MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

EX DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231

Approvato dal Consiglio di Amministrazione di Telepass S.p.A.
il 3 luglio 2024

Sommario

DEFINIZIONI

Telepass o Società	Telepass S.p.A.
Mundys	Mundys S.p.A.
Gruppo Telepass o Gruppo	Telepass e le società dalla stessa controllate ai sensi dell'art. 2359, 1° e 2° comma, Codice Civile.
Gruppo Mundys	Mundys e le società dalla stessa controllate ai sensi dell'art. 2359, 1° e 2° comma, Codice Civile.
Decreto o D. Lgs. 231/2001	Decreto Legislativo 8 giugno 2001 n. 231.
Linee Guida di Confindustria	Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo *ex* D. Lgs. 231/2001 emanate da Confindustria in data 3 novembre 2003 e successive integrazioni.
Modello o MOG	Modello di Organizzazione, Gestione e Controllo previsto dal D. Lgs. 231/2001 e adottato dalla Società al fine di prevenire la commissione dei Reati di cui al Decreto.
Codice Etico	Codice Etico del Gruppo Mundys, che identifica l'insieme dei valori e delle regole di condotta cui la Società intende fare riferimento nell'esercizio delle attività imprenditoriali.
Reati o Reati presupposto	Reati rilevanti ai sensi del D. Lgs. 231/2001.
Area a rischio	Area di attività considerate potenzialmente a rischio in relazione ai Reati di cui al D. Lgs. 231/2001.
Presidi	Complesso delle di norme, protocolli e disposizioni aziendali finalizzate alla prevenzione dei rischi di reato, quali, a titolo esemplificativo e non esaustivo, le procedure, le norme operative, i manuali, la modulistica e i comunicati al personale dipendente.
Organismo di Vigilanza o OdV	Organismo interno preposto alla vigilanza sul funzionamento, sull'efficacia, sull'osservanza del Modello ed al relativo aggiornamento, di cui all'art. 6, comma 1, lett. b) del D. Lgs. 231/2001.
Organi Sociali	Consiglio di Amministrazione e Collegio Sindacale di Telepass.

Soggetti Apicali	Ai sensi dell'art. 5, comma 1, lett. a) del D. Lgs. 231/2001, persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persone che esercitano, anche di fatto, la gestione e il controllo dello stesso.
Soggetti Subordinati	Ai sensi dell'art. 5, comma 1, lett. b) del D. Lgs. 231/2001, persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).
Destinatari	Soggetti a cui sono indirizzate le regole di condotta e i principi etici contenuti nel Codice Etico, nel Modello e nei Presidi adottati da Telepass.
Terzi destinatari	Soggetti che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con la Società e che contrattualmente si obbligano al rispetto dei principi etici e/o del Modello di Telepass.
P.A.	Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio.
CCNL	Contratto Collettivo Nazionale di Lavoro applicabile alla Società (CCNL Commercio, CCNL per il personale dipendente da società e consorzi concessionari di autostrade e trafori, CCNL Industria per il personale con qualifica dirigenziale).
Whistleblowing	Istituto che tutela il dipendente o il collaboratore che segnala condotte illecite di cui è venuto a conoscenza nello svolgimento delle proprie mansioni.
Team Segnalazioni	Organismo collegiale responsabile del processo di gestione delle segnalazioni. Si compone dei responsabili delle seguenti strutture organizzative di Telepass: Internal Audit, Risorse Umane e Legal Affairs. Il Team Segnalazioni esercita la propria attività su Telepass e su tutte le società da quest'ultima controllate.
Procedura Flussi	Procedura che regola i flussi informativi dalle strutture organizzative di Telepass verso l'Organismo di Vigilanza.
c.p.	Codice Penale.

PARTE GENERALE

PREMESSA

Il Decreto Legislativo n. 231 dell'8 giugno 2001 e sue successive modifiche e integrazioni ha introdotto nell'ordinamento giuridico la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*".

La Società, sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali a tutela della posizione del mercato assunta, della propria immagine, delle aspettative dei propri azionisti e del lavoro dei propri dipendenti, ha:

a) recepito il Codice Etico, la Policy Anticorruzione, il Codice di Condotta per la prevenzione delle discriminazioni e la tutela della dignità delle donne e degli uomini, la Procedura Gestione delle Segnalazioni del Gruppo Telepass, per disciplinare il corretto svolgimento delle proprie attività;

b) nominato, nella seduta del Consiglio di Amministrazione del 7 novembre 2017, il Responsabile Anticorruzione in conformità con la Policy Anticorruzione del Gruppo Mundys;

c) ritenuto opportuno adottare ed attuare un Modello di Organizzazione, Gestione e Controllo volto a definire un sistema strutturato di regole e controlli cui attenersi per perseguire lo scopo sociale, in piena conformità alle vigenti disposizioni di legge, anche al fine di prevenire la commissione dei Reati previsti dal Decreto.

L'adozione di un MOG consente a Telepass di minimizzare il rischio che, al proprio interno, possano essere commessi illeciti penali a interesse o a vantaggio della Società stessa.

Benché il MOG sia uno strumento che la legge prevede per tutelare la Società in sede di processo penale, preme rilevare come l'osservanza del MOG e dei Presidi da parte dei Destinatari contribuisca ad evitare che la persona fisica commetta, più o meno consapevolmente, illeciti nello svolgimento dell'attività lavorativa.

Il MOG, pertanto, costituisce uno strumento di tutela sia della persona giuridica sia delle persone fisiche che, a vario titolo, operano nella struttura aziendale.

1. IL DECRETO LEGISLATIVO N. 231/2001

1.1. Il regime di responsabilità amministrativa a carico degli Enti

Il D. Lgs. 231/2001, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", ha adeguato la normativa italiana in materia di responsabilità amministrativa delle persone giuridiche e delle associazioni anche prive di personalità giuridica ("Enti") alle Convenzioni europee emanate in materia[1].

Il Decreto ha introdotto nell'ordinamento italiano un regime di responsabilità formalmente amministrativa, ma sostanzialmente penalistica, a carico degli Enti per determinati Reati commessi nell'interesse o vantaggio degli stessi da parte di:

a) persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione degli Enti o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi ("Soggetti Apicali");
b) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati ("Soggetti Subordinati").

La responsabilità amministrativa dell'Ente si aggiunge a quella penale della persona fisica che ha materialmente commesso il Reato e sono entrambe oggetto di accertamento nel medesimo procedimento innanzi al giudice penale. Peraltro, la responsabilità dell'Ente permane anche nel caso in cui la persona fisica autrice del Reato non sia stata identificata o non sia imputabile.

La responsabilità dell'Ente ad oggi sussiste esclusivamente nel caso di commissione delle seguenti fattispecie di Reato presupposto richiamati espressamente nel Decreto:

i) Reati contro la Pubblica Amministrazione (artt. 24 e 25, D. Lgs. 231/2001);

ii) Reati informatici e trattamento illecito di dati (art. 24-bis, D. Lgs. 231/2001);

iii) Reati di criminalità organizzata (art. 24-ter, D. Lgs. 231/2001);

iv) Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis, D. Lgs. 231/2001);

v) Reati contro l'industria ed il commercio (art. 25-bis.1, D. Lgs. 231/2001);

vi) Reati societari e corruzione tra privati (art. 25-ter, D. Lgs. 231/2001);

vii) Reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater, D. Lgs. 231/2001);

viii) Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1, D. Lgs. 231/2001);

ix) Reati contro la personalità individuale (art. 25-quinquies, D. Lgs. 231/2001);

[1] La Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee; la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri; la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali; la Convenzione e i Protocolli delle nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001, ratificato con Legge 146 del 2006.

x) Reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25-sexies, D. Lgs. 231/2001);

xi) Reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies, D. Lgs. 231/2001);

xii) Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies, D. Lgs. 231/2001);

xiii) Reati in materia di strumenti di pagamento diversi dal contante (art. 25-octies.1, D. Lgs. 231/2001);

xiv) Reati in materia di violazione del diritto d'autore (art. 25-novies, D. Lgs. 231/2001);

xv) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies, D. Lgs. 231/2001);

xvi) Reati ambientali (art. 25-undeciesD. Lgs. 231/2001);

xvii) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies del D. Lgs. 231/2001);

xviii) Razzismo e xenofobia (art. 25-terdecies, D. Lgs. 231/2001);

xix) Reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies del D. Lgs. 231/2001);

xx) Reati tributari (art. 25-quinquesdecies, D. Lgs. n. 231/2001);

xxi) Reati di contrabbando (art. 25-sexdecies, D. Lgs. 231/2001);

xxii) Delitti contro il patrimonio culturale (art. 25-septiesdecies, D. Lgs. 231/2001);

xxiii) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies, D. Lgs. 231/2001)

xxiv) Reati transnazionali in materia di associazioni criminose, riciclaggio, traffico di migranti, intralcio alla giustizia (Legge 16 marzo 2006 n. 146 artt. 3 e 10).

All'esito dell'analisi delle attività svolte dalla Società illustrata nel prosieguo, si ritiene che possano potenzialmente riguardare Telepass gli illeciti riportati *sub* i), ii), iii), v), vi), vii), ix), x), xi), xii), xiii), xiv), xv), xvi), xvii), xx), xxi) e xxiv) se commessi nell'interesse o a vantaggio della Società ai sensi dell'art. 5 del D. Lgs. 231/2001.

Le fattispecie di Reato che non rientrano nel novero di quelle astrattamente applicabili per la Società sono state escluse in ragione della natura dell'attività svolta dalla Società stessa e non essendo state rilevate al momento fattispecie concrete di possibili rischi.

Si ritiene che il complesso dei Presidi – organizzativi e procedurali – adottati dalla Società ai fini della prevenzione degli illeciti suddetti o, più in generale, per assicurare il corretto svolgimento delle attività aziendali, sia idoneo ad eliminare o minimizzare il rischio di commissione di tutte le fattispecie di reato previste dal D. Lgs. 231/2001.

1.2. **I reati commessi all'estero**

L'Ente risponde anche dei Reati commessi all'estero, purché nei confronti dell'Ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto. Nell'ipotesi in cui per la punizione del colpevole sia prevista la richiesta del Ministro della giustizia, si procede verso l'Ente solo se la richiesta è formulata anche nei confronti di quest'ultimo. In particolare, in base all'art. 4 del Decreto, l'Ente che ha sede in Italia può esser chiamato a rispondere, in relazione a Reati consumati all'estero, secondo i seguenti presupposti:

a) il Reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente (art. 5, comma 1, del Decreto);
b) l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
c) l'Ente può rispondere solo nei casi e nelle condizioni previste dagli artt. 7 (Reati commessi all'estero), 8 (Delitto politico commesso all'estero), 9 (Delitto comune del cittadino all'estero) e 10 (Delitto comune dello straniero all'estero) del Codice Penale.

Inoltre, secondo quanto previsto all'art. 10 della Legge 146/2006, è prevista la responsabilità dell'Ente per alcuni Reati aventi carattere transnazionale (quali, ad esempio, il reato di associazione per delinquere anche di tipo mafioso, il reato associazione finalizzata al traffico di sostanze stupefacenti e il reato di traffico di migranti).

In detti casi è necessario che la condotta illecita, commessa da un gruppo criminale organizzato, sia alternativamente:

i) commessa in più di uno Stato;
ii) commessa in uno Stato ma abbia effetti sostanziali in un altro Stato;
iii) commessa in un solo Stato, sebbene una parte sostanziale della sua preparazione o pianificazione o direzione e controllo debbano avvenire in un altro Stato;
iv) commessa in uno Stato, ma in essa sia coinvolto un gruppo criminale organizzato protagonista di attività criminali in più di uno Stato.

1.3. **Le sanzioni**

Le sanzioni previste per i Reati contemplati nel Decreto sono:

1) sanzioni pecuniarie;
2) sanzioni interdittive;
3) confisca;
4) pubblicazione della sentenza.

Le **sanzioni pecuniarie**, applicabili a tutti gli illeciti, sono determinate attraverso un sistema basato su "quote". Il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare od attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'Ente, allo scopo di assicurare l'efficacia della sanzione (art. 11 del Decreto).

Le **sanzioni interdittive** possono essere applicate all'Ente in via cautelare quando sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'Ente nella commissione del Reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa natura di quello per cui si procede (art. 45 del Decreto).

Se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'Ente, il giudice, in luogo dell'applicazione della sanzione, può disporre la prosecuzione dell'attività dell'Ente da parte di un commissario per un periodo di uguale durata a quello della misura interdittiva, se l'Ente svolge un servizio pubblico o di pubblica necessità, la cui interruzione potrebbe provocare grave pregiudizio alla collettività o se l'interruzione dell'attività può provocare rilevanti ripercussioni sull'occupazione.

L'inosservanza delle sanzioni interdittive costituisce un reato autonomo previsto dal Decreto come fonte di possibile responsabilità amministrativa dell'Ente (art. 23 del Decreto).

In particolare, le sanzioni interdittive, di durata non inferiore a tre mesi e non superiore a due anni, hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'Ente e sono costituite da:

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

Le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà in relazione alla commissione dei delitti di cui al Capo I del Decreto (artt. 24 a 25-duodecies del Decreto) nella forma del tentativo (art. 26 del Decreto).

Oltre alle predette sanzioni, il Decreto prevede che venga sempre disposta la **confisca** del prezzo o del profitto del Reato, che può avere ad oggetto anche beni o altre utilità di valore equivalente, nonché la **pubblicazione della sentenza di condanna** quando all'Ente è applicata una sanzione interdittiva. La sentenza è pubblicata mediante affissione nel comune ove l'Ente ha la sede principale ed è inoltre pubblicata sul sito internet del Ministero della Giustizia.

Si segnala che, in aggiunta alle suddette sanzioni previste dal Decreto, anche la semplice apertura di un'indagine penale per la commissione di un illecito amministrativo può comportare un **danno all'immagine** della Società e del Gruppo, e ciò anche qualora il procedimento dovesse risolversi in un'archiviazione o un'assoluzione. Ogni Destinatario dovrà quindi porre particolare attenzione alle previsioni del MOG, proprio per evitare qualsivoglia coinvolgimento in indagini penali.

1.4. Procedimento di accertamento dell'illecito e verifica dell'adeguatezza del Modello da parte del giudice

La responsabilità per illecito amministrativo derivante da Reato viene accertata nell'ambito di un procedimento penale, che dovrà rimanere riunito - ove possibile - al processo penale instaurato nei confronti della persona fisica autore del Reato presupposto della responsabilità dell'Ente.

L'accertamento della responsabilità dell'Ente, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del Reato presupposto per la responsabilità dell'Ente;
- l'accertamento in ordine alla sussistenza dell'interesse o del vantaggio dell'Ente alla commissione del Reato;
- il sindacato di idoneità ed efficace attuazione del Modello adottato.

Il sindacato del giudice circa l'astratta idoneità del Modello a prevenire i Reati di cui al Decreto è condotto a posteriori e, nel formulare il giudizio, il giudice si colloca, idealmente, nella realtà aziendale al momento in cui si è verificato l'illecito, al fine di verificare l'efficacia del Modello adottato a prevenire la commissione dell'illecito**.**

1.5. **L'adozione del Modello quale possibile esimente della responsabilità amministrativa**

Gli artt. 6 e 7 del Decreto prevedono forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i Reati commessi nel suo interesse o a suo vantaggio sia da Soggetti Apicali sia da Soggetti Subordinati.

In particolare, l'art. 6 del Decreto, nel caso di Reati commessi da Soggetti Apicali prevede una forma specifica di esonero dalla responsabilità amministrativa qualora l'Ente dimostri che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, Modelli idonei a prevenire i Reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e sull'osservanza dei Modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dotato di autonomi poteri di iniziativa e controllo;
c) le persone che hanno commesso i Reati hanno agito eludendo fraudolentemente i suddetti Modelli;
d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Nel caso, invece, di Reati commessi dai Soggetti Subordinati, l'art. 7 del Decreto prevede che l'Ente è responsabile se la commissione del Reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Tale inosservanza è, in ogni caso, esclusa se l'Ente, prima della commissione del Reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire Reati della specie di quello verificatosi.

Il Decreto prevede, inoltre, che il Modello debba essere idoneo a rispondere alle seguenti esigenze:

1) individuare le attività nel cui ambito possono essere commessi i Reati previsti dal Decreto;
2) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai Reati da prevenire;
3) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali Reati;
4) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello con riferimento anche al *whistleblowing*, come specificato in seguito.

2. LA SOCIETA'

Telepass è una società italiana che opera nel settore dei servizi per la mobilità in ambito urbano ed extraurbano basati su App, come di seguito definita, per creare un ecosistema di servizi che offra a privati e aziende un numero sempre maggiore di opzioni per una mobilità integrata flessibile, sicura e sostenibile.

In particolare, Telepass svolge attività relative (i) all'erogazione del servizio di telepedaggio, che consente la fruizione dei servizi di pagamento e di accesso agevolato alla rete autostradale a pedaggio mediante corsie dedicate, senza necessità di fermata, in entrata e in uscita, nelle stazioni di esazione (caselli autostradali), nonché (ii) all'erogazione di ulteriori servizi inerenti il pagamento e/o l'accesso agevolato ad aree, strutture, infrastrutture e/o beni e servizi relativi alla mobilità presso i soggetti abilitati all'accettazione dei pagamenti anche tramite i propri apparati.

Inoltre, l'area di attività della Società si è progressivamente ampliata, sempre nell'ambito dei servizi legati alla mobilità, sino a contemplare anche l'attività della intermediazione assicurativa, come soggetto iscritto alla Sezione E del Registro Unico degli Intermediari (RUI) tenuto da IVASS. Per il perimetro aggiornato delle attività si rinvia all'Oggetto sociale contenuto nello Statuto approvato dall'Assemblea della Società in data 12 aprile 2021.

Dal 2016 la Società è controllata da Mundys.

In data 14 aprile 2021 si è perfezionata la cessione del 49% del capitale di Telepass al gestore di investimenti globale Partners Group AG.

In data 1° maggio 2022 Telepass Pay S.p.A., già controllata di Telepass, è stata fusa per incorporazione in Telepass. Quest'ultima, pertanto, autorizzata da Banca d'Italia, è diventata un Istituto di Moneta Elettronica, mediante un Patrimonio Destinato, come di seguito definito, dedicato esclusivamente ai servizi di emissione e distribuzione di moneta elettronica ed affini e funzioni aziendali dedicate esclusivamente alla gestione delle relative attività ("IMEL ibrido").

In virtù di quanto sopra, Telepass è autorizzata da Banca d'Italia a:
- emettere e distribuire moneta elettronica;
- prestare servizi di pagamento non connessi all'attività di moneta elettronica, come definiti all'articolo 1, comma 2, lettera h-septies.1), del Decreto Legislativo 1° settembre 1993, n. 385 al fine di offrire nuovi servizi legati al "mondo della mobilità", diversi dai servizi ad oggi offerti "in esenzione" da Telepass.

Nell'ambito dell'operatività connessa ai servizi di pagamento, Telepass:
- "emette e accetta" strumenti di pagamento ed in particolare:
  - l'apparato fisico ("OBU");
  - l'applicazione mobile scaricabile sullo smartphone ("App");
- esegue ordini di pagamento, permettendo ai propri clienti di iniziare ed effettuare operazioni di pagamento anche tramite un sito web (accessibile da computer o da smartphone tramite mobile web), garantendo in ogni caso l'autenticazione forte del cliente.

Telepass controlla, in modo totalitario o maggioritario, le seguenti società:
1) Telepass Broker S.r.l.;
2) URBANnext S.A.;
3) Telepass Assicura S.r.l.;
4) Telepass Innova S.p.A.;

5) Wash Out S.r.l.;
6) Eurotoll S.A.

Nell'ambito delle attività sopra richiamate, Telepass è sottoposta alla vigilanza di varie Autorità amministrative, tra cui, a titolo esemplificativo e non esaustivo, Banca d'Italia, l'Autorità Garante della Concorrenza e del Mercato, l'IVASS, il Garante Privacy e il Ministero delle Infrastrutture e dei Trasporti.

3. ADOZIONE DEL MODELLO

3.1. Definizione, finalità e Destinatari del presente Modello

Il Modello si può definire come un complesso organico di principi, regole, disposizioni, schemi organizzativi e connessi compiti e responsabilità, funzionale alla attuazione ed alla diligente gestione di un sistema di controllo e monitoraggio delle attività a rischio, con riferimento ai Reati previsti dal Decreto.

Il presente Modello si propone le seguenti **finalità**:

- rafforzare il sistema di corporate governance;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla eliminazione o riduzione del rischio di commissione dei Reati di cui al D. Lgs. 231/2001, anche nella forma del tentativo, connessi all'attività aziendale, con particolare riguardo alla eliminazione o riduzione di eventuali comportamenti illegali;
- determinare, in tutti coloro che operano in nome, per conto o comunque nell'interesse di Telepass nelle Aree a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni del Modello, in un illecito punito, non solo nei confronti del suo autore ma anche nei confronti della Società, con sanzioni penali e amministrative;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Telepass che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni;
- ribadire che Telepass non tollera comportamenti illeciti, non rilevando in alcun modo la finalità perseguita ovvero l'erroneo convincimento di agire nell'interesse o a vantaggio della Società, in quanto tali comportamenti sono comunque contrari ai principi etici cui la Società intende attenersi e, dunque, in contrasto con l'interesse della stessa;
- censurare le violazioni del Modello con la comminazione di sanzioni disciplinari e/o contrattuali.

Si considerano **Destinatari** del presente Modello e, come tali, tenuti alla sua conoscenza ed osservanza nell'ambito delle specifiche competenze:

- i componenti del Consiglio di Amministrazione, cui spetta il compito di fissare gli obiettivi, decidere le attività, realizzare i progetti, proporre gli investimenti ed adottare ogni decisione o azione relativa all'andamento della Società;
- i componenti del Collegio Sindacale, nell'espletamento della funzione di controllo e verifica della correttezza formale e sostanziale dell'attività della Società e del funzionamento del sistema di controllo interno;
- l'Amministratore Delegato ed i dirigenti della Società;
- i dipendenti e tutti i collaboratori con cui si intrattengono rapporti contrattuali, a qualsiasi titolo, anche occasionali e/o soltanto occasionali;
- tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con la Società.

3.2. Struttura del Modello adottato da Telepass

Il Modello adottato da Telepass è costituito dalla presente Parte Generale e dalle Parti Speciali predisposte per le tipologie di Reato relativamente alle quali si è ravvisata la sussistenza di rischi per la Società.

Le Parti Speciali del presente Modello sono suddivise per "Famiglie di Reato" che sono state ritenute rilevanti:

PARTE SPECIALE	FAMIGLIA DI REATO	DECRETO 231
A	Reati in danno della Pubblica Amministrazione	artt. 24 e 25
B	Reati societari e corruzione tra privati	art. 25-ter
C	Reati ed illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione del mercato	artt. 25-sexies Decreto e 187-quinquies TUF
D	Reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro	art. 25-septies
E	Reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Legge 231/2007 e dall'art. 25-octies Decreto
F	Reati informatici	art. 24-bis Decreto e Legge 48/2008
G	Reati ambientali	art. 25-undecies
H	Reati di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare e Reati contro la personalità individuale, con particolare riferimento al Reato previsto dall'art. 603-bis Codice Penale "Intermediazione illecita e sfruttamento del lavoro"	art. 25-duodecies e 25-quinquies
I	Delitti contro l'industria e il commercio e delitti in materia di violazione del diritto d'autore	25-bis 1 e 25-novies
J	Reati tributari	art. 25-quinquiesdecies
K	Reati in materia di contrabbando	art. 25-sexiesdecies
L	Reati commessi con strumenti di pagamento diversi dai contanti	art. 25-octies.1.
M	Delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	art. 25-decies
N	Reati associativi, sia nella forma base di cui all'art. 416 Codice Penale, sia nella forma transnazionale, di cui alla Legge n. 146/2006	art. 24-ter, 25 quater e la L. 146/2006

Per tutti gli altri illeciti che, in base all'analisi svolta, si ritiene che non riguardino potenzialmente la Società e per i quali non è stata predisposta una specifica Parte Speciale, opera in ogni caso il complesso dei Presidi di controllo, organizzativi e procedurali, adottati dalla Società e richiamati nel presente Modello e nel Codice Etico.

3.3. **Aggiornamento del Modello**

Tenuto conto della complessità della struttura organizzativa della Società, per favorire la *compliance* delle diverse attività aziendali alle disposizioni del Decreto e, contemporaneamente, garantire un efficace controllo del rischio di commissione di Reati presupposto, è previsto un procedimento di monitoraggio continuo e di aggiornamento del Modello al verificarsi di una o più delle seguenti condizioni:

a. innovazioni legislative e/o giurisprudenziali della disciplina della responsabilità degli Enti per gli illeciti amministrativi dipendenti da reato;
b. significative modifiche della struttura organizzativa e/o dei settori di attività della Società;
c. significative violazioni del Modello, risultati del *risk assessment*, verifiche sull'efficacia del Modello, *best practice* di settore.

Il Modello è approvato dal Consiglio di Amministrazione di Telepass.

Il Modello è stato oggetto, successivamente alla prima emissione, di interventi di aggiornamento, in funzione dell'evoluzione del quadro normativo e organizzativo.

In particolare:

i. con riferimento alle integrazioni apportate al Decreto dalla Legge 62/2005 (cd. Legge comunitaria 2004) nonché dalla Legge 262/2005 (c.d. Legge sul risparmio), Telepass ha provveduto a un aggiornamento del Modello, affinché lo stesso tenesse conto dei rischi connessi alla commissione dei reati e illeciti amministrativi di manipolazione del mercato e abuso di informazioni riservate, nonché di omessa comunicazione del conflitto di interessi;
ii. successivamente, nell'aggiornamento del **2010**, sono state analizzate le estensioni della responsabilità degli Enti in relazione ai reati di omicidio e lesioni colpose in violazione della normativa in materia di sicurezza e igiene nei luoghi di lavoro, ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita contemplati dall'art. 25-octies; ai reati informatici e al trattamento illecito di dati; ai reati di criminalità organizzata; ai delitti contro l'industria e il commercio e in tema di violazione del diritto d'autore; e, infine, ai reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria;
iii. nel **2013** è stato analizzato l'ulteriore ampliamento del novero dei reati presupposto, in relazione ai reati ambientali, all'impiego di cittadini di paesi terzi il cui soggiorno è irregolare, all'induzione indebita a dare o promettere utilità, alla corruzione tra privati:
iv. nel **2017** sono state analizzate le estensioni della responsabilità amministrativa degli Enti in relazione al reato di autoriciclaggio, ai reati ambientali, di cui alla Legge n. 68/2015, e alle disposizioni in materia di reati contro la personalità individuale e impiego di cittadini di paesi terzi il cui soggiorno è irregolare, di delitti contro la pubblica amministrazione, di associazione di tipo mafioso e di falso in bilancio di cui alla Legge n. 69/2015. Inoltre, l'aggiornamento del 2017 rifletteva l'evoluzione dell'assetto organizzativo della Società;
v. nell'aggiornamento del **2019** sono state analizzate e introdotte le novità normative con riferimento a:
    a. aggiornamento al reato di "istigazione alla corruzione tra privati" previsto dalla D. Lgs. 38/2017 (art. 25-ter del D. Lgs. 231/2001);
    b. aggiornamento rispetto alle modifiche apportate al reato di "impiego di cittadini di paesi terzi il cui soggiorno è irregolare" previste dalla Legge 161/2017 (art. 25-duodecies del D. Lgs. 231/2001);

c. introduzione del reato "razzismo e xenofobia" previsto dalla Legge 167/2017 (art. 25-terdecies del D. Lgs. 231/2001), successivamente modificato D. Lgs. 21/2018;
d. introduzione delle "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" (*Whistleblowing*) previste dalla L. 179/2017;
e. modifiche apportate ai reati ambientali (art. 25-undecies del D. Lgs. 231/2001) dal D. Lgs. 21/2018;
f. modifiche apportate ai reati di abuso di mercato (art. 25-sexies, D. Lgs. 231/2001) dal D. Lgs. 107/2018;
g. introduzione della Legge n. 3/2019 intitolata "Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici";

vi. nell'aggiornamento del **2021** sono state analizzate e recepite nel Modello:
a. le novità normative relative all'introduzione dell'art. 25-quinquiesdecies "Reati tributari" inserito ad opera del c.d. Decreto Fiscale convertito in Legge n. 157/2019;
b. le modifiche apportate agli artt. 24, 25, 25-quinquiesdecies del D. Lgs. 231/2001 e inserimento del Reato di Contrabbando nel nuovo art. 25-sexiesdecies in attuazione della c.d. "Direttiva PIF" ad opera del D. Lgs. n. 75/2020[2];
c. le modifiche organizzative e procedurali che hanno interessato la Società;

vii. nell'aggiornamento del **2022** è stata effettuata una revisione complessiva del Modello in virtù, tra l'altro, delle seguenti esigenze:
a. fusione tra Telepass e la società controllata Telepass Pay S.p.A., perfezionatasi il 1° maggio 2022 e che ha portato alla creazione di un Patrimonio Destinato all'interno di Telepass per le attività di IMEL;
b. riorganizzazione interna di Telepass, dovuta sia alla fusione sia all'evoluzione delle attività della Società;
c. introduzione di nuovi reati presupposto astrattamente rilevanti per Telepass (i.e. i reati in materia di strumenti di pagamento diversi dai contanti, di cui al D.lgs. nr. 184/2021).

viii. nel **2024**, infine, vi sono stati alcuni aggiornamenti del Modello dovuti ai seguenti fattori:
a. modifica della normativa in materia di Whistleblowing a seguito della introduzione del D.lgs. nr. 24/2023 e delle attività di adeguamento di Telepass alla nuova disciplina;
b. introduzione di nuovi reati presupposto ad opera della Legge nr. 137/23, recante disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura;
c. conferimento in favore della controllata K-Master S.r.l.[3] del ramo di azienda di titolarità di Telepass costituito dalle unità organizzative "Smart Device Unit" e "R&D and Innovation Unit";

[2] Attuazione della Direttiva (UE) 2017/1371 "relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".
[3] Poi fusa per incorporazione in Infoblu S.p.A., che ha successivamente cambiato la denominazione in Telepass Innova S.p.A.

d. modifica della denominazione della società controllante “Atlantia S.p.A.” in “Mundys S.p.A.”;
e. acquisizione da parte di Telepass di una nuova controllata;
f. aggiornamento delle certificazioni ISO detenute da Telepass;

L’attività di aggiornamento svolta nel 2024 non ha richiesto una nuova valutazione dei rischi aziendali per le seguenti motivazioni:

- con riferimento all’indicazione di cui alla lett. a, si è proceduto ad una revisione complessiva della parte del MOG relativa al sistema di segnalazione, esplicitando le tutele previste dalla nuova normativa e facendo riferimento alla versione aggiornata della Procedura Gestione delle Segnalazioni; si è, infine, proceduto con l’inserimento di specifiche indicazioni nell’ambito del sistema disciplinare volte a sanzionare la mancata tutela del whistleblower;
- con riferimento all’indicazione di cui alla lett. b, i reati di nuova introduzione si inseriscono in aree a rischio già individuate nelle precedenti versioni del Modello di Telepass e la Società ha già in essere Protocolli di prevenzione idonei alla prevenzione anche di tale nuovi Reati presupposto;
- con riferimento all’indicazione di cui alla lett. c, si è proceduto alla revisione delle Parti Speciali su cui ha impattato la cessione del ramo di azienda, alla luce di un’analisi documentale (atto di cessione del ramo di azienda, contratti di service esistenti tra Telepass e la sua controllata) nonché ad un confronto con le funzioni di Telepass o di Telepass Innova S.p.A. maggiormente interessate;
- con riferimento alle indicazioni di cui alle lettere d – e - f si è proceduto ad una revisione sostanzialmente nominalistica.

In tutti i casi in cui le modifiche normative ovvero le modifiche aziendali impongano una rivalutazione dei rischi aziendali, la Società procede come di seguito descritto.

3.3.1 Mappatura delle attività a rischio di Reato

In primo luogo, vengono valutate le attività aziendali, gli ambiti organizzativi e i processi nell’ambito delle quali astrattamente potrebbe essere commesso uno dei Reati presupposto nell’interesse o a vantaggio della Società nonché quelle che potrebbero essere strumentali alla commissione di tali illeciti, rendendo possibile o agevolando il perfezionamento del Reato presupposto.

L’identificazione dei processi/attività a rischio viene attuata attraverso il previo esame della documentazione aziendale (organigrammi, processi principali, procure, disposizioni organizzative, ecc.), l’analisi dei processi critici della Società e la successiva effettuazione di una serie di interviste con i soggetti chiave nell’ambito dei processi/attività a rischio.

Pertanto, tra le Aree a rischio vengono considerate anche quelle che, oltre ad avere un rilievo **diretto** come attività che potrebbero integrare condotte di Reato, possono anche avere un rilievo **indiretto/strumentale** per la commissione degli stessi Reati. In particolare, si intendono strumentali quelle attività che possono creare le condizioni di fatto per la commissione dei Reati presupposto.

3.3.2 Risk assessment

Dalle interviste svolte e dalla documentazione analizzata si ottengono gli elementi necessari per svolgere l'attività di *risk assessment.*

A tal fine, in relazione ad ogni Area a rischio si valutata la possibilità di commissione di ogni singolo Reato presupposto previsto dal Decreto.

3.3.3 Presidi di controllo adottati da Telepass

Individuati i rischi potenziali, si procede ad analizzare il sistema dei Presidi esistenti nei processi/attività a rischio, al fine di valutarne l'adeguatezza nella prevenzione dei rischi di Reato.

In tale fase, pertanto, si provvede alla rilevazione dei Presidi di controllo interno esistenti (procedure formali e/o prassi adottate, verificabilità, documentabilità o "tracciabilità" delle operazioni e dei controlli, separazione o segregazione delle funzioni, ecc.) attraverso l'analisi delle informazioni e della documentazione fornita dalle strutture aziendali.

Nell'ambito delle attività di *risk assessment*, si analizzano le seguenti componenti del sistema di controllo preventivo:

1) sistema delle deleghe e delle procure;
2) sistema organizzativo;
3) sistema di controllo di gestione e dei flussi finanziari;
4) presidi;
5) sistema di controllo integrato.

Le verifiche sul sistema di controllo riguardano anche le attività svolte con il supporto di società del Gruppo Telepass o esterne (*outsourcing*).

Tali verifiche vengono condotte sulla base dei seguenti criteri:

- la formalizzazione delle prestazioni fornite in specifici contratti di servizi;
- la previsione di idonei presidi di controllo sull'attività in concreto espletata dalle società di servizi sulla base delle prestazioni contrattualmente definite;
- l'esistenza di procedure formalizzate/linee guida aziendali relative alla definizione dei contratti di servizi e all'attuazione dei presidi di controllo, anche con riferimento ai criteri di determinazione dei corrispettivi e alle modalità di autorizzazione dei pagamenti.

Sistema delle deleghe e delle procure

Telepass adotta un modello di amministrazione e controllo di tipo tradizionale, ove:

- il Consiglio di Amministrazione esercita la funzione di supervisione strategica;
- l'Amministratore Delegato esercita la funzione di gestione;
- il Collegio Sindacale esercita la funzione di controllo come da Statuto, mentre il controllo contabile è affidato ad una società di revisione.

Il Consiglio di Amministrazione ha istituito, in linea con l'art. 42 dello Statuto sociale approvato dall'Assemblea il 12 aprile 2021, i seguenti comitati endoconsiliari:

- Comitato Risorse Umane e Remunerazione;
- Comitato Controllo, Rischi e Sostenibilità;
- Comitato Tecnologia e Innovazione.

Così come richiesto dalla buona pratica aziendale e specificato anche nelle Linee Guida di Confindustria, il Consiglio di Amministrazione di Telepass attribuisce, determinandone il contenuto, e revoca le deleghe al Presidente, all'Amministratore Delegato ed eventualmente ad Amministratori investiti di particolari deleghe.

Il Consiglio di Amministrazione di Telepass conferisce formalmente al proprio Presidente, all'Amministratore Delegato e dirigenti (se necessario), poteri fino a una determinata soglia di spesa. Oltre tale soglia, è prevista la preventiva approvazione da parte del Consiglio di Amministrazione e il conferimento del conseguente mandato.

Il Presidente e l'Amministratore Delegato, nell'ambito dei poteri conferiti dal Consiglio di Amministrazione e in coerenza con le responsabilità organizzative e gestionali definite, conferiscono procure o deleghe operative ai dirigenti, dipendenti e anche a terzi, prevedendo una puntuale indicazione delle soglie di spesa.

Il livello di autonomia, il potere di rappresentanza ed i limiti di spesa assegnati ai vari titolari di deleghe e procure all'interno della Società risultano sempre individuati e fissati in stretta coerenza con il livello gerarchico del destinatario della delega o della procura. I poteri così conferiti sono aggiornati in funzione dei cambiamenti organizzativi intervenuti nella struttura della Società.

In materia di tutela della salute e sicurezza sul lavoro il Consiglio di Amministrazione ha conferito i poteri di Datore di lavoro al Chief People and Organization Officer.

In virtù della qualifica di **IMEL ibrido** acquisita dal 1° maggio 2022, Telepass ha costituito un patrimonio destinato inerente la moneta elettronica e i servizi di pagamento ("Patrimonio Destinato"), coincidente con il perimetro del ramo di attività e servizi sino a quella data svolti dalla società controllata Telepass Pay S.p.A. (fusa per incorporazione in Telepass). A tale proposito:

i) i beni e i rapporti giuridici assegnati al Patrimonio Destinato sono funzionali esclusivamente al soddisfacimento dei diritti degli utenti dei servizi di pagamento, costituendo, a tutti gli effetti, un patrimonio separato dal restante patrimonio generico di Telepass ("Patrimonio Libero");

ii) in caso di incapienza del Patrimonio Destinato, Telepass risponde anche con il restante proprio patrimonio delle obbligazioni nei confronti degli utenti dei servizi di pagamento e di quanti vantino diritti derivanti dall'esercizio delle attività accessorie e strumentali;

iii) Telepass deve tenere separatamente, per il Patrimonio Destinato, i libri e le scritture contabili prescritti dagli artt. 2214 e seguenti del Codice Civile, nel rispetto dei principi contabili internazionali; in particolare, gli Amministratori di Telepass devono redigere un separato rendiconto per il Patrimonio Destinato, da allegare al bilancio d'esercizio della Società;

iv) il rendiconto del Patrimonio Destinato deve essere oggetto di una specifica relazione redatta dal soggetto incaricato della revisione legale dei conti che attesti la coerenza dei dati ivi contenuti con quelli riportati nel bilancio di Telepass;

v) Telepass ha individuato e nominato con delibera del Consiglio di Amministrazione del 28 maggio 2021, un Direttore Generale e Responsabile del Patrimonio Destinato e delle funzioni aziendali dedicate alle attività di IMEL ibrido.

Il Direttore Generale, quale Responsabile del Patrimonio Destinato, ha, in sintesi, i seguenti compiti:

i) assicurare, con gli organi aziendali, che l'assetto organizzativo della Società sia adeguato alla sua dimensione, complessità e operatività e, a tal fine, gli è attribuita, a titolo esemplificativo e non esaustivo, la responsabilità di:
   a. definire, insieme all'Amministratore Delegato, i flussi informativi volti ad assicurare agli organi aziendali la conoscenza dei fatti di gestione rilevanti;
   b. definire compiti e responsabilità delle strutture aziendali a suo riporto, in modo, tra l'altro, da prevenire potenziali conflitti di interesse e assicurare che le strutture siano dirette da personale qualificato in relazione alle attività da svolgere;
   c. definire ed attuare la politica aziendale in materia di esternalizzazione di funzioni aziendali;
   d. assicurare, insieme all'Amministratore Delegato, che il personale e gli agenti utilizzati per la prestazione di servizi di pagamento, nonché il personale e i soggetti convenzionati utilizzati per la distribuzione e il rimborso della moneta elettronica, siano adeguatamente formati con riferimento ai prodotti commercializzati e ai servizi prestati, agli adempimenti in materia di prevenzione dei fenomeni di riciclaggio e di finanziamento al terrorismo, alla normativa in materia di trasparenza;

ii) definire le procedure di governo e controllo sui prodotti previste ai sensi delle Disposizioni di Trasparenza;

iii) con riferimento alla prestazione di servizi di pagamento e all'emissione di moneta elettronica, le decisioni di carattere strategico relative all'ingresso in nuovi settori e/o all'introduzione di nuovi prodotti e/o servizi vengono assunte dal Consiglio di Amministrazione sulla base delle proposte avanzate dall'Amministratore Delegato, previa consultazione e approvazione del Direttore Generale per le tematiche di natura regolamentare;

iv) definire la Procedura Generale Antiriciclaggio ("Policy AML") tenendo conto delle indicazioni e delle linee guida espresse dalle autorità competenti e dai diversi organismi internazionali nonché delle evoluzioni del quadro normativo, nonché definire le procedure di gestione e controlli interni nell'ambito della disciplina antiriciclaggio.

Sistema organizzativo

La struttura organizzativa interna della Società viene rappresentata:

- a livello macro, in un organigramma, nel quale sono specificate:
  - le strutture in cui si suddivide l'attività aziendale di 1° livello gerarchico con indicazione nominativa dei responsabili di ciascuna struttura;
  - le linee di dipendenza gerarchica;

- a livello micro, indicando, per ciascuna struttura:
  - l'articolazione organizzativa, con indicazione nominativa del responsabile, e linee di dipendenza gerarchica;
  - le risorse che operano nelle singole aree, il livello di inquadramento e la posizione organizzativa.

I documenti relativi alla struttura organizzativa interna vengono aggiornati periodicamente dalla struttura People and Organization.

In materia di salute e sicurezza sul lavoro, la Società, in linea con l'assetto organizzativo vigente e con i poteri conferiti dal Datore di Lavoro, individua le figure operanti in tale ambito e previste dal D. Lgs. 81/2008 nonché le relative responsabilità.

Nel processo di aggiornamento del Modello, la verifica dell'adeguatezza del sistema organizzativo è stata effettuata sulla base dei seguenti criteri:

- formalizzazione del sistema;
- chiara definizione delle responsabilità attribuite e delle linee di dipendenza gerarchica;
- esistenza della segregazione e contrapposizione di funzioni;
- corrispondenza tra le attività effettivamente svolte e quanto previsto dalle missioni e dalle responsabilità descritte nell'organigramma della Società.

Alcune strutture organizzative sono utilizzate esclusivamente per l'operatività del Patrimonio Destinato tra le quali:

- il **Responsabile Antiriciclaggio e Delegato SOS**, che ha il compito di prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo;
- il **Referente per le Attività Esternalizzate** ("RAE"), che è posto a diretto riporto del Direttore Generale. Ferme restando le competenze del Consiglio di Amministrazione e dell'Amministratore Delegato in relazione alle decisioni di esternalizzare le funzioni aziendali, il RAE ha il compito di gestire e supervisionare i rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni.

Al fine di garantire il rispetto della normativa regolamentare in tema di organizzazione amministrativa e contabile e in merito ai controlli interni, sono stati definiti, *inter alia*, i seguenti Presidi:

- il Consiglio di Amministrazione è coadiuvato nell'esercizio delle proprie competenze dai comitati endoconsiliari - in particolare dal Comitato Controllo, Rischi e Sostenibilità - i quali sono dotati di funzioni istruttorie e consultive con riferimento a qualsiasi tematica regolamentare collegata alla prestazione di servizi di pagamento e moneta elettronica e, dunque, all'operatività del Patrimonio Destinato;
- è stato predisposto un adeguato sistema dei controlli interni che vigila sulla conformità ai requisiti previsti dalle disposizioni dell'Autorità di vigilanza.

Inoltre, sussistono, sia per le attività rientranti nel Patrimonio Destinato sia per le attività non regolamentate, le seguenti funzioni/organismi a presidio:

- il **Data Protection Officer** ("DPO"), che ha il compito di assicurare il monitoraggio delle evoluzioni normative in ambito *privacy*, informare e fornire consulenza sugli obblighi relativi alla protezione dei dati, verificare l'attuazione del regolamento e delle disposizioni di legge relative alla protezione dei dati, nonché delle politiche adottate in

materia, fornire, ove richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati, fungere da punto di contatto con il Garante per la protezione dei dati personali;

- il **Chief Information Security Officer** ("CISO"), che ha il compito di assicurare il monitoraggio dei sistemi per la sicurezza informatica, oltre che di sviluppare e mettere in campo processi volti a mitigare i rischi informatici;
- **l'Ethics Officer**, che riferisce al Consiglio di Amministrazione e all'Amministratore Delegato e che ha il compito di monitorare sul rispetto del Codice Etico, anche rappresentando un punto di contatto a cui tutti i dipendenti di Telepass e delle società controllate possono rivolgersi in caso di dubbi di carattere etico, nonché di supportare la Società nella programmazione iniziative volte a mantenere una solida cultura etica;
- il **Team Segnalazioni**, le cui funzioni e compiti sono descritti al paragrafo 5.5 che segue.

Sistema di controllo di gestione e dei flussi finanziari

Il sistema di controllo di gestione operativa di Telepass è basato sui seguenti principi di controllo:

- definizione, su base annuale, delle risorse (monetarie e non) a disposizione delle singole strutture aziendali e del perimetro nell'ambito del quale tali risorse possono essere impiegate, attraverso la programmazione e definizione del budget;
- rilevazione/analisi degli scostamenti rispetto a quanto predefinito in sede di budget, analizzando le cause e riportando i risultati delle valutazioni agli appropriati livelli gerarchici per gli opportuni interventi di adeguamento, attraverso la relativa consuntivazione;
- monitoraggio della conformità del processo autorizzativo rispetto al sistema di deleghe e procure interno.

La gestione delle risorse finanziarie è definita sulla base di principi improntati alla segregazione delle funzioni, tale da garantire che tutti gli esborsi siano richiesti, effettuati e controllati da soggetti distinti.

La gestione della liquidità è ispirata a criteri di conservazione del patrimonio, con connesso divieto di effettuare operazioni finanziarie a rischio.

Telepass si avvale, inoltre, di un sistema di revisione legale dei conti.

Presidi

La Società ha messo a punto un complesso di procedure volto a regolamentare l'articolazione dei processi aziendali di cui l'organizzazione si compone, descrivendo le modalità di svolgimento delle attività, individuando i contenuti e le responsabilità nonché le attività di controllo e monitoraggio da espletare al fine di garantire la correttezza, l'efficacia e l'efficienza delle attività aziendali che abbiano particolare rilevanza e definiscono le corrette modalità di gestione da seguire.

Nelle Parti Speciali del presente Modello, saranno richiamate di volta in volta le procedure, le Policy, le linee guida e i protocolli comunque denominati implementati in Telepass.

La Società, inoltre, ha conseguito le seguenti Certificazioni:

1) ISO 45001:2018, Sistema di gestione per la salute e sicurezza sul lavoro;
2) ISO 27001:2022, Sistema di gestione della sicurezza delle informazioni;
3) ISO 14001:2015, Sistema di gestione ambientale;

4) ISO 9001:2015, Sistema di gestione della qualità.

La valutazione dell'adeguatezza dei Presidi, nel processo di aggiornamento del Modello, ha tenuto conto non soltanto delle fasi negoziali ma anche di quelle di istruzione e formazione delle decisioni aziendali.

In particolare, per quanto concerne le attività di IMEL, Telepass si è dotata di un complesso di procedure idonee alla prevenzione del rischio di riciclaggio e di finanziamento del terrorismo, richiamate nelle relative Parti Speciali.

Sistema di controllo integrato

Il sistema di controllo integrato di Telepass è articolato, come suggerito dalle *best practice* in materia, in tre livelli:

- 1° livello: anche detto "controllo di linea", ossia il controllo operato direttamente dai responsabili delle aree operative che hanno la responsabilità della gestione dei rischi e dell'attuazione dei Presidi di controllo;
- 2° livello: il controllo proprio delle strutture aziendali preposte al monitoraggio e alla gestione dei rischi tipici;
- 3° livello: il controllo svolto dalla Funzione Internal Audit del Gruppo Telepass.

Con riferimento ai **controlli di 2° livello**, Telepass ha adottato un sistema di controllo costituito da due funzioni:

1) la funzione Risk Management,
2) la funzione Compliance & AML Financial Services.

Nell'ambito della funzione di **Risk Management**, il Risk Officer ha il compito di concorrere alla definizione delle metodologie di misurazione dei rischi aziendali, di verificare il rispetto dei limiti assegnati alle varie strutture operative e di controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di Risk Appetite assegnati.

Il responsabile della funzione **Compliance & AML Financial Services**, riporta funzionalmente al Direttore Generale e Responsabile del Patrimonio Destinato e gerarchicamente all'Amministratore Delegato. Ha il compito di valutare l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione di norme imperative (leggi e regolamenti) e di autoregolamentazione (statuti, codici di condotta, codici di autodisciplina) applicabili a Telepass.

I **controlli di 3° livello** sono l'attività di controllo periodico svolta dalla funzione **Internal Audit**, la quale riporta direttamente al Consiglio di Amministrazione, così che il suo responsabile non sia sottoposto gerarchicamente ai responsabili delle funzioni sottoposte a controllo e si ispira agli *standard* metodologici internazionali per la pratica professionale dell'*internal auditing*: International Professional Practices Framework ("IPPF"). Nell'ambito del controllo di 3° livello, l'Internal Audit identifica e valuta l'adeguatezza e l'efficacia del Sistema di Controllo Interno e Gestione dei Rischi ("SCIGR") adottato sui processi e sulle attività oggetto di analisi, analizzando le evidenze acquisite con indipendenza, professionalità, integrità, obiettività, riservatezza e competenza. Inoltre, valuta i necessari aggiornamenti al Piano di Audit per rischi emergenti e considera, per

l'esecuzione di interventi "extra piano", gli *input* ricevuti - oltre che dagli Organi Sociali - anche dall'Organismo di Vigilanza.

Inoltre, il **Responsabile Anticorruzione** assicura il monitoraggio costante del rischio di corruzione e riferisce periodicamente sulle proprie attività all'Organismo di Vigilanza della Società, assicurando il raccordo con il medesimo Organismo per l'efficace assolvimento dei rispettivi compiti, nonché al Consiglio di Amministrazione e all'Amministratore Delegato.

In materia di tutela della **salute e sicurezza sul lavoro**, nel citato sistema di gestione integrato, la Società ha inoltre adottato e opportunamente formalizzato il sistema di monitoraggio degli adempimenti in materia, riferito direttamente ai Datori di Lavoro (sul punto si rimanda a quanto descritto nella Parte Speciale D).

L'analisi del sistema di controllo integrato, nel processo di aggiornamento del Modello, ha riguardato l'esistenza di un idoneo sistema di monitoraggio dei processi per la verifica dei risultati e di eventuali non conformità nonché l'esistenza di un idoneo sistema di gestione della documentazione, tale da consentire la tracciabilità delle operazioni.

Gap Analysis

Il disegno dei controlli rilevato viene quindi confrontato con le caratteristiche e gli obiettivi richiesti dal Decreto e/o suggeriti dalle Linee Guida di Confindustria e dalle migliori pratiche nazionali e internazionali.

La valutazione complessiva di adeguatezza del sistema di controllo viene effettuata tenendo conto del livello di rischio accettabile approvato di volta in volta dal Consiglio di Amministrazione.

3.4. Adozione di un modello o di meccanismi di *compliance* "231" da parte delle società controllate di Telepass

Ciascuna Società del Gruppo Telepass, in quanto singolarmente destinataria dei precetti del D. Lgs. 231/2001, è chiamata a valutare l'opportunità di predisporre e revisionare un proprio Modello di Organizzazione Gestione e Controllo ovvero dotarsi di meccanismi di *compliance* in materia "231" che tengano conto delle specificità aziendali (in termini di dimensioni, organizzazione e business, etc.), confermando l'autonomia della singola società nell'ambito del Gruppo.

Solo ciascuna società può, infatti, realizzare la puntuale ed efficace ricognizione e gestione dei rischi di possibile commissione di reato, necessaria affinché al modello sia riconosciuta l'efficacia esimente di cui all'art. 6 del Decreto.

La società controllata che si doti di un proprio modello, in base alla specifica realtà, istituisce un autonomo e indipendente Organismo di Vigilanza con il compito primario di vigilare sull'attuazione del Modello secondo le procedure in esso descritte e sulla base delle indicazioni contenute negli artt. 6 e 7 del Decreto.

Il Modello di Telepass rappresenta il punto di riferimento per la definizione dei modelli di organizzazione delle società controllate con particolare riguardo ai principi definiti nello stesso.

Resta ferma l'individuazione, da parte di ogni società controllata, delle attività sensibili e dei protocolli specifici in ragione delle peculiarità della propria realtà aziendale. In ogni caso, tutte le modifiche e integrazioni al Modello di Telepass devono essere tempestivamente comunicate alle società controllate affinché, nell'ambito della

richiamata autonomia, valutino l'eventuale opportunità di adeguamento dei rispettivi Modelli di Organizzazione Gestione e Controllo o dei meccanismi di *compliance* adottati.

3.5. **Comunicazione del Modello**

Telepass promuove la conoscenza del Modello, del sistema normativo interno e dei relativi aggiornamenti tra tutti i Destinatari con grado di approfondimento diversificato a seconda della posizione e del ruolo.

I Destinatari sono quindi tenuti a conoscerne il contenuto, ad osservarlo e contribuirne all'attuazione, anche mediante la formazione obbligatoria in materia di *compliance* "231".

Per i dipendenti, il Modello è reso disponibile sulla intranet "T-Space" digitale, a cui gli stessi possono accedere nello svolgimento ordinario dell'attività lavorativa.

All'assunzione viene, inoltre, consegnata ai dipendenti l'Informativa sulle disposizioni aziendali, in cui viene fatta menzione, tra l'altro, del Modello e delle disposizioni normative d'interesse per la Società, la cui conoscenza è necessaria per il corretto svolgimento delle attività lavorative.

La Parte Generale del presente Modello e il Codice Etico sono messi a disposizione dei soggetti terzi e di qualunque altro interlocutore della Società che sia tenuto al rispetto delle relative previsioni, mediante pubblicazione sul sito internet della Società.

4. ORGANISMO DI VIGILANZA

4.1. Identificazione dell'Organismo di Vigilanza

In attuazione del Decreto e nel rispetto delle previsioni delle Linee Guida di Confindustria, il Consiglio di Amministrazione di Telepass ha istituito un organismo ("Organismo di Vigilanza" o "OdV") cui ha affidato il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello nonché di curarne l'aggiornamento.

In considerazione della specificità dei compiti che ad esso fanno capo, l'Organismo di Vigilanza è plurisoggettivo, con almeno un componente esterno, che assume la funzione di Coordinatore. Gli altri componenti dell'Organismo di Vigilanza sono individuati sia tra soggetti esterni sia tra soggetti interni alla Società, non sottoposti, nell'ambito dello svolgimento della propria mansione, al potere gerarchico di alcun organo o funzione societaria.

4.2. Nomina

I componenti dell'Organismo di Vigilanza sono nominati dal Consiglio di Amministrazione che provvede a individuare il Coordinatore. La nomina sarà comunicata a ciascun componente dell'Organismo di Vigilanza attraverso il sistema di comunicazione delle delibere del Consiglio di Amministrazione. Ciascun componente dell'Organismo di Vigilanza, a sua volta, dovrà accettare formalmente l'incarico.

La composizione, i compiti, le prerogative e le responsabilità dell'Organismo di Vigilanza nonché le finalità della sua costituzione sono comunicati a tutti i livelli aziendali.

4.3. Requisiti dell'Organismo di Vigilanza

Sulla base di quanto disposto dagli artt. 6 e 7 del Decreto e tenendo nel debito conto le Linee Guida di Confindustria, dovranno sempre essere adeguatamente garantite l'autonomia e l'indipendenza, la professionalità e la continuità di azione dell'Organismo di Vigilanza.

L'autonomia e l'indipendenza, delle quali l'Organismo di Vigilanza deve necessariamente disporre, sono assicurate anche dalla presenza, con funzioni di Coordinatore, di un autorevole componente esterno, privo di mansioni operative e di interessi che possano condizionarne l'autonomia di giudizio. Inoltre, l'Organismo di Vigilanza opera in assenza di vincoli gerarchici nel contesto della *corporate governance* societaria, riportando al Consiglio di Amministrazione, al Collegio Sindacale, nonché al Presidente e Amministratore Delegato.

Nella individuazione dei componenti dell'OdV, il Consiglio di Amministrazione tiene conto delle specifiche competenze ed esperienze professionali, sia nel campo giuridico, in particolare nel settore della prevenzione dei reati *ex* D. Lgs. 231/2001 e nel diritto penale, che nella gestione ed organizzazione aziendale, al fine di assicurarne la professionalità.

Inoltre, tenuto conto della peculiarità delle attribuzioni e dei contenuti professionali specifici richiesti nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza di Telepass si avvale del supporto delle altre strutture della Società o del Gruppo Telepass e/o di eventuali consulenti esterni che, di volta in volta, si rendano a tal fine necessari.

La continuità di azione è garantita dalla circostanza che l'OdV opera presso la Società e che i suoi componenti hanno una conoscenza effettiva ed approfondita dei processi aziendali, essendo così in grado di avere immediata conoscenza di eventuali criticità.

La nomina quale componente dell'Organismo di Vigilanza è condizionata all'assenza di cause di incompatibilità con la nomina stessa e al possesso dei requisiti di onorabilità. In

particolare, costituiscono motivi di ineleggibilità e/o di decadenza da componente dell'Organismo di Vigilanza:

- essere Amministratore o componente del Collegio Sindacale di Telepass e/o delle società dalla stessa controllate;
- avere rapporti di coniugio, parentela o di affinità entro il quarto grado con Amministratori o con i componenti del Collegio Sindacale di Telepass;
- intrattenere, direttamente o indirettamente, con esclusione del rapporto di lavoro a tempo indeterminato in essere, relazioni economiche e/o rapporti contrattuali, a titolo oneroso o gratuito, con Telepass, e/o con i rispettivi Amministratori, di rilevanza tale da condizionarne l'autonomia di giudizio;
- essere titolare, direttamente o indirettamente, di partecipazioni azionarie in Telepass tali da permettere di esercitare il controllo o un'influenza notevole sulla società, ovvero comunque da comprometterne l'indipendenza;
- essere titolari di deleghe, procure o, più in generale, poteri o compiti che possano minarne l'indipendenza del giudizio.

In relazione ai requisiti di onorabilità che i componenti dell'Organismo di Vigilanza devono possedere, costituisce causa di ineleggibilità e di incompatibilità alla permanenza nella carica l'essere imputato di delitto doloso ovvero essere raggiunto da un provvedimento cautelare personale.

4.4. **Durata e revoca**

La determinazione della durata dell'incarico di componente dell'Organismo di Vigilanza spetta al Consiglio di Amministrazione. In ogni caso, ciascun componente dell'Organismo di Vigilanza rimane in carica fino alla nomina del suo successore o alla costituzione del nuovo Organismo.

La revoca dell'Organismo di Vigilanza o di un suo componente compete esclusivamente al Consiglio di Amministrazione, sentito il Collegio Sindacale. Il Consiglio di Amministrazione può revocare per giusta causa, in qualsiasi momento, i componenti dell'Organismo di Vigilanza. Per giusta causa di revoca deve intendersi: a) l'interdizione o l'inabilitazione, ovvero una grave infermità che renda il componente dell'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni di vigilanza; b) l'attribuzione al componente dell'Organismo di Vigilanza di funzioni e responsabilità operative incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo di Vigilanza; c) un grave inadempimento dei doveri propri dell'Organismo di Vigilanza, così come definiti nel Modello; d) il venir meno all'obbligo di riservatezza; e) il venir meno dei requisiti di onorabilità.

Qualora la revoca del mandato sia esercitata nei confronti di tutti i componenti dell'Organismo di Vigilanza, il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, provvederà ad istituire un nuovo Organismo.

Ove sussistano gravi ragioni, il Consiglio di Amministrazione procederà a disporre – sentito il parere del Collegio Sindacale e, ove non coinvolti, degli altri componenti dell'Organismo di Vigilanza – la sospensione dalle funzioni di uno o tutti i componenti dell'Organismo di Vigilanza, provvedendo tempestivamente alla nomina di un nuovo componente o dell'intero Organismo di Vigilanza.

4.5. **Funzioni e poteri dell'Organismo di Vigilanza**

All'Organismo di Vigilanza di Telepass è affidato sul piano generale il compito:

a) di vigilare sull'adeguatezza del Modello a prevenire la commissione dei Reati di cui al Decreto;

b) di vigilare sull'osservanza delle prescrizioni del Modello da parte dei Destinatari interni alla Società e di promuovere la stessa osservanza anche da parte dei Terzi destinatari (consulenti, fornitori, ecc.);

c) di curare l'aggiornamento del Modello in relazione all'evoluzione della struttura organizzativa, del quadro normativo di riferimento o a seguito dell'attività di vigilanza in esito alla quale siano scoperte significative violazioni delle prescrizioni.

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

- effettuare costantemente una ricognizione delle attività aziendali e della normativa di riferimento, per l'aggiornamento da parte della Società della mappatura delle attività a rischio reato e proporre l'aggiornamento e l'integrazione del Modello e delle procedure, ove se ne evidenzi la necessità;
- monitorare la validità nel tempo del Modello e delle procedure e la loro effettiva attuazione, promuovendo, anche previa consultazione delle strutture aziendali interessate, tutte le azioni necessarie al fine di assicurarne l'efficacia. Tale compito comprende la formulazione di proposte di adeguamento e la verifica successiva dell'attuazione e della funzionalità delle soluzioni proposte;
- effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle attività a rischio;
- verificare i poteri autorizzativi e di firma esistenti, al fine di accertare la loro coerenza con le responsabilità organizzative e gestionali definite e proporre il loro aggiornamento e/o modifica ove necessario;
- definire e curare, in attuazione del Modello, il flusso informativo periodico, secondo una frequenza adeguata al livello di rischio reato delle singole aree, che consenta all'Organismo di Vigilanza di essere periodicamente aggiornato dalle strutture aziendali interessate sulle attività valutate a rischio di reato, nonché stabilire modalità di comunicazione, al fine di acquisire conoscenza di presunte violazioni del Modello;
- attuare, in conformità al Modello, un flusso informativo periodico verso gli organi sociali competenti in merito all'efficacia e all'osservanza del Modello;
- condividere i programmi di formazione promossi dalla Società per la diffusione della conoscenza e la comprensione del Modello;
- verificare le iniziative adottate dalla Società per agevolare la conoscenza e la comprensione del Modello e delle procedure ad esso relative, da parte di tutti coloro che operano per conto della Società;
- verificare la fondatezza delle segnalazioni pervenute in merito a comportamenti indicati come integranti fattispecie di reato previste dal Decreto;
- accertare le cause che hanno condotto alla presunta violazione del Modello e di chi l'abbia commessa;
- verificare le violazioni del Modello segnalate o apprese direttamente e curare la loro comunicazione alle competenti strutture a fini disciplinari.

Per lo svolgimento dei propri compiti, all'Organismo di Vigilanza sono attribuiti i poteri qui di seguito indicati:

- accedere ad ogni documento e/o informazione aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo di Vigilanza ai sensi del Modello. È fatto obbligo, in capo a qualunque funzione aziendale, dipendente e/o componente degli organi sociali, di fornire le informazioni in loro possesso a fronte di richieste da parte dell'Organismo di Vigilanza o al verificarsi di eventi o circostanze rilevanti ai fini dello svolgimento delle attività di competenza dello stesso;
- accedere, senza necessità di alcun consenso preventivo, presso tutte le strutture della Società onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei propri compiti;
- ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di competenza;
- assicurarsi che i responsabili delle strutture aziendali forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste;
- richiedere, qualora si renda necessario, l'audizione diretta dei dipendenti, degli Amministratori e dei Componenti del Collegio Sindacale della Società;
- richiedere informazioni a consulenti esterni, partner commerciali e revisori.

Ai fini di un migliore e più efficace espletamento dei compiti e delle funzioni attribuiti, l'Organismo di Vigilanza si può avvalere, per supportare lo svolgimento della propria attività operativa, della Funzione Internal Audit di Gruppo Telepass, in coordinamento con la stessa, nonché delle altre strutture aziendali, che di volta in volta si potranno rendere utili per l'espletamento delle attività indicate.

A garanzia della propria indipendenza, l'Organismo di Vigilanza si rapporta direttamente al Consiglio di Amministrazione e, nell'espletamento delle proprie funzioni, agisce in piena autonomia disponendo di mezzi finanziari adeguati ad assicurargli totale indipendenza operativa.

A tal fine, il Consiglio di Amministrazione assegna all'Organismo di Vigilanza i mezzi finanziari dallo stesso indicati per le spese da sostenere nell'espletamento dell'incarico.

Nello svolgimento delle attività operative delegate dall'OdV, le strutture incaricate riferiscono solo all'OdV del proprio operato e, parimenti, l'OdV risponde al Consiglio di Amministrazione dell'attività svolta per suo conto da parte di strutture aziendali e di consulenti esterni.

4.6. **Reporting verso gli Organi Sociali**

L'Organismo di Vigilanza riferisce annualmente della propria attività al Consiglio di Amministrazione ed al Collegio Sindacale, fatte salve particolari esigenze dell'Organismo di Vigilanza di fornire relazioni o rivolgere altre comunicazioni in genere al Consiglio di Amministrazione, al Collegio Sindacale o ad altri organi anche in altri momenti. In particolare, la relazione avrà ad oggetto:

- l'attività complessivamente svolta nel corso del periodo, con particolare riferimento al monitoraggio dell'adeguatezza e dell'effettiva attuazione del Modello;
- le criticità emerse sia in termini di comportamenti o eventi interni alla Società, che possano comportare violazioni delle prescrizioni del Modello;
- gli interventi correttivi e migliorativi del Modello proposti ed il loro stato di attuazione;

- eventuali segnalazioni ricevute nel corso dell'anno e delle azioni intraprese dall'Organismo di Vigilanza stesso e dagli altri soggetti interessati;
- ogni altra informazione ritenuta utile allo scopo.

L'OdV dovrà, inoltre, riferire tempestivamente al Presidente e all'Amministratore Delegato in merito a:

- qualsiasi violazione del Modello ritenuta fondata, di cui sia venuto a conoscenza per segnalazione da parte dei dipendenti o che abbia accertato l'Organismo di Vigilanza stesso;
- rilevate carenze organizzative o procedurali idonee a determinare il concreto pericolo di commissione di reati rilevanti ai fini del Decreto;
- modifiche normative particolarmente rilevanti ai fini dell'attuazione ed efficacia del Modello;
- mancata collaborazione da parte delle strutture aziendali;
- ogni altra informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte del Presidente e dell'Amministratore Delegato.

4.7. **Regolamento di funzionamento dell'Organismo di Vigilanza**

Con apposito regolamento, l'Organismo di Vigilanza disciplina ed approva il proprio funzionamento interno ("Regolamento dell'Organismo di Vigilanza").

4.8. **Rapporti tra l'Organismo di Vigilanza e gli Organismi di Vigilanza delle società del Gruppo Telepass**

Nel rispetto della reciproca autonomia e della riservatezza delle informazioni afferenti alle diverse società del Gruppo Telepass, l'Organismo di Vigilanza può relazionarsi con gli Organismi di Vigilanza, ove presenti, delle società controllate per l'efficace attuazione dei rispettivi modelli.
I flussi comunicativi possono riguardare le modalità di programmazione delle attività, le iniziative assunte, eventuali violazioni del Modello, sanzioni applicate e criticità riscontrate nell'attività di vigilanza al fine di individuare e conoscere settori di attività rivelatisi a rischio.

4.9. **Rapporti tra l'Organismo di Vigilanza e il Collegio Sindacale**

Nel rispetto della reciproca autonomia, l'Organismo di Vigilanza informa il Collegio Sindacale, a richiesta dello stesso, in merito all'osservanza e all'aggiornamento del Modello.

5. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

5.1. Flussi informativi trasmessi dalle strutture aziendali

L'obbligo di un flusso informativo strutturato è uno degli strumenti per garantire l'attività di vigilanza sull'adeguatezza ed efficacia del Modello da parte dell'OdV e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto.

Dovrà essere portata a conoscenza dell'Organismo di Vigilanza, oltre a quanto previsto nelle Parti Speciali del Modello e nelle procedure aziendali, ogni informazione utile proveniente anche da terzi ed attinente all'attuazione del Modello nelle attività "a rischio".
In particolare, le strutture organizzative aziendali, ciascuna per la parte di propria competenza, sono tenute a riferire all'Organismo di Vigilanza qualsiasi notizia relativa a:

- la commissione di reati o compimento di atti idonei alla realizzazione degli stessi;
- la realizzazione di illeciti amministrativi;
- comportamenti non in linea con le regole di condotta previste dal presente Modello e dai protocolli ad esso relativi;
- eventuali variazioni nella struttura aziendale od organizzativa e nelle procedure vigenti;
- eventuali variazioni del sistema di deleghe e procure;
- operazioni di particolare rilievo o che presentino profili di rischio tali da indurre a ravvisare il ragionevole pericolo di commissione di reati;
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, nei confronti di dipendenti o collaboratori di Telepass nell'esercizio delle loro funzioni lavorative o di Telepass o di una sua società controllata;
- richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento penale4;
- rapporti predisposti dai responsabili delle strutture aziendali nell'ambito della loro attività di controllo e dai quali emergono possibili violazioni delle regole del MOG;
- notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate oppure dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- avvio di interventi di natura ispettiva da parte di organismi pubblici (magistratura, Guardia di Finanza, altre Autorità, ecc.) nell'ambito delle attività a rischio.

Altri flussi informativi da trasmettere all'OdV sono richiamati nella relativa procedura dedicata.

Come meglio specificato nella Procedura Gestione delle Segnalazioni e nel paragrafo 5.4. del presente Modello, è possibile indirizzare direttamente all'Organismo di Vigilanza anche le segnalazioni relative a presunte violazioni del Modello.
L'Organismo di Vigilanza agisce in modo da garantire i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante secondo quanto previsto dalla normativa in materia di

[4] Cfr. Linee Guida "Regole di Condotta relative alla gestione del patrocinio legale di dipendenti e dirigenti coinvolti in procedimenti giudiziari" del 01/04/2021.

Whistleblowing, dalla Procedura Gestione delle Segnalazioni e dalle indicazioni del Modello organizzativo.
La Società, al fine di consentire l'inoltro delle segnalazioni anche direttamente all'Organismo di Vigilanza, ha attivato dei canali di comunicazione dedicati:

- casella di posta elettronica: organismodivigilanza@telepass.it;
- posta ordinaria all'indirizzo: Organismo di Vigilanza, Telepass S.p.A., Via Laurentina n. 449 – 00142 Roma

La gestione della Segnalazione avviene secondo le modalità descritte dal par. 5.4 del presente Modello, a cui si fa integrale rimando.

5.2. **Obblighi di informativa relativi ad atti ufficiali**

Oltre alle informazioni di cui al paragrafo precedente, devono essere obbligatoriamente trasmesse all'OdV di Telepass le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto riferibili alla Società;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto riferibili alla Società;
- i rapporti preparati dai responsabili delle strutture aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

5.3. **Raccolta, conservazione e accesso all'archivio dell'OdV**

L'intera documentazione inerente i flussi informativi ricevuti deve essere conservata a cura del Segretario dell'Organismo di Vigilanza.

5.4. **Whistleblowing**

Il *whistleblowing* è un istituto giuridico di matrice comunitaria finalizzato a prevenire la commissione di illeciti nelle organizzazioni pubbliche e private e a tutelare i soggetti che segnalano illeciti o attività fraudolente svolte all'interno della struttura (pubblica o privata) di appartenenza.
Tale istituto era stato già disciplinato, per il settore privato, dal D. Lgs. 231/2001 (art. 6, commi 2-*bis*, 2-*ter*, 2-*quater*).
Con il D. Lgs. n. 24/2023 – strumento normativo con cui si è data attuazione della Direttiva Europea 2019/1937 sulla protezione dei Whistleblower - si è resa obbligatoria l'adozione di un sistema di *whistleblowing* per determinate tipologie di imprese operanti nel settore privato e si sono disciplinate le modalità di gestione operativa della segnalazione.
L'Autorità Nazionale Anticorruzione ha poi emanato specifiche Linee Guida contenenti la disciplina di dettaglio per la predisposizione di idonei canali per la gestione delle segnalazioni[5], a cui Telepass si è uniformata.

[5] Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne del 12 luglio 2023.

Per adeguarsi alla nuova normativa, Telepass, che già nel vigore della precedente normativa si era dotata di un sistema di gestione del whistleblowing, ha aggiornato la procedura di Gestione delle Segnalazioni, applicabile a tutte le società del Gruppo Telepass.

Tale procedura disciplina:

- il processo di ricezione, analisi e trattamento delle segnalazioni;
- le modalità di gestione della relativa istruttoria, nel rispetto della normativa in materia di privacy e/o altra normativa vigente nel Paese dove si è verificato il fatto segnalato, applicabile al soggetto e all'oggetto della segnalazione:
- le tutele garantite al segnalante e agli altri soggetti individuati dalla legge;
- il contenuto delle segnalazioni;
- i ruoli, le responsabilità e gli ambiti di applicazione.

Telepass, al fine di facilitare la trasmissione delle segnalazioni, si è dotato dei seguenti canali ufficiali:

- posta elettronica, all'indirizzo mail: segnalazioni.telepass@telepass.com;
- posta ordinaria, all'indirizzo: Telepass S.p.A., Team Segnalazioni, via Laurentina, 449 - 00142 Roma;
- piattaforma informatica, accessibile da parte di tutti i Segnalanti (dipendenti, terzi, ecc.) sul sito internet di Telepass.

Le segnalazioni in forma orale possono essere effettuate attraverso idonei canali (es. casella vocale) o attraverso un incontro diretto con il Team Segnalazioni o uno o più componenti, su richiesta del segnalante.

La piattaforma digitale non sostituisce gli altri canali di segnalazione ma amplia le possibilità di inviare una segnalazione: consente, infatti, a chiunque (dipendenti e collaboratori, fornitori e qualsiasi altro soggetto che abbia avuto od intenda avere rapporti d'affari con le Società del Gruppo) di segnalare ipotesi di condotte illecite o irregolarità, violazioni di norme, violazioni del Modello, violazioni del Codice Etico, violazioni della Policy Anticorruzione e comunque violazioni di procedure e disposizioni aziendali in genere.

In particolare, il segnalante, pur dovendosi registrare alla piattaforma, ha la facoltà di effettuare segnalazioni non nominative in quanto, le relative credenziali di accesso, ove presenti, sono custodite, protette ed accessibili esclusivamente dal soggetto terzo che gestisce la piattaforma e non sono associate alla segnalazione trasmessa a Telepass.

Il segnalante, se lo ritiene, può altrimenti indicare nella segnalazione il proprio nominativo fornendo espresso consenso affinché le proprie generalità siano comunicate al Team Segnalazioni.

Per le segnalazioni trasmesse attraverso i canali di posta cartacea ed elettronica, la riservatezza della identità del segnalante (come anche del contenuto della segnalazione) è tutelata con le seguenti modalità:

- la corrispondenza cartacea indirizzata al Team Segnalazioni viene consegnata in busta chiusa (così come recapitata dal servizio postale) alla Segreteria Tecnica del Team Segnalazioni;
- alla casella mail possono accedere esclusivamente i componenti del Team Segnalazioni e la Segreteria Tecnica; l'amministratore del sistema di posta elettronica aziendale competente può accedere alla casella di riferimento esclusivamente per necessità tecniche, previa richiesta motivata caso per caso da

inoltrare per iscritto al Coordinatore del Team Segnalazioni, e l'accesso sarà consentito solo dietro preventiva autorizzazione scritta del Coordinatore del Team Segnalazioni.

In tutti i casi in cui sia stato comunicato il nominativo del segnalante, nella trattazione delle segnalazioni da parte del Team Segnalazioni lo stesso nominativo viene separato dal contenuto della segnalazione e sostituito con il codice alfanumerico attribuitogli in fase di prima annotazione nell'apposito Registro custodito presso la Segreteria Tecnica.

Qualora la contestazione sulla segnalazione sia fondata, in tutto o in parte, e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. È dato avviso alla persona segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, secondo quanto previsto dalla normativa.

Nei seguenti casi, invece, non si è tenuti per legge a tutelare la riservatezza della identità della persona segnalante:

- la segnalazione risulti falsa e fatta allo scopo di danneggiare o recare pregiudizio al segnalato (c.d. "segnalazione in mala fede") e si configuri una responsabilità a titolo di calunnia o di diffamazione ai sensi di legge;
- nella segnalazione vengano rivelati fatti e/o circostanze tali che, seppur estranei alla sfera aziendale, rendano opportuna e/o dovuta la segnalazione all'Autorità Giudiziaria (ad es. reati di terrorismo, spionaggio).

L'organismo collegiale deputato a gestire il processo di valutazione delle segnalazioni è il **Team Segnalazioni**, il quale esercita le proprie funzioni su Telepass e su tutte le società da quest'ultima controllate, nel rispetto di quanto indicato nella Procedura sulla Gestione delle segnalazioni.

Il **Team Segnalazioni** presenta all'Organismo di Vigilanza e al Responsabile Anticorruzione (se e per quanto di rispettiva competenza) i risultati dell'istruttoria prima della chiusura definitiva della stessa, allo scopo di raccogliere le eventuali ulteriori esigenze di approfondimento. Se le segnalazioni non sono attinenti alla materia della *compliance* "231" o dell'anticorruzione, le inoltra al diverso soggetto competente.

Il Gruppo Telepass garantisce la riservatezza dell'identità del segnalante a partire dalla fase di ricezione della segnalazione, nel rispetto delle previsioni di legge.

Nel rispetto della legge, Telepass vieta e sanziona ogni forma di ritorsione o di discriminazione nei confronti di chiunque abbia effettuato una segnalazione, a prescindere che la segnalazione si sia poi rivelata fondata o meno.

I divieti di ritorsione e le misure di protezione previste per il whistleblower si applicano anche:

- al facilitatore (colui che aiuta il segnalante nell'effettuazione della segnalazione);
- alle persone che sono legate al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone;

Per "atto di ritorsione" deve intendersi qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'Autorità Giudiziaria o contabile o della divulgazione pubblica e che provoca o può

provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto. Le condotte di natura ritorsiva sono esemplificate all'art. 17, comma 4 del D. Lgs. n. 24/2023.

L'assenza di natura ritorsiva dei comportamenti, atti o omissioni previsti dall'art. 17 del D. Lgs n. 24/2023 nei confronti del segnalante deve essere provata da colui che li ha posti in essere; salvo prova contraria, si presume che gli stessi siano conseguenza della segnalazione.

Tutto il personale del Gruppo Telepass, coinvolto a vario titolo nella gestione delle segnalazioni, è tenuto a garantire la riservatezza sull'esistenza e sul contenuto della segnalazione, nonché sulla identità dei soggetti segnalanti (ove comunicati) e segnalati. Inoltre, costituiscono condotte sanzionabili sia la violazione da parte di un Destinatario delle misure di tutela del segnalante definite dalla Società che l'effettuazione, con dolo o colpa grave, di segnalazioni che si rivelino infondate.
Si sottolinea a riguardo che, sia in fase di trasmissione della Segnalazione, sia in fase di gestione e archiviazione della Segnalazione, sono messe in atto le misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali, in conformità con la normativa privacy.

Quanto al contenuto della segnalazione, essa deve riguardare:

- violazioni (o presunte tali) del Codice Etico, del Modello, della Policy Anticorruzione o del quadro normativo aziendale interno (policy, procedure, ecc.).;
- eventi suscettibili di arrecare un pregiudizio patrimoniale o di immagine al Gruppo Telepass;
- violazioni (o presunte tali) di normative nazionali o europee, come definite dall'art. 2, comma 1 lett a) del D.lgs. nr. 24 del 2023[6].

Come stabilito dalla legge, infine, la segnalazione non deve riguardare contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante.

[6] Si tratta, nello specifico, di: (i) illeciti amministrativi, contabili, civili e penali che ledono gli interessi, il decoro e l'integrità della società; (ii) condotte illecite rilevanti ai sensi del D.Lgs. 231/01 o violazioni del Modello di Organizzazione, Gestione e Controllo; (iii) illeciti che rientrano nell'ambito della Direttiva Comunitaria che disciplina specifici settori quali appalti pubblici, servizi, prodotti, sicurezza dei trasporti, tutela dell'ambiente, radioprotezione e sicurezza nucleare, sicurezza degli alimenti e dei mangimi e salute e benessere degli animali, salute pubblica, protezione dei consumatori e tutela dei dati personali sicurezza delle reti e dei sistemi informativi; (iv) atti e omissioni che ledono gli interessi finanziari dell'Unione; (v) atti e omissioni riguardanti il mercato interno dell'Unione Europea.

6. FORMAZIONE

6.1. Formazione del personale

La formazione del personale è un importante requisito dell'attuazione del Modello. Telepass si impegna a agevolare e promuovere la conoscenza del Modello da parte del *management* e dei dipendenti, con grado di approfondimento anche diversificato a seconda di posizione e ruolo, e il loro contributo costruttivo all'approfondimento dei suoi principi e contenuti.

I principi e i contenuti del D. Lgs. 231/2001 e del Modello sono divulgati mediante corsi di formazione la cui partecipazione è obbligatoria. La struttura dei corsi di formazione è approvata dall'Organismo di Vigilanza su proposta delle funzioni aziendali competenti.

La funzione People and Organization gestisce la formazione del personale della Società diffondendo la conoscenza del Decreto e del Modello attraverso uno specifico piano e provvede a fornire all'Organismo di Vigilanza una periodica informativa su tali attività.

La tracciabilità della partecipazione ai momenti formativi sulle disposizioni del Decreto è attuata attraverso la richiesta della firma di presenza nell'apposito modulo oppure, per quanto concerne le attività in modalità *e-learning*, attraverso l'attestato di fruizione dei nominativi o comunque tramite altra modalità di registrazione della finalizzazione del corso.

Eventuali sessioni formative di aggiornamento, oltre che una specifica informativa sul tema fornita ai neoassunti nell'ambito del processo di inserimento nella Società, saranno effettuate in caso di rilevanti modifiche apportate al Modello, al Codice Etico o relative a sopravvenute normative rilevanti per l'attività della Società.

6.2. Informativa a collaboratori e partner

Telepass promuove la conoscenza e l'osservanza del Codice Etico e della presente Parte Generale del Modello anche tra i *partner* commerciali e finanziari, i consulenti, i collaboratori a vario titolo, i clienti ed i fornitori della Società. I documenti sono disponibili sul sito istituzionale della Società.

Al fine di formalizzare l'impegno al rispetto dei principi del Codice Etico e della presente Parte Generale del Modello da parte di terzi aventi rapporti contrattuali con la Società, è previsto l'inserimento nel contratto di riferimento di una apposita clausola risolutiva espressa. Tale clausola prevede la facoltà della Società di risolvere il contratto di diritto e con effetto immediato nell'ipotesi di violazione del Codice Etico e/o della presente Parte Generale del Modello da parte del contraente.

Inoltre, la Società ha adottato una serie di protocolli e procedure volte alla migliore selezione – anche sul piano etico e di compliance - delle controparti contrattuali.

In questo modo, Telepass persegue l'obiettivo di interfacciarsi con soggetti che condividono i principi etici della Società e che perseguono il medesimo obiettivo di legalità.

7. SISTEMA DISCIPLINARE

Ai sensi degli artt. 6 e 7 del D. Lgs. 231/2001, ai fini dell'efficace attuazione del Modello deve essere, tra l'altro, previsto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso indicate.

Telepass, quindi, ha adottato un sistema disciplinare volto a sanzionare le violazioni dei principi e delle misure previsti nel Modello e nei protocolli aziendali, nel rispetto delle vigenti disposizioni di legge nonché delle norme previste dalla contrattazione collettiva nazionale, da parte dei Destinatari del Modello.

Sulla base di quanto indicato dall'art. 5 del Decreto, sono passibili di sanzione sia le violazioni del Modello e dei protocolli aziendali commesse dai soggetti posti in posizione "Apicale" sia dai soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto della Società. Inoltre, sono soggetti destinatari del presente Sistema disciplinare gli eventuali collaboratori e *partner* della Società.

L'instaurazione del procedimento disciplinare e l'eventuale applicazione di sanzioni, prescinde dalla pendenza o meno di un procedimento penale per lo stesso fatto e non tiene conto del suo esito.

7.1. Condotte rilevanti

Ai fini del presente Sistema disciplinare e nel rispetto delle previsioni e della contrattazione collettiva, costituiscono condotta rilevante, per l'applicazione di eventuale sanzione, le azioni o i comportamenti, anche omissivi, posti in essere in violazione del Modello.

Nell'individuazione della sanzione correlata si tiene conto dei profili oggettivi e soggettivi della condotta rilevante. In particolare, gli elementi oggettivi della condotta rilevante, graduati in un ordine crescente di gravità, sono:

1. violazioni del Modello che non hanno comportato esposizione a rischio o hanno comportato modesta esposizione a rischio;
2. violazioni del Modello che hanno comportato una apprezzabile o significativa esposizione a rischio;
3. violazioni del Modello che hanno integrato un fatto penalmente rilevante.

Costituisce altresì condotta violativa del Modello il mancato rispetto delle disposizioni riportate in materia di Whistleblowing dal D.lgs. nr. 24/23. In particolare, costituisce violazione del Modello:

- la segnalazione falsa, effettuata con dolo o colpa grave, con lo scopo di danneggiare il segnalante (cd. segnalazione in mala fede);
- l'attuazione o la minaccia di misure ritorsive nei confronti del segnalante o degli altri soggetti protetti dalla legge;
- la mancata tutela della riservatezza dell'identità del segnalante.

Le condotte rilevanti assumono, inoltre, maggiore o minore gravità a seconda della diversa valenza degli elementi soggettivi di seguito indicati e, in generale, delle circostanze in cui è stato commesso il fatto. In particolare, in ottemperanza al principio di gradualità e proporzionalità nella determinazione della sanzione da infliggere, si tiene conto di:

- eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- eventuale recidività del suo o dei suoi autore/i;

- livello di responsabilità gerarchica e/o tecnica del soggetto cui è riferibile la condotta contestata;
- eventuale condivisione di responsabilità con altri soggetti che abbiano concorso nel determinare la mancanza.

7.2. **Sanzioni nei confronti del Consiglio di Amministrazione[7] e dei componenti del Collegio Sindacale**

Qualora sia accertata la violazione di cui al punto 7.1[8], da parte di un Soggetto Apicale, potranno essere applicate nei suoi confronti, le seguenti sanzioni:

- richiamo formale scritto;
- sanzione pecuniaria, pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;
- revoca dall'incarico.

La scelta della sanzione da irrogare nel caso concreto avverrà sulla base dei principi di proporzionalità e gradualità identificati nel paragrafo 7.1.

7.3. **Sanzioni nei confronti dei Dipendenti (Dirigenti[9], Quadri, Impiegati)**

Il mancato rispetto e/o la violazione delle regole imposte dal Modello, da parte di dipendenti della Società, costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro *ex* art. 2104 Codice Civile e illecito disciplinare.

L'adozione da parte di un dipendente della Società di un comportamento qualificabile, in base a quanto indicato al punto precedente, come illecito disciplinare, costituisce inoltre violazione dell'obbligo dei lavoratori di eseguire con la massima diligenza i compiti loro affidati, attenendosi alle direttive della Società, così come previsto dal vigente CCNL applicabile, nonché dalle previsioni del Codice Disciplinare.

Le sanzioni vengono applicate sulla base del rilievo che assumono le singole fattispecie considerate e proporzionate a seconda della loro gravità, secondo quanto previsto al precedente paragrafo 7.1.

Qualora sia accertata una violazione del Modello ascrivibile al dipendente[10], tenuto conto delle disposizioni di cui all'art. 7 della Legge n. 300/1970 e del CCNL applicabile, potranno essere applicati i seguenti provvedimenti disciplinari:

---

[7] Limitatamente ai Consiglieri che non hanno un rapporto di lavoro subordinato.

[8] In via esemplificativa e non esaustiva di quanto indicato nel precedente paragrafo 7.1, possono costituire presupposto per l'applicazione delle sanzioni di seguito indicate, le seguenti fattispecie di condotta:

- mancato rispetto dei principi e dei protocolli contenuti nel Modello;
- violazione e/o elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dai protocolli aziendali ovvero nell'impedimento ai soggetti preposti e all'OdV del controllo o dell'accesso alle informazioni richieste ed alla documentazione;
- violazione delle disposizioni relative ai poteri di firma e, in generale, al sistema delle deleghe, ad eccezione dei casi di necessità e di urgenza, di cui dovrà essere data tempestiva informazione al Consiglio di Amministrazione;
- violazione dell'obbligo di informativa all'OdV e/o all'eventuale Soggetto sovra ordinato circa comportamenti diretti alla commissione di un reato o di un illecito amministrativo ricompreso fra quelli previsti dal Decreto.

[9] I criteri sanzionatori e il procedimento disciplinare tengono conto del tipo di rapporto di lavoro che lega tali soggetti alla Società.

[10] A titolo puramente esemplificativo e non esaustivo di quanto indicato nel precedente par. 7.1 e salvo quanto previsto dal CCNL applicabile ai fini dell'applicazione di eventuali misure disciplinari, si indicano alcune condotte rilevanti:

1) provvedimenti disciplinari conservativi:
   a. rimprovero verbale;
   b. rimprovero scritto;
   c. multa non superiore a quattro ore della retribuzione globale giornaliera di cui al punto 1 dell'art. 22;
   d. sospensione dal servizio e dalla retribuzione fino a 10 giorni (per il personale a tempo parziale fino a 50 ore);
2) provvedimenti disciplinari risolutivi:
   a. licenziamento con preavviso;
   b. licenziamento senza preavviso.

Ferme restando le previsioni di cui al CCNL applicabile e al Codice Disciplinare, scelta della sanzione da irrogare nel caso concreto avverrà sulla base dei principi di proporzionalità e gradualità identificati nel paragrafo 7.1.

Ai sensi dell'art. 38 del CCNL Autostrade e Trafori, inoltre, la Società, qualora la natura della mancanza incida sul rapporto fiduciario, può procedere alla sospensione cautelativa del dipendente in attesa che vengano effettuati gli opportuni accertamenti.

Per quanto riguarda il personale dirigente, stante la natura eminentemente fiduciaria e considerato che i dirigenti esplicano le proprie funzioni al fine di promuovere, coordinare e gestire la realizzazione degli obiettivi dell'impresa, le violazioni del Modello saranno valutate in relazione alla contrattazione collettiva, coerentemente con le peculiarità del rapporto stesso.

7.4. **Sanzioni applicabili nei confronti dei "Terzi Destinatari"**

Il presente Sistema Disciplinare ha la funzione di sanzionare le violazioni del Codice Etico e del Modello commesse dai Terzi Destinatari.

Nell'ambito di tale categoria, possono farsi rientrare:

- coloro che intrattengono con Telepass un rapporto contrattuale (ad es. i consulenti, i professionisti, ecc.);
- gli incaricati della revisione e del controllo contabile;
- i collaboratori a qualsiasi titolo;
- i procuratori e coloro che agiscono in nome e/o per conto della Società;
- i fornitori ed i *partner*.

- violazione delle procedure interne o adozione, nell'espletamento di attività a rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una non esecuzione degli ordini impartiti dalla Società sia in forma scritta che verbale (ad esempio il dipendente che non osservi le procedure prescritte, ometta di dare comunicazione all'Organismo di Vigilanza delle informazioni prescritte, ometta di svolgere controlli, ecc.);
- adozione, nell'espletamento delle attività a rischio, di un comportamento non conforme alle prescrizioni del Modello o violazione dei principi dello stesso, dovendosi ravvisare in tali comportamenti una inosservanza degli ordini impartiti dalla Società (ad esempio il ldipendente che si rifiuti di sottoporsi agli accertamenti sanitari di cui all'art. 5 della Legge 20 maggio 1970 n. 300; falsifichi e/o alteri documenti interni o esterni; non applichi volontariamente le disposizioni impartite dall'Azienda, al fine di trarre vantaggio per se o per l'Azienda stessa; sia recidivo, in qualsiasi delle mancanze che abbiano dato luogo alla applicazione delle misure disciplinari conservative).

Ogni violazione posta in essere dai soggetti sopra indicati potrà determinare l'applicazione di penali o la risoluzione del rapporto contrattuale, in ragione della violazione contestata e della maggiore o minore gravità del rischio cui la Società è esposta.

7.5. **Procedimento di istruttoria**

La procedura di irrogazione delle sanzioni prevede:

- la fase istruttoria;
- la fase della contestazione della violazione all'interessato;
- la fase di determinazione e di successiva irrogazione della sanzione.

La fase istruttoria ha avvio sulla base delle attività di verifica e ispezione condotte dall'Organismo di Vigilanza, che, sulla scorta della propria attività istruttoria ovvero dell'analisi delle segnalazioni ricevute, informa tempestivamente e, successivamente, relaziona per iscritto il Titolare del potere disciplinare, come di seguito individuato, circa l'eventuale violazione rilevata ed il soggetto (o i soggetti) cui è riferibile.

Procedimento di istruttoria nei confronti dei Componenti del Consiglio di Amministrazione

Qualora riscontri la violazione del Modello da parte di uno o più soggetti che rivestano la carica di Consigliere, non legato alla Società da un rapporto di lavoro subordinato[11], l'Organismo di Vigilanza trasmette al Consiglio di Amministrazione ed al Collegio Sindacale una relazione contenente:

- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- il soggetto responsabile della violazione;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

A seguito dell'acquisizione della relazione dell'Organismo di Vigilanza, il Consiglio di Amministrazione convoca il Consigliere e a cui è contestata la violazione.

La convocazione deve:

- essere effettuata per iscritto;
- contenere l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione;
- comunicare all'interessato la data della convocazione, con l'avviso della facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte che verbali.

La convocazione deve essere effettuata in base alle stabilite modalità di convocazione del Consiglio di Amministrazione.

In occasione della convocazione del Consiglio di Amministrazione, cui è invitato a partecipare anche l'Organismo di Vigilanza, vengono disposti l'audizione dell'interessato, l'acquisizione delle eventuali deduzioni da questi formulate e l'espletamento degli eventuali ulteriori accertamenti ritenuti opportuni.

[11] Nel caso in cui la violazione del Modello sia ascrivibile a un Consigliere legato alla Società da un rapporto di lavoro subordinato, il Titolare del potere disciplinare è il Consiglio di Amministrazione e il procedimento di istruttoria e di eventuale contestazione è sottoposto alle cautele di cui all'art. 7, Legge 300/1970 e al CCNL applicabile.

Il Consiglio di Amministrazione, con l'astensione del consigliere interessato, valuta la fondatezza degli elementi acquisiti e, a norma degli artt. 2392 e seguenti del Codice Civile, convoca l'Assemblea per le determinazioni del caso.

La decisione del Consiglio di Amministrazione, nel caso di infondatezza, o quella della Assemblea convocata, viene comunicata per iscritto, a cura del Consiglio di Amministrazione, all'interessato nonché all'Organismo di Vigilanza.

Qualora l'Organismo di Vigilanza riscontri la violazione del Modello da parte dell'intero Consiglio di Amministrazione o della maggioranza dei Consiglieri, l'Organismo di Vigilanza informa il Collegio Sindacale affinché questo convochi senza indugio l'Assemblea per gli opportuni provvedimenti.

Procedimento di istruttoria nei confronti dei Componenti del Collegio Sindacale

In caso di violazione del presente Modello da parte di un Sindaco, l'Organismo di Vigilanza informa l'intero Collegio Sindacale e il Consiglio di Amministrazione della Società per il tramite dei rispettivi Presidenti mediante una relazione contenente:

- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;
- l'indicazione del soggetto responsabile della violazione;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

A seguito dell'acquisizione della relazione dell'Organismo di Vigilanza, il Collegio Sindacale, in riunione congiunta con il Consiglio di Amministrazione, convoca il Sindaco interessato a cui è contestata la violazione.

La convocazione deve:

- essere effettuata per iscritto;
- contenere l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione;
- comunicare all'interessato la data della convocazione, con l'avviso della facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte che verbali.

La convocazione deve essere effettuata in base alle stabilite modalità di convocazione del Consiglio di Amministrazione.

Il Consiglio di Amministrazione della Società, valutata la rilevanza della segnalazione, provvede ad attivare l'Assemblea per le determinazioni del caso.

Qualora l'Organismo di Vigilanza riscontri la violazione del Modello da parte di più Sindaci o dell'intero Collegio Sindacale, informa il Consiglio di Amministrazione affinché questo convochi senza indugio l'Assemblea per gli opportuni provvedimenti.

Procedimento di istruttoria nei confronti dei Dipendenti (Dirigenti, Quadri, Impiegati)

Qualora riscontri la violazione del Modello da parte di un dipendente, la procedura di accertamento della violazione è espletata nel rispetto delle disposizioni normative vigenti nonché del contratto collettivo applicabile.

In particolare, l'Organismo di Vigilanza trasmette all'Amministratore Delegato una relazione contenente:

- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Modello che risultano essere state violate;

- l'indicazione del soggetto responsabile della violazione;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

A seguito dell'acquisizione della relazione dell'Organismo di Vigilanza, l'Amministratore Delegato convoca il soggetto interessato, mediante invio di apposita contestazione scritta contenente:

- l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione;
- i termini entro i quali il soggetto interessato ha facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte che verbali.

Nel caso in cui il soggetto interessato intenda rispondere oralmente alla contestazione, a tale incontro è invitato a partecipare anche l'Organismo di Vigilanza. In tale sede sono acquisiti gli elementi rappresentati dal soggetto interessato.

A conclusione delle attività sopra indicate, l'Amministratore Delegato si pronuncia in ordine alla eventuale determinazione della sanzione, nonché circa la concreta comminazione della stessa.

Il provvedimento di comminazione dell'eventuale sanzione è comunicato per iscritto all'interessato, nel rispetto degli eventuali termini previsti dalla contrattazione collettiva applicabile nel caso concreto.

Le competenti strutture curano, nel caso, l'effettiva irrogazione della sanzione, nel rispetto delle norme di legge e di regolamento, nonché delle previsioni di cui alla contrattazione collettiva e ai regolamenti aziendali, laddove applicabili.

All'Organismo di Vigilanza è inviato, per conoscenza, il provvedimento di irrogazione della sanzione.

Procedimento di istruttoria nei confronti dei Terzi Destinatari

Al fine di consentire l'assunzione delle iniziative previste dalle sopra citate clausole contrattuali volte a garantire il rispetto dei principi del Codice Etico e della presente Parte Generale del Modello da parte di terzi che abbiano rapporti contrattuali con la Società, l'Organismo di Vigilanza trasmette al responsabile della direzione/funzione aziendale che gestisce il rapporto contrattuale una relazione contenente:

- gli estremi del soggetto responsabile della violazione;
- la descrizione della condotta contestata;
- l'indicazione delle previsioni del Codice Etico e della presente Parte Generale del Modello che risultano essere state violate;
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro.

Tale relazione, qualora il contratto sia stato deliberato dal Consiglio di Amministrazione, dovrà essere trasmessa anche all'attenzione del medesimo e del Collegio Sindacale.

Il Responsabile della funzione aziendale che gestisce il rapporto contrattuale, d'intesa con il Dipartimento Legal Affairs, ove richiesta, invia all'interessato una comunicazione scritta contenente l'indicazione della condotta constatata, le previsioni oggetto di violazione, nonché l'indicazione delle specifiche clausole contrattuali inserite nelle lettere di incarico, nei contratti o negli accordi di partnership che si intendono applicare.

ORGANISATION, MANAGEMENT AND CONTROL MODEL

PURSUANT TO LEGISLATIVE DECREE NO. 231 OF 8 JUNE 2001

Approved by the Board of Directors of Telepass S.p.A. on 3 July 2024

SUMMARY

DEFINITIONS

Telepass or the Company:	Telepass S.p.A.
Mundys	Mundys S.p.A.
Telepass Group or **the Group**	Telepass and the companies controlled by it pursuant to Article 2359, paragraphs 1 and 2, of the Italian Civil Code.
Mundys Group	Mundys and the companies controlled by it pursuant to Article 2359, paragraphs 1 and 2, of the Italian Civil Code.
Decree or **Legislative Decree 231/2001**	Legislative Decree No. 231 of June 8, 2001.
Confindustria Guidelines	Guidelines for the drafting of organizational, management, and control models pursuant to Legislative Decree No. 231/2001, issued by Confindustria on November 3, 2003, and subsequently updated.
Model or **MOG**	Organizational, Management, and Control Model adopted by the Company pursuant to Legislative Decree No. 231/2001 to prevent the commission of the offenses provided for under the Decree.
Code of Ethics	The Code of Ethics of the Mundys Group, which outlines the values and conduct principles guiding the Company's business activities.
Offenses or **predicate Offenses**	Offenses deemed relevant pursuant to Legislative Decree No. 231/2001.
Risk Area	Business activities considered potentially at risk for the commission of offenses under Legislative Decree No. 231/2001.
Control Measures	The set of norms, protocols, and corporate provisions aimed at preventing criminal risks, including but not limited to procedures, operational rules, manuals, forms, and employee communications.
Supervisory Body or **SB (*Organismo di Vigilanza*)**	The internal body tasked with overseeing the functioning, effectiveness, and compliance of the Model, as well as its updating, pursuant to Article 6,

	paragraph 1, letter b) of Legislative Decree No. 231/2001.
Corporate Bodies	The Board of Directors and the Board of Statutory Auditors of Telepass.
Top Management	Pursuant to Article 5, paragraph 1, letter a) of Legislative Decree No. 231/2001, individuals holding representation, administration, or management roles in the entity or one of its organizational units with financial and functional autonomy, as well as individuals who, de facto, manage or control the entity.
Subordinate Individuals	Pursuant to Article 5, paragraph 1, letter b) of Legislative Decree No. 231/2001, individuals subject to the direction or supervision of a member of Top Management.
Recipients	Those to whom the rules of conduct and ethical principles contained in the Code of Ethics, the Model, and the adopted Control Measures are addressed.
Third-Party Recipients	Parties engaging in commercial and/or financial relations of any kind with the Company who are contractually bound to comply with the ethical principles and/or the Model adopted by Telepass.
Public Administration (PA)	Public Administration entities, including their officials and individuals performing public service duties.
National Collective Labor Agreement (CCNL)	The National Collective Labor Agreement applicable to the Company (e.g., CCNL Commerce, CCNL for employees of companies and consortia operating motorways and tunnels, CCNL Industry for managerial staff).
Whistleblowing	The system protecting employees or collaborators who report unlawful conduct encountered during their professional duties.
Reporting Team (*Team Segnalazioni*)	A collegial body responsible for managing reports. It comprises the heads of Telepass's organizational units in charge of Internal Audit, Human Resources,

	and Legal Affairs. The Reporting Team operates within Telepass and all companies controlled by it.
Reporting Procedure	The procedure governing information flows from Telepass organizational units to the Supervisory Body.
Criminal Code (c.p.)	The Italian Criminal Code.

GENERAL SECTION

INTRODUCTION

Legislative Decree No. 231 of June 8, 2001, as subsequently amended and supplemented, introduced into the legal system the "*Regulation of administrative liability of legal entities, companies, and associations, including those without legal personality*".

The Company, committed to ensuring fairness and transparency in conducting business and corporate activities to safeguard its market position, reputation, shareholder expectations, and employees' work, has:

a) adopted the Code of Ethics, the Anti-Corruption Policy, the Code of Conduct for the prevention of discrimination and the protection of the dignity of women and men, and the Telepass Group Whistleblowing Management Procedure, to regulate the proper conduct of its activities;

b) appointed, during the Board of Directors meeting on November 7, 2017, the Anti-Corruption Officer in compliance with the Mundys Group Anti-Corruption Policy;

c) deemed it appropriate to adopt and implement an Organizational, Management, and Control Model (MOG) designed to establish a structured system of rules and controls to pursue the Company's objectives in full compliance with applicable laws, also aimed at preventing the commission of the Offenses contemplated in the Decree.

The adoption of the MOG enables Telepass to minimize the risk of criminal offenses being committed within the Company's structure to its advantage or in its interest.

Although the MOG is a legal instrument designed to protect the Company during criminal proceedings, it is important to emphasize that adherence to the MOG and its Control Measures by the Recipients helps prevent individuals from committing, either knowingly or unknowingly, unlawful acts during the performance of their work activities.

The MOG, therefore, serves as a protective tool for both the legal entity and the individuals who, in various capacities, operate within the corporate structure.

1. LEGISLATIVE DECREE NO. 231/2001

1.1 The Administrative Liability Regime for Entities

Legislative Decree No. 231/2001, titled *"Regulation of administrative liability of legal entities, companies, and associations, including those without legal personality"*, aligns Italian law on the administrative liability of legal entities and unincorporated associations ("Entities") with European conventions issued on the subject[1].

The Decree introduces a regime of liability that is formally administrative but substantively criminal in nature, applicable to Entities for certain Offenses committed in their interest or to their advantage by:

a) individuals in positions of representation, administration, or management of the Entity or its organizational units with financial and functional autonomy, as well as individuals who, even de facto, manage or control the Entity ("Top Management");

b) individuals subject to the direction or supervision of Top Management ("Subordinate Individuals").

The Entity's administrative liability is additional to the criminal liability of the natural person who materially committed the Offense. Both are ascertained within the same criminal proceeding before a penal judge. Moreover, the Entity's liability persists even if the natural person who committed the offense is not identified or is not legally culpable.

Currently, the Entity's liability arises exclusively in connection with the commission of the following predicate Offenses explicitly listed in the Decree:

i) Crimes against Public Administration (Articles 24 and 25, Legislative Decree 231/2001);

ii) Cybercrimes and unlawful data processing (Article 24-bis, Legislative Decree 231/2001);

iii) Organized crime offenses (Article 24-ter, Legislative Decree 231/2001);

iv) Forgery of money, public credit instruments, revenue stamps, and identification tools or signs (Article 25-bis, Legislative Decree 231/2001);

v) Crimes against industry and commerce (Article 25-bis.1, Legislative Decree 231/2001);

vi) Corporate crimes and private-to-private corruption (Article 25-ter, Legislative Decree 231/2001);

vii) Crimes for terrorism or subversion of democratic order (Article 25-quater, Legislative Decree 231/2001);

viii) Practices involving female genital mutilation (Article 25-quater.1, Legislative Decree 231/2001);

ix) Crimes against individual liberty (Article 25-quinquies, Legislative Decree 231/2001);

[1] The Brussels Convention of July 26, 1995 on the protection of the financial interests of the European Communities; the Brussels Convention of May 26, 1997 on cassombating corruption involving officials of the European Community or officials of Member States; the OECD Convention of December 17, 1997 on combating bribery of foreign public officials in international business transactions; the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the General Assembly on November 15, 2000, and May 31, 2001, ratified in Italy by Law No. 146 of 2006.

x) Insider trading and market manipulation offenses (Article 25-sexies, Legislative Decree 231/2001);

xi) Negligent homicide or serious/very serious injuries due to workplace health and safety violations (Article 25-septies, Legislative Decree 231/2001);

xii) Receiving, laundering, and utilizing illicitly obtained money, goods, or benefits, as well as self-laundering (Article 25-octies, Legislative Decree 231/2001);

xiii) Offenses involving payment instruments other than cash (Article 25-octies.1, Legislative Decree 231/2001);

xiv) Copyright infringement crimes (Article 25-novies, Legislative Decree 231/2001);

xv) Inducing individuals to withhold statements or to provide false statements to judicial authorities (Article 25-decies, Legislative Decree 231/2001);

xvi) Environmental crimes (Article 25-undecies, Legislative Decree 231/2001);

xvii) Employment of third-country nationals whose stay is irregular (Article 25-duodecies, Legislative Decree 231/2001);

xviii) Hate crimes related to racism and xenophobia (Article 25-terdecies, Legislative Decree 231/2001);

xix) Fraud in sports competitions, unauthorized gambling, and illegal gaming operations via banned devices (Article 25-quaterdecies, Legislative Decree 231/2001)

xx) Tax crimes (Article 25-quinquiesdecies, Legislative Decree 231/2001);

xxi) Smuggling offenses (Article 25-sexiesdecies, Legislative Decree 231/2001);

xxii) Crimes against cultural heritage (Article 25-septiesdecies, Legislative Decree 231/2001);

xxiii) Laundering of cultural property and destruction or looting of cultural or landscape assets (Article 25-duodevicies, Legislative Decree 231/2001);

xxiv) Transnational crimes such as organized crime, money laundering, trafficking in migrants, and obstruction of justice (Law No. 146 of March 16, 2006, Articles 3 and 10).

Following an analysis of the Company's activities, it is believed that the offenses potentially relevant to Telepass include those under sub-paragraphs i), ii), iii), v), vi), vii), ix), x), xi), xii), xiii), xiv), xv), xvi), xvii), xx), xxi), and xxiv), provided they are committed in the interest or to the advantage of the Company pursuant to Article 5 of Legislative Decree 231/2001.

Offenses not considered potentially applicable to the Company have been excluded based on the nature of its activities and the absence of concrete risk scenarios.

The Control Measures – organizational and procedural – adopted by the Company are deemed adequate to prevent or minimize the risk of committing any of the offenses covered under Legislative Decree 231/2001.

1.2 **Offenses committed abroad**

An Entity can also be held liable for offenses committed abroad, provided that the Entity is not already being prosecuted by the state where the offense was committed. If the punishment of the perpetrator requires a formal request by the Minister of Justice, the Entity may be prosecuted only if such a request is also directed at the Entity. Specifically, pursuant to Article 4 of the Decree, an Entity with

its principal office in Italy may be held accountable for offenses committed abroad if the following conditions are met:

a) the Offense was committed abroad by an individual functionally linked to the Entity (Article 5, paragraph 1, of the Decree);

b) the Entity has its principal place of business within Italian territory;

c) the Entity can be held accountable only in the cases and under the conditions provided for in Articles 7 (*Offenses committed abroad*), 8 (*Political offenses committed abroad*), 9 (*Common* offenses *committed abroad by an Italian citizen*), and 10 (*Common offenses committed abroad by a foreign citizen*) of the Italian Criminal Code.

Additionally, under Article 10 of Law No. 146/2006, an Entity can be held liable for certain transnational Offenses (such as the offense of criminal association, including mafia-type associations, the offense of association aimed at drug trafficking, and the offense of trafficking in migrants).

In such cases, the unlawful conduct, committed by an organized criminal group, must meet one of the following conditions:

i) be committed in multiple States;

ii) be committed in one state but have substantial effects in another State;

iii) be committed in one State, although a significant part of its preparation, planning, direction, or control takes place in another State;

iv) be committed in one State, involving an organized criminal group that engages in criminal activities across multiple States.

1.3 **Penalties**

The penalties provided for Offenses under the Decree are:

1) financial penalties;

2) prohibitory penalties;

3) confiscation;

4) publication of the ruling.

Financial penalties, applicable to all offenses, are determined based on a "quota" system. The judge establishes the number of quotas, taking into account the gravity of the act, the degree of the Entity's responsibility, and the actions taken to mitigate the consequences of the offense or prevent further offenses. The amount of each quota is set based on the Entity's economic and financial condition to ensure the penalty’s effectiveness (Article 11 of the Decree).

Prohibitory penalties can be applied to the Entity as a precautionary measure when there are serious indications suggesting its liability for the Offense, and when specific evidence indicates a tangible risk of similar offenses being committed (Article 45 of the Decree).

If a prohibitory penalty would result in the Entity's operations being interrupted, the judge may, instead of imposing the penalty, authorize the continuation of the Entity's activities under the management of a commissioner for a period equal to that of the prohibitory penalty. This is applicable if the Entity performs a public service or an essential service, where interruption would cause serious harm to the public, or if the interruption would have significant repercussions on employment.

Non-compliance with prohibitory penalties constitutes an independent offense under the Decree, potentially leading to further administrative liability for the Entity (Article 23 of the Decree).

Prohibitory penalties, lasting no less than three months and no more than two years, apply specifically to the activity related to the Offense and may include:

1) suspension of the business activity;
2) prohibition from contracting with Public Administration;
3) suspension or revocation of licenses, authorizations, or concessions related to the offense;
4) exclusion from public subsidies, contributions, or financing, or the revocation of those already granted;
5) prohibition from advertising goods or services.

Financial and prohibitory penalties are reduced by one-third to one-half when offenses under Articles 24 to 25-duodecies of the Decree are committed in the form of an attempt (Article 26 of the Decree).

In addition to the above penalties, the Decree mandates the **confiscation** of the price or proceeds of the offense, which may also include assets or other items of equivalent value, and the **publication of the ruling** when a prohibitory penalty is applied. The ruling is published in the municipality where the Entity's principal office is located and on the Ministry of Justice website.

It is worth noting that, in addition to the penalties provided under the Decree, the mere initiation of a criminal investigation for an administrative offense may result in a **reputational damage** to the Company and the Group, even if the proceedings result in dismissal or acquittal. Accordingly, all Recipients must strictly comply with the provisions of the MOG to avoid any involvement in criminal investigations.

1.4 Proceedings for Establishing the Offense and Evaluating the Adequacy of the Model by the Judge

Liability for an administrative offense arising from a predicate Offense is established within a criminal proceeding, which should remain combined – wherever possible – with the criminal proceeding against the individual who committed the predicate Offense for which the Entity is liable.

The determination of the Entity's liability, assigned to the criminal court, involves:

- verifying the existence of the predicate Offense;
- establishing whether the Entity benefited from or had an interest in the commission of the Offense;
- assessing the adequacy and effective implementation of the adopted Model.

The judge evaluates whether the Model is abstractly capable of preventing the Offenses covered under the Decree. This assessment is conducted retroactively, with the judge situating themselves within the corporate context as it existed at the time the offense occurred, to determine the effectiveness of the adopted Model in preventing the commission of the offense.

1.5 Adoption of the Model as a possible exemption from administrative liability

Articles 6 and 7 of the Decree provide specific conditions under which an Entity may be exempt from administrative liability for Offenses committed in its interest or to its advantage by either Top Management or Subordinate Individuals.

Specifically, Article 6 of the Decree stipulates that, in cases where Offenses are committed by Top Management, an Entity is exempt from administrative liability if it can demonstrate that:

a) the governing body adopted and effectively implemented, prior to the commission of the Offense, Models designed to prevent Offenses of the type that occurred;

b) the task of supervising the functioning of and compliance with the Models, as well as ensuring their updates, was assigned to a body with autonomous powers of initiative and control;

c) the individuals who committed the Offenses acted fraudulently to circumvent the Models;

d) there was no failure to supervise or insufficient supervision by the body referred to in letter b).

In the case of Offenses committed by Subordinate Individuals, Article 7 of the Decree states that the Entity is liable if the commission of the Offense was made possible by the failure to comply with management or supervision obligations. However, such failure is excluded if the Entity adopted and effectively implemented, prior to the Offense, a Model designed to prevent Offenses of the type in question.

The Decree further specifies that the Model must be adequate to address the following requirements:

1) identify the activities within which Offenses specified in the Decree could be committed;

2) provide specific protocols for planning and implementing the Entity’s decisions related to preventing such Offenses;

3) establish procedures for managing financial resources that prevent the commission of these Offenses;

4) impose obligations to inform the body responsible for overseeing the Model's implementation and compliance;

5) introduce an internal disciplinary system to sanction non-compliance with the measures outlined in the Model, including whistleblowing provisions as detailed later in the document.

2. THE COMPANY

Telepass is an Italian company operating in the field of urban and interurban mobility services based on apps, as defined below, aiming to create an ecosystem of services offering private individuals and companies an increasing number of flexible, secure, and sustainable integrated mobility options.

Specifically, Telepass engages in activities related to: (i) providing telepass services, enabling payment and seamless access to the toll motorway network through dedicated lanes without the need to stop at entry and exit toll stations; and (ii) providing additional services related to payment and/or facilitated access to areas, structures, infrastructures, and/or goods and services associated with mobility at facilities authorized to accept payments, including through its devices.

Furthermore, the Company's scope of activity has progressively expanded within the mobility services sector to include insurance brokerage, as a registered entity in Section E of the Single Register of Intermediaries (RUI) managed by IVASS. For the updated scope of activities, reference is made to the corporate purpose outlined in the Articles of Association approved at the Company's General Meeting on April 12, 2021.

Since 2016, the Company has been controlled by Mundys.

On April 14, 2021, 49% of Telepass's share capital was sold to the global investment manager Partners Group AG.

On May 1, 2022, Telepass Pay S.p.A., previously a subsidiary of Telepass, was merged into Telepass. Consequently, Telepass, authorized by the Bank of Italy, became an Electronic Money Institution (IMEL) through the establishment of a Dedicated Asset, as defined below, exclusively devoted to the issuance and distribution of electronic money and related services, as well as business functions dedicated solely to managing these activities (a "hybrid IMEL").

Based on the above, Telepass is authorized by the Bank of Italy to:

- issue and distribute electronic money;
- provide payment services unrelated to electronic money, as defined in Article 1, paragraph 2, letter h-septies.1), of Legislative Decree No. 385 of September 1, 1993, to offer new mobility-related services beyond those currently provided by Telepass under exemptions.

In the context of payment services operations, Telepass:

- issues and accepts payment instruments, specifically:
  - the physical device ("OBU");
  - the mobile application downloadable to smartphones ("App");
- executes payment orders, enabling its clients to initiate and complete payment operations through a website (accessible via computer or mobile web on smartphones), always ensuring strong customer authentication.

Telepass has either full or majority control over the following companies:

1) Telepass Broker S.r.l.;
2) URBANnext S.A.;
3) Telepass Assicura S.r.l.;
4) Telepass Innova S.p.A.;

5) Wash Out S.r.l.;

6) Eurotoll S.A.

Within the aforementioned activities, Telepass is subject to oversight by various administrative authorities, including, but not limited to, the Bank of Italy, the Italian Competition Authority (AGCM), IVASS, the Italian Data Protection Authority, and the Ministry of Infrastructure and Transport.

3. ADOPTION OF THE MODEL

3.1 Definition, objectives, and Recipients of this Model

The Model can be defined as a comprehensive set of principles, rules, provisions, organizational schemes, and related tasks and responsibilities, designed for the implementation and diligent management of a system for controlling and monitoring high-risk activities, with reference to the Offenses set forth in the Decree.

The **objectives** of this Model are as follows:

- to strengthen the corporate governance system;
- to establish a structured and systematic prevention and control system aimed at eliminating or reducing the risk of committing the Offenses under Legislative Decree 231/2001, including attempted offenses, related to the Company's activities, with particular attention to eliminating or reducing any illegal behaviours;
- to make all those who operate in the name, on behalf of, or in the interest of Telepass in high-Risk Areas aware that, in the event of a violation of the Model's provisions, they may incur a criminal or administrative offense, punishable not only against the individual author but also against the Company;
- to inform all those who operate in any capacity in the name, on behalf of, or in the interest of Telepass that violating the provisions contained in the Model will result in the application of appropriate sanctions;
- to emphasize that Telepass does not tolerate illegal behaviour, regardless of the pursued objective or the mistaken belief of acting in the Company's interest or for its benefit, as such behaviours are contrary to the ethical principles the Company aims to follow and, therefore, in contrast to its own interest;
- to address violations of the Model through the imposition of disciplinary and/or contractual sanctions.

The **Recipients** of this Model, who are required to be familiar with and comply with it within their specific competencies, are as follows:

- the members of the Board of Directors, responsible for setting objectives, deciding on activities, implementing projects, proposing investments, and making all decisions or actions related to the Company's operations;
- the members of the Board of Statutory Auditors, in the performance of their role of control and verification of the formal and substantial correctness of the Company's activities and the functioning of the internal control system;
- the CEO and the managers of the Company;
- employees and all collaborators with whom the Company maintains contractual relationships, in any capacity, including occasional and/or temporary relationships;
- all those who have commercial and/or financial relationships of any kind with the Company.

3.2 Structure of the Model adopted by Telepass

The Model adopted by Telepass consists of this General Section and the Special Sections prepared for the types of Offenses for which risks have been identified for the Company.

The Special Parts of this Model are divided into "Offense Families" that have been deemed relevant:

SPECIAL SECTION	OFFENCE FAMILY	DECREE
A	Offenses to the detriment of the Public Administration	Articles 24 and 25
B	Corporate crimes and corruption between private parties	Article 25-ter
C	Crimes and administrative offenses related to insider trading and market manipulation	Articles 25-sexies of the Decree and 187-quinquies TUF
D	Crimes of manslaughter or serious or very serious injury committed by violating health and safety at work regulations	Article 25-septies
E	Offenses of receiving, money laundering, and using money, goods, or benefits from illegal sources, as well as self-laundering	Law 231/2007 and Article 25-octies of the Decree
F	Computer crimes	Article 24-bis of the Decree and Law 48/2008
G	Environmental crimes	Article 25-undecies
H	Offenses involving the employment of citizens from third countries with irregular residency, and crimes against the individual's personality, particularly the crime under Article 603-bis of the Penal Code, "Illegal mediation and exploitation of labor"	Articles 25-duodecies and 25-quinquies
I	Crimes against industry and commerce and crimes related to copyright infringement	Articles 25-bis 1 and 25-novies
J	Tax crimes	Article 25-quinquiesdecies
K	Smuggling crimes	Article 25-sexiesdecies

L	Crimes committed with non-cash payment instruments	Article 25-octies.1
M	Crime of inducing false statements or withholding statements to the judicial authority	Article 25-decies
N	Criminal associations, both in the basic form under Article 416 of the Penal Code and in the transnational form under Law No. 146/2006	Articles 24-ter, 25-quater and Law No. 146/2006

For all other offenses which, based on the analysis conducted, are deemed not to potentially concern the Company, and for which no specific Special Section has been prepared, the overall system of control, organizational, and procedural Control Measures adopted by the Company and referenced in this Model and in the Code of Ethics will apply.

3.3 **Update of the Model**

Given the complexity of the Company's organizational structure, to promote the compliance of the various business activities with the provisions of the Decree and, at the same time, ensure effective control over the risk of committing predicate Offenses, a continuous monitoring and updating process of the Model is foreseen in the event of one or more of the following conditions:

a. legislative and/or jurisprudential innovations regarding the liability of entities for administrative offenses resulting from crimes;

b. significant changes to the organizational structure and/or business sectors of the Company;

c. significant violations of the Model, results of the risk assessment, checks on the effectiveness of the Model, and industry best practices.

The Model is approved by the Board of Directors of Telepass.

After its initial issuance, the Model has been subject to updates based on the evolution of the regulatory and organizational framework.

Specifically:

i. in relation to the amendments introduced to the Decree by Law 62/2005 (the so-called Community Law 2004) and Law 262/2005 (the so-called Savings Law), Telepass updated the Model to account for the risks related to market manipulation and insider trading offenses, as well as the failure to communicate conflicts of interest;

ii. subsequently, in the 2010 update, the extensions of corporate liability were analyzed in relation to offenses of manslaughter and negligent injury due to violations of workplace health and safety regulations; offenses of receiving stolen goods, money laundering, and the use of money, goods, or benefits of illicit origin as provided by Article 25-octies; computer crimes and the unlawful processing of data; organized crime offenses; crimes against industry and commerce, and violations of copyright law; and, finally, offenses involving inducement not to make statements or to make false statements to the judicial authority;

iii. in **2013**, the Model was updated to account for the further expansion of predicate offenses, such as environmental crimes, the employment of third-country nationals with irregular residency, undue inducement to provide or promise benefits, and private corruption;

iv. in **2017**, the responsibility of entities was analysed further, in relation to the crime of self-laundering, environmental crimes under Law No. 68/2015, and provisions related to offenses against the individual, employment of third-country nationals with irregular residency, crimes against the public administration, mafia-type associations, and false accounting under Law No. 69/2015. Additionally, the 2017 update reflected the evolution of the Company's organizational structure;

v. in the **2019** update, the following legislative updates were incorporated:

   a. the crime of "incitement to private corruption" as per Legislative Decree 38/2017 (Article 25-ter of Legislative Decree 231/2001);

   b. amendments to the crime of "employing third-country nationals with irregular residency" as per Law 161/2017 (Article 25-duodecies of Legislative Decree 231/2001);

   c. introduction of the crime of "racism and xenophobia" under Law 167/2017 (Article 25-terdecies of Legislative Decree 231/2001), later amended by Legislative Decree 21/2018;

   d. introduction of "whistleblowing" provisions for the protection of those who report crimes or irregularities learned during public or private employment (Law 179/2017);

   e. amendments to environmental crimes (Article 25-undecies of Legislative Decree 231/2001) under Legislative Decree 21/2018;

   f. amendments to market abuse crimes (Article 25-sexies of Legislative Decree 231/2001) under Legislative Decree 107/2018;

   g. introduction of Law No. 3/2019 titled "Measures to combat crimes against public administration, prescription of crimes, and transparency of political parties and movements";

vi. in the **2021** update, the following were analysed and incorporated:

   a. new provisions regarding "tax crimes" introduced by the so-called Fiscal Decree converted into Law No. 157/2019 (Article 25-quinquiesdecies of Legislative Decree 231/2001);

   b. amendments to Articles 24, 25, and 25-quinquiesdecies of Legislative Decree 231/2001 and the inclusion of the crime of smuggling in the new Article 25-sexiesdecies, in implementation of the "PIF Directive" by Legislative Decree No. 75/2020[2];

   c. organizational and procedural changes affecting the Company;

vii. in the **2022** update, a comprehensive revision of the Model was carried out due to, among other factors:

   a. the merger between Telepass and its subsidiary Telepass Pay S.p.A., finalized on May 1, 2022, leading to the creation of a dedicated asset within Telepass for IMEL activities;

   b. internal reorganization of Telepass due to both the merger and the evolution of the Company's activities;

   c. introduction of new potentially relevant predicate offenses for Telepass (i.e., crimes related to non-cash payment instruments, as per Legislative Decree No. 184/2021).

[2] Implementation of Directive (EU) 2017/1371, *"on the fight against fraud to the Union's financial interests by means of criminal law."*

viii. Finally, in **2024**, the Model was updated due to the following factors:

a. amendments to the Whistleblowing regulation following the introduction of Legislative Decree No. 24/2023 and Telepass's adaptation to the new regulations;

b. introduction of new predicate offenses by Law No. 137/23, covering urgent measures regarding criminal and civil procedures, forest fire control, recovery from drug addiction, health, and culture;

c. transfer to the subsidiary K-Master S.r.l.[3] of the business unit owned by Telepass, consisting of the "Smart Device Unit" and the "R&D and Innovation Unit";

d. name change of the parent company from "Atlantia S.p.A." to "Mundys S.p.A.";

e. acquisition of a new subsidiary by Telepass;

f. update of the ISO certifications held by Telepass.

The 2024 update did not require a new risk assessment for the following reasons:

- regarding point a, a comprehensive review of the Model's reporting system was conducted, explicitly detailing protections under the new regulations and referring to the updated Whistleblowing Management Procedure. Specific guidelines were also introduced in the disciplinary system to sanction the failure to protect whistleblowers;
- regarding point b, the newly introduced offenses fall within risk areas already identified in previous versions of the Telepass Model, and the Company already has appropriate prevention protocols in place to address these new predicate Offenses;
- regarding point c, the Special Parts affected by the business unit transfer were reviewed based on a document analysis (deed of transfer, existing service contracts between Telepass and its subsidiary) and in consultation with the relevant departments of Telepass or Telepass Innova S.p.A.;
- regarding points d, e, and f, changes were mainly nominal in nature.

In all cases where legislative or business changes require a reassessment of the business risks, the Company proceeds as described below.

3.3.1 Mapping of activities at risk of Offenses

First, the Company evaluates business activities, organizational areas, and processes where predicate offenses could theoretically be committed in the interest or for the benefit of the Company, as well as activities that could facilitate or contribute to the commission of such offenses.

The identification of at-risk processes/activities is carried out by examining corporate documentation (e.g., organizational charts, key processes, powers of attorney, organizational directives), analysing the Company's critical processes, and conducting a series of interviews with key individuals involved in at-risk processes/activities.

Among the Risk Areas, the Company includes not only those activities **directly** linked to the potential commission of Offenses but also those that may **indirectly**/**instrumentally** contribute to their

[3] Subsequently merged into Infoblu S.p.A., which later changed its name to Telepass Innova S.p.A.

commission. Instrumental activities, in particular, are those that can create the factual conditions necessary to commit Offenses.

3.3.2 Risk Assessment

The information gathered through interviews and the analysis of documentation provides the necessary elements to perform a risk assessment.

For each identified Risk Area, the Company evaluates the likelihood of each specific predicate Offense contemplated under the Decree being committed.

3.3.3 Control Measures adopted by Telepass

Once potential risks are identified, the Company analyses the system of Control Measures within the at-risk processes/activities to assess their adequacy in preventing the identified risks of Offenses.

During this phase, the existing Control Measures are examined (e.g., formal procedures, adopted practices, traceability and documentation of operations and controls, segregation of duties) by analysing the information and documentation provided by corporate structures.

In the context of the risk assessment, the following components of the preventive control system are analysed:

1) delegation and power of attorney system;
2) organizational system;
3) management control and financial flow system;
4) control measures;
5) integrated control system.

The checks on the control system also encompass activities conducted with the support of Telepass Group companies or external providers (outsourcing).

These checks are based on the following criteria:

- the formalization of services provided in specific service contracts;
- the inclusion of adequate control measures for activities carried out by service companies based on the contractually defined services;
- the existence of formalized procedures/guidelines for drafting service contracts and implementing control measures, including criteria for determining fees and payment authorization procedures.

Delegation and Power of Attorney System

Telepass adopts a traditional administration and control model, where:

- the Board of Directors exercises strategic oversight functions;
- the CEO exercises management functions;

- the Board of Statutory Auditors exercises supervisory functions as defined in the Articles of Association, while the auditing of accounts is entrusted to an external audit firm.

The Board of Directors has established, in accordance with Article 42 of the Articles of Association approved at the General Meeting on April 12, 2021, the following Board Committees:

- Human Resources and Remuneration Committee;
- Control, Risk, and Sustainability Committee;
- Technology and Innovation Committee.

As recommended by corporate best practices and specified in the Confindustria Guidelines, the Telepass Board of Directors assigns and revokes powers to the Chairman, the CEO, and any Directors entrusted with specific delegations, defining their scope and content.

The Board of Directors formally grants powers to the Chairman, CEO, and, when necessary, managers, up to a defined expenditure threshold. Beyond this threshold, prior approval from the Board of Directors is required, along with the issuance of the corresponding mandate.

The Chairman and the CEO, within the powers conferred by the Board of Directors and in line with defined organizational and managerial responsibilities, delegate operational powers to managers, employees, and third parties, specifying clear expenditure thresholds.

The level of autonomy, representation authority, and spending limits assigned to individuals holding delegations and powers of attorney within the Company are established in strict compliance with the hierarchical level of the recipient. These powers are updated based on organizational changes within the Company's structure.

In matters of health and safety in the workplace, the Board of Directors has assigned the role of Employer to the Chief People and Organization Officer.

Following its designation as **hybrid IMEL** on May 1, 2022, Telepass established a dedicated asset related to electronic money and payment services (the"Dedicated Asset"), corresponding to the activities and services previously managed by its subsidiary Telepass Pay S.p.A. (merged into Telepass). Specifically:

i) the assets and legal relationships assigned to the Dedicated Asset are exclusively intended to fulfill the rights of payment service users, constituting a separate asset from Telepass's residual general assets (the "Free Asset");

ii) in the event of insufficiency of the Dedicated Asset, Telepass is also liable with its general assets for obligations towards payment service users and other parties holding rights arising from the exercise of related and ancillary activities;

iii) Telepass must keep, for the Dedicated Asset, separate books and accounting records as prescribed by Articles 2214 *et seq.* of the Italian Civil Code, in compliance with international accounting standards. Specifically, Telepass's Directors must prepare a separate financial statement for the Dedicated Asset, to be attached to the Company's annual financial statements.

iv) The financial statement of the Dedicated Asset must be accompanied by a specific report prepared by the entity responsible for the statutory audit, certifying the consistency of the data contained therein with those reported in Telepass's financial statements.

v) On May 28, 2021, the Board of Directors of Telepass appointed a General Manager and Dedicated Asset Manager, tasked with overseeing the functions and activities related to the hybrid IMEL operations.

The General Manager, as the Dedicated Asset Manager, is tasked, in summary, with the following responsibilities:

i) ensuring, in coordination with the corporate bodies, that the Company's organizational structure is adequate to its size, complexity, and operations. To this end, the General Manager is entrusted with, by way of example and not limitation, the following responsibilities:

   a. defining, in collaboration with the CEO, information flows to ensure that corporate bodies are fully informed of significant management matters;

   b. defining the duties and responsibilities of the corporate structures under their supervision, with the aim, among other things, of preventing potential conflicts of interest and ensuring that such structures are led by personnel qualified for the activities to be performed;

   c. establishing and implementing the Company's policy regarding the outsourcing of corporate functions;

   d. ensuring, in collaboration with the CEO, that personnel and agents engaged in the provision of payment services, as well as personnel and parties contracted for the distribution and redemption of electronic money, are adequately trained on the marketed products and provided services, compliance with anti-money laundering and counter-terrorism financing regulations, and transparency requirements.

ii) defining governance and control procedures for products as required by transparency regulations;

iii) with reference to the provision of payment services and the issuance of electronic money, strategic decisions regarding entry into new sectors and/or the introduction of new products and/or services are made by the Board of Directors, based on proposals submitted by the CEO, and following consultation and approval by the General Manager for regulatory matters;

iv) establishing the General Anti-Money Laundering Procedure ("AML Policy"), taking into account the guidance and recommendations provided by competent authorities and various international bodies, as well as developments in the regulatory framework, and defining internal management and control procedures within the scope of anti-money laundering regulations.

Organizational system

The internal organizational structure of the Company is represented:

- at the macro level, through an organizational chart specifying:
  - the structures into which the Company's activities are divided at the first hierarchical level, including the names of the managers responsible for each structure;
  - the lines of hierarchical dependency.
- at the micro level, by specifying for each structure:
  - the organizational breakdown, including the name of the manager and the hierarchical dependencies;

- the resources operating in each area, their employment level, and their organizational position.

Documents related to the internal organizational structure are periodically updated by the People and Organization department.

In matters of health and safety at work, the Company, in line with the current organizational structure and the powers assigned to the Employer, identifies the roles and responsibilities required under Legislative Decree No. 81/2008.

As part of the Model updating process, the adequacy of the organizational system has been assessed based on the following criteria:

- formalization of the system;
- clear definition of responsibilities and hierarchical dependencies;
- existence of segregation and checks between functions;
- consistency between the activities actually carried out and the missions and responsibilities described in the Company's organizational chart.

Some organizational structures are exclusively dedicated to the operation of the Dedicated Asset, including:

- the **Anti-Money Laundering Officer and Suspicious Activity Delegate**, responsible for preventing and combating money laundering and terrorist financing activities;
- the **Outsourced Activities Referent** ("RAE"), reporting directly to the General Manager. While the Board of Directors and the CEO retain decision-making authority on outsourcing business functions, the RAE manages and supervises risks related to outsourcing agreements within the internal control system.

To ensure compliance with regulatory requirements regarding administrative and accounting organization, as well as internal controls, the following safeguards have been implemented:

- the Board of Directors is supported in its responsibilities by internal committees – particularly the Control, Risk, and Sustainability Committee – which has preparatory and advisory functions regarding any regulatory issues related to the provision of payment services and electronic money, and therefore the operation of the Dedicated Asset.
- an adequate internal control system has been established to monitor compliance with the requirements set by the supervisory Authorities.

In addition, for both activities related to the Dedicated Asset and non-regulated activities, the following functions and entities serve as safeguards:

- **Data Protection Officer** ("DPO"), responsible for monitoring regulatory developments in data privacy, providing information and advice on data protection obligations, verifying compliance with regulations and internal policies, and offering, when requested, opinions on data protection impact assessments. The DPO also serves as the point of contact with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali).
- **Chief Information Security Officer** ("CISO"), responsible for monitoring IT security systems, developing, and implementing processes to mitigate cybersecurity risks.

- **Ethics Officer**, who reports to the Board of Directors and the CEO; responsible for monitoring compliance with the Code of Ethics, serving as a point of contact for Telepass employees and those of its subsidiaries for ethical concerns, and supporting the Company in planning initiatives to foster a strong ethical culture.
- **Whistleblowing Team**, whose roles and responsibilities are described in Section 5.5.

Management control system and financial flows

The operational management control system of Telepass is based on the following control principles:

- definition, on an annual basis, of the resources (both financial and non-financial) allocated to each company structure, along with the scope within which these resources can be used, through the programming and definition of the budget;
- monitoring/ analysis of variations from the budgeted amounts, examining the causes and reporting the results of these assessments to the appropriate hierarchical levels for the necessary corrective actions, through the corresponding final account statements;
- monitoring of the compliance of the authorization process in accordance with the internal delegation and power of attorney system.

The management of financial resources is based on principles of segregation of duties, ensuring that all expenses are requested, executed, and controlled by distinct individuals.

The management of liquidity follows principles aimed at the preservation of assets, with a related prohibition on performing high-risk financial transactions.

Additionally, Telepass utilizes a system of legal auditing of accounts.

Control Measures

The Company has developed a set of procedures aimed at regulating the structure of the business processes that make up the organization. These procedures describe the methods of carrying out activities, identify the contents and responsibilities, and outline the control and monitoring activities to be performed in order to ensure the correctness, effectiveness, and efficiency of the corporate activities that are of particular importance, as well as to define the correct management procedures to follow.

In the Special Sections of this Model, the procedures, policies, guidelines, and protocols, regardless of their designation, implemented by Telepass will be referenced as appropriate.

Furthermore, the Company has obtained the following certifications:

1) ISO 45001:2018, Occupational Health and Safety Management System;
2) ISO 27001:2022, Information Security Management System;
3) ISO 14001:2015, Environmental Management System;
4) ISO 9001:2015, Quality Management System.

The evaluation of the adequacy of the Control Measures, in the process of updating the Model, has taken into account not only the negotiation phases but also those related to the instruction and training of corporate decisions.

In particular, with regard to the activities of IMEL, Telepass has implemented a set of procedures designed to prevent the risk of money laundering and financing of terrorism, which are outlined in the relevant Special Sections.

Integrated control system

Telepass' integrated control system is structured, as recommended by best practices in the field, into three levels:

- 1st level: also referred to as "line control", it involves the control directly exercised by the managers of operational areas who are responsible for risk management and the implementation of Control Measures;
- 2nd level: this control is exercised by the corporate functions responsible for monitoring and managing typical risks.
- 3rd level: this control is performed by the Internal Audit function of the Telepass Group.

With respect to **2nd level controls**, Telepass has adopted a control system consisting of two functions:

1) Risk Management Function;
2) Compliance & AML Financial Services Function.

Within the **Risk Management** function, the Risk Officer is tasked with contributing to the definition of methodologies for measuring business risks, verifying compliance with the limits assigned to various operational areas, and ensuring the consistency of operations with the risk appetite objectives assigned.

The head of the **Compliance & AML Financial Services** function reports functionally to the General Manager and the Head of the Designated Assets, and hierarchically to the CEO. This function is responsible for assessing the adequacy of internal procedures with respect to the objective of preventing violations of mandatory laws and regulations, as well as self-regulation (statutes, codes of conduct, self-discipline codes) applicable to Telepass.

3rd level controls involve periodic oversight carried out by the **Internal Audit** function, which reports directly to the Board of Directors, ensuring that its head is not hierarchically subordinate to the heads of the functions under review. This function adheres to international methodological standards for the professional practice of internal auditing: the International Professional Practices Framework ("IPPF"). Within 3rd level control, Internal Audit identifies and assesses the adequacy and effectiveness of the adopted Internal Control and Risk Management System (*Sistema di Controllo Interno e Gestione dei Rischi*, "SCIGR") applied to the processes and activities under analysis, evaluating the evidence collected with independence, professionalism, integrity, objectivity, confidentiality, and competence. Additionally, Internal Audit assesses necessary updates to the Audit Plan for emerging risks and considers, for "extra-plan" interventions, input received not only from the corporate bodies but also from the Supervisory Body.

Furthermore, the **Anti-Corruption Officer** ensures continuous monitoring of the risk of corruption and periodically reports on their activities to the Company's Supervisory Body, ensuring coordination with the same Body for the effective performance of their respective duties, as well as to the Board of Directors and the CEO.

Regarding **health and safety at work**, within the aforementioned integrated management system, the Company has also adopted and formally implemented a monitoring system for compliance with

health and safety obligations, which directly reports to the Employers (for details, see the Special Section D).

The analysis of the integrated control system in the process of updating the Model addressed the existence of an adequate monitoring system for process verification, including the results and any non-conformities, as well as an appropriate documentation management system ensuring traceability of operations.

Gap Analysis

The design of the identified controls is then compared with the characteristics and objectives required by the Decree and/or suggested by the Confindustria Guidelines and best national and international practices.

The overall assessment of the adequacy of the control system is carried out taking into account the acceptable level of risk, which is approved by the Board of Directors from time to time.

3.4 Adoption of a "231" compliance model or mechanisms by Telepass subsidiaries

Each company within the Telepass Group, as an individual subject to the provisions of Legislative Decree No. 231/2001, must evaluate the appropriateness of adopting and periodically reviewing its own Organizational, Management, and Control Model or implementing "231" compliance mechanisms tailored to its specific characteristics (in terms of size, organization, business, etc.), thereby confirming the autonomy of each subsidiary within the Group.

Only the individual subsidiary can perform a precise and effective assessment and management of the risks associated with the potential commission of offenses, which is necessary for the Model to be recognized as having the exempting effectiveness described in Article 6 of the Decree.

A subsidiary that adopts its own Model, tailored to its specific context, must establish an independent and autonomous Supervisory Body, primarily responsible for overseeing the implementation of the Model according to the procedures described therein and in compliance with Articles 6 and 7 of the Decree.

The Telepass Model serves as a reference for defining the organizational models of its subsidiaries, particularly with regard to the principles outlined therein.

Each subsidiary must identify its own sensitive activities and specific protocols based on the peculiarities of its corporate reality. Additionally, any amendments or updates to the Telepass Model must be promptly communicated to the subsidiaries so that, within their autonomy, they can evaluate the potential need to update their respective Organizational, Management, and Control Models or the adopted compliance mechanisms.

3.5 Communication of the Model

Telepass promotes awareness of the Model, the internal regulatory framework, and relevant updates among all Recipients, with varying levels of detail depending on their position and role.

Recipients are therefore required to familiarize themselves with the content of the Model, adhere to its provisions, and contribute to its implementation, including through mandatory training on "231" compliance.

For employees, the Model is made available on the digital intranet platform “T-Space”, which they can access during their routine work activities.

Upon hiring, employees also receive an Information notice on corporate provisions, which includes, among other things, a reference to the Model and relevant regulations pertinent to the Company, whose knowledge is necessary for the proper performance of work activities.

The General Section of this Model and the Code of Ethics are made available to third parties and any other stakeholders of the Company required to comply with its provisions, through publication on the Company's website.

4. SUPERVISORY BODY

4.1 Identification of the Supervisory Body

In compliance with the Decree and the Confindustria Guidelines, the Board of Directors of Telepass has established a body (the "Supervisory Body" or "SB") tasked with overseeing the functioning, effectiveness, and compliance of the Model, as well as ensuring its updates.

Given the specificity of its duties, the Supervisory Body is composed of multiple members, including at least one external member who acts as the Coordinator. Other members of the Supervisory Body are selected from both external and internal individuals within the Company who, in the course of their duties, are not subject to the hierarchical authority of any corporate body or function.

4.2 Appointment

The members of the Supervisory Body are appointed by the Board of Directors, which also identifies the Coordinator. The appointment is communicated to each member of the Supervisory Body through the Company's Board resolution communication system. Each member must formally accept the appointment.

The composition, duties, prerogatives, and responsibilities of the Supervisory Body, as well as the purpose of its establishment, are communicated across all corporate levels.

4.3 Requirements of the Supervisory Body

Pursuant to Articles 6 and 7 of the Decree and considering the Confindustria Guidelines, the Supervisory Body must consistently ensure its autonomy and independence, professionalism, and continuity of action.

The autonomy and independence are guaranteed through the presence of a respected external member serving as Coordinator, free of operational duties or interests that could impair their independent judgment. Additionally, the Supervisory Body operates without hierarchical constraints within the corporate governance framework, reporting directly to the Board of Directors, the Board of Statutory Auditors, and the Chairman and CEO.

When selecting the members of the Supervisory Body (SB), the Board of Directors considers specific skills and professional experience in legal fields – particularly in the prevention of offenses under Legislative Decree No. 231/2001 and criminal law – as well as in corporate management and organization, to ensure the Body's professionalism.

Furthermore, given the unique nature of the tasks and the specific professional expertise required for the assigned duties, the Telepass Supervisory Body utilizes the support of other structures within the Company or the Telepass Group and/or external consultants as needed.

The continuity of action is ensured by the fact that the Supervisory Body operates within the Company and that its members possess in-depth and comprehensive knowledge of corporate processes, enabling them to promptly identify any critical issues.

The appointment as a member of the Supervisory Body is conditional upon the absence of incompatibility and the possession of good standing. Causes of ineligibility or disqualification include:

- being a Director or statutory auditor of Telepass or its subsidiaries;

- having close familial relationships (up to the fourth degree) with Directors or statutory auditors of Telepass;
- maintaining, directly or indirectly (excluding an existing permanent employment relationship), economic relationships and/or contractual agreements, whether for consideration or free of charge, with Telepass and/or its Directors that are significant enough to impair independent judgment;
- holding, directly or indirectly, shareholdings in Telepass that enable control or significant influence over the Company or otherwise compromise independence;
- holding delegations, powers of attorney, or, more generally, roles or responsibilities that could undermine independent judgment.

With regard to the good standing requirements that members of the Supervisory Body must meet, the following constitute grounds for ineligibility and incompatibility for holding the position: being under indictment for an intentional crime or being subject to a personal precautionary measure.

4.4 Term and revocation

The Board of Directors determines the term of office for Supervisory Body members. Each member serves until their successor is appointed or a new Supervisory Body is formed.

The Board of Directors, after consulting the Board of Statutory Auditors, has exclusive authority to revoke the Supervisory Body or its members at any time for just cause, which includes: a) disqualification, interdiction, or a serious illness rendering the member unable to perform their supervisory duties; b) assignment of operational functions and responsibilities to the member that are incompatible with the Supervisory Body's requirements for autonomy, independence, and continuity of action; c) serious breach of the duties of the Supervisory Body as defined in the Model; d) breach of the obligation of confidentiality; e) loss of good standing requirements.

In cases of revocation of all members, the Board of Directors, after consulting the Board of Statutory Auditors, must establish a new Supervisory Body.

In the presence of serious reasons, the Board of Directors, after consulting the Board of Statutory Auditors and, if not involved, the other members of the Supervisory Body, will arrange for the suspension of one or all members of the Supervisory Body and promptly appoint a new member or an entirely new Supervisory Body.

4.5 Functions and powers of the Supervisory Body

The Supervisory Body of Telepass is entrusted with the following general duties:

a) to monitor the adequacy of the Model in preventing the commission of the Offences referred to in the Decree;

b) to oversee compliance with the provisions of the Model by internal Recipients of the Company and to promote the same compliance by Third-Party Recipients (consultants, suppliers, etc.);

c) to ensure the updating of the Model in relation to changes in the organizational structure, the regulatory framework, or as a result of the monitoring activities following which significant violations of the provisions are discovered.

On a more operational level, the Supervisory Body of Telepass is tasked with:

- constantly carrying out a review of the company's activities and the applicable regulations, for the purpose of updating the Company's mapping of activities at risk of criminal offences and proposing the update and integration of the Model and procedures, where necessary;
- monitoring the ongoing validity of the Model and procedures and their effective implementation, promoting, also after consulting the relevant company departments, all necessary actions to ensure their effectiveness. This task includes the formulation of proposals for adjustments and subsequent verification of the implementation and functionality of the proposed solutions;
- periodically conducting targeted checks on specific transactions or acts carried out within high-risk activities;
- verifying the existing authorization and signing powers, in order to assess their consistency with the defined organizational and management responsibilities, and proposing their update and/or modification when necessary;
- defining and managing, in accordance with the Model, the periodic information flow, with a frequency appropriate to the criminal risk level of each area, to allow the Supervisory Body to be regularly updated by the relevant departments on activities assessed as being at risk of criminal offences, as well as establishing communication procedures to gather information on potential violations of the Model;
- implementing, in compliance with the Model, a periodic information flow to the relevant corporate bodies regarding the effectiveness and compliance with the Model;
- sharing the training programs promoted by the Company to spread knowledge and understanding of the Model;
- verifying the initiatives taken by the Company to facilitate the knowledge and understanding of the Model and its related procedures by all those who act on behalf of the Company;
- verifying the credibility of reports received regarding behaviors considered to constitute criminal offenses under the Decree;
- investigating the causes that led to the alleged violation of the Model and identifying the individuals responsible for it;
- verifying reported or discovered violations of the Model and ensuring that they are communicated to the relevant departments for disciplinary purposes.

For the performance of its duties, the Supervisory Body is vested with the following powers:

- to access any relevant company document and/or information necessary for the performance of the functions assigned to the Supervisory Body under the Model. All company functions, employees, and members of the corporate bodies are required to provide any information in their possession upon request by the Supervisory Body or when relevant events or circumstances arise for the execution of the Body's activities;
- to access, without the need for prior consent, any company structure in order to obtain any information or data deemed necessary for the performance of its duties;
- to engage external consultants with proven expertise where necessary for the execution of its tasks;

- to ensure that the heads of company departments provide the requested information, data, and/or reports in a timely manner;
- to request, if necessary, the direct hearing of employees, Directors, and members of the Board of Statutory Auditors of the Company;
- to request information from external consultants, commercial partners, and auditors.

In order to better and more effectively carry out the duties and functions assigned to it, the Supervisory Body may avail itself, to support its operational activities, of the Telepass Group Internal Audit Function, in coordination with the latter, as well as other company departments, which may prove useful from time to time in the performance of the indicated activities.

To guarantee its independence, the Supervisory Body reports directly to the Board of Directors and, in performing its functions, operates with full autonomy, having adequate financial resources to ensure its total operational independence.

To this end, the Board of Directors allocates to the Supervisory Body the financial resources it deems necessary for the expenses incurred in the performance of its duties.

In the execution of the operational activities delegated by the Supervisory Body, the departments in charge report solely to the Supervisory Body on their activities, and similarly, the Supervisory Body reports to the Board of Directors on the activities carried out on its behalf by company departments and external consultants.

4.6 **Reporting to corporate bodies**

The Supervisory Body reports annually on its activities to the Board of Directors and the Board of Statutory Auditors, without prejudice to the specific need for the Supervisory Body to provide reports or communicate with the Board of Directors, the Board of Statutory Auditors, or other corporate bodies at other times. In particular, the report shall cover the following:

- the overall activities carried out during the period, with particular reference to the monitoring of the adequacy and actual implementation of the Model;
- any issues that have arisen, both in terms of internal behaviors or events within the Company, that may lead to violations of the Model's provisions;
- corrective and improvement actions proposed for the Model and their implementation status;
- any reports received during the year and the actions taken by the Supervisory Body and other relevant parties;
- any other information deemed useful for the purpose.

The Supervisory Body must also report promptly to the Chairman and the Chief Executive Officer regarding:

- any violation of the Model deemed well-founded, of which it has become aware either through reports from employees or following direct investigations by the Supervisory Body;
- identified organizational or procedural deficiencies that may create a tangible risk of the commission of offences relevant under the Decree;
- particularly significant regulatory changes that affect the implementation and effectiveness of the Model;

- lack of cooperation from company departments;
- any other information deemed useful for urgent decisions to be made by the Chairman and the Chief Executive Officer.

4.7 Operating Regulations

The Supervisory Body adopts and approves internal regulations governing its operations ("Supervisory Body Regulations").

4.8 Relationships with upervisory Bodies of Telepass Group companies

In compliance with the mutual autonomy and confidentiality of the information pertaining to the various companies within the Telepass Group, the Supervisory Body may communicate with the Supervisory Bodies, where present, of the subsidiary companies for the effective implementation of their respective models.

The communication flows may cover the methods of activity planning, the initiatives undertaken, any violations of the Model, sanctions imposed, and issues identified during the monitoring activities, in order to identify and understand areas of activity that have been found to be at risk.

4.9 Relationships with the Board of Statutory Auditors

In respect of mutual autonomy, the Supervisory Body shall inform the Board of Statutory Auditors, at its request, regarding the compliance with and updating of the Model.

5. INFORMATION FLOWS TO THE SUPERVISORY BODY

5.1 Information flows from Company departments

The obligation to establish a structured information flow is one of the tools to ensure the Supervisory Body's monitoring of the adequacy and effectiveness of the Model and for the possible retrospective investigation of the causes that enabled the commission of offences covered by the Decree.

The Supervisory Body must be made aware of all relevant information, in addition to that specified in the Special Sections of the Model and company procedures, including any information from third parties related to the implementation of the Model in "at-risk" activities.

In particular, the company's organizational structures, each within their area of responsibility, are required to report to the Supervisory Body any information regarding:

- the commission of crimes or the performance of acts that may result in their commission;
- the commission of administrative offences;
- behaviours not in line with the conduct rules set out in this Model and related protocols;
- any changes in the company's organizational structure or procedures;
- any changes to the delegation and proxy system;
- operations of particular importance or that present such levels of risk that they raise a reasonable concern about the potential commission of crimes;
- measures and/or information from law enforcement agencies or any other authority indicating that investigations are being carried out against Telepass employees or collaborators in the course of their work functions for Telepass or its subsidiaries;
- requests for legal assistance submitted by executives and/or employees in the event of the initiation of criminal proceedings[4];
- reports prepared by the heads of company departments within their control activities, from which possible violations of the Model's rules emerge;
- information regarding the actual implementation of the Model at all levels of the company, including details of any disciplinary proceedings conducted, any sanctions imposed, or any decisions to close such proceedings, with related justifications;
- initiation of inspection actions by public bodies (e.g., judiciary, the Italian finance police (*Guardia di Finanza*), other Authorities, etc.) within the scope of high-risk activities.

Other information flows to be transmitted to the Supervisory Body are referred to in the specific procedure dedicated to them.

As further specified in the Whistleblowing Management Procedure and section 5.4 of this Model, reports regarding alleged violations of the Model can also be submitted directly to the Supervisory Body.

The Supervisory Body shall act in a manner that guarantees whistleblowers protection from any form of retaliation, discrimination, or penalization, and also ensures the confidentiality of the

[4] See the Guidelines "Code of Conduct regarding the management of legal representation for employees and executives involved in judicial proceedings" dated 01/04/2021.

whistleblower's identity, in accordance with the legislation on whistleblowing, the Whistleblowing Management Procedure, and the guidelines of the Organizational Model.

To facilitate the direct submission of reports to the Supervisory Body, the Company has established dedicated communication channels:

- email address: organismodivigilanza@telepass.it;
- ordinary mail at the address: Organismo di Vigilanza, Telepass S.p.A., Via Laurentina n. 449 – 00142 Rome, Italy.

The management of reports is carried out according to the procedures described in section 5.4 of this Model, to which full reference is made.

5.2 Reporting obligations regarding official acts

In addition to the information mentioned in the previous section, the following information must be compulsorily transmitted to the Supervisory Body of Telepass:

- measures and/or information from law enforcement agencies or any other authority indicating that investigations, even against unknown individuals, are being carried out for offences under the Decree attributable to the Company;
- requests for legal assistance submitted by executives and/or employees in the event of the initiation of judicial proceedings for offences under the Decree attributable to the Company;
- reports prepared by the heads of company departments within their control activities, from which facts, acts, events, or omissions with critical profiles regarding compliance with the provisions of the Decree may emerge;
- information regarding the actual implementation of the organizational Model at all company levels, including details of any disciplinary proceedings conducted and any sanctions imposed (including measures against employees), or any decisions to close such proceedings, with related justifications.

5.3 Collection, storage, and access to the Supervisory Body's archive

All documentation related to the information flows received must be stored under the responsibility of the Secretary of the Supervisory Body.

5.4 Whistleblowing

Whistleblowing is a legal concept originating from European Union law aimed at preventing unlawful activities in both public and private organizations and protecting individuals who report illegal activities or fraudulent actions within the organization (public or private) to which they belong.

This concept had already been regulated for the private sector by Legislative Decree 231/2001 (Article 6, paragraphs 2-bis, 2-ter, 2-quater).

With Legislative Decree no. 24/2023 – the regulatory instrument implementing European Directive 2019/1937 on the protection of whistleblowers – the adoption of a whistleblowing system became mandatory for certain types of companies operating in the private sector, and the operational management of reporting procedures was regulated.

The National Anti-Corruption Authority subsequently issued specific Guidelines containing detailed rules for establishing suitable channels for managing reports[5], to which Telepass has adhered.

To comply with the new regulations, Telepass, which had already implemented a whistleblowing management system under previous regulations, has updated its Whistleblowing Management Procedure, applicable to all Telepass Group companies.

This procedure governs:

- the process for receiving, analyzing, and handling reports;
- the procedures for managing the related investigations, in compliance with privacy laws and/or other applicable laws in the country where the reported event occurred, applicable to the individual and subject of the report;
- the protections provided to the whistleblower and other individuals identified by law;
- the content of reports;
- the roles, responsibilities, and areas of application.

Telepass, to facilitate the submission of reports, has established the following official channels:

- email address: segnalazioni.telepass@telepass.com;
- physical mail: Telepass S.p.A., Segnalazioni Team (*Reporting Team*), Via Laurentina, 449 - 00142 Rome;
- online platform, accessible by all whistleblowers (employees, third parties, etc.) on the Telepass website.

Oral reports may be made via suitable channels (e.g., voicemail) or through a direct meeting with the Reporting Team or one or more of its members, at the request of the whistleblower.

The digital platform does not replace other reporting channels but expands the possibilities for submitting a report. It allows anyone (employees, collaborators, suppliers, or any other individual who has had or intends to establish business relations with the Telepass Group companies) to report suspected illegal conduct or irregularities, violations of rules, violations of the Model, violations of the Code of Ethics, violations of the Anti-Corruption Policy, and violations of corporate procedures and regulations in general.

In particular, the whistleblower, while required to register on the platform, has the option to make anonymous reports, as their access credentials, if present, are securely stored, protected, and accessible only by the third-party platform manager and are not associated with the report submitted to Telepass.

If the whistleblower prefers, they may provide their name in the report, explicitly consenting to the disclosure of their identity to the Reporting Team.

For reports sent via physical mail and email channels, the confidentiality of the whistleblower's identity (as well as the content of the report) is protected as follows:

[5] Guidelines on the Protection of Persons Reporting Violations of Union Law and the Protection of Persons Reporting Violations of National Regulatory Provisions. Procedures for the Submission and Management of External Reports, 12 July 2023.

- physical mail addressed to the Reporting Team is delivered in a sealed envelope (as delivered by the postal service) to the Technical Secretariat of the Reporting Team;
- the email inbox is accessible only by members of the Reporting Team and the Technical Secretariat; the administrator of the corporate email system may access the inbox only for technical needs, upon written request on a case-by-case basis submitted to the Reporting Team Coordinator, and access will be granted only with prior written authorization from the Reporting Team Coordinator.

In cases where the whistleblower's name has been disclosed, the whistleblower's identity is separated from the content of the report during the handling process, and replaced by an alphanumeric code assigned to the whistleblower during the initial registration in the dedicated Register kept by the Technical Secretariat.

If the allegation is founded, in whole or in part, and knowledge of the whistleblower's identity is essential for the defence of the accused individual, the report may only be used for disciplinary proceedings if the whistleblower has explicitly consented to the disclosure of their identity. The whistleblower will be notified in writing of the reasons for disclosing their confidential data, as required by law.

In the following cases, however, there is no legal obligation to protect the confidentiality of the whistleblower's identity:

- the report is found to be false and made with the intent to harm or damage the reported party (so-called "bad faith reporting"), and constitutes criminal defamation or slander under the law;
- the report reveals facts and/or circumstances that, although unrelated to the company sphere, make it appropriate and/or necessary to report the matter to the judicial authority (e.g., terrorism or espionage offenses).

The body responsible for managing the process of evaluating reports is the **Reporting Team**, which carries out its functions for Telepass and all companies controlled by it, in accordance with the Reporting Management Procedure.

The **Reporting Team** presents the results of its investigation to the Supervisory Body and the Anti-Corruption Officer (if and to the extent relevant) before the final closure of the investigation, in order to gather any additional needs for further investigation. If the reports are unrelated to compliance with the "231" model or anti-corruption matters, the Reporting Team forwards them to the relevant department.

The Telepass Group ensures the confidentiality of the whistleblower's identity starting from the receipt of the report, in accordance with legal provisions.
In compliance with the law, Telepass prohibits and sanctions any form of retaliation or discrimination against anyone who has made a report, whether or not the report is subsequently proven to be valid. The prohibition of retaliation and the protection measures for the whistleblower also apply to:

- the facilitator (someone who assists the whistleblower in making the report);
- individuals related to the whistleblower by a stable personal or family relationship within the fourth degree;
- colleagues of the whistleblower who work in the same work environment and have a habitual and ongoing relationship with the whistleblower;

- entities owned by the whistleblower or for which they work, as well as entities operating within the same work environment as the whistleblower.

A "retaliatory act" is defined as any behaviour, act, or omission, even if attempted or threatened, carried out because of the report, the denunciation to the Judicial or Accounting Authority, or the public disclosure of the report, which causes or may cause unjust harm to the whistleblower or the person who made the report, either directly or indirectly. Retaliatory conduct is exemplified in Article 17, paragraph 4 of Legislative Decree no. 24/2023.

The absence of retaliatory intent in actions, acts, or omissions under Article 17 of Legislative Decree no. 24/2023 must be proven by the person who has carried out the action; in the absence of proof to the contrary, it is presumed that such actions are a consequence of the report.

All employees of the Telepass Group involved in the management of reports are required to maintain confidentiality regarding the existence and content of the report, as well as the identity of the individuals who reported and those reported. Furthermore, any violation of the whistleblower protection measures defined by the company or the submission, with intent or gross negligence, of unfounded reports, will result in disciplinary action.

It is emphasized that, both during the transmission and management of the reports, as well as during their archiving, appropriate technical and organizational measures are in place to ensure the security of personal data in compliance with privacy laws.

As for the content of the reports, they must relate to:

- violations (or suspected violations) of the Code of Ethics, the Model, the Anti-Corruption Policy, or the company's internal regulatory framework (policies, procedures, etc.);
- events that may cause financial or reputational harm to the Telepass Group;
- violations (or suspected violations) of national or European laws, as defined in Article 2, paragraph 1(a) of Legislative Decree no. 24/2023[6].

Finally, as required by law, reports should not concern personal grievances, claims, or requests related to the personal interests of the whistleblower.

[6] This specifically refers to: (i) administrative, accounting, civil, and criminal offenses that harm the interests, decorum, and integrity of the company; (ii) unlawful conduct relevant under Legislative Decree 231/01 or violations of the Organizational, Management, and Control Model; (iii) offenses falling within the scope of the European Directive regulating specific sectors such as public procurement, services, products, transport safety, environmental protection, radiation protection and nuclear safety, food and feed safety, animal health and welfare, public health, consumer protection, and data protection, as well as the security of networks and information systems; (iv) acts and omissions that harm the financial interests of the Union; (v) acts and omissions concerning the internal market of the European Union.

6. TRAINING

6.1 Employee Training

Employee training is a key requirement for the implementation of the Model. Telepass is committed to facilitating and promoting the knowledge of the Model among management and employees, with varying levels of depth depending on position and role, and their constructive contribution to the understanding of its principles and contents.

The principles and contents of Legislative Decree 231/2001 and the Model are communicated through mandatory training courses. The structure of these courses is approved by the Supervisory Body upon proposal from the relevant company functions.

The People and Organization function manages the training of the Company's personnel, disseminating knowledge of the Decree and the Model through a specific training plan and regularly providing the Supervisory Body with reports on such activities.

The traceability of participation in training sessions on the provisions of the Decree is ensured through the requirement for participants to sign an attendance sheet or, for e-learning activities, through the issuance of certificates of completion, or otherwise through other means of registering the completion of the course.

Any update training sessions, as well as specific information on the subject provided to new hires during the onboarding process, will be conducted in the event of significant changes to the Model, the Code of Ethics, or new relevant regulations affecting the Company's operations.

6.2 Information for collaborators and partners

Telepass promotes the knowledge and observance of the Code of Ethics and this General Section of the Model among commercial and financial partners, consultants, collaborators of any kind, customers, and suppliers of the Company. These documents are available on the Company's official website.

In order to formalize the commitment to comply with the principles of the Code of Ethics and this General Section of the Model by third parties with contractual relationships with the Company, a specific termination clause is included in the relevant contract. This clause grants the Company the right to terminate the contract by law and with immediate effect in the event of a breach of the Code of Ethics and/or this General Section of the Model by the contracting party.

Furthermore, the Company has adopted a series of protocols and procedures aimed at the better selection – also from an ethical and compliance perspective – of contractual counterparties.

In this way, Telepass pursues the objective of engaging with parties who share the Company's ethical principles and who pursue the same goal of legality.

7. DISCIPLINARY SYSTEM

Pursuant to Articles 6 and 7 of Legislative Decree 231/2001, for the effective implementation of the Model, a disciplinary system must be in place to sanction any failure to comply with the measures set out in the Model.

Telepass has therefore adopted a disciplinary system aimed at sanctioning violations of the principles and measures provided for in the Model and the corporate protocols, in compliance with applicable legal provisions and the regulations established by national collective bargaining, by the Recipients of the Model.

In accordance with Article 5 of the Decree, violations of the Model and the corporate protocols committed by individuals in Top Management positions as well as those who are subject to the direction or supervision of others or who operate in the name and/or on behalf of the Company are subject to sanctions. Additionally, this disciplinary system applies to any collaborators and partners of the Company.

The initiation of a disciplinary procedure and the possible application of sanctions is independent of whether a criminal proceeding is pending for the same act and does not depend on its outcome.

7.1 Relevant conduct

For the purposes of this Disciplinary System and in accordance with the provisions of collective bargaining agreements, relevant conduct, for the purpose of applying a possible sanction, includes actions or behaviours, including omissions, carried out in violation of the Model.

When determining the related sanction, both the objective and subjective aspects of the relevant conduct are considered. Specifically, the objective elements of the relevant conduct, ranked in increasing order of severity, are:

1. violations of the Model that did not expose the Company to risk or exposed it to only minor risk;
2. violations of the Model that resulted in considerable or significant exposure to risk;
3. violations of the Model that constituted a criminally relevant act.

A further violation of the Model is the failure to comply with the provisions relating to Whistleblowing under Legislative Decree No. 24/2023. Specifically, the following constitute violations of the Model:

- a false report made with intent or gross negligence, aimed at harming the whistleblower (so-called "bad faith" reporting);
- the implementation or threat of retaliatory measures against the whistleblower or other persons protected by the law;
- failure to protect the confidentiality of the whistleblower’s identity.

The severity of relevant conduct is further influenced by the subjective elements outlined below and, in general, by the circumstances in which the violation occurred. Specifically, in compliance with the principle of graduality and proportionality in determining the sanction to be imposed, the following factors are taken into account:

- the commission of multiple violations within the same conduct, in which case the aggravation will be applied based on the sanction for the most serious violation;

- the recidivism of the person(s) involved;
- the hierarchical and/or technical level of responsibility of the individual to whom the contested conduct is attributed;
- the possible sharing of responsibility with other individuals who contributed to the misconduct.

7.2 Sanctions for the Board of Directors[7] and members of the Board of Statutory Auditors

If a violation outlined in section 7.1[8] is committed by a Top Management, the following sanctions may be applied:

- formal written warning;
- a financial penalty, ranging from two to five times the monthly remuneration;
- removal from office.

The choice of the sanction to be imposed in the specific case will be based on the principles of proportionality and graduality identified in section 7.1.

7.3 Sanctions against Employees (managers[9], supervisors, administrative employees)

Failure to comply with and/or violations of the rules set out in the Model by employees of the Company constitutes a breach of the obligations arising from the employment relationship under Article 2104 of the Italian Civil Code and a disciplinary offense.

The adoption by an employee of the Company of conduct that qualifies, as indicated in the previous paragraph, as a disciplinary offense also constitutes a violation of the employees' obligation to perform their duties with the utmost diligence, following the directives of the Company, as provided by the applicable National Collective Labor Agreement (CCNL), as well as by the provisions of the Disciplinary Code.

Sanctions are applied based on the significance of each specific case considered and are proportional to their severity, in accordance with what is set out in the previous paragraph 7.1.

If a violation of the Model attributable to the employee is established[10], and considering the provisions of Article 7 of Law No. 300/1970 and the applicable CCNL, the following disciplinary measures may be applied:

---

[7] Limited to the Directors who do not have an employment relationship.

[8] By way of example and without limitation to what is indicated in the previous paragraph 7.1, the following types of conduct may constitute the grounds for the application of the sanctions outlined below:

- failure to comply with the principles and protocols set out in the Model;
- violation and/or circumvention of the control system, carried out through the removal, destruction, or alteration of documentation required by the company protocols, or by obstructing authorized persons and the Supervisory Body (SB) from carrying out control or accessing the requested information and documentation;
- violation of the provisions regarding signature powers and, in general, the delegation system, except in cases of necessity and urgency, in which case timely information must be provided to the Board of Directors;
- violation of the duty to inform the SB and/or any superior officer regarding behaviours aimed at the commission of a crime or an administrative offense included among those provided for by the Decree.

[9] The sanctioning criteria and the disciplinary procedure take into account the type of employment relationship between these individuals and the Company.

[10] By way of purely illustrative and non-exhaustive example of what is indicated in the previous paragraph 7.1, and subject to the provisions of the applicable CCNL for the application of potential disciplinary measures, the following are some relevant behaviours:

1) conservative disciplinary measures:
    a. verbal reprimand;
    b. written reprimand;
    c. a fine not exceeding four hours of the global daily salary as per point 1 of Article 22
    d. suspension from service and pay for up to 10 days (for part-time employees, up to 50 hours);
2) disciplinary measures resulting in termination:
    a. dismissal with notice;
    b. dismissal without notice.

Without prejudice to the provisions of the applicable CCNL and the Disciplinary Code, the choice of the sanction to be applied in the specific case will be made based on the principles of proportionality and graduality as identified in paragraph 7.1.

Pursuant to Article 38 of the CCNL for Highways and Tunnels (*Autostrade e Trafori*), the Company, if the nature of the offense affects the trust-based relationship, may proceed with the precautionary suspension of the employee pending appropriate investigations.

As for managerial staff, given the highly fiduciary nature of the relationship and considering that managers carry out their functions in order to promote, coordinate, and manage the achievement of the company's objectives, violations of the Model will be assessed in relation to collective bargaining agreements, in line with the specificities of the managerial relationship.

7.4 Sanctions Applicable to Third-Party Recipients

The present Disciplinary System serves to sanction violations of the Code of Ethics and the Model committed by Third-Party Addressees.

This category may include:

- those who have a contractual relationship with Telepass (e.g., consultants, professionals, etc.);
- those responsible for auditing and accounting control;
- collaborators in any capacity;
- attorneys and individuals acting in the name and/or on behalf of the Company;
- suppliers and partners.

- violation of internal procedures or the adoption, in the performance of high-risk activities, of conduct that is inconsistent with the provisions of the Model itself, such conduct being considered as non-compliance with orders given by the Company, both in written and verbal form (e.g., an employee who fails to follow prescribed procedures, omits to inform the Supervisory Body of the required information, fails to carry out checks, etc.);
- adoption, in the performance of high-risk activities, of conduct that is inconsistent with the provisions of the Model or a violation of its principles, such conduct being considered as non-compliance with orders given by the Company (e.g., an employee who refuses to undergo medical checks as per Article 5 of Law No. 300 of May 20, 1970; falsifies and/or alters internal or external documents; deliberately fails to apply the directives issued by the Company in order to gain an advantage for themselves or for the Company; is a repeat offender of any of the misconducts that led to the application of conservative disciplinary measures).

Any violation committed by the aforementioned individuals may result in the application of penalties or the termination of the contractual relationship, depending on the violation in question and the level of risk to which the Company is exposed.

7.5 Investigative procedure

The procedure for the imposition of sanctions consists of:

- the investigative phase;
- the phase of notifying the alleged violation to the person concerned;
- the phase of determining and subsequently imposing the sanction.

The investigative phase begins based on the verification and inspection activities carried out by the Supervisory Body, which, following its investigative activities or the analysis of the reports received, promptly informs and then submits a written report to the person with disciplinary authority, as identified below, regarding any identified violation and the person(s) responsible for it.

Investigative procedure concerning members of the Board of Directors

If the Supervisory Body identifies a violation of the Model by one or more individuals holding the office of Director, who are not bound by an employment relationship with the Company[11], the Supervisory Body shall forward a report to the Board of Directors and the Board of Statutory Auditors containing:

- a description of the contested conduct;
- an indication of the provisions of the Model that have been violated;
- the individual responsible for the violation;
- any documents proving the violation and/or other corroborating elements.

Following the receipt of the Supervisory Body's report, the Board of Directors will convene the Director to whom the violation is attributed. The convocation must:

- be made in writing;
- include the description of the contested conduct and the provisions of the Model that have been violated;
- inform the individual concerned of the date of the meeting, with notice of their right to submit any observations and/or defenses, either written or verbal.

The convocation must be made according to the established procedures for convening the Board of Directors.

During the Board of Directors' meeting, at which the Supervisory Body is also invited to participate, the hearing of the concerned individual will take place, along with the consideration of any observations submitted by them and the carrying out of any further investigations deemed necessary.

[11] In the event that the violation of the Model is attributable to a Director who has an employment relationship with the Company, the authority to impose disciplinary measures lies with the Board of Directors, and the investigation and possible contestation procedure shall be subject to the safeguards provided for under Article 7 of Law No. 300/1970 and the applicable CCNL.

The Board of Directors, with the abstention of the concerned director, shall assess the validity of the acquired evidence and, in accordance with Articles 2392 and following of the Italian Civil Code, convene the Shareholders' Meeting to make the necessary determinations.

The decision of the Board of Directors, in the case of unfounded allegations, or that of the convened Shareholders' Meeting, shall be communicated in writing by the Board of Directors to the concerned individual and to the Supervisory Body.

If the Supervisory Body identifies a violation of the Model by the entire Board of Directors or by the majority of the Directors, the Supervisory Body shall inform the Board of Statutory Auditors so that it may promptly convene the Shareholders' Meeting for appropriate measures.

Investigative procedure for the Statutory Auditors

In the event of a violation of this Model by a Statutory Auditor, the Supervisory Body shall inform the entire Board of Statutory Auditors and the Board of Directors of the Company, through their respective Presidents, by means of a report containing:

- a description of the contested conduct;
- an indication of the provisions of the Model that have been violated;
- the identification of the person responsible for the violation;
- any documents supporting the violation and/or other relevant evidence.

Following the receipt of the Supervisory Body's report, the Board of Statutory Auditors, in a joint meeting with the Board of Directors, shall convene the Statutory Auditor concerned to address the alleged violation.

The notice of the meeting must:

- be issued in writing;
- indicate the contested conduct and the provisions of the Model that have been violated;
- inform the individual of the date of the meeting, with the right to make any comments and/or submissions, both written and oral.

The notice must be given in accordance with the established procedures for convening the Board of Directors.

The Board of Directors of the Company, after assessing the significance of the report, shall activate the Shareholders' Meeting for the appropriate decisions.

If the Supervisory Body identifies a violation of the Model by multiple Statutory Auditors or the entire Board of Statutory Auditors, it shall inform the Board of Directors so that it may promptly convene the Shareholders' Meeting to take the necessary actions.

Investigative procedure for Employees (managers, supervisors, administrative employees)

In the event of a violation of the Model by an employee, the procedure for verifying the violation is carried out in compliance with the applicable legal provisions as well as the applicable collective labor agreement.

In particular, the Supervisory Body submits a report to the CEO containing:

- a description of the contested conduct;

- an indication of the provisions of the Model that have been violated;
- the identification of the person responsible for the violation;
- any documents supporting the violation and/or other relevant evidence.

Following the receipt of the Supervisory Body's report, the CEO summons the person concerned by sending a formal written notice of the violation containing:

- a description of the contested conduct and the provisions of the Model that have been violated;
- the time frame within which the person concerned may submit any comments and/or defenses, both written and oral.

If the person concerned wishes to respond orally to the notice, the Supervisory Body is invited to attend the meeting. During this meeting, any points raised by the individual will be recorded.

At the conclusion of the activities outlined above, the CEO will decide whether to impose a sanction and will determine the specific sanction to be applied.

The decision to impose a sanction, if applicable, is communicated in writing to the person concerned, in accordance with any time frames set by the applicable collective labor agreement.

The relevant departments are responsible for ensuring the effective imposition of the sanction, in compliance with legal and regulatory requirements, as well as the provisions of the applicable collective labor agreement and company regulations, where applicable.

The Supervisory Body is notified, for information purposes, of the decision to impose a sanction.

Investigative Procedure for Third Parties

In order to enable the adoption of the measures outlined in the above-mentioned contractual clauses aimed at ensuring compliance with the principles of the Ethical Code and the present General Section of the Model by third parties with contractual relationships with the Company, the Supervisory Body submits a report to the responsible head of the business unit/department managing the contractual relationship. The report shall contain:

- the identification details of the party responsible for the violation;
- a description of the contested conduct;
- the identification of the provisions of the Ethical Code and the present General Section of the Model that have been violated;
- any documents supporting the violation and/or other relevant evidence.

This report, if the contract was approved by the Board of Directors, must also be forwarded to the attention of the Board of Directors and the Board of Statutory Auditors.

The head of the business unit/department managing the contractual relationship, in agreement with the Legal Affairs Department, if requested, shall send a written communication to the party concerned. This communication shall include a description of the identified conduct, the provisions that have been violated, and an indication of the specific contractual clauses included in the engagement letters, contracts, or partnership agreements that are intended to be applied.