si configura anche quando la condotta integra gli estremi dell'illecito amministrativo. In tale ambito le relative sanzioni sono applicate dalla Consob. Anche in tema di reati tributari, la responsabilità dell'ente ex D.Lgs. 231/2001 si aggiunge a quella prevista dal D.lgs. 471/1997, che comporta l'applicazione di sanzioni amministrative.

L'Ente può essere ritenuto responsabile qualora uno dei reati specificamente previsti dal D. Lgs. 231/2001 sia commesso nel suo interesse o a suo vantaggio:

a) da una persona fisica che riveste funzioni di rappresentanza, di amministrazione o di direzione dell'Ente (c.d. soggetti apicali) o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da una persona che esercita, anche di fatto, la gestione e il controllo dello stesso;
b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui al precedente punto.

Quando l'autore del reato è un soggetto apicale, il Legislatore prevede una presunzione di responsabilità per l'Ente, in considerazione del fatto che tali soggetti esprimono, rappresentano e concretizzano la politica gestionale dello stesso (art. 5, comma 1, lett. a) del D. Lgs. 231/2001).

In particolare, relativamente alla definizione di soggetto apicale si riporta quanto previsto dalle Linee Guida di ABI: "Circa i soggetti cui il decreto fa riferimento (soggetti apicali), vengono innanzitutto in considerazione coloro che svolgono funzioni inerenti alla gestione e al controllo dell'Ente o di sue articolazioni: il legislatore ha dunque scelto di individuare tale categoria attraverso un criterio oggettivo/funzionale, facendo cioè riferimento alla concreta attività svolta, piuttosto che alla qualifica formalmente rivestita. Di particolare interesse appare l'equiparazione ai soggetti che ricoprono funzioni di rappresentanza, di amministrazione o di direzione dell'ente delle persone che rivestono le medesime funzioni in una "unità organizzativa dotata di autonomia finanziaria e funzionale": si tratta, come noto, di una figura sempre più diffusa nella nostra realtà economica, soprattutto nell'ambito delle imprese di dimensioni medio grandi".

La distinzione tra le due categorie di soggetti (apicali e sottoposti a direzione e vigilanza) riveste indubbia rilevanza, in quanto ne deriva una diversa graduazione di responsabilità dell'Ente coinvolto, nonché una differente previsione dell'onere della prova; infatti, nel caso di reati commessi da soggetti apicali, sussiste in capo all'Ente una presunzione di responsabilità determinata dalla circostanza che tali soggetti esprimono e rappresentano la politica aziendale dell'Ente stesso e, quindi, la sua volontà e azione esteriore.

Quando l'autore dell'illecito è un soggetto sottoposto all'altrui direzione o vigilanza, la responsabilità dell'Ente è configurabile soltanto qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza (art. 5, comma 1, lett. b) del D. Lgs. 231/2001): tale inosservanza deve essere dimostrata dal Pubblico Ministero.

La responsabilità dell'Ente è comunque esclusa nel caso in cui le persone che hanno commesso il reato abbiano agito nell'interesse esclusivo proprio o di terzi.

L'Ente è responsabile anche qualora l'autore del reato non sia stato identificato o non sia imputabile e anche nel caso in cui il reato si estingua per una causa diversa dall'amnistia (art. 8 comma 1, lett. a) e b) del D. Lgs. 231/2001).

In caso di illecito commesso all'estero, gli Enti che hanno la loro sede principale nel territorio dello Stato italiano sono comunque perseguibili, sempre che lo Stato del luogo ove il fatto-reato è stato commesso non proceda nei loro confronti (art. 4, comma 1, del D. Lgs. 231/2001).

Alla data di aggiornamento del presente Modello, la responsabilità amministrativa degli Enti può derivare dalla commissione di specifiche tipologie di reato previste dal Decreto, che di seguito si elencano:

- Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture: **art. 24**[1]
- Delitti informatici: **art. 24-*bis***[2]
- Delitti di criminalità organizzata: **art. 24-*ter***
- Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione: **art. 25**[3]
- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento: **art. 25-*bis***
- Delitti contro l'industria e il commercio: **art. 25-*bis*.1**[4]
- Reati societari: **art. 25-*ter***
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico: **art. 25-*quater***[5]
- Pratiche di mutilazione degli organi genitali femminili: **art. 25-*quater*.1**
- Delitti contro la personalità individuale: **art. 25-*quinquies***[6]
- Intermediazione illecita e sfruttamento del lavoro: ***art. 25 quinquies, comma 1, lettera a)***
- Abusi di mercato: **art. 25-*sexies***
- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro: **art. 25-*septies***

[1] Articolo modificato dal D.Lgs. 75/2020 e integrato dalla Legge 137/2023
[2] Articolo modificato dalla Legge 90/2024
[3] Articolo modificato dal D.Lgs. 75/2020 e dalla Legge 114/2024
[4] Articolo modificato dalla Legge 75/2026
[5] Articolo integrato dal Decreto Legge 48/2025
[6] Articolo integrato dal Decreto Legislativo 115/2026

- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio: **art. 25-*octies*[7]**
- Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori: **art. 25-octies 1[8]**
- Reati in materia di violazione di misure restrittive dell'Unione europea: **art. 25-octies.2[9]**
- Delitti in materia di violazione del diritto d'autore: **art. 25-*novies***
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria: **art. 25-*decies***
- Reati ambientali: **art. 25-*undecies*[10]**
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare: **art. 25-*duodecies*[11]**
- Razzismo e Xenofobia: ***art. 25-terdecies*[12]**
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati: **art. 25-*quaterdecies*[13]**
- Reati tributari: **art. 25-*quinquiesdecies*[14]**
- Reati di contrabbando: **art. 25-*sexiesdecies*[15]**
- Delitti contro il patrimonio culturale: **art. 25-*septiesdecies*[16]**
- Delitti contro gli animali: **art. 25-undevicies[17]**
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici: **art. 25-duodevicies[18]**

La responsabilità dell'Ente può essere sancita anche in relazione ai reati transnazionali di cui all'art 10 della legge n. 146/2006 "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001" (reati associativi, intralcio alla giustizia, favoreggiamento dell'immigrazione clandestina).

Nel caso in cui venga commesso uno dei reati specificatamente indicati, alla responsabilità penale della persona fisica che ha materialmente realizzato il fatto, si aggiunge, se e in quanto siano integrati tutti gli altri presupposti normativi, anche la responsabilità "amministrativa" dell'Ente.

Ulteriori approfondimenti sui reati previsti dal D. Lgs. 231/2001 possono leggersi nell'Allegato 4.

Ai fini della predisposizione del presente Modello di organizzazione, gestione e controllo, sono state prese in considerazione tutte le fattispecie di reato presenti nel Decreto alla data di approvazione del Modello stesso e sono state ritenute astrattamente ipotizzabili le fattispecie di reato di seguito riportate:

Delitti nei rapporti con la Pubblica Amministrazione (artt.24 e 25 del Decreto)

- Malversazione di erogazioni pubbliche (art. 316-*bis*, cod. pen.);
- Indebita percezione di erogazioni pubbliche (art. 316-*ter*, cod. pen.);
- Corruzione per l'esercizio della funzione (art. 318, cod. pen.);
- Corruzione per un atto contrario ai doveri di ufficio (art. 319, cod. pen.);
- Corruzione in atti giudiziari (art. 319-*ter*, cod. pen.);
- Induzione indebita a dare o promettere utilità (art 319-*quater* cod. pen.);
- Corruzione di persona incaricata di un pubblico servizio (art. 320, cod. pen.);
- Istigazione alla corruzione (art. 322, cod. pen.)
- Traffico di influenze illecite (art 346-*bis*, cod. pen.);
- Truffa in danno dello Stato, di un altro ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1

[7] Il decreto legislativo 195/2021 ha delle implicazioni indirette sull'articolo 25-*octies*, pur non modificandolo, in quanto apporta modifiche agli articoli del codice penale richiamati nell'articolo 25-*octies* stesso. Di queste modifiche si è tenuto conto nella relativa Parte Speciale.
[8] Articolo introdotto dal D.Lgs. 184/2021 e integrato dalla Legge 137/2023
[9] Articolo introdotto dal D.Lgs. 211/2025
[10] Articolo modificato dal Decreto Legge 116/2025 e dal D. lgs. 81/2026
[11] Articolo modificato dalla Legge n. 161 del 2017, che ha esteso la responsabilità dell'Ente ai delitti previsti dai commi 3, 3-*bis*, 3-*ter* e 5 dell'articolo 12 del D.Lgs. 286/1998 (T.U. Immigrazione)
[12] Articolo modificato dal D. Lgs. 21/2018: il delitto richiamato (ex articolo 3, comma 3-bis, legge 13 ottobre 1975, n. 654) è stato spostato nel codice penale (articolo 604-bis).
[13] Articolo introdotto dalla Legge 39/2019
[14] Articolo introdotto dalla Legge 157/2019 e modificato dal D. Lgs. 75/2020
[15] Articolo introdotto dal D.Lgs. 75/2020 e modificato dal D. Lgs. 141/2024
[16] Articolo introdotto dalla Legge n. 22 del 2022
17 Articolo introdotto dalla Legge 82/2025
[18] Articolo introdotto dalla Legge n. 22 del 2022

cod. pen.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis*, cod. pen.);
- Frode informatica (art. 640 -*ter*, cod. pen.).

Per una breve descrizione delle fattispecie concernenti i delitti contro la Pubblica Amministrazione e la esemplificazione delle relative condotte si rinvia alla **Parte Speciale 1** "Delitti nei rapporti con la Pubblica Amministrazione".

Reati societari (art. 25-ter del Decreto)

- False comunicazioni sociali (art. 2621, cod. civ.);
- Impedito controllo (art. 2625, cod. civ.);
- Illegale ripartizione degli utili e delle riserve (art. 2627, cod. civ.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628, cod. civ.);
- Omessa comunicazione del conflitto d'interessi (art. 2629-*bis* cod. civ.);
- Corruzione tra privati (art 2635 cod. civ.);
- Istigazione alla corruzione tra privati (2635 bis, cod. civ.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, cod. civ.);
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54, D.Lgs. 19/2023).

Per una breve descrizione delle fattispecie concernenti i reati societari e la esemplificazione delle relative condotte si rinvia alla **Parte Speciale 2** "Reati Societari".

Delitti e illeciti amministrativi di abuso di informazioni privilegiate, manipolazione del mercato e aggiotaggio (artt. 25-sexies e 25 -ter del Decreto)

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate di cui all'art. 184 T.U.F.;
- Abuso e comunicazione illecita di informazioni privilegiate di cui all'art. 187-*bis* T.U.F.;
- Manipolazione del mercato di cui agli artt. 185 e 187-*ter* T.U.F;
- Aggiotaggio di cui all'art. 2637 cod. civ.

Per una breve descrizione delle fattispecie concernenti i reati e illeciti amministrativi di abuso di informazioni privilegiate, manipolazione del mercato e aggiotaggio e la esemplificazione delle relative condotte si rinvia alla **Parte Speciale 3** "Delitti e illeciti amministrativi di abuso di informazioni privilegiate, manipolazione del mercato e aggiotaggio".

Delitti di ricettazione, riciclaggio, autoriciclaggio e delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 25-octies e 25-quater del Decreto)

- Ricettazione (art. 648, cod. pen.);
- Riciclaggio (art. 648-*bis*, cod. pen.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter*, cod. pen.);
- Autoriciclaggio (art, 648 ter 1, cod. pen.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-*bis*, cod. pen.).

Per una breve descrizione delle fattispecie concernenti i delitti di ricettazione e riciclaggio, e i delitti con finalità di terrorismo o di eversione dell'ordine democratico e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 4** "Delitti di ricettazione, riciclaggio, autoriciclaggio e delitti con finalità di terrorismo o di eversione dell'ordine democratico".

Delitti informatici (art. 24-bis del Decreto)

- Documenti informatici (art. 491-*bis* cod. pen.);
- Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* cod. pen.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater* cod. pen.);

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* cod. pen.);
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. pen.);
- Estorsione (art. 629, comma 3, cod. pen.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* cod. pen.);
- Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-*ter* cod. pen.);
- Danneggiamento di sistemi informatici o telematici (art. 635-*quater* cod. pen.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico (art. 635-*quater*.1);
- Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* cod. pen.).

Per una breve descrizione delle fattispecie concernenti i delitti informatici e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 5** "Delitti informatici".

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies del Decreto)

- Omicidio colposo (art. 589 cod. pen.);
- Lesioni personali colpose (art. 590, cod. pen.).

Per una breve descrizione delle fattispecie concernenti i delitti di omicidio colposo e lesioni commessi con violazione delle norme antinfortunistiche e di tutela della salute e sicurezza sul lavoro e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 6** "Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro".

Delitti di criminalità organizzata e reati transnazionali (art. 24-ter del Decreto e Legge 16 marzo 2006, 146)

- Associazione per delinquere (art. 416 cod. pen.);
- Associazioni di tipo mafioso anche straniere (art. 416-*bis* cod. pen.);
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-*bis*, 3-*ter* e 5, D.Lgs. 286/1998 – T.U. Immigrazione).

Per una breve descrizione delle fattispecie concernenti i delitti di criminalità organizzata e reati transnazionali e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 7** "Delitti di criminalità organizzata e reati transnazionali".

Reati ambientali (art. 25-undecies del Decreto)

- Abbandono di rifiuti non pericolosi in casi particolari (art. 255-bis, D. Lgs. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 D. Lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, comma 4, secondo periodo, D. Lgs. 152/2006);
- Traffico illecito di rifiuti (art. 259, comma 1, D. Lgs. 152/2006).

- Impedimento del controllo (art. 452 septies, cod. pen.).

Per una breve descrizione delle fattispecie concernenti i reati ambientali, e la esemplificazione delle relative condotte si rinvia alla **Parte Speciale 8** "Reati ambientali".

Delitti in materia di violazione del diritto d'autore (art. 25-novies del Decreto)

- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (artt. 171, 171-*bis*, 171-*ter*, 171-*septies* e 171-*octies* L. 633/1941).

Per una breve descrizione delle fattispecie concernenti i delitti in materia di violazione del diritto d'autore e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 9** "Delitti in materia di violazione del diritto

d'autore".

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies del Decreto)

- Lavoro subordinato a tempo determinato e indeterminato (art. 22, comma 12-*bis*, D.Lgs. 286/98).

Per una breve descrizione della fattispecie concernente il delitto di impiego di cittadini di paesi terzi il cui permesso di soggiorno è irregolare e la esemplificazione delle relative condotte, si rinvia alla **Parte Speciale 10** "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies del Decreto)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* cod. pen.).

Per una breve descrizione della fattispecie concernente il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria e la esemplificazione delle relative condotte si rinvia alla **Parte Speciale 11** "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria".

Intermediazione illecita e sfruttamento del lavoro (art. 25-quinquies del Decreto)

- Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis*, cod. pen.).

Per una breve descrizione del reato di intermediazione illecita e sfruttamento del lavoro e l'esemplificazione delle relative condotte si rinvia alla **Parte Speciale 12** "Intermediazione illecita e sfruttamento del lavoro".

Reati tributari (art. 25-quinquiesdecies del Decreto)

- 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, 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).

Per una breve descrizione delle fattispecie concernenti i reati tributari e l'esemplificazione delle relative condotte si rinvia alla **Parte Speciale 13** "Reati tributari".

Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies 1 del Decreto)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-*ter* cod. pen.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* cod. pen.);
- Trasferimento fraudolento di valori (art. 512-*bis* cod. pen.).

Per una breve descrizione delle fattispecie concernenti i delitti in materia di strumenti di pagamento diversi dai contanti e il trasferimento fraudolento di valori e l'esemplificazione delle relative condotte illecite, si rinvia alla **Parte Speciale 14** "Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori".

Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-octies 2 del Decreto)

- Violazione delle misure restrittive dell'Unione europea (art. 275-*bis* cod. pen.);
- Violazione degli obblighi informativi imposti da una misura restrittiva dell'Unione europea (art. 275-*ter* cod. pen.).

Per una breve descrizione delle fattispecie concernenti i reati in materia di violazione delle misure restrittive dell'Unione europea e l'esemplificazione delle relative condotte illecite, si rinvia alla **Parte Speciale 15** "Reati in materia di violazione delle misure restrittive dell'Unione europea".

1.3 Sanzioni a carico dell'Ente

Le sanzioni previste per gli illeciti amministrativi dipendenti da reato sono:

(a) Sanzione amministrativa pecuniaria;

(b) Sanzioni interdittive;

(c) Confisca;

(d) Pubblicazione della sentenza di condanna.

(a) La sanzione amministrativa pecuniaria

La sanzione amministrativa pecuniaria, disciplinata dagli artt. 10 e seguenti del D. Lgs. 231/2001, costituisce la sanzione "di base" di necessaria applicazione, del cui pagamento risponde l'Ente con il suo patrimonio o con il fondo comune.

Il Legislatore ha adottato un criterio innovativo di commisurazione di tale sanzione, attribuendo al Giudice l'obbligo di procedere a due diverse e successive operazioni di apprezzamento, al fine di un maggiore adeguamento della sanzione alla gravità del fatto ed alle condizioni economiche dell'Ente.

La determinazione delle sanzioni pecuniarie irrogabili ai sensi del D. Lgs. 231/2001 si fonda su un sistema di quote. Per ciascun illecito, infatti, la legge in astratto determina un numero minimo e massimo di quote, sul modello delle cornici edittali che tradizionalmente caratterizzano il sistema sanzionatorio.

Con la prima valutazione il Giudice determina il numero delle quote (non inferiore a cento, né superiore a mille[19], fatto salvo quanto previsto dall'art. 25-*septies* "*Omicidio colposo o lesioni colpose gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*" che al primo comma in relazione al delitto di cui all'articolo 589 c.p. commesso con violazione dell'art. 55, comma 2, D. Lgs. 81/2008 prevede una sanzione pari a mille quote), tenendo conto:

– della gravità del fatto;

– del grado di responsabilità dell'Ente;

– dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Nel corso della seconda valutazione il Giudice determina, entro i valori minimi e massimi predeterminati in relazione agli illeciti sanzionati, il valore di ciascuna quota (da un minimo di Euro 258 ad un massimo di Euro 1.549) "*sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione*" (art. 11, comma 2, D. Lgs. 231/2001).

L'art. 12 del D. Lgs. 231/2001 prevede una serie di casi in cui la sanzione pecuniaria viene ridotta. Essi sono schematicamente riassunti nella tabella sottostante, con indicazione della riduzione apportata e dei presupposti per l'applicazione della riduzione stessa.

[19] Il numero massimo delle quote è stato innalzato a milleduecento per effetto del Decreto-legge 116/2025 limitatamente ad alcuni reati presupposto in materia ambientale

1/2 (e non può comunque essere superiore a Euro 103.291,38)	• L'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato un vantaggio o ne ha ricavato un vantaggio minimo; *oppure* • Il danno patrimoniale cagionato è di particolare tenuità.
da 1/3 a 1/2	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *oppure* • È stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
da 1/2 a 2/3	[Prima della dichiarazione di apertura del dibattimento di primo grado] • L'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; *e* • È stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Una significativa eccezione al criterio basato sul suddetto sistema delle quote è rappresentata dall'art. 6 del Decreto Legislativo 211/2025, che ha introdotto, relativamente ai reati in materia di violazione di misure restrittive dell'Unione europea, sanzioni pecuniarie nella percentuale dallo 0,5 al 5 per cento del fatturato globale dell'ente nell'esercizio finanziario precedente a quello in cui è stato commesso il reato o, se inferiore, nell'esercizio finanziario precedente l'applicazione della sanzione pecuniaria.

(b) Le sanzioni interdittive

Le sanzioni interdittive previste dal D. Lgs. 231/2001 sono:

1. l'interdizione dall'esercizio dell'attività;
2. il divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
3. la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
4. l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e la revoca di quelli eventualmente già concessi;
5. il divieto di pubblicizzare beni o servizi.

Differentemente dalla sanzione amministrativa pecuniaria, indefettibile, le sanzioni interdittive si applicano solo in relazione ai reati per i quali sono espressamente previste al ricorrere di almeno una delle condizioni di cui all'art. 13, D.Lgs.. 231/2001, di seguito indicate:

– "*l'ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative*";

– "*in caso di reiterazione degli illeciti*" (l'art. 20 specifica che si ha reiterazione "*quando l'ente già condannato in via definitiva almeno una volta per un illecito dipendente da reato, ne commette un altro nei cinque anni successivi alla condanna definitiva"*).

In ogni caso, non si procede all'applicazione delle sanzioni interdittive quando il reato è stato commesso nel prevalente interesse dell'autore o di terzi e l'Ente ne ha ricavato un vantaggio minimo o nullo, ovvero il danno patrimoniale cagionato è di particolare tenuità.

Esclude, altresì, l'applicazione delle sanzioni interdittive il fatto che l'Ente abbia posto in essere le condotte riparatorie previste dall'art. 17, D.Lgs. 231/2001 e, più precisamente, quando concorrono le seguenti condizioni:

– "*l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso*";

– "*l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi*";

– "*l'ente ha messo a disposizione il profitto conseguito ai fini della confisca*".

Le sanzioni interdittive hanno una durata compresa tra tre mesi e due anni e la scelta della misura da applicare e della sua durata viene effettuata dal Giudice sulla base degli stessi criteri in precedenza indicati per la commisurazione della sanzione pecuniaria, "*tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso*" (art. 14, D. Lgs. 231/2001). Gli artt. 25 comma 5 e 25 octies.2 del D.Lgs. 231/2001 prevedono una significativa eccezione, il primo con riguardo a taluni delitti di corruzione, il secondo relativamente ai reati in materia di violazione di misure restrittive dell'Unione europea, per i quali viene disposto un rilevante aumento della durata delle sanzioni interdittive:

– se il reato è commesso dal soggetto apicale, la durata delle sanzioni interdittive è compresa tra 4 e 7 anni ai sensi dell'art. 25 comma 5 e tra 2 e 6 anni ai sensi dell'art. 25 octies.2;

– se il reato è commesso dal soggetto "sottoposto", la durata delle sanzioni interdittive è compresa tra 2 e 4 anni ai sensi dell'art. 25 comma 5 e tra 1 e 3 anni ai sensi dell'art. 25 octies.2.

L'interdizione dell'attività ha natura residuale rispetto alle altre sanzioni interdittive.

Si precisa altresì che il Pubblico Ministero comunica l'iscrizione degli Enti indicati nel registro delle notizie di reato anche a Consob, Banca d'Italia e IVASS, in quanto quest'ultimi sono gli unici soggetti deputati all'esecuzione delle suddette sanzioni interdittive.

(c) La confisca

Ai sensi dell'art. 19, D.Lgs. 231/2001 è sempre disposta, con la sentenza di condanna, la confisca, anche per equivalente, del prezzo (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del profitto (utilità economica immediata ricavata) del reato, salvo per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede.

Come evidenziato dalla giurisprudenza (Cass., VI sez. pen. Sent. N. 34505 del 2012), per disporre il sequestro preventivo il Giudice deve valutare la concreta fondatezza dell'accusa e ravvisare gravi indizi di responsabilità dell'Ente.

(d) La pubblicazione della sentenza di condanna

La pubblicazione in uno o più giornali della sentenza di condanna, per estratto o per intero, può essere disposta dal Giudice, unitamente all'affissione nel comune dove l'Ente ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della Cancelleria del Giudice a spese dell'Ente.

1.4 Esenzione dalla responsabilità

Il D. Lgs. 231/2001 stabilisce che l'Ente non risponde dei reati sopraindicati nel caso in cui:

- i soggetti in posizione apicale e i soggetti subordinati abbiano agito nell'esclusivo interesse proprio o di terzi;
- i soggetti in posizione apicale abbiano agito eludendo fraudolentemente il Modello;
- la società provi di aver adottato ed efficacemente attuato "modelli di organizzazione, gestione e controllo" idonei a prevenire la realizzazione degli illeciti penali della specie di quello verificatosi (art. 6, D. Lgs. 231/2001);
- abbia affidato ad un organismo dell'Ente, dotato di autonomi poteri di iniziativa e controllo, il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

L'adozione di un Modello specificamente calibrato sui rischi-reato, cui è esposto concretamente l'Ente, volto ad impedire attraverso la fissazione di regole di condotta la commissione di determinati illeciti, adempie pertanto a una funzione preventiva e costituisce il primo presidio del sistema volto al controllo dei rischi.

L'Ente non sarà, dunque, assoggettato alla sanzione tutte le volte in cui dimostri di aver adottato ed attuato misure organizzative, gestionali e di controllo dirette a evitare la realizzazione del reato e, tali comunque, da risultare:

- idonee, vale a dire atte a garantire lo svolgimento delle attività nel rispetto della legge, nonché a individuare ed eliminare tempestivamente situazioni di rischio;
- efficaci, cioè proporzionate rispetto all'esigenza di assicurare il rispetto della legge e, quindi, oggetto di revisione periodica allo scopo di operare le eventuali modifiche che si rendano necessarie nel caso di significative violazioni delle prescrizioni, ovvero in caso di mutamenti nell'organizzazione o nell'attività. Deve, tra l'altro, essere previsto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure organizzative.

La Legge prevede, inoltre, che i Modelli possano essere adottati sulla base di codici di comportamento redatti dalle associazioni di categoria (“Linee Guida”), comunicati al Ministero di Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sulla idoneità dei modelli a prevenire i Reati.

2 I RIFERIMENTI UTILIZZATI PER L'ELABORAZIONE DEL MODELLO

La redazione del presente Modello ha tenuto conto, tra l'altro, della *best practice* di riferimento, con particolare riguardo alle Linee Guida Confindustria, alle Linee Guida ABI e alle indicazioni della giurisprudenza penale

2.1 Le Linee Guida Confindustria

Nelle Linee Guida Confindustria sono delineate le attività fondamentali che ciascun Ente deve svolgere, propedeutiche all'attuazione del proprio Modello, rappresentate:

- dall'identificazione dei rischi potenziali: ossia l'analisi del contesto aziendale per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati dal Decreto;
- dalla progettazione del sistema di controllo (cd. "protocolli" per la programmazione della formazione e attuazione delle decisioni dell'ente), ossia la valutazione del sistema esistente all'interno dell'Ente per la prevenzione dei reati ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente i rischi identificati.

Le componenti del sistema di controllo devono essere ispirate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione ("*ogni /operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua*");
- applicazione del principio di segregazione delle funzioni ("*nessuno può gestire in autonomia un intero processo*");
- documentabilità dei controlli ("*i controlli devono essere documentati*");
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del codice etico e dei Modelli;
- individuazione dei requisiti dell'OdV, come rappresentati al successivo paragrafo 5;
- previsione di modalità di gestione delle risorse finanziarie;
- obblighi di informazione nei confronti dell'OdV;
- previsione di un sistema interno di segnalazione delle violazioni (c.d. "*whistleblowing*").

Resta fermo che i Modelli adottati dagli Enti devono essere necessariamente redatti con specifico riferimento alla propria realtà concreta, e pertanto possono anche discostarsi dalle Linee Guida le quali, per loro natura, hanno carattere generale.

2.2 Le Linee Guida ABI

Le Linee Guida ABI stabiliscono che, al fine di ottemperare alle esigenze indicate dall'art. 6 del D. Lgs. 231/2001, "*ciascuna Società debba provvedere alla mappatura delle attività o funzioni aziendali nell'ambito delle quali possono essere commessi reati di cui al Decreto, al fine di commisurare i presidi da adottare in relazione all'esistenza di rischi concreti*".

Proseguendo nell'individuazione dei contenuti essenziali del modello organizzativo, il documento dell'associazione di categoria del settore bancario stabilisce, nella logica di enucleare appositi presidi preventivi a seconda delle macro-categorie di attività bancaria e dei connessi rischi di commissione dei reati, una sostanziale distinzione tra:

- reati cosiddetti *peculiari*, che possono presentare "*rischi di verificazione in ragione di specifiche attività della Società ed in relazione ai quali si rende necessaria la verifica dei sistemi di controllo relativi alle specifiche aree di rischio al fine del loro adeguamento alle prescrizioni del decreto*";
- reati cosiddetti *generali*, ossia "*non connessi, se non in virtù di un rapporto occasionale, allo svolgimento dell'impresa bancaria e quindi non riconducibili a specifiche aree di attività: in relazione a tali ipotesi si ritengono sufficienti modelli organizzativi generali, che richiamano i principi di correttezza e probità nei*

comportamenti degli operatori bancari".

Alla luce della distinzione sopraccitata, le Linee Guida ABI ritengono opportuno che l'Ente preveda, ovvero migliori laddove già esistenti, "*meccanismi di procedimentalizzazione delle decisioni, rendendo documentate e verificabili le varie fasi del processo decisionale, così da rendere inattuabili gestioni improprie di risorse finanziarie dell'ente*".

3 ADOZIONE DEL MODELLO

3.1 Il ruolo e le attività di UnipolPay

UnipolPay S.p.A. è un istituto di moneta elettronica iscritto all'albo di cui all'art. 114-quater del T.U.B., con decorrenza dal 5 luglio 2021, soggetto all'attività di direzione e coordinamento di Unipol Assicurazioni S.p.A. e da questa interamente controllato.

La Società ha conseguito l'autorizzazione di Banca d'Italia all'emissione di moneta elettronica e alla prestazione dei servizi di pagamento di cui all'art. 1, comma 2, lett. h-septies.1), nn. 3, 7 e 8 del TUB.

In particolare, UnipolPay si pone come centro di competenza delle soluzioni e delle esperienze di pagamento per il Gruppo Unipol, inteso come società del Gruppo e altri attori ad esso connessi (es. fornitori, *partner,* etc.). In tale ambito si iscrivono i prodotti "Conto Corporate" e "Conto Partner" che prevedono la prestazione di servizi di pagamento (es. l'esecuzione di bonifici SEPA, in invio e in ricezione, e di operazioni PagoPA, nonché l'incasso di addebiti diretti) e di servizi accessori a valore aggiunto (es. il servizio di verifica del beneficiario, il servizio IBAN Check, etc.).

3.2 Il sistema di controllo interno e di gestione dei rischi di UnipolPay

Il sistema di controllo interno e di gestione dei rischi, elemento fondante del sistema di governo societario, è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della Società. In particolare, mira ad assicurare, tra l'altro:

- l'efficienza e l'efficacia dei processi aziendali;
- l'identificazione, la valutazione anche prospettica, la gestione e l'adeguato controllo dei rischi;
- l'adeguatezza e la tempestività del sistema di *reporting* delle informazioni aziendali;
- l'affidabilità e l'integrità delle informazioni contabili e gestionali, nonché delle procedure informatiche;
- la salvaguardia del valore del patrimonio aziendale, anche in un'ottica di medio-lungo periodo;
- la conformità dell'attività dell'impresa alla normativa vigente, alle direttive ed alle procedure aziendali.

Il sistema di controllo interno e di gestione dei rischi viene definito nelle Direttive in materia di Sistema di Governo Societario di Gruppo che definiscono, tra l'altro, il ruolo e le responsabilità dei soggetti coinvolti.

Il sistema di controllo interno e di gestione dei rischi è impostato, tra l'altro, secondo i seguenti principi:

- separazione di compiti e responsabilità: le competenze e le responsabilità sono ripartite tra gli organi e le strutture aziendali in modo chiaro, al fine di evitare mancanze o sovrapposizioni che possano incidere sulla funzionalità aziendale;
- formalizzazione: l'operato dell'organo amministrativo e dei soggetti delegati deve essere sempre documentato, al fine di consentire il controllo sugli atti gestionali e sulle decisioni assunte;
- integrità, completezza e correttezza dei dati conservati: il sistema di registrazione dei dati e della relativa reportistica deve garantire di disporre di adeguate informazioni.

In particolare, quali specifici strumenti diretti a programmare la formazione e l'attuazione delle decisioni della Società anche in relazione ai reati da prevenire, la medesima opera in base a:

- la normativa italiana e straniera, anche regolamentare, applicabile;
- lo Statuto sociale;
- la Carta dei Valori e il Codice Etico del Gruppo Unipol;
- il sistema di autoregolamentazione della disciplina aziendale, come declinato nel successivo paragrafo 3.3;
- il sistema delle deleghe di poteri in essere;

- il sistema disciplinare e sanzionatorio di cui al Contratto Collettivo Nazionale di Lavoro ed allo Statuto dei Lavoratori.

I principali organi che svolgono attività di supervisione, controllo, monitoraggio e vigilanza nella Società sono:

- Consiglio di Amministrazione;
- Collegio Sindacale;
- Organismo di Vigilanza ai sensi del D.Lgs. 231/2001.

Sono inoltre istituite presso la Società, nel rispetto delle disposizioni di vigilanza applicabili agli istituti di moneta elettronica, le funzioni aziendali di controllo di compliance, risk management, antiriciclaggio, mentre la funzione di revisione interna è esternalizzata a Unipol.

3.3 Il sistema normativo interno del Gruppo

La Capogruppo ha adottato un articolato sistema di autoregolamentazione della disciplina aziendale, applicabile a tutte le Società del Gruppo, costituito da diverse tipologie di documenti di comunicazione aziendale (i "DCA").

Le principali tipologie di DCA sono classificate in funzione del contenuto e dell'ambito di applicazione.

I DCA approvati dal Consiglio di Amministrazione della Capogruppo e/o delle Società del Gruppo e rivolti esclusivamente al personale dipendente sono:

- Politica e Procedura di emanazione consiliare di Gruppo
- Politica e Procedura di emanazione consiliare di Società.

Con riferimento ai restanti DCA, quelli che si rivolgono esclusivamente al personale dipendente operante per le Società del Gruppo sono:

- Ordine di Servizio (anche "ODS")
- Disposizione Interna
- Regola Operativa (anche "ROP")
- Procedura Tecnica di Settore (anche "PTS").

I DCA che possono rivolgersi sia al personale dipendente operante per le Società del Gruppo, sia alle Reti di Vendita sono:

- Comunicato (anche "COM")
- Circolare (anche "CIR")

Unipol ha definito, altresì, l'insieme delle verifiche preventive, svolte da specifiche Funzioni aziendali, prodromiche alla pubblicazione dei DCA, al fine di assicurare l'adeguatezza di ogni documento rispetto alle materie di propria competenza.

Tutti i DCA sono pubblicati all'interno della rete intranet aziendale o altro repository in essere al fine di consentirne la presa visione da parte di tutti i destinatari.

3.4 Principi generali di controllo

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di:

- esplicita formalizzazione delle norme comportamentali;
- chiara, formale e conoscibile descrizione ed individuazione delle attività, dei compiti e dei poteri attribuiti a ciascuna funzione e alle diverse qualifiche e ruoli professionali;
- precisa descrizione delle attività di controllo e loro tracciabilità;
- adeguata segregazione di ruoli operativi e ruoli di controllo.

In particolare, devono essere perseguiti i seguenti principi:

Norme comportamentali

- deve essere prevista l'esistenza di un Codice Etico che descriva regole comportamentali di carattere generale a presidio delle attività svolte;
- i sistemi premianti e di incentivazione della Società devono essere concepiti per assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente Modello, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

Definizioni di ruoli e responsabilità

- la regolamentazione interna deve declinare ruoli e responsabilità delle unità organizzative a tutti i livelli, descrivendo le attività proprie di ciascuna struttura;
- tale regolamentazione deve essere resa disponibile e conosciuta all'interno dell'organizzazione.

Procedure e norme interne

- le attività sensibili devono essere regolamentate, in modo coerente e congruo, attraverso strumenti normativi aziendali, così che in ogni momento si possano identificare le modalità operative di svolgimento delle attività, dei relativi controlli e le responsabilità di chi ha operato;
- deve essere individuato un Responsabile per ciascun processo aziendale, tipicamente coincidente con il responsabile della struttura organizzativa competente per la gestione dell'attività stessa.

Segregazione dei compiti

- all'interno di ogni processo aziendale rilevante, devono essere separate le funzioni o i soggetti incaricati della decisione e della sua attuazione rispetto a chi la registra e chi la controlla;
- non deve esservi identità soggettiva tra coloro che assumono o attuano le decisioni, coloro che elaborano evidenza contabile delle operazioni decise e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno.

Poteri autorizzativi e di firma

- deve essere definito un sistema di deleghe all'interno del quale vi sia una chiara identificazione ed una specifica assegnazione di poteri e limiti ai soggetti che operano impegnando la Società e manifestando la sua volontà;
- i poteri organizzativi e di firma (deleghe, procure e connessi limiti di spesa) devono essere coerenti con le responsabilità organizzative assegnate;
- le procure devono essere coerenti con il sistema interno delle deleghe;
- devono essere previsti meccanismi di pubblicità delle procure verso gli interlocutori esterni;
- il sistema di deleghe deve identificare, tra l'altro:
  - i requisiti e le competenze professionali che il delegato deve possedere in ragione dello specifico ambito di operatività della delega;
  - le modalità operative di gestione degli impegni di spesa;
- le deleghe devono essere attribuite secondo i principi di:
  - autonomia decisionale e finanziaria del delegato;
  - idoneità tecnico-professionale del delegato;
  - disponibilità autonoma di risorse adeguate al compito e continuità delle prestazioni.

Attività di controllo e tracciabilità

- nell'ambito delle procedure o di altra regolamentazione interna devono essere formalizzati i controlli operativi e le loro caratteristiche (responsabilità, evidenza, periodicità);
- i documenti rilevanti per lo svolgimento delle attività sensibili devono essere adeguatamente formalizzati e riportare la data di compilazione, presa visione del documento e la firma riconoscibile del compilatore; gli stessi devono essere archiviati in luoghi idonei alla conservazione, al fine di tutelare la riservatezza dei dati in essi contenuti e di evitare danni, deterioramenti e smarrimenti;

- devono essere ricostruibili la formazione degli atti e i relativi livelli autorizzativi, lo sviluppo delle operazioni, materiali e di registrazione, con evidenza della loro motivazione e della loro causale, a garanzia della trasparenza delle scelte effettuate;
- il responsabile dell'attività deve produrre e mantenere adeguati report che contengano evidenza dei controlli effettuati e di eventuali anomalie;
- deve essere prevista, laddove possibile, l'adozione di sistemi informatici, che garantiscano la corretta e veritiera imputazione di ogni operazione, o di un suo segmento, al soggetto che ne è responsabile e ai soggetti che vi partecipano;
- il sistema deve prevedere l'impossibilità di modifica (non tracciata) delle registrazioni;
- i documenti riguardanti l'attività della Società, ed in particolare i documenti o la documentazione informatica riguardanti attività sensibili devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- l'accesso ai documenti già archiviati deve essere sempre motivato e consentito solo alle persone autorizzate in base alle norme interne, al Collegio Sindacale, all'Area Audit di Unipol, alle Funzioni Risk Management e Compliance della Società e all'OdV, per quanto di competenza;
- i processi affidati in *outsourcing*, specialmente se riguardano attività sensibili, devono essere attentamente monitorati.

3.5 Funzione e scopo del Modello

UnipolPay, ravvisando nella correttezza e nella trasparenza i presupposti per lo svolgimento dell'attività aziendale, ha inteso dotarsi di un modello di organizzazione, gestione e controllo idoneo a prevenire la commissione di comportamenti illeciti da parte dei destinatari.

Sebbene l'adozione del Modello non costituisca un obbligo imposto dal Decreto, bensì una scelta facoltativa rimessa a ciascun singolo ente, UnipolPay ha deciso di adeguarsi alle prescrizioni del Decreto.

Scopo del MOG è, pertanto, prevedere un sistema strutturato e organico di prevenzione, dissuasione e controllo, finalizzato a sviluppare nei soggetti che, direttamente o indirettamente, operano nell'ambito delle attività sensibili, la consapevolezza di poter determinare, in caso di comportamenti illeciti, conseguenze sanzionatorie non solo per sé stessi, ma anche per la Società.

Il Modello predisposto dalla Società sulla base dell'individuazione delle attività nell'ambito delle quali si potrebbe, in astratto, configurare il rischio di commissione di reati, si propone come finalità quelle di:

- creare, in tutti coloro che svolgono, in nome, per conto e nell'interesse della Società attività a rischio reato, come meglio individuate nelle Parti Speciali del presente documento, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni riportate nel MOG, in un illecito passibile di sanzioni, sul piano penale e amministrativo, irrogabili non solo nei loro confronti, ma anche nei confronti di UnipolPay;
- condannare ogni forma di comportamento illecito da parte della Società, in quanto contrari, oltre che alle disposizioni di legge, anche ai principi etici adottati dalla stessa;
- garantire alla Società, grazie all'azione di controllo delle attività a rischio reato, la concreta ed effettiva possibilità di intervenire tempestivamente per prevenire la commissione dei reati stessi.

Il Modello si propone, altresì, di:

- introdurre, integrare, sensibilizzare, diffondere e circolarizzare a tutti i livelli aziendali le regole di condotta ed i protocolli per la programmazione della formazione e dell'attuazione delle decisioni della Società, al fine di gestire e, conseguentemente, evitare il rischio della commissione di reati;
- informare tutti coloro che operano con la Società che la violazione delle prescrizioni contenute nel MOG comporterà l'applicazione di apposite penali ovvero la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società;
- individuare preventivamente le attività a rischio reato, con riferimento alle attività svolte dalla Società;

- dotare l'OdV di adeguati poteri al fine di porlo in condizione di vigilare efficacemente sull'effettiva attuazione, sul costante funzionamento ed aggiornamento del Modello, nonché di valutare il mantenimento nel tempo dei requisiti di solidità e funzionalità del MOG medesimo;
- garantire la registrazione corretta e conforme ai protocolli di tutte le operazioni della Società nell'ambito delle attività a rischio reato, al fine di rendere possibile una verifica ex post dei processi di decisione, la loro autorizzazione ed il loro svolgimento all'interno di UnipolPay. Il tutto conformemente al principio di controllo espresso nelle Linee Guida Confindustria in virtù del quale "*ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua*";
- assicurare l'effettivo rispetto del principio della separazione delle funzioni aziendali, in ossequio al principio di controllo secondo il quale "*nessuno può gestire in autonomia un intero processo*", in modo tale che l'autorizzazione all'effettuazione di un'operazione sia sotto la responsabilità di una persona diversa da quella che la contabilizza, la esegue operativamente o la controlla;
- delineare e delimitare le responsabilità nella formazione e nell'attuazione delle decisioni della Società;
- stabilire che i poteri autorizzativi siano assegnati in coerenza con le responsabilità organizzative e gestionali assegnate, che siano rese note le deleghe di potere, le responsabilità ed i compiti all'interno di UnipolPay e che gli atti con i quali si conferiscono poteri, deleghe e autonomie siano compatibili con i principi di controllo preventivo;
- individuare le modalità di gestione delle risorse finanziarie, tali da impedire la commissione dei reati;
- valutare l'attività di tutti i soggetti che interagiscono con UnipolPay, nell'ambito delle aree a rischio di commissione di reati, nonché il funzionamento del Modello, curandone il necessario aggiornamento periodico in senso dinamico, nell'ipotesi in cui le analisi e le valutazioni operate rendano necessario effettuare correzioni, integrazioni ed adeguamenti.

Attraverso il Modello, infatti, si consolida un sistema strutturato ed organico di procedure ed attività di controllo (*ex ante* ed *ex post*) che ha come obiettivo la riduzione del rischio di commissione dei reati mediante l'individuazione dei processi sensibili e la loro conseguente proceduralizzazione.

Tra le finalità del Modello vi è, quindi, quella di sviluppare la consapevolezza nei dipendenti, organi sociali, consulenti a qualsiasi titolo, collaboratori e *partner*, che svolgano, per conto e nell'interesse della Società, attività a rischio reato, di poter incorrere, in caso di comportamenti non conformi alle prescrizioni del Modello, nonché delle norme del Codice Etico e alle altre norme e procedure aziendali (oltre che alla legge), in illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

Inoltre, si intende censurare fattivamente ogni comportamento illecito attraverso la costante attività di controllo dell'OdV sui processi sensibili e la comminazione, da parte di UnipolPay, di sanzioni disciplinari o contrattuali.

3.6 La costruzione del Modello e la sua struttura

La predisposizione e l'aggiornamento del presente MOG sono state precedute da una serie di attività preparatorie suddivise in differenti fasi e dirette alla costruzione di un sistema di prevenzione e gestione dei rischi, in linea con le disposizioni del D. Lgs. 231/2001 e ispirate, oltre che alle norme in esso contenute, anche ai principi e suggerimenti dettati al riguardo dalle Linee Guida ABI e Confindustria.

Si descrivono qui di seguito, brevemente, le fasi in cui si articolano la predisposizione e l'aggiornamento del MOG.

a. Fase preliminare

In tale fase, finalizzata alla predisposizione della documentazione di supporto ed alla pianificazione delle attività di rilevazione, sono state condotte analisi puntuali sulla documentazione esistente (organigrammi, rilevazioni di processo, rilevazioni e valutazione dei rischi e controlli) e confronti con le funzioni aziendali interessate, allo scopo di identificare i soggetti, apicali e sottoposti, da coinvolgere nella successiva fase di valutazione dei rischi e del sistema dei controlli.

Inoltre, sono state individuate le aree di attività (ambiti societari, ambiti organizzativi, processi e sottoprocessi operativi) nelle quali esiste il rischio di commissione dei reati previsti dal D. Lgs. 231/2001 (matrice processi/reati - cfr. tabella MACROPROCESSI) e, allo scopo di facilitare la successiva fase di valutazione dei rischi, sono state identificate le possibili modalità di estrinsecazione delle condotte illecite.

b. Fase di mappatura rischi e controlli

In tale fase, tenuto conto anche di quanto suggerito dalle Linee Guida Confindustria, è stata effettuata un'approfondita indagine della complessiva organizzazione di UnipolPay, ovvero una ricognizione delle aree, dei settori e degli uffici, delle relative funzioni e procedure e delle entità esterne, in vario modo correlate con la Società.

Per ciascuna di tali aree sono state condotte puntuali analisi documentali e interviste alle figure apicali e sottoposte coinvolte nelle attività esaminate, per identificare i reati potenzialmente commissibili, le concrete modalità di commissione, la natura dei controlli esistenti (ad es. quelli di tipo organizzativo connessi alla chiara individuazione e segregazione di responsabilità e funzioni; quelli di tipo procedurale, connessi alla formalizzazione delle attività in regole interne; quelli derivanti dalle soluzioni ICT attraverso la previsione di passaggi formali obbligatori, ecc.) e la loro efficacia. Nel dettaglio si è proceduto a:

- analizzare l'operatività della Società con riferimento ai cosiddetti processi "sensibili" nell'ambito dei quali possono essere commessi reati ex D. Lgs. 231/2001;
- descrivere, nell'ambito organizzativo analizzato, le posizioni e i soggetti coinvolti, le loro responsabilità ed i loro poteri, distinguendo fra figure "apicali" o "sottoposte", così come indicato nel D. Lgs. 231/2001;
- identificare e descrivere i reati commissibili e le conseguenze che essi potrebbero avere;
- individuare e descrivere le possibili condotte illecite proprie dell'attività in esame, ossia le modalità pratiche attraverso cui i reati potrebbero essere commessi;
- individuare in maniera puntuale i controlli esistenti (preventivi e successivi) e valutare l'allineamento della struttura di controllo ai dettami del D. Lgs. 231/2001 in termini di esistenza, efficacia ed efficienza dei controlli, esistenza di procedure formalizzate, adeguatezza del sistema delle deleghe e procure, esistenza e adeguatezza del sistema disciplinare.

La fase di rilevazione dei rischi e dei controlli ha consentito di pervenire alla identificazione delle funzioni e dei soggetti coinvolti nell'ambito dei processi sensibili, della loro responsabilità, nonché dei sistemi di controllo adottati per la mitigazione dei rischi.

c. Fase di valutazione rischi e controlli

In tale fase si è provveduto, per ciascuno dei processi sensibili, alla valutazione del grado di rischiosità con il metodo del "*Control and Risk Assessment*" (Valutazione di Controlli e Rischi Guidata):

- insieme al responsabile di ciascun processo, si è valutato il rischio che, in tale ambito, vengano commessi illeciti amministrativi dipendenti da reato, tenuto conto del grado di efficacia e di efficienza delle procedure e dei sistemi di controllo esistenti all'interno del processo, in quanto idonei a valere anche come misure di prevenzione dei reati;
- sulla base di dette valutazioni sono state determinate le eventuali criticità, sotto il profilo del rischio ai sensi del D. Lgs. 231/2001, nell'ambito di ciascun processo;
- in relazione ai rischi rilevati e alle relative criticità, sono state individuate le opportune azioni correttive per ridurre il livello di criticità e migliorare il sistema dei controlli.

Affinché tale momento potesse rappresentare una reale occasione di sensibilizzazione e coinvolgimento, l'intero processo valutativo e le relative evidenze emerse sono state condivise con il *management*.

Al fine di fornire una adeguata formalizzazione alle rilevazioni condotte, viene utilizzato un sistema informativo specifico adottato dalle Funzioni Audit, Risk Management e Compliance presenti nel Gruppo, che permette di gestire le mappature dei rischi effettuate ai sensi del Decreto, coerentemente ai modelli di rilevazione dei processi aziendali e di generale valutazione dei rischi operativi, consentendo di:

- disporre di un'unica base dati per l'archiviazione di tutte le informazioni raccolte;
- valutare sulla base di metriche concordate a livello di Gruppo il livello di rischio effettivo sulle singole aree oggetto di rischi ai sensi del D. Lgs. 231/2001;
- fornire una valutazione dei rischi ai sensi del D. Lgs. 231/2001;
- identificare e gestire il piano di interventi di miglioramento scaturiti dall'analisi condotta.

3.7 Definizione dei Protocolli: individuazione e analisi dei processi sensibili

UnipolPay ha individuato alcuni processi sensibili nel cui ambito potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati richiamati dal D.Lgs. 231/2001 (cfr. tabella MACROPROCESSI).

Con riferimento a tali processi, sono state, pertanto, rilevate le procedure di gestione e di controllo in essere e sono state definite, ove ritenuto opportuno, le eventuali implementazioni necessarie, nel rispetto dei seguenti principi:

- segregazione funzionale delle attività operative e di controllo;
- documentabilità delle operazioni a rischio e dei controlli posti in essere per impedire la commissione di reati;
- ripartizione e attribuzione dei poteri autorizzativi e decisionali, delle competenze e responsabilità, basate su principi di trasparenza, chiarezza e verificabilità e coerenti con l'attività in concreto svolta;
- sicurezza degli accessi e tracciabilità dei flussi finanziari.

Tale processo di rilevazione, per operare efficacemente, deve essere svolto nel continuo o comunque svolto con una periodicità adeguata e deve essere rivisto con particolare attenzione in occasione di cambiamenti aziendali (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, modifiche della struttura organizzativa, ecc.), ovvero di introduzione di nuovi reati.

3.8 Definizione dei principi etici

UnipolPay ha adottato la Carta dei Valori ed il Codice Etico del Gruppo Unipol, che ne costituiscono l'impianto valoriale.

Nella Carta dei Valori sono stati pertanto individuati i cinque principi di seguito elencati:

- Accessibilità: favorisce la disponibilità reciproca e il confronto, generando quindi più efficacia organizzativa;
- Lungimiranza: favorisce l'attitudine a interpretare correttamente i segnali del mercato anticipandone le tendenze, generando continuità nei risultati e sviluppo dei profitti in un'ottica di sostenibilità "allargata", che sappia coniugare, e nello stesso tempo favorirne il miglioramento, esigenze ambientali, economiche e sociali per permettere all'impresa di progredire nel lungo periodo;
- Rispetto: favorisce l'ascolto delle esigenze di tutti gli interlocutori, generando qualità del servizio e riconoscimento reciproco;
- Solidarietà: favorisce l'attitudine alla collaborazione e alla fiducia nelle regole, generando efficienza gestionale;
- Responsabilità: è il motore dell'affidabilità professionale, che permette di rispondere di quanto si fa nei tempi e nei modi definiti dalle regole del settore, del mercato e della propria etica societaria.

Il Codice Etico di Gruppo ha le seguenti peculiarità:

- adotta la formulazione c.d. *principle based*, ovverosia richiama principi e non descrive comportamenti;
- il suo impianto eredita sia la struttura, sia i contenuti della Carta dei Valori; è ispirato a un approccio formativo ed educativo;
- adotta appositi dispositivi di "giustizia riparativa" tesi a individuare comportamenti in grado di ripristinare, nei modi ritenuti più opportuni, lo status quo ante le violazioni accertate.

È stato nominato l'Ethics Officer del Gruppo Unipol, quale figura di riferimento proattiva a cui rivolgersi per ottenere pareri e/o consigli in merito alla corretta applicazione del Codice Etico e come centro di raccolta e filtraggio delle eventuali segnalazioni di violazione.

Il Codice Etico dovrà trovare apposite forme di impegno al suo rispetto da parte di tutti coloro che operano nell'orbita del Gruppo Unipol. L'impegno sui valori è riferito agli *stakeholder* del Gruppo, identificati in sei categorie di soggetti:

- azionisti ed investitori;
- dipendenti e collaboratori;
- clienti;
- fornitori;

- comunità civile;
- generazione future.

I principi di riferimento del presente Modello si integrano, quindi, con quelli della Carta dei Valori e del Codice Etico adottato da UnipolPay, anche se il Modello, dando attuazione alle disposizioni di cui al D. Lgs. 231/2001, ha portata e finalità diverse rispetto al Codice Etico.

Sotto tale profilo, infatti, si rende opportuno precisare che:

- il Codice Etico ha una portata generale, in quanto contiene una serie di principi di "deontologia aziendale" che UnipolPay riconosce come propri e sui quali intende richiamare l'osservanza di tutti coloro che cooperano al perseguimento dei fini aziendali;
- il presente Modello risponde e soddisfa, invece, conformemente a quanto previsto nel D. Lgs.231/2001, l'esigenza di predisporre un sistema di regole interne dirette a prevenire la commissione di particolari tipologie di illeciti.

3.9 La procedura di adozione del Modello

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, il Consiglio di Amministrazione della Società, in conformità alle proprie politiche aziendali, ha ritenuto di procedere in tal senso.

Contestualmente all'adozione del Modello è stato nominato l'OdV, quale organismo dell'Ente avente il compito di vigilare sul funzionamento ed osservanza del Modello, nonché di curarne l'aggiornamento (cfr. capitolo 5).

Le successive modifiche e integrazioni sostanziali del Modello sono rimesse alla competenza del Consiglio di Amministrazione di UnipolPay, anche su proposta e comunque previo parere dell'OdV, essendo il Modello un "*atto di emanazione dell'organo dirigente*" in conformità alle prescrizioni dell'art. 6 del D. Lgs. 231/2001.

Nella riunione consiliare del 28 settembre 2026, il Consiglio di Amministrazione di UnipolPay ha approvato l'aggiornamento del presente Modello ed ha espressamente dichiarato di impegnarsi al rispetto dello stesso. Il Collegio Sindacale ha preso atto del presente Modello e si è impegnato formalmente al rispetto del Modello medesimo.

Relativamente all'ambito di applicazione del MOG, occorre inoltre considerare che talune attività sono esternalizzate da UnipolPay alla controllante Unipol e ad altri fornitori.

L'estensione del presente Modello nei confronti degli *outsourcer* deve ritenersi limitata allo svolgimento dei processi sensibili effettuati dai medesimi in nome e per conto di UnipolPay e avviene sulla base di accordi contrattuali che disciplinano i rapporti tra la Società e gli *outsourcer,* prevedendo un'accurata disciplina dei controlli da parte della Società e le relative periodiche attività di *reporting*.

Ad ogni modo, Unipol ha adottato un proprio Modello organizzativo ai sensi del D.Lgs. 231/2001 che racchiude e coordina numerosi presidi etici, organizzativi, gestionali e di controllo.

Su tale circostanza UnipolPay ripone ulteriore affidamento per la costruzione e l'attuazione del proprio sistema di controllo ai sensi e per gli effetti del D.lgs. 231/2001.

I collaboratori e i fornitori sono tenuti a rilasciare a UnipolPay una dichiarazione ove si attesti la integrale conoscenza dei contenuti e prescrizioni contenute nel D. Lgs. 231/2001 e l'impegno al rispetto dello stesso, prevedendo specifica informativa nell'ambito del contratto.

4 I PROCESSI AZIENDALI ESPOSTI ALLA COMMISSIONE DEI REATI INDICATI NEL D. LGS. 231/2001

A seguito di una dettagliata analisi dell'operatività aziendale e della mappatura dei rischi ex D. Lgs. 231/2001, UnipolPay è giunta all'individuazione dei processi aziendali rilevanti ai fini del D. Lgs. 231/2001, ossia i cosiddetti processi sensibili.

Dall'analisi svolta, emerge che le categorie di reato che potrebbero essere commessi nell'ambito dei processi aziendali sensibili sono le seguenti:

1. Delitti nei rapporti con la Pubblica Amministrazione;
2. Reati societari;
3. Delitti e illeciti amministrativi di abuso di informazioni privilegiate, manipolazione del mercato e aggiotaggio;
4. Delitti di ricettazione, riciclaggio, autoriciclaggio e delitti con finalità di terrorismo o di eversione dell'ordine democratico;
5. Delitti informatici;
6. Omicidio colposo o lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
7. Delitti di criminalità organizzata e reati transnazionali;
8. Reati ambientali;
9. Delitti in materia di violazione del diritto d'autore;
10. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
11. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
12. Intermediazione illecita e sfruttamento del lavoro;
13. Reati tributari;
14. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori;
15. Reati in materia di violazione delle misure restrittive dell'Unione europea.

Di seguito, si riporta una tabella che rappresenta la corrispondenza tra le categorie di reato sopra elencate e i processi aziendali, opportunamente raggruppati in categorie più ampie denominate "macroprocessi", in cui le fattispecie illecite potrebbero essere commesse.

MACROPROCESSI	PA	Societari	Mkt abuse	Ricettazione, autoriciclaggio e terrorismo	Informatici	Omicidio colposo/lesioni colpose	Criminalità organizzata e transnazionali	Ambientali	Violazione diritto autore	Impiego irregolari	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci	Intermediazione illecita e sfruttamento lavoro	Tributari	Mezzi di pagamento e trasferimento valori	Misure restrittiv
Gestione del rapporto[20]	✔	✔		✔			✔								✔
Customer Service	✔	✔		✔			✔							✔	
Incassi e pagamenti	✔	✔		✔			✔								
Amministrazione	✔	✔	✔	✔			✔						✔		
Gestione del rischio e determinazione del patrimonio di vigilanza		✔					✔								
Gestione tesoreria aziendale	✔	✔		✔			✔								
Gestione organi sociali e partecipazioni		✔	✔				✔							✔	
Gestione della compliance		✔					✔								
Gestione dei controlli interni		✔					✔								
Sviluppo e gestione del piano di marketing	✔	✔	✔				✔								
Gestione dei canali di contatto con la clientela							✔							✔	
Gestione sicurezza (informatica e nei luoghi di lavoro)	✔	✔			✔	✔	✔		✔			✔			
Gestione sistemi informativi	✔	✔			✔		✔		✔						
Relazioni esterne	✔	✔					✔								
Risorse umane	✔	✔				✔	✔			✔	✔	✔	✔		
Supporto e consulenza legale e tributaria	✔	✔		✔			✔				✔				✔
Acquisti e supporto logistico e tecnico	✔	✔		✔		✔	✔	✔		✔		✔	✔		

5 L'ORGANISMO DI VIGILANZA

5.1 Individuazione, requisiti e nomina dell'Organismo di Vigilanza

a) nomina e composizione dell'Organismo di Vigilanza

Il Decreto prevede l'istituzione di un Organismo di Vigilanza interno all'Ente dotato di autonomi poteri di iniziativa e di controllo, cui è assegnato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

In ottemperanza a quanto stabilito dall'art. 6, comma 1, lett. b) del D. Lgs. 231/2001 la Società identifica l'OdV in un organo collegiale, composto da massimo tre membri, individuati come segue:

- un amministratore non esecutivo o un sindaco, in quanto dotato della visibilità e del potere di farsi diretto portavoce anche in occasione delle sedute del Consiglio di Amministrazione degli orientamenti e delle decisioni assunte dall'OdV per assicurare una concreta ed efficace implementazione del Modello, ovvero da un terzo esterno alla Società;
- il Responsabile (o un esponente) della Funzione Compliance di UnipolPay ovvero il titolare (o un esponente) dell'Area Compliance di Unipol, in quanto dotato di specifiche professionalità, di conoscenza delle strutture societarie e dell'organizzazione;
- il titolare (o un esponente) dell'Area Audit di Unipol, in quanto dotato di una strutturale indipendenza e autonomia dalle aree operative della società, oltre che del potere/dovere di svolgere una costante attività di verifica sul corretto funzionamento dei sistemi dei controlli della Società.

In coerenza con quanto normativamente prescritto, tale composizione assicura la sussistenza dei requisiti di autonomia e indipendenza, professionalità ed efficienza operativa dell'OdV.

Il compenso dei membri dell'OdV è determinato dal Consiglio di Amministrazione al momento della nomina e rimane invariato per l'intero periodo di durata dell'incarico.

Inoltre, il Consiglio di Amministrazione, annualmente e su proposta dell'OdV, approva la previsione delle spese, anche di carattere straordinario, necessarie allo svolgimento, delle attività di vigilanza e controllo previste dal Modello, nonché il consuntivo delle spese eventualmente sostenute nell'anno precedente.

b) requisiti soggettivi di eleggibilità dei componenti dell'Organismo di Vigilanza

I componenti dell'OdV devono essere in possesso di particolari requisiti soggettivi in funzione degli specifici compiti loro affidati.

Il requisito di professionalità richiede che i membri dell'OdV abbiano competenze in materia giuridica, economica e finanziaria, al fine di garantire l'efficacia dei poteri di controllo e propositivo ad essi demandati.

Il profilo professionale e personale di ciascun componente dell'OdV deve altresì essere idoneo a garantire autorevolezza, imparzialità di giudizio ed eticità della condotta.

I membri dell'Organismo devono attestare:

- di non avere relazioni di coniugio, parentela o affinità entro il 4° grado incluso, con componenti dell'organo decisionale dell'Ente o della Società di Revisione, o con i revisori incaricati dalla Società di Revisione, o tra di loro;
- di non essere membri esecutivi dell'organo decisionale dell'Ente o della Società di Revisione;
- di non essere portatori di conflitti di interesse, anche potenziali, con l'Ente tali da pregiudicare la propria indipendenza;
- di non aver svolto funzioni di amministrazione, direzione o controllo in imprese sottoposte a fallimento, liquidazione coatta amministrativa o procedure equiparate ovvero in imprese operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedura di amministrazione straordinaria;

- di non essere stati assoggettati a misure di prevenzione disposte dall'Autorità giudiziaria ai sensi del D. Lgs. 159/2011 e s.m.i., salvi gli effetti della riabilitazione;
- di non essere stati condannati con sentenza, anche non definitiva, per reati previsti dal D. Lgs. 231/2001, salvi gli effetti della riabilitazione.

I membri dell'OdV si impegnano a comunicare immediatamente alla Società e al Consiglio di Amministrazione qualsiasi evento che comporti la perdita, anche solo temporanea, di uno o più dei sopra descritti requisiti.

Il Consiglio di Amministrazione valuta, preventivamente all'insediamento dell'interessato nel ruolo di membro dell'OdV, e successivamente, con periodicità annuale oppure al momento di ricezione della comunicazione di cui al capoverso precedente, la sussistenza dei suddetti requisiti soggettivi o comunque l'idoneità dei componenti dell'OdV a ricoprire l'incarico a essi assegnato.

Il mancato possesso, prima dell'insediamento, o il venire meno, in costanza di mandato, di uno o più dei requisiti indicati dalla lettera b) del presente paragrafo, ovvero l'insorgenza di cause di incompatibilità, determina l'ineleggibilità o la decadenza dall'incarico. Con riferimento al requisito di cui alla lettera b), numero 4., del presente paragrafo, il mancato possesso, prima dell'insediamento, o il venire meno, in costanza di mandato, dello stesso, non comporta l'automatica ineleggibilità o decadenza del membro dell'OdV, ma richiede una valutazione da parte del Consiglio di Amministrazione. La valutazione è condotta avendo riguardo agli obiettivi di sana e prudente gestione nonché di salvaguardia dell'impresa e della fiducia del pubblico. Nel caso in cui, all'esito della predetta valutazione, emerga un quadro grave, preciso e concordante su condotte che possono porsi in contrasto con gli obiettivi di cui sopra, il componente dell'OdV è dichiarato ineleggibile o decade dall'incarico. In tali casi, il Consiglio di Amministrazione provvede tempestivamente alla nomina di altro componente o alla sostituzione del componente decaduto, nel rispetto dei principi indicati.

Il membro così nominato resterà in carica fino al termine del mandato dell'OdV in carica.

c) autonomia, Indipendenza

L'OdV deve essere dotato, nella sua collegialità, di specifici requisiti di autonomia, indipendenza e professionalità.

I predetti requisiti presuppongono che l'Organismo:

- svolga le attività di competenza con continuità d'azione;
- sia composto da soggetti le cui condizioni personali e/o gli interessi non confliggano con l'incarico affidato, né incidano sull'alto grado di autorevolezza necessario per esercitare la rispettiva indipendenza di giudizio e di valutazione;
- riferisca della propria attività esclusivamente al Consiglio di Amministrazione e mantenga contatti con il Collegio Sindacale e la Società di Revisione.

d) durata in carica e cause di cessazione dei componenti dell'Organismo di Vigilanza

La durata in carica dell'OdV è pari a quella del Consiglio di Amministrazione.

L'OdV viene nominato nella prima riunione utile del Consiglio di Amministrazione successiva all'Assemblea di nomina del Consiglio di Amministrazione e decade alla data del rinnovo del Consiglio di Amministrazione medesimo.

La cessazione dalla carica o dal ruolo aziendale ricoperto dal/dai componente/i interno/i determina la cessazione dell'incarico di componente dell'OdV. In tal caso, il Consiglio di Amministrazione provvederà pertanto a reintegrare l'Organismo.

La revoca di un componente dell'OdV potrà avvenire soltanto per giusta causa (ossia per grave negligenza nell'esercizio delle funzioni), con delibera del Consiglio di Amministrazione, sentito il parere, obbligatorio ma non vincolante, del Collegio Sindacale.

5.2 Funzioni e poteri dell'Organismo di Vigilanza

All'OdV è affidato sul piano generale il compito di vigilare:

- sulla reale efficacia e adeguatezza del MOG in relazione alla struttura aziendale, sulla effettiva capacità dello stesso di prevenire la commissione dei reati di cui al D. Lgs. 231/2001, anche in termini di idoneità e adeguatezza dei contenuti. Tale attività si concretizza in una valutazione delle disposizioni del Modello in relazione alla normativa pro tempore vigente, alle best practice e alla giurisprudenza in tema di responsabilità da reato degli enti collettivi;
- sull'effettiva osservanza del Modello da parte dei destinatari: dipendenti, organi sociali e, nei limiti ivi previsti, collaboratori e fornitori;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative, sollecitando a tal fine gli organi competenti.

L'OdV provvede a disciplinare le regole per il proprio funzionamento, formalizzandole in apposito regolamento, approvato in autonomia.

Le riunioni dell'OdV e gli incontri con gli altri organi di controllo societario devono essere verbalizzati e le copie dei verbali custodite a cura dell'Organismo stesso.

Su un piano più operativo, all'OdV è affidato il compito di:

- promuovere l'adozione delle procedure previste per l'implementazione del sistema di controllo;
- promuovere iniziative finalizzate alla diffusione della conoscenza e della comprensione dei principi di cui al MOG;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello;
- coordinarsi con le competenti funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività nelle aree sensibili. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle suddette aree a rischio. All'OdV devono essere inoltre segnalate da parte del management eventuali situazioni dell'attività aziendale che possono esporre l'azienda al rischio di reato;
- coordinarsi con la funzione aziendale responsabile del controllo delle attività esternalizzate (c.d. Outsourcing Officer), per il miglior monitoraggio delle attività sensibili esternalizzate. A tal fine l'OdV viene tenuto periodicamente informato sulle suddette attività;
- richiedere, ove ritenuto opportuno, appositi confronti o scambi documentali con la società di revisione;
- controllare l'efficacia della documentazione richiesta, in conformità a quanto previsto nei protocolli e nei piani di azione per il sistema di controllo. In particolare, all'OdV devono essere segnalate, con modalità da concordare formalmente, le attività più significative e le operazioni effettuate, anche con riferimento ai piani di azione eventualmente predisposti, e devono essere messi a disposizione gli aggiornamenti della documentazione, al fine di consentire l'effettuazione dei controlli;
- condurre le verifiche interne, d'intesa con le competenti funzioni aziendali, per l'accertamento di presunte violazioni delle prescrizioni di cui al MOG;
- coordinarsi con i vari Responsabili delle Funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello (formazione del personale, esigenze di interpretazione della normativa rilevante);
- assegnare a soggetti terzi, in possesso delle competenze specifiche necessarie per la migliore esecuzione dell'incarico, eventuali compiti di natura tecnica;
- effettuare, al fine di valutare le esigenze di aggiornamento del MOG, apposite riunioni con le Funzioni aziendali interessate.

Tenuto conto delle responsabilità attribuite e dei contenuti professionali specifici richiesti, l'OdV:

- si avvale, nello svolgimento dei propri compiti, dell'Area Audit di Unipol e della Funzione Compliance di UnipolPay, alle quali può altresì chiedere specifici approfondimenti e/o analisi;
- viene informato dall'Area Audit di Unipol e dalla Funzione Compliance di UnipolPay sulle risultanze delle attività di verifica svolte che abbiano una rilevanza ai fini 231;
- può avvalersi del supporto di altre funzioni aziendali, nonché di consulenti esterni.

Al fine di dare piena attuazione ai compiti ad esso affidati di accertamento di eventuali violazioni del Modello,

all'OdV sono conferiti specifici poteri di iniziativa e di controllo esercitabili nei confronti di tutti i settori dell'Ente, compreso l'organo decisionale e i suoi componenti, nonché nei confronti dei collaboratori, fornitori e consulenti dello stesso.

In particolare, per le suddette finalità, l'OdV può effettuare verifiche, richiedere informazioni, effettuare ispezioni, accedere sia a locali, sia a dati, archivi e documentazione, in coordinamento con le funzioni aziendali preposte.

A titolo esemplificativo, all'OdV è attribuita la facoltà di effettuare verifiche mirate, anche senza preavviso, su determinate operazioni o specifici atti posti in essere da UnipolPay, soprattutto nell'ambito delle attività sensibili, i cui risultati devono essere riassunti in sede di reporting agli organi societari competenti.

All'esito delle predette attività di verifica, all'OdV è infine conferito il compito di monitorare la corretta attuazione degli adempimenti procedurali necessari all'emanazione di eventuali provvedimenti nei confronti dei responsabili delle violazioni del Modello.

L'esercizio dei citati poteri deve avvenire nel limite strettamente funzionale all'assolvimento dei compiti dell'OdV, al quale non competono in alcun modo poteri di gestione.

L'attività svolta è sintetizzata nel report annuale al Consiglio di Amministrazione in cui vengono evidenziate anche eventuali criticità riscontrate e miglioramenti da attuare.

5.3 Reporting dell'Organismo di Vigilanza verso il vertice aziendale

Premesso che l'OdV potrà essere convocato in qualsiasi momento, con congruo anticipo, dal Consiglio di Amministrazione per riferire in merito al funzionamento del Modello o a situazioni specifiche, è assegnata all'OdV, in piena aderenza ai dettami del D. Lgs. 231/2001 nonché della dottrina prevalente, e potrà a sua volta presentare richiesta in tal senso, la seguente linea di reporting nei confronti del Consiglio di Amministrazione:

- con cadenza almeno annuale, l'OdV trasmette al Consiglio di Amministrazione un report scritto in merito all'attività svolta e al piano delle attività previste per l'anno successivo. Tale report ha per oggetto:
  1. l'attività svolta dall'OdV;
  2. le eventuali criticità emerse, sia in termini di comportamenti o eventi interni all'Ente, sia in termini di efficacia del MOG;
  3. le eventuali proposte di miglioramento.

Al verificarsi di situazioni che l'OdV reputi straordinarie, o di segnalazioni aventi carattere d'urgenza ai sensi della disciplina di cui al D. Lgs. 231/2001, l'OdV predispone un'immediata comunicazione nei confronti dell'organo decisionale.

5.4 Flussi informativi verso l'Organismo di Vigilanza: informazioni di carattere generale e informazioni specifiche obbligatorie

Tra le esigenze che il Modello deve soddisfare per essere ritenuto idoneo a prevenire i reati ricompresi tra le fattispecie di cui al D. Lgs. 231/2001, l'articolo 6 prevede l'istituzione di "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*". Detti flussi informativi rappresentano infatti lo strumento per agevolare l'attività di vigilanza sull'efficacia del Modello e per accertare a posteriori le cause che hanno reso possibile il verificarsi dell'eventuale reato.

Al fine di soddisfare tali esigenze, sono previste due tipologie di flussi informativi:

- flussi periodici;
- flussi *ad hoc*.

I Flussi Periodici differiscono a seconda dell'attività aziendale e consentono di monitorare l'evoluzione dell'attività oggetto di analisi e il funzionamento dei relativi presidi di controllo, evidenziando:

- per quanto concerne le criticità:

- gli eventi maggiormente significativi, individuati anche in base a soglie quali-quantitative, in termini di potenziale rischio di commissione di reati e gli eventuali indici di anomalia;
- i rapporti predisposti dai titolari dell'Area Audit di Unipol e della Funzione Compliance di UnipolPay, nonché dal Dirigente Preposto alla redazione dei documenti contabili societari della controllante nell'ambito della propria attività di verifica, dai quali si evincano eventuali omissioni o profili di criticità ai sensi del D. Lgs. 231/2001;
- l'informativa periodica inerente alla fruizione dei percorsi formativi sul D. Lgs. 231/2001 da parte dei dipendenti e degli apicali;
- l'informativa periodica inerente agli interventi organizzativi diretti all'effettiva attuazione, a tutti i livelli aziendali, del Modello;
- l'informativa inerente a eventuali: (i) modifiche organizzative (a titolo esemplificativo ingresso o uscita di linee di *business*), (ii) evoluzioni normative afferenti al D. Lgs. 231/2001 che possono comportare carenze e necessità di apportare modifiche al MOG;

- per quanto riguarda l'attività di monitoraggio, l'informativa periodica da parte delle aree aziendali relativamente ai processi c.d. "sensibili" maggiormente significativi, anche in assenza di problematiche specifiche;
- per quanto afferisce a ulteriori profili di anomalia:
  - l'informativa contenente eventuali problematiche sorte con riferimento all'applicazione dei protocolli di prevenzione (norme interne) previsti dal Modello;
  - l'informativa relativa a eventuali fatti, anomalie, infrazioni emerse in relazione alla gestione dei sistemi informativi aziendali;
  - l'OdV acquisisce anche l'esito delle attività di verifica svolte dall'Area Audit di Unipol con riferimento ai processi del tutto o in parte esternalizzati a società facenti parte del Gruppo.

I flussi *ad hoc* riguardano le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili, consistenti cioè in accertamenti focalizzati su singoli fatti che possono aver dato luogo alla commissione di reati o comunque indicativi di anomalie; questi possono consistere in:

- informativa in merito all'eventuale avvio di procedimenti giudiziari relativi ad ipotesi di reato ricomprese tra le fattispecie di cui al D. Lgs. 231/2001;
- informativa contenente notizia di ispezioni da parte di Autorità di Vigilanza (Banca d'Italia, Autorità Garante della Concorrenza e del Mercato, ecc.) o di Pubblici Ufficiali con funzioni di controllo (Guardia di Finanza, ecc.);
- report contenente informativa di eventuali ispezioni e/o fatti/anomalie/infrazioni emerse in materia di sicurezza sui luoghi di lavoro ai sensi del D. Lgs. 81/2008;
- segnalazioni di violazioni del Modello commesse da parte dei dipendenti o degli apicali;
- segnalazioni di violazioni del Modello commesse da parte di soggetti non dipendenti.

L'OdV provvede, di concerto con le funzioni aziendali, ad individuare le informazioni necessarie per lo svolgimento della sua funzione di vigilanza sul funzionamento e sull'osservanza del Modello, che gli devono essere inviate (con relativa tempistica).

Tutte le informazioni, segnalazioni e report previsti nel presente Modello sono conservati dall'OdV per un periodo di 10 anni.

Sono previsti periodici scambi di informazioni tra l'OdV e il Collegio Sindacale della Società, nonché con la Società di Revisione.

5.5 Comunicazioni da parte degli Organismi di Vigilanza delle Società del Gruppo

Al fine di garantire un efficace ed efficiente coordinamento dell'attività di vigilanza, da svolgersi nel pieno nel rispetto dei principi di autonomia e indipendenza come in precedenza declinati, l'OdV mantiene, con cadenza annuale, contatti informativi con l'Organismo di Vigilanza di Unipol.

Inoltre, nel caso di attività del tutto o in parte esternalizzate internamente al Gruppo, l'Organismo può attivare specifiche forme di cooperazione con gli analoghi Organismi operanti nell'ambito del Gruppo Unipol medesima finalizzate a una maggiore efficacia all'attività di vigilanza di ciascun Organismo su processi o attività trasversali.

5.6 Obblighi di riservatezza dell'Organismo di Vigilanza

I componenti dell'OdV devono assicurare il mantenimento di un alto grado di riservatezza sulle informazioni raccolte nell'esercizio delle loro funzioni, astenendosi dall'utilizzo di tali informazioni per fini diversi da quelli afferenti alla disciplina di cui al D. Lgs. 231/2001. In ogni caso, ogni informazione in loro possesso è trattata in conformità alla normativa pro tempore vigente.

5.7 La segnalazione di reati o di violazioni del Modello

A norma dell'art. 6, comma 2-bis[21], del D. Lgs. 231/2001, il Modello prevede un sistema interno per la segnalazione delle violazioni che consente a:

- azionisti;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- lavoratori subordinati della Società, ivi inclusi eventuali dipendenti distaccati da altre Società, lavoratori somministrati ed apprendisti;
- lavoratori autonomi anche occasionali, liberi professionisti, consulenti, volontari e tirocinanti (retribuiti e non retribuiti), che prestano la propria attività presso la Società;
- lavoratori e collaboratori che svolgono la propria attività lavorativa presso fornitori di beni o servizi, appaltatori o sub appaltatori di cui si servono le Società in perimetro;

di comunicare, a tutela dell'interesse pubblico e dell'integrità dell'ente, informazioni, compresi i fondati sospetti, riguardanti, tra l'altro, condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 o violazioni del MOG, commesse o che, sulla base di elementi concreti, potrebbero essere commesse, di cui siano venuti a conoscenza nel proprio contesto lavorativo, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni.

Il sistema interno per la segnalazione delle violazioni è formalizzato in una specifica procedura di Gruppo (la "Procedura")[22], approvata dal Consiglio di Amministrazione della Società.

La Procedura individua (i) la persona o la funzione autonoma e con personale specificamente formato preposta alla ricezione, all'esame e alla valutazione delle segnalazioni (la "Struttura Preposta Principale/ Alternativa[23]") e (ii) i mezzi attraverso cui le stesse possono essere trasmesse, in forma scritta, in forma orale o mediante incontro diretto. Il segnalante ha la possibilità di scegliere se utilizzare i canali istituiti presso la Società, oppure quelli istituiti presso la Capogruppo[24].

I canali e i mezzi di segnalazione di cui sopra garantiscono la riservatezza dell'identità del segnalante, della persona coinvolta o menzionata, nonché del contenuto della segnalazione e della relativa documentazione nelle attività di gestione delle segnalazioni.

Le segnalazioni relative a condotte illecite rilevanti ai sensi del D. Lgs. 231/2001 o a violazioni del Modello sono portate a conoscenza dell'Organismo, da parte della Struttura Preposta, secondo le modalità previste dalla

[21] Articolo introdotto dalla Legge 30 novembre 2017, n. 179 "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*"

[22] Procedura per la segnalazione delle violazioni (c.d. "*whistleblowing*").

[23] La segnalazione può essere indirizzata alla Struttura Preposta Alternativa della Società qualora i membri della Struttura Preposta Principale siano gerarchicamente o funzionalmente subordinati all'eventuale soggetto segnalato, ovvero siano essi stessi i presunti responsabili della violazione o abbiano un potenziale interesse correlato alla segnalazione, tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

[24] Qualora, ad esempio, ritenga che ciò sia maggiormente sicuro o che la gestione da parte della Capogruppo possa essere più efficace in relazione al caso di specie.

Procedura anche al fine di raccogliere eventuali indicazioni da parte dello stesso. La Struttura Preposta provvede a mantenere l'OdV costantemente aggiornato sullo stato di avanzamento della segnalazione.

UnipolPay vieta qualsiasi comportamento finalizzato a ostacolare, o a tentare di ostacolare, i segnalanti e si impegna a tutelare i medesimi - con l'esclusione di segnalazioni infondate effettuate con dolo o colpa grave[25] - da qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e che provoca o può provocare alla persona segnalante, in via diretta o indiretta, un danno ingiusto.

A tal proposito, si rinvia al par.6.9 con riferimento alle sanzioni previste nei confronti di chi viola le misure di tutela del segnalante o ne ostacola la segnalazione.

Il segnalante che ritiene di aver subito ritorsioni o una discriminazione può agire nei modi e nelle forme previsti dall'art.19, comma 1 del D.Lgs. 24/2023 ("Decreto *whistleblowing*").

Ai sensi dell'art. 19, comma 3 del Decreto *whistleblowing*, il licenziamento e qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante sono nulli. È onere del datore di lavoro, in caso procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi ad oggetto l'accertamento dei comportamenti, atti o omissioni vietati dall'art. 17 del Decreto *whistleblowing*, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Si rinvia alla Procedura, pubblicata nella sezione dedicata del sito *web* della Società[26], per ogni ulteriore dettaglio.

[25] Ai sensi dell'art. 20 comma 3 del Decreto *whistleblowing* "(…) *quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele di cui al presente capo non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare*".

[26] https://www.unipolpay.it

6 DISPOSIZIONI DISCIPLINARI E SANZIONATORIE

6.1 Principi Generali

Ai sensi degli artt. 6, comma 2, lettera e) e 7, comma 4, lett. b) del D. Lgs. 231/2001 è prevista la predisposizione di un adeguato sistema sanzionatorio in caso di violazione delle disposizioni del MOG.

La mancata osservanza delle disposizioni del Modello e del Codice Etico, ledendo il rapporto tra UnipolPay e i "portatori di interessi", comporta, quale conseguenza, l'applicazione di sanzioni disciplinari a carico dei soggetti interessati, indipendentemente dall'eventuale esercizio dell'azione penale da parte dell'Autorità giudiziaria.

Le regole di condotta imposte dal presente MOG sono assunte da UnipolPay in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del Modello medesimo possono determinare.

6.2 Criteri generali di irrogazione delle sanzioni

La tipologia e l'entità delle sanzioni applicate in ciascun caso di violazione rilevato saranno proporzionate alla gravità delle infrazioni e, comunque, definite in base ai seguenti criteri generali:

- valutazione soggettiva della condotta a seconda del dolo o della colpa;
- rilevanza degli obblighi violati;
- livello di responsabilità gerarchica e/o tecnica del soggetto coinvolto;
- eventuale condivisione della responsabilità con altri soggetti che abbiano concorso nel determinare il reato;
- presenza di circostanze aggravanti o attenuanti con particolare riguardo alla professionalità, alle precedenti prestazioni lavorative, ai precedenti disciplinari, alle circostanze in cui è stato commesso il fatto.

L'eventuale irrogazione della sanzione disciplinare, prescindendo dall'instaurazione del procedimento e/o dall'esito del giudizio penale, dovrà essere per quanto possibile, ispirata ai principi di tempestività, immediatezza ed equità.

6.3 Ambito di applicazione

Ai sensi del combinato disposto degli artt. 5, lett. b) e 7 del D. Lgs. 231/2001, le sanzioni previste dai Contratti Collettivi Nazionali ed Integrativi di Lavoro, nonché dalla legge, potranno essere applicate, a seconda della gravità, nei confronti del personale di UnipolPay che ponga in essere illeciti disciplinari derivanti da:

- mancato rispetto delle disposizioni previste dal Modello;
- mancata o non veritiera evidenza dell'attività svolta relativamente alle modalità di documentazione, di conservazione e controllo degli atti previsti dalle procedure e normative aziendali e dai protocolli;
- omessa vigilanza dei superiori gerarchici sul comportamento dei propri sottoposti;
- violazione degli obblighi di informazione nei confronti dell'OdV;
- violazione e/o elusione del sistema di controllo, posto in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dalle procedure, ovvero impedendo il controllo o l'accesso alle informazioni e alla documentazione ai soggetti preposti, ivi incluso l'OdV.

Ai fini dell'applicazione delle sanzioni, la gravità degli illeciti disciplinari sarà valutata dall'Amministratore Delegato di volta in volta sulla base dei principi contenuti nel precedente paragrafo.

6.4 Misure nei confronti dei lavoratori dipendenti

La violazione delle disposizioni del Modello potrà costituire inadempimento delle obbligazioni contrattuali, con ogni conseguenza di legge, anche in ordine all'eventuale risarcimento del danno, nel rispetto, in particolare, degli artt. 2104, 2106 e 2118 del codice civile, dell'art. 7 della Legge n. 300/1970 ("Statuto dei Lavoratori"), della Legge n. 604/1966 e successive modifiche e integrazioni sui licenziamenti individuali nonché dei contratti collettivi di lavoro, sino all'applicabilità dell'art. 2119 del codice civile, che dispone la possibilità di licenziamento per giusta causa.

Saranno applicate le sanzioni previste dal Contratto Collettivo Nazionale di Lavoro del settore e l'adozione delle stesse dovrà avvenire nel rispetto delle procedure previste dallo Statuto dei Lavoratori, nonché dal citato CCNL.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, tali attività competono all'Amministratore Delegato.

6.5 Misure nei confronti dei dirigenti

Al mancato rispetto delle disposizioni del presente Modello da parte dei dirigenti, a seconda della gravità delle infrazioni e tenuto conto della particolare natura fiduciaria del rapporto di lavoro, potrà conseguire:

a) Consegna di lettera di richiamo

Questa misura viene applicata quando vengono ravvisati comportamenti, nell'espletamento delle attività nelle aree a rischio, che costituiscano violazioni di lieve entità rispetto alle disposizioni del Modello.

b) Risoluzione del rapporto di lavoro

Questa misura viene applicata quando vengono ravvisati comportamenti, nell'espletamento delle attività nelle aree a rischio, che costituiscano violazioni di grave entità rispetto alle disposizioni del MOG.

6.6 Misure nei confronti degli Amministratori

In caso di violazione delle disposizioni da parte dei Consiglieri di Amministrazione, l'OdV informa il Collegio Sindacale e l'intero Consiglio di Amministrazione, i quali provvederanno ad assumere le opportune iniziative previste dalla vigente normativa (azione di responsabilità).

6.7 Misure nei confronti dei Sindaci

L'OdV comunica al Collegio Sindacale e al Consiglio di Amministrazione la notizia di una violazione del Modello commessa da parte di un Sindaco. Il Collegio Sindacale, con l'astensione del soggetto coinvolto, procede agli accertamenti necessari e assume, sentito il Consiglio di Amministrazione, i provvedimenti opportuni. Se la violazione è ascrivibile a più di un Sindaco, essa viene comunicata al solo Consiglio di Amministrazione per l'adozione dei provvedimenti opportuni.

6.8 Misure nei confronti di collaboratori e fornitori

Nei confronti di tutti coloro che operano in qualità di collaboratori e fornitori di UnipolPay valgono le seguenti disposizioni: ogni comportamento posto in essere dai collaboratori e dai fornitori in contrasto con le linee di condotta indicate dal Modello e dalla Carta dei Valori e Codice Etico, potrà determinare, secondo quanto previsto dalle specifiche clausole inserite nelle lettere di incarico o negli accordi contrattuali, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società.

6.9 Misure a tutela del sistema interno di segnalazione delle violazioni

Ai sensi dell'art. 21 comma 2 del Decreto *whistleblowing* e in ottemperanza a quanto previsto dal comma 2-bis[27], lettera d), dell'articolo 6 del D.Lgs. 231/2001, sono equiparati al mancato rispetto delle disposizioni del presente Modello e soggiacciono pertanto alle medesime sanzioni i seguenti comportamenti:

- violazione delle misure di tutela di chi effettua le segnalazioni previste dal capitolo 5.6 del Modello e disciplinate dalla Procedura;
- commissione degli altri illeciti di cui all'art. 21 comma 1[28] del Decreto *whistleblowing*.

7 LA DIFFUSIONE DEL MODELLO TRA I DESTINATARI

Ai fini dell'efficacia del presente Modello, risulta necessario garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute sia nei confronti dei dipendenti che degli apicali. Tale obiettivo riguarda tutte le risorse aziendali sia che si tratti di risorse già presenti in azienda sia che si tratti di quelle da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività sensibili.

L'OdV, per quanto di competenza, supervisiona ed integra il sistema di informazione e formazione in collaborazione con l'HR Manager della Società.

7.1 Informativa e formazione per dipendenti e apicali

La diffusione del Modello è effettuata attraverso la pubblicazione sul sito *intranet* aziendale, accompagnato da un'informativa di carattere generale relativa al D. Lgs. 231/2001.

L'adozione del Modello e i relativi aggiornamenti sono comunicati ai dipendenti al momento dell'adozione stessa o dell'aggiornamento tramite comunicazione aziendale notificata via e-mail (o analogo strumento elettronico) a tutti i dipendenti in organico da parte della struttura competente.

Ai nuovi assunti viene consegnato un set informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza. Tale set informativo contiene, oltre ai documenti di regola consegnati al neo-assunto, la Carta dei Valori e Codice Etico, il Modello e il D. Lgs. 231/2001.

Oltre agli interventi di sensibilizzazione già condotti dalla Società su tutti i dipendenti e apicali, viene svolta un'attività di formazione e informazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001, differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari:

- formazione in aula alle prime linee ed ai responsabili operativi, con una presentazione a beneficio dei suddetti soggetti nel corso della quale:
  - si informa in merito alle disposizioni del D. Lgs. 231/2001;
  - si sensibilizzano i presenti sull'importanza attribuita dalla Società all'adozione di un sistema di governo e di controllo dei rischi;
  - si descrivono la struttura e i contenuti principali del Modello adottato, nonché l'approccio metodologico seguito per la sua realizzazione e il suo aggiornamento;

---

[27] Comma modificato dal Decreto *whistleblowing.*

[28] "*Fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile le seguenti sanzioni amministrative pecuniarie: a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza di cui all'articolo 12; b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quelle di cui agli articoli 4 e 5, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute; c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile*."

  - si descrivono i comportamenti da tenere in materia di comunicazione e formazione dei propri subordinati, in particolare del personale operante nelle aree aziendali ritenute sensibili;
  - si illustrano i comportamenti da tenere nei confronti dell'OdV, in materia di comunicazioni, segnalazioni e collaborazione alle attività di vigilanza e aggiornamento del MOG.
- informazione ai dipendenti operanti nell'ambito di procedure sensibili ai reati contemplati dal D. Lgs. 231/2001: sensibilizzazione da parte dei responsabili delle funzioni aziendali potenzialmente a rischio di reato dei propri subordinati, in relazione al comportamento da osservare, alle conseguenze derivanti da un mancato rispetto delle stesse e, in generale, del Modello adottato dalla Società;
- corso di formazione per tutti i dipendenti con la finalità di diffondere la conoscenza del D. Lgs. 231/2001 e del MOG.

La partecipazione ai programmi di formazione sopra descritti è obbligatoria. Al termine dei percorsi formativi è prevista l'esecuzione di specifici *test* di apprendimento e il rilascio di un attestato finale.

L'omessa partecipazione ai programmi di formazione in assenza di giustificato motivo è suscettibile di essere valutata sotto il profilo disciplinare.

La verifica circa l'effettiva fruizione è demandata alla funzione Academy Unipol, che relaziona all'OdV.

7.2 Informativa per i collaboratori e fornitori

I collaboratori e i fornitori sono informati del contenuto del Modello, anche mediante rinvio alla pubblicazione del medesimo sul sito *internet* della Società e dell'esigenza di UnipolPay che il loro comportamento sia conforme a quanto disposto nel D. Lgs. 231/2001.

I collaboratori e i fornitori sono tenuti a rilasciare a UnipolPay una dichiarazione ove si attesta la integrale conoscenza dei contenuti e prescrizioni contenute nel D. Lgs. 231/2001 e l'impegno al rispetto dello stesso, prevedendo specifica informativa nell'ambito del contratto.

UnipolPay S.p.A.
Via Stalingrado, 37
Bologna

www.unipolpay.it