

Oracle Italia S.r.l.

***MODELLO DI ORGANIZZAZIONE, GESTIONE E
CONTROLLO***

EX DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

Approvato con delibera del Consiglio di Amministrazione del 28 Novembre 2024

INDICE

DEFINIZIONI.....	4
1. IL DECRETO LEGISLATIVO N. 231/2001	9
1.1 Caratteristiche fondamentali della normativa	9
1.2 I Reati Presupposto	10
1.3 I reati presupposto commessi all'estero	13
1.4 L'apparato sanzionatorio	13
1.5 Il modello organizzativo come forma di esonero dalla responsabilità	15
1.6 Le Linee Guida di Confindustria	17
2. PROCESSO DI REDAZIONE ED IMPLEMENTAZIONE DEL MODELLO 231	19
2.1 La scelta della Società	19
2.2 Approccio metodologico adottato	19
2.3 Stesura del Modello di Organizzazione, Gestione e Controllo	21
3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI ORACLE ITALIA	21
3.1 Finalità del Modello	21
3.2 Destinatari del Modello	23
3.3 Natura del Modello e rapporti con il Codice di Comportamento	23
3.4 Adozione, efficace attuazione, modifica e integrazione del Modello	24
3.5 Efficace implementazione del Modello – Ruoli e responsabilità	24
3.6 La struttura e l'organizzazione del Modello (Parte Generale e Protocolli)	27
4. LE COMPONENTI DEL SISTEMA DI CONTROLLO INTERNO	27
4.1 Sistema di principi etici e regole di comportamento	29
4.2 Sistema organizzativo	30
4.3 Sistema autorizzativo e decisionale	31
4.4 Sistema di policy e procedure	33
4.5 Programma di formazione e informazione	34
4.6 Sistema disciplinare	34
4.7 Sistemi informativi e applicativi informatici	34
5. ORGANISMO DI VIGILANZA	35
5.1 Requisiti dell'Organismo di Vigilanza	35
5.2 Identificazione dell'Organismo di Vigilanza	36
5.3 Modalità di nomina dell'OdV e durata in carica	37
5.4 Cause di ineleggibilità, motivi e poteri di revoca	37
5.5 Funzioni dell'OdV	39
5.6 Obblighi di informazione verso l'OdV	41
5.7 Reporting dell'OdV	44
5.8 Conservazione delle informazioni	44
6. SEGNALAZIONI DI ILLECITI O DI VIOLAZIONI DEL MODELLO	45
6.1 Principi generali	45
6.2 Sistema di segnalazione	45
6.3 Divieto di ritorsioni	46
7. DIFFUSIONE DEL MODELLO	46
7.1 Attività informativa	47
7.2 Formazione del personale	47
8. SISTEMA DISCIPLINARE	48
8.1 Violazioni del Modello	48
8.2 Misure nei confronti dei dipendenti	49

8.3	Misure nei confronti dei dirigenti.....	52
8.4	Misure nei confronti dei membri del Consiglio di Amministrazione, del Collegio Sindacale, dei membri dell'OdV	53
8.5	Misure nei confronti dei collaboratori coinvolti nelle Attività Sensibili, dei Consulenti esterni, dei Fornitori, dei Partner, degli Appaltatori	55
8.6	Sistema disciplinare per le violazioni del sistema di segnalazione	55
9.	INTRODUZIONE ALLA PARTE SPECIALE	56

DEFINIZIONI

Appaltatori	convenzionalmente si intendono tutti gli appaltatori di opere o di servizi ai sensi del codice civile, nonché i subappaltatori, i somministranti, i lavoratori autonomi che abbiano stipulato un contratto d'opera con la Società e di cui questa si avvale nelle Attività Sensibili.
Approval Matrix	documento emanato a cura della Corporation che definisce ruoli e responsabilità dei soggetti coinvolti nell'iter autorizzativo delle offerte.
Attività Sensibili	attività della Società nel cui ambito sussiste il rischio di commissione di reati di cui al Decreto o rilevanti per la gestione delle risorse finanziarie
CCNL	Contratto Collettivo Nazionale di Lavoro per i dipendenti dalle industrie metalmeccaniche private e della installazione di impianti. Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende industriali.
Consulenti esterni	soggetti non dipendenti della Società che agiscono in nome e/o per conto di Oracle Italia S.r.l. sulla base di un mandato o di un altro rapporto di collaborazione professionale nell'ambito delle attività sensibili.
Corporation	Oracle Corporation
Decreto	Decreto Legislativo 8 giugno 2001, n. 231
Delega	l'atto interno di attribuzione di funzioni e compiti nell'ambito dell'organizzazione aziendale.
Destinatari	tutti i soggetti cui è rivolto il Modello e, in particolare: gli organi societari ed i loro componenti, i dipendenti, ivi compresi i dirigenti, i Fornitori, i Consulenti esterni, i Partner, gli Appaltatori, i dipendenti di altre Società del Gruppo coinvolti nelle Attività Sensibili e/o distaccati presso la Società, i collaboratori, a diverso titolo coinvolti nelle Attività Sensibili (ivi compresi i lavoratori somministrati, i lavoratori a progetto e gli

	stagiaires) nonché i membri dell'Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.
EMEA	acronimo dell'area geografica di gruppo "Europe, Middle East and Africa".
Fornitori	soggetti diversi dai Partner, dei quali la società si avvale per la fornitura di beni (merci e materiali vari) e servizi (escluse le consulenze, ad es. servizi di logistica, trasporto e smaltimento di rifiuti), nell'ambito delle Attività Sensibili.
Linee Guida Confindustria	documento di Confindustria (approvato il 7 marzo 2002 e aggiornato al marzo 2014 e successivamente nel giugno 2021) per la predisposizione dei Modelli di organizzazione, gestione e controllo di cui al D.Lgs. 231/2001
LOB	Line Of Business che con riferimento a Oracle Italia sono riconducibili a 8 e nella fattispecie: Oracle University, Tecnologia, Applications, Consulting, Support e Alliances & Channels.
Modello	Modello di organizzazione, gestione e controllo adottato dalla Società ai sensi del D.Lgs. 231/2001
Organismo di Vigilanza o OdV	Organismo previsto dall'art. 6 del D.Lgs. 231/2001, cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e sul suo aggiornamento e controllo e individuato nel Capitolo 5 del presente Modello.
Organo Dirigente	Consiglio di Amministrazione di Oracle Italia S.r.l.
Partner	i soggetti con i quali Oracle Italia S.r.l. ha definito direttamente o per il tramite della Corporation (Capogruppo), accordi commerciali di varia tipologia. Tali soggetti sono individuabili nelle seguenti categorie: Independent software vendor; System Integrator; Distributori, denominati Value Added Distributor (VAD); Reseller, denominati Value Added Reseller (VAR).
Process Owner	il soggetto che per posizione organizzativa ricoperta o per le attività svolte è maggiormente coinvolto nell'Attività Sensibile di riferimento o ne ha maggiore visibilità ai fini del Modello 231.
Procedure	Procedure, policy, disposizioni organizzative, ordini di servizio e tutte le altre disposizioni, provvedimenti e atti della Società,

compreso il set procedurale adottato in conformità alle norme ISO 9001:2008.

Procura	l'atto unilaterale con cui la società attribuisce dei poteri di rappresentanza nei confronti dei terzi.
Protocolli	documenti che compongono la Parte Speciale e contengono la disciplina delle Attività Sensibili, i presidi di controllo, finalizzati o comunque idonei a ridurre il rischio di commissione dei reati previsti dal Decreto.
Reati	le fattispecie di reato considerate dal Decreto.
Reati 2009	le specifiche fattispecie di reato considerate dal Decreto, entrate in vigore a partire dal 2009, e precisamente: i reati in materia di criminalità organizzata (art. 24 ter); i reati di falso in materia di proprietà industriale (art. 25 bis, lett. f bis); i reati contro l'industria ed il commercio (art. 25 bis.1); i reati in materia di violazione del diritto d'autore (art. 25 novies); l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25 decies).
Società	Oracle Italia Srl (di seguito anche solo "Oracle Italia" o "Oracle") numero di iscrizione al Registro delle Imprese di Milano 01603630599, REA n. 1419895, con sede legale in Milano, via Massimo D'Azeglio, n. 4.
Società del Gruppo	ai fini del presente documento, per Società del Gruppo si intendono tutte le società appartenenti al gruppo facente capo a Oracle Corporation, ivi compresa Oracle Italia.
Terze Parti	soggetti terzi che svolgono attività di consulenza direttamente allocabili ai progetti relativi alla LOB Consulting e che sono impiegati come forza lavoro.

PREMESSA

Oracle Italia S.r.l. ha per oggetto lo sviluppo, la produzione, l'acquisto, la vendita, la locazione, l'importazione, l'esportazione, la spedizione, il trasporto, l'immagazzinaggio, l'assemblaggio, e, in genere, il commercio, sia in Italia che all'estero, sia in proprio che per conto terzi, in via diretta e/o indiretta, di qualsiasi genere di prodotti hardware e software, nonché sia direttamente che indirettamente: acquistare, registrare, depositare o cedere, anche solo come licenziante o licenziataria, brevetti industriali e diritti di proprietà industriale in genere; prestare ogni sorta di servizi di installazione, di assistenza tecnica, di manutenzione ed elaborazione in proprio e/o per conto terzi, di prodotti hardware e software svolgere attività di progettazione, realizzazione, installazione, ampliamento, trasformazione e manutenzione di servizi integrati per il controllo e gestione di impianti tecnologici, elettrici ed elettronici, ivi compresa l'organizzazione di corsi di formazione e aggiornamento professionale per l'applicazione e l'impiego dei sistemi tecnologici suddetti.

La Società ha altresì per oggetto la pianificazione, la gestione e la vendita di studi clinici, studi non interventistici ed osservazionali.

La Società può inoltre compiere tutte le operazioni finanziarie, commerciali, industriali, mobiliari ed immobiliari ritenute dal Consiglio di Amministrazione necessarie od utili per il conseguimento dell'oggetto sociale, con espressa esclusione di ogni attività professionale riservata e dell'esercizio delle suddette attività finanziarie nei confronti del pubblico.

Oracle Italia appartiene al Gruppo Oracle ed è controllata al 100% da Oracle Netherlands BV.

Il Consiglio di Amministrazione di Oracle Italia S.r.l., nella riunione del 27 gennaio 2005, ha approvato una prima versione del "Modello di organizzazione, gestione e controllo" ai sensi del Decreto Legislativo 8 giugno 2001 n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300".

Contestualmente all'adozione del Modello, il Consiglio di Amministrazione ha nominato uno specifico organismo, denominato Organismo di Vigilanza, a cui ha conferito i compiti di vigilanza e controllo previsti dal Decreto medesimo.

Successivamente, prima nel corso del 2007, poi nel corso del 2010 e da ultimo nel 2012, a seguito di un processo di riorganizzazione interna, dovuto anche alla fusione per incorporazione della società Sun Microsystems Italia S.p.A., nonché delle modifiche intervenute nel corpo del testo del D.lgs. 231/2001, la Società ha provveduto ad aggiornare ed integrare il risk assessment a suo tempo condotto, contemplando da un lato i cambiamenti organizzativi intervenuti e, dall'altro, le ipotesi delittuose nel frattempo inserite nel corpo del D. Lgs. 231/2001.

Facendo seguito a quanto stabilito in occasione del primo aggiornamento del Modello, approvato con delibera del Consiglio di Amministrazione del 27

Maggio 2010, Oracle, dunque, ha proceduto già nel corso del 2012 alla predisposizione di un Control & Risk Self Assessment ex D. Lgs. 231/2001, con specifico Focus sui Reati 2009 e sul nuovo assetto organizzativo, anche conseguentemente alla fusione per incorporazione della società Sun Microsystems Italia S.p.A., all'esito del quale la Società ha aggiornato il proprio Modello.

Successivamente, alla luce delle ulteriori modifiche organizzative intervenute e delle novelle legislative intercorse dal 2013 al 2015, Oracle ha proceduto alla predisposizione di un nuovo Control & Risk Self Assessment ex D. Lgs. 231/2001, con specifico Focus sui Reati inseriti quale fattispecie presupposto della responsabilità degli enti tra il 2014 e il 2015 e sugli ulteriori nuovi assetti organizzativi interni. A seguito di tali attività è stata approvata una nuova versione del Modello dal Consiglio di Amministrazione nella riunione 26 settembre 2016.

Alla luce delle novità legislative intervenute dopo l'ultima approvazione del Modello, Oracle ha condotto due nuovi Control & Risk Self Assessment ex D. Lgs. 231/2001, l'uno con specifico Focus sul nuovo reato di "Intermediazione illecita e sfruttamento del lavoro" e l'altro con Focus sulle fattispecie di "corruzione tra privati" - recentemente riformulata - e "istigazione alla corruzione tra privati" di nuova introduzione. A seguito di tali attività è stata approvata una nuova versione del Modello dal Consiglio di Amministrazione nella riunione del 13/02/2020.

Per tener conto sia dei nuovi Reati introdotti all'interno del Decreto, sia delle modifiche organizzative, successivi all'ultima approvazione del Modello, la Società ha condotto un nuovo Control & Risk Self Assessment ex D. Lgs. 231/2001, all'esito della quale ha aggiornato il proprio Modello, anche riorganizzando i contenuti della Parte Speciale per Protocolli, come meglio specificato al capitolo seguente. A seguito di tali modifiche, il Modello aggiornato è stato approvato dal Consiglio di Amministrazione della Società in data 16 Marzo 2023.

Nel corso del 2023 la Società ha aggiornato il Modello in coerenza con quanto previsto dal D.Lgs. 24/2023 in materia di whistleblowing.

Nel corso del 2024 la Società, al fine di tener conto dei nuovi Reati introdotti all'interno del Decreto dalla Legge n. 137/2022, ha condotto un nuovo *Control & Risk Self Assessment* ex D. Lgs. 231/2001, all'esito della quale ha approvato la versione aggiornata del proprio Modello, vigente a far data dal 28 novembre 2024.

STRUTTURA DEL MODELLO

Il presente documento è composto da una Parte Generale e una Parte Speciale, costituita dai Protocolli a disciplina delle Attività Sensibili.

La Parte Generale tratta i seguenti argomenti:

- la normativa di cui al D.Lgs. 231/2001;
- il sistema di governance della Società;

- la metodologia di predisposizione del Modello;
- i soggetti ai quali si applica il Modello;
- la composizione e il funzionamento dell'Organismo di Vigilanza;
- il sistema sanzionatorio a presidio delle violazioni del Modello;
- la diffusione del Modello e la formazione del personale.

I Protocolli che compongono la Parte Speciale contengono invece la disciplina delle Attività Sensibili e riportano i presidi di controllo, finalizzati o comunque idonei a ridurre il rischio di commissione dei reati previsti dal Decreto. Tali presidi di controllo trovano attuazione nelle Procedure.

Costituiscono inoltre parte integrante del Modello:

- il documento "Control & Risk Self Assessment e Gap Analysis ex D.Lgs. 231/2001", che formalizza le risultanze dell'attività di Control and Risk self assessment finalizzata all'individuazione delle Attività Sensibili
- il documento "Codice di Comportamento", (nel seguito anche soltanto "Codice Etico") che racchiude i valori etici fondamentali da seguire durante tutte le attività legate al business della Società e contiene presidi di controllo, finalizzati o comunque idonei a ridurre il rischio di commissione dei reati previsti dal Decreto;
- le Procedure aziendali.

Tali documenti sono reperibili secondo le modalità previste per la loro diffusione al personale della Società.

PARTE GENERALE

1. IL DECRETO LEGISLATIVO N. 231/2001

1.1 Caratteristiche fondamentali della normativa

Con l'entrata in vigore del Decreto Legislativo 8 giugno 2001, n. 231, è stata introdotta nel nostro ordinamento una responsabilità in sede penale (formalmente qualificata come responsabilità "amministrativa") degli enti.

Il Legislatore italiano si è in questo modo conformato ad una serie di provvedimenti comunitari ed internazionali che richiedevano una maggiore responsabilità degli enti che fossero coinvolti nella commissione di alcuni tipi di illeciti aventi rilevanza penale.

La normativa in questione prevede una responsabilità degli enti che si aggiunge a quella delle persone fisiche che hanno materialmente realizzato l'illecito e che sorge qualora determinati reati siano commessi nell'interesse o a vantaggio dell'ente, in Italia o all'estero, da parte di:

- persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società, o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da parte di persone che esercitano anche di fatto la gestione e il controllo (i c.d. soggetti apicali);
- persone sottoposte alla direzione o alla vigilanza di uno dei predetti

soggetti apicali.

I destinatari della normativa sono ai sensi del Decreto: gli enti forniti di personalità giuridica e le società e associazioni anche prive di personalità giuridica. Sono espressamente sottratti all'ambito di validità del Decreto: lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici, nonché gli enti che svolgono funzioni di rilievo costituzionale.

1.2 I Reati Presupposto

La responsabilità dell'ente sorge solo per reati tassativamente indicati dal Decreto, dalle sue successive integrazioni, nonché dalle leggi che espressamente richiamano la disciplina del Decreto (c.d. **Reati Presupposto**).

L'enumerazione dei reati è stata ampliata successivamente a quella originaria contenuta nel Decreto, concernente i reati contro la Pubblica Amministrazione. Sono intervenute le seguenti estensioni: D.L. 25 settembre 2001, n. 350 che ha introdotto l'art. 25-bis "Falsità in monete, in carte di pubblico credito e in valori di bollo", in seguito modificato in "Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumentario segni di riconoscimento" dalla L. 23 luglio 2009, n. 99; D.Lgs. 11 aprile 2002, n. 61 che ha introdotto l'art. 25-ter "Reati Societari", in seguito modificato dalla Legge 28 dicembre 2005, n. 262; L. 14 gennaio 2003, n. 7 che ha introdotto l'art. 25-quater "Delitti con finalità di terrorismo o di eversione dell'ordine democratico"; L. 9 gennaio 2006, n. 7, che ha introdotto l'art. 25-quater.1 "Pratiche di mutilazione degli organi genitali femminili"; L. 11 agosto 2003, n. 228 che ha introdotto l'art. 25-quinquies "Delitti contro la personalità individuale"; L. 18 aprile 2005, n. 62 che ha introdotto l'art. 25-sexies "Abusi di mercato"; L. 16 marzo 2006, n. 146 che prevede all'art. 10 la responsabilità degli enti per i reati transnazionali; L. 3 agosto 2007, n. 123 che ha introdotto l'art. 25-septies "Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro", in seguito modificato in "Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro" dal D.Lgs. 9 aprile 2008, n. 81; D.Lgs. 21 novembre 2007, n. 231 che ha introdotto l'art. 25-octies "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita", modificato con Legge del 15 Dicembre 2014, n. 186, in vigore dal 1.01.2015, in "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio"; L. 18 marzo 2008, n. 48 che ha introdotto l'art. 24-bis "Delitti informatici e trattamento illecito di dati"; L. 15 luglio 2009, n. 94 che ha introdotto l'art. 24-ter "Delitti di criminalità organizzata"; L. 23 luglio 2009, n. 99, già citata, che ha inoltre introdotto l'art. 25-bis.1 "Delitti contro l'industria e il commercio" e l'art. 25-novies "Delitti in materia di violazione del diritto d'autore"; L. 3 agosto 2009, n. 116 che ha introdotto l'art. 25-novies "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria"; D.Lgs. 7 luglio 2011, n. 121 che ha introdotto l'art. 25-undecies "Reati ambientali"; D.Lgs. 16 luglio 2012, n. 109 che ha introdotto l'art. 25-duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare"; Legge 6 Novembre 2012, n. 190, che ha inserito all'art. 25, tra i reati contro la Pubblica Amministrazione, il nuovo reato di "induzione indebita a dare o promettere utilità", nonché all'art. 25-ter, tra i reati societari, il nuovo reato di "corruzione tra privati"; Legge n.

186/2014, che ha inserito all'art. 25 octies, tra i reati in materia di riciclaggio, il nuovo reato di "autoriciclaggio"; Legge n. 68/2015, che ha inserito ulteriori fattispecie di delitti contro l'ambiente all'art. 25-undecies "Reati ambientali"; Legge n. 69/2015, che ha riformulato il reato di "false comunicazioni sociali" inserendolo all'art. 25-ter "Reati Societari", unitamente ai reati di "false comunicazioni sociali delle società quotate" ed ai "fatti di lieve entità" e poi dal d.lgs. 15 marzo 2017, n. 38 che ha sostituito la lett. s-bis) dell'articolo 25-ter in conseguenza della nuova formulazione dell'art. art. 2635 c.c. rubricato «corruzione tra privati» e della previsione del nuovo reato di «istigazione alla corruzione tra privati» (art. 2635-bis c.c.); L. 29 ottobre 2016, n. 199 che ha inserito all'art. 25 quinquies l'art. 603 bis del c.p. rubricato "intermediazione illecita e sfruttamento del lavoro"; Legge 17 ottobre 2017, n. 161 che ha inserito, all'art. 25 duodecies le fattispecie relative all'immigrazione clandestina" previste dall'art. 12, commi 3, 3 bis, 3 ter e 5 del d.lgs. n. 286 del 1998; l'art. 5 del D.Lgs. 20 novembre 2017, n.167, ha introdotto all'art. 25 terdecies il reato di "razzismo e xenofobia". Infine, la Legge 3 maggio 2019 n.39 ha introdotto all'art.25 quaterdecies i reati di "frodi in competizione sportive e esercizio abusivo di gioco e scommesse". Decreto Legge 21 settembre 2019, n. 105 che ha introdotto all'art. 24-bis del D.Lgs. 231/2001 una nuova fattispecie in materia di "cybersecurity"; Legge 19 dicembre 2019, n.157 che ha introdotto l'art. 25-quinquiesdecies del D.Lgs. 231/2001 «Reati tributari»; D.Lgs. 14 luglio 2020, n. 75, che ha introdotto all'art. 24 del D.Lgs. 231/2001 i delitti di frode nelle pubbliche forniture e di frode in agricoltura, all'art. 25 del D.Lgs. 231/2001 i delitti di peculato e di abuso d'ufficio in danno degli interessi finanziari dell'Unione europea, all'art. 25-quinquiesdecies del D.Lgs. 231/2001 i reati di dichiarazione infedele, omessa dichiarazione e indebita compensazione (se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a 10 milioni di Euro), e che ha introdotto al nuovo art. 25-sexiesdecies del D.Lgs. 231/2001 i reati di contrabbando; D.Lgs. 184/2021, che ha introdotto l'art. 25-octies.1 del D.Lgs. 231/2001 "Delitti in materia di mezzi di pagamento diversi dai contanti", modificato dalla L. 137/2023. Legge 9 marzo 2022, n. 22 che introduce nel D.Lgs. 231/2001 due famiglie di reato ai nuovi articoli 25-septiesdecies "Delitti contro il patrimonio culturale" e 25-duodevicies "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici". Il D.L. 13/2022 che ha modificato gli artt. 316-bis, 316-ter, 640-bis e 240-bis c.p. Il D.Lgs. 156/2022 che ha: modificato l'art. 322-bis c.p., modificato i delitti di contrabbando (art. 301 D.P.R. 43/1973), modificato il delitto di frode in agricoltura (punito dall'art. 2 Legge 898/1986, richiamato dall'art. 24 D.Lgs. 231/2001), modificato i reati tributari (modifiche all'art. 6 D.Lgs. 74/2000 che richiama gli artt. 2-3-4 D.Lgs. 74/2000) e modificato l'art. 25-quinquiesdecies. D.Lgs. 2 marzo 2023 n. 19 che ha integrato l'art. 25-ter con la nuova lettera s-ter) che richiama il delitto di "False o omesse dichiarazioni per il rilascio del certificato preliminare" (art. 54 D.Lgs. 2 marzo 2023 n. 19); L. 137/2023 che ha modificato i reati contro la Pubblica amministrazione di cui all'art. 24 introducendo i reati di "turbata libertà degli incanti" (353 c.p.) e "turbata libertà del procedimento di scelta del contraente" (353-bis c.p.), e ha modificato l'art. 25-octies1 mediante l'introduzione del reato di "trasferimento fraudolento di valori" (art. 512-bis c.p.). Decreto Legge n. 19/2024 conv., con modif., dalla L. 56/2024 che ha esteso la punibilità per il reato di "trasferimento fraudolento di valori"

aggiungendo un secondo comma all'art. 512-*bis* c.p., richiamato dall'art. 25-*octies* 1; L. 90/2024 che, tra le altre, ha introdotto il reato di "estorsione informatica" all'art. 24-*bis* del Decreto; L. 114/2024 che ha abrogato il reato di "abuso d'ufficio" e riformulato il reato di "traffico di influenze illecite"; d.l. 4 luglio 2024, n. 92, conv., con modif., dalla L. 112/2024 che ha inserito il nuovo reato di "indebita destinazione di denaro o cose mobili" all'art. 24 del Decreto; il D.Lgs. 141/2024 che ha esteso l'ambito di applicazione dell'art. 25-*sexiesdecies* del Decreto ai reati previsti dalle disposizioni nazionali complementari al codice doganale dell'Unione, di cui al decreto legislativo emanato ai sensi degli articoli 11 e 20, commi 2 e 3, della legge 9 agosto 2023, n. 111, e dal testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi e relative sanzioni penali e amministrative, di cui al decreto legislativo 26 ottobre 1995, n. 504.

Alla data di approvazione del presente Modello, i reati presupposto appartengono alle categorie di seguito indicate:

- reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- delitti informatici e trattamento illecito dei dati (art. 24-*bis*);
- delitti di criminalità organizzata (art. 24-*ter*);
- reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*);
- delitti contro l'industria e il commercio (art. 25-*bis*.1);
- reati societari, ivi incluso i reati di corruzione tra privati e istigazione alla corruzione tra privati (art. 25-*ter*);
- delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater*);
- pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1);
- delitti contro la personalità individuale (art. 25-*quinqies*);
- abusi di mercato (art. 25-*sexies*);
- omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro (art. 25-*septies*);
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies*);
- delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-*octies*.1);
- delitti in materia di violazione del diritto d'autore (art. 25-*novies*);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-*decies*);
- reati ambientali (art. 25-*undecies*);
- delitti in materia di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*);
- reati transnazionali (art. 10, L. 146/2006);
- razzismo e xenofobia (art. 25-*terdecies*);
- frodi in competizione sportive e esercizio abusivo di gioco e scommesse (art. 25-*quaterdecies*);
- reati tributari (art. 25-*quinqiesdecies*);
- delitti di contrabbando (art. 25-*sexiesdecies*);
- delitti contro il patrimonio culturale (art. 25-*septiesdecies*);
- riciclaggio di beni culturali e devastazione e saccheggio dei beni culturali

e paesaggistici (art. 25 *duodevicies*).

I Reati Presupposto sono suscettibili di essere ulteriormente ampliati in futuro.

1.3 I reati presupposto commessi all'estero

Secondo l'art. 4 del Decreto, l'ente che ha la sede principale in Italia può essere chiamato a rispondere, ai sensi del D.Lgs. 231/2001, anche per reati commessi all'estero¹. Il reato deve essere commesso da un soggetto funzionalmente legato all'ente, sia esso apicale o sottoposto, e deve rientrare nei casi e nelle condizioni previsti dagli artt. 7, 8, 9, 10 c.p.².

1.4 L'apparato sanzionatorio

Il Decreto prevede che per gli illeciti sopra descritti agli enti possano essere applicate sanzioni pecuniarie e sanzioni interdittive, possa essere disposta

¹ e "(...) purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti di quest'ultimo."

² Art. 7 c.p.: "Reati commessi all'estero - È punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati: 1) delitti contro la personalità dello Stato italiano; 2) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto; 3) delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano; 4) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni; 5) ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana". Art. 8 c.p.: "Delitto politico commesso all'estero - Il cittadino o lo straniero, che commette in territorio estero un delitto politico non compreso tra quelli indicati nel numero 1 dell'articolo precedente, è punito secondo la legge italiana, a richiesta del Ministro della giustizia. Se si tratta di delitto punibile a querela della persona offesa, occorre, oltre tale richiesta, anche la querela. Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. È altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici." Art. 9 c.p.: "Delitto comune del cittadino all'estero - Il cittadino, che, fuori dei casi indicati nei due articoli precedenti, commette in territorio estero un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del Ministro della giustizia ovvero a istanza o a querela della persona offesa. Nei casi previsti dalle disposizioni precedenti, qualora si tratti di delitto commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del Ministro della giustizia, sempre che l'extradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto." Art. 10 c.p.: "Delitto comune dello straniero all'estero - Lo straniero, che, fuori dei casi indicati negli articoli 7 e 8, commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del Ministro della giustizia, ovvero istanza o querela della persona offesa. Se il delitto è commesso a danno delle Comunità europee di uno Stato estero o di uno straniero, il colpevole è punito secondo la legge italiana, a richiesta del Ministro della giustizia, sempre che: 1) si trovi nel territorio dello Stato; 2) si tratti di delitto per il quale è stabilita la pena dell'ergastolo ovvero della reclusione non inferiore nel minimo di tre anni; 3) l'extradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto, o da quello dello Stato a cui egli appartiene."

la pubblicazione della sentenza e la confisca del prezzo o del profitto del reato.

Le **sanzioni pecuniarie** si applicano ogniqualvolta un ente commetta uno degli illeciti previsti dal Decreto. Esse vengono applicate per quote in un numero non inferiore a cento né superiore a mille (l'importo di una quota va da un minimo di € 258,22 ad un massimo di € 1.549,37) e possono variare da un minimo di € 25.822,00 ad un massimo di € 1.549.370,00. Ai fini della quantificazione delle quote il giudice deve tenere conto:

- della gravità del fatto;
- del grado di responsabilità dell'ente;
- dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

L'importo della quota viene invece fissato sulla base delle condizioni economiche e patrimoniali dell'ente. In certi casi la sanzione pecuniaria può essere anche ridotta.

Le **sanzioni interdittive** possono essere applicate solo in relazione ai reati per i quali sono espressamente previste dal Decreto, qualora ricorra almeno una delle seguenti condizioni:

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

Le sanzioni interdittive applicabili agli enti ai sensi del Decreto sono:

- l'interdizione dall'esercizio dell'attività, con conseguente sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento della stessa;
- la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- la esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi.

Il tipo e la durata (che può variare da tre mesi a due anni) delle sanzioni interdittive sono stabiliti dal giudice, sulla base dei criteri indicati per la commisurazione delle sanzioni pecuniarie. Il Decreto prevede, inoltre, la possibilità di applicare alcune sanzioni in via definitiva (quindi superando il limite massimo di durata di due anni), qualora si verificano determinati eventi considerati particolarmente gravi dal legislatore. Se necessario, le sanzioni interdittive possono essere applicate anche congiuntamente.

Il giudice può disporre in luogo dell'applicazione della sanzione interdittiva che determina l'interruzione dell'attività dell'ente la prosecuzione dell'attività dell'ente da parte di un commissario giudiziale per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, qualora ricorra almeno una delle seguenti condizioni:

- l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

In caso di inosservanza delle sanzioni interdittive la punizione può essere la reclusione da sei mesi a tre anni a carico di chiunque, nello svolgimento dell'attività dell'ente cui è stata applicata la sanzione interdittiva, trasgredisca agli obblighi o ai divieti inerenti la stessa.

In tale caso, nei confronti dell'ente nell'interesse o a vantaggio del quale il reato è stato commesso si applica la sanzione amministrativa pecuniaria da 200 a 600 quote e la confisca del profitto.

Qualora sussistano gravi indizi per ritenere la responsabilità dell'ente per un illecito dipendente da reato e vi sono fondati motivi e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole, le sanzioni interdittive di cui sopra possono anche essere applicate in via cautelare.

Oltre alle predette sanzioni, il Decreto prevede che venga sempre disposta con la sentenza di condanna la **confisca** del prezzo o del profitto del reato nonché la **pubblicazione** della sentenza di condanna in presenza di una sanzione interdittiva a spese dell'ente.

1.5 Il modello organizzativo come forma di esonero dalla responsabilità

Il Decreto prevede che l'ente non risponda dei reati commessi dai soggetti c.d. apicali qualora dimostri:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, Modelli di organizzazione e di gestione idonei a prevenire reati della specie di quelli verificatisi;
- di aver affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo il compito di vigilare sul funzionamento e l'osservanza dei Modelli e di curare il loro aggiornamento;
- che il soggetto in posizione apicale ha commesso il reato eludendo fraudolentemente i suddetti modelli di organizzazione e di gestione;
- che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo su indicato.

Per i reati commessi da soggetti non in posizione apicale (cd. "soggetti subordinati") l'ente è responsabile solo qualora la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. In ogni caso è esclusa l'omissione degli obblighi di direzione e vigilanza se, prima

della commissione del reato, l'ente ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto prevede che gli enti, per soddisfare le predette esigenze, possano adottare modelli di organizzazione e di gestione "sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni osservazioni sulla idoneità dei modelli a prevenire i reati". In conformità a tale disposizione Oracle Italia, nella predisposizione del presente Modello, si è ispirata alle linee guida emanate ed aggiornate periodicamente da Confindustria. Occorre tuttavia ricordare che tali indicazioni rappresentano un semplice quadro di riferimento a cui ogni società può rifarsi ai fini dell'adozione del Modello. Si tratta di suggerimenti cui la società è libera di ispirarsi nell'elaborazione del Modello. Ogni società dovrà, infatti, adeguare le linee guida alla realtà concreta che la caratterizza e, quindi, alle sue dimensioni ed alla specifica attività che svolge e scegliere, di conseguenza, le modalità tecniche con cui procedere all'adozione del Modello.

Inoltre, con specifico riferimento alla materia della salute e sicurezza sul luogo di lavoro, è doveroso ricordare che l'art. 30 del D.Lgs. 9 Aprile 2008, n. 81, stabilisce che il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa degli enti di cui al Decreto, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Il suddetto modello organizzativo e gestionale deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività in precedenza elencate.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione dello stesso e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

Il riesame e l'eventuale modifica del modello organizzativo devono essere

adottati quando:

- siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero
- in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Infine, il suddetto art. 30 stabilisce che, in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente:

- alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001, ovvero
- al British Standard OHSAS 18001:2007

si presumono conformi ai requisiti più sopra enunciati per le parti corrispondenti.

Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale potranno essere indicati dalla Commissione consultiva permanente per la salute e la sicurezza sul lavoro, istituita presso il Ministero del Lavoro e della Previdenza Sociale dall'art. 6 del D.Lgs. n. 81/2008.

1.6 Le Linee Guida di Confindustria

Come già ricordato al precedente Paragrafo 1.2, al fine di agevolare gli enti nell'attività di predisposizione di idonei Modelli, il co. 3 dell'art. 6 del Decreto prevede che le associazioni di categoria possano esercitare una funzione guida attraverso la realizzazione di appositi codici di comportamento, a supporto delle imprese nella costruzione dei modelli di organizzazione, gestione e controllo.

In tale contesto, Confindustria ha elaborato le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001", approvandone il testo definitivo già in data 7 marzo 2002.

Dette Linee Guida possono essere schematizzate secondo i seguenti punti fondamentali:

- A. individuazione delle aree di rischio, ossia delle aree/settori aziendali nei quali sia possibile la realizzazione degli eventi pregiudizievoli previsti dal Decreto;
- B. predisposizione di un sistema di controllo in grado di prevenire la commissione dei reati presupposti dal Modello attraverso l'adozione di appositi protocolli;
- C. Previsione di obblighi di informazione da parte dell'OdV e verso l'OdV.

Le componenti più rilevanti del sistema di controllo delineato da Confindustria a cui ci si riferisce nel precedente punto B sono:

- Codice di Comportamento;
- Sistema organizzativo;

- Procedure manuali ed informatiche;
- Poteri autorizzativi e di firma;
- Sistemi di controllo e gestione;
- Comunicazione al personale e sua formazione.

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

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- principio di separazione delle funzioni, in ragione del quale ne Oracle può gestire in autonomia un intero processo e per cui l'autorizzazione all'effettuazione di un'operazione, deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione;
- documentazione dei controlli.

Il sistema di controllo deve prevedere inoltre:

- un adeguato sistema sanzionatorio per la violazione delle norme del Codice di Comportamento e delle procedure previste dal Modello;
- l'individuazione dei requisiti dell'Organismo di Vigilanza (OdV) tra i quali in modo particolare: autonomia e indipendenza, professionalità e continuità di azione.

In data 3 ottobre 2002, Confindustria ha predisposto una "Appendice integrativa alle Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001 con riferimento ai reati introdotti dal D. Lgs. n. 61/2002".

Obiettivo dell'estensione ai reati societari della disciplina prevista dal Decreto è stato quello di assicurare un'accresciuta trasparenza delle procedure e dei processi interni alle società e, quindi, di assicurare maggiori possibilità di controllo sull'operato dei managers.

Da ciò è nata, dunque, la duplice esigenza di:

- approntare specifiche misure organizzative e procedurali – nell'ambito del modello già delineato dalle Linee Guida per i reati contro la Pubblica Amministrazione – atte a fornire ragionevole garanzia di prevenzione di questa tipologia di reati;
- precisare i compiti principali dell'OdV per assicurare l'effettivo, efficace e continuo funzionamento del Modello stesso.

Le suddette Linee Guida sono state oggetto di successivi aggiornamenti, gli ultimi dei quali risalgono rispettivamente al marzo 2008, al marzo 2014 e a giugno 2021.

Tali aggiornamenti sono stati determinati dalla necessità di adeguare le Linee Guida alle successive modifiche legislative che hanno introdotto nel *corpus* del Decreto i reati contro la personalità individuale, i reati di abuso di informazioni privilegiate e di manipolazione del mercato (c.d. reati di Market Abuse), i reati transnazionali, i reati di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme sulla tutela

della salute e sicurezza sul lavoro, nonché i reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, corruzione tra privati, reati ambientali, reati tributari e reati di contrabbando.

È opportuno evidenziare che il mancato rispetto di punti specifici delle Linee Guida non inficia la validità del Modello. Il singolo modello, infatti, dovendo essere redatto con riferimento alla realtà concreta della società, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

2. PROCESSO DI REDAZIONE ED IMPLEMENTAZIONE DEL MODELLO **231**

2.1 La scelta della Società

Nonostante il Decreto non imponga l'adozione di un Modello di Organizzazione, Gestione e Controllo, Oracle Italia ha ritenuto indispensabile provvedere in tal senso al fine di garantire un comportamento eticamente condiviso e perseguire il rispetto dei principi di legittimità, correttezza e trasparenza nello svolgimento dell'attività aziendale.

Inoltre la scelta di adottare un Modello di Organizzazione, Gestione e Controllo corrisponde all'esigenza di Oracle Italia di perseguire la propria missione nel rispetto rigoroso dell'obiettivo di creazione di valore per i propri azionisti.

Oracle ha quindi deciso di avviare, già nel corso del 2005, un progetto di adeguamento rispetto a quanto espresso dal Decreto, revisionando il proprio assetto organizzativo, nonché gli strumenti di gestione e controllo, al fine di adottare un proprio Modello. Quest'ultimo rappresenta non solo un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Società affinché tengano comportamenti corretti e lineari nell'espletamento delle proprie attività, ma anche un imprescindibile mezzo di prevenzione contro il rischio di commissione dei reati previsti dal Decreto.

2.2 Approccio metodologico adottato

Come anticipato in Premessa la presente versione del Modello adottata da Oracle Italia S.r.l. è il risultato di un processo di aggiornamento e integrazione delle attività di risk assessment a suo tempo condotte, resosi necessario alla luce dell'evoluzione del quadro normativo di riferimento e dell'assetto organizzativo della Società. Da ultimo nel corso del 2021 la Società ha svolto un percorso di aggiornamento integrale dei risk assessment precedenti che ha condotto all'aggiornamento del Modello.

Pertanto il presente Modello, ispirato all'ultimo aggiornamento delle Linee Guida di Confindustria, è stato elaborato tenendo conto della struttura e dell'attività concretamente svolta dalla Società, della natura e delle dimensioni della sua organizzazione. In particolare l'articolazione del processo di redazione ed implementazione del Modello è di seguito descritta in sintesi.

La Società ha proceduto ad un'analisi preliminare del proprio contesto aziendale e successivamente ad una analisi delle aree di attività che presentano profili potenziali di rischio in relazione alla commissione dei reati

indicati dal Decreto ritenuti applicabili per Oracle Italia.

In particolar modo sono stati analizzati, a mero titolo esemplificativo, ancorché non esaustivo:

- la storia della Società e il contesto societario;
- il settore di appartenenza;
- l'assetto organizzativo (formalizzato in organigrammi aziendali, ordini di servizio, etc.);
- il sistema di corporate governance esistente;
- il sistema dei poteri delegati;
- i rapporti giuridici esistenti con soggetti terzi, anche con riferimento ai contratti di servizio che regolano i rapporti infragruppo;
- la modalità tipiche di conduzione del business;
- la tipologia delle relazioni e delle attività (es. commerciale, finanziaria, di controllo, regolamentare, di rappresentanza, di contrattazione collettiva, etc.) intrattenute con pubbliche amministrazioni;
- i casi di eventuali e presunte irregolarità avvenute in passato;
- le prassi e le procedure formalizzate e diffuse all'interno della Società per lo svolgimento delle attività aziendali.

Sulla base delle analisi preliminari sono state quindi identificate le funzioni aziendali coinvolte nelle aree di attività che presentano profili potenziali di rischio in relazione alla commissione dei reati indicati, nonché i soggetti appartenenti a tali funzioni che occupano ruoli chiave nell'organizzazione aziendale, c.d. *Key Officers*, al fine di poter condurre le interviste relative alla successiva fase di indagine.

Ai fini della preparazione del presente documento, la Società ha quindi proceduto, mediante interviste con i *Key Officers* e l'analisi documentale:

- all'individuazione delle Attività Sensibili, ovvero le aree in cui è possibile che siano commessi i Reati ritenuti applicabili per Oracle edelle possibili modalità attuative degli stessi;
- all'identificazione delle modalità operative di esecuzione delle Attività Sensibili, dei soggetti coinvolti e del sistema di ripartizione delle responsabilità;
- all'autovalutazione dei rischi (cd. "*Control & Risk Self Assessment*") di commissione di reato e del sistema di controllo interno idoneo a prevenire comportamenti potenzialmente illeciti;
- all'identificazione di adeguati presidi di controllo, necessari per la prevenzione dei reati suddetti o per la mitigazione del rischio di commissione;
- l'identificazione delle eventuali carenze e/o ambiti di miglioramento dei presidi di controllo.

La fase conclusiva è rappresentata dalla stesura del presente Modello.

Nel Modello sono stati quindi individuati, alla luce dei risultati delle attività di Control & Risk Self Assessment, i principi generali di comportamento, le regole di prevenzione e i presidi di controllo specifici per ciascuna Attività Sensibile, che devono essere attuati per prevenire, per quanto

ragionevolmente possibile, la commissione dei Reati rilevanti per la Società. A tal fine, la Società ha tenuto conto degli strumenti di controllo e di prevenzione già esistenti, diretti a regolamentare il governo societario, quali lo Statuto, il sistema di deleghe e procure, i contratti nonché le procedure e istruzioni operative redatte dalle singole funzioni aziendali.

In particolare i risultati delle analisi condotte e descritte in precedenza riconducibili al *Control & Risk Self Assessment (CRSA)* sono contenuti o richiamati nella documentazione in cui sono formalizzate le evidenze emerse dal CRSA stesso, con particolare riferimento ai seguenti elementi:

- Le Attività Sensibili e le modalità attuative delle stesse;
- i soggetti (interni ed esterni alla Società) coinvolti nelle Attività Sensibili;
- le esemplificazioni delle possibili modalità di commissione dei Reati nell'ambito delle Attività Sensibili;
- i protocolli e i sistemi di controllo specifici individuati dalla Società a presidio/mitigazione dei "rischi reato" riconducibili alle Attività Sensibili.

Tale documentazione costituisce presupposto del presente Modello.

La documentazione in formato elettronico e/o cartaceo inerente alla Società e gli output prodotti nelle diverse fasi del progetto di aggiornamento del Modello sono stati archiviati e resi disponibili in uno specifico archivio consultabile dai componenti dell'OdV (in seguito "Archivio").

2.3 Stesura del Modello di Organizzazione, Gestione e Controllo

Le attività di Risk Assessment precedentemente descritte e le relative risultanze sono state oggetto di condivisione con il management e con l'Organismo di Vigilanza della Società.

A detta fase di analisi, diagnosi e progettazione è seguita dunque la fase di redazione che ha condotto alla stesura del presente Modello e alla definizione degli elementi che lo compongono.

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI ORACLE ITALIA

3.1 Finalità del Modello

L'adozione del Modello è tesa alla creazione di un sistema di prescrizioni e strumenti organizzativi aventi l'obiettivo di garantire che l'attività della Società sia svolta nel pieno rispetto del Decreto e di prevenire e sanzionare eventuali tentativi di porre in essere comportamenti a rischio di commissione di una delle fattispecie di reato previste dal Decreto.

Pertanto il Modello si propone le seguenti finalità:

- migliorare il sistema di Corporate Governance;
- introdurre nella Società ulteriori principi e regole di comportamento volte a promuovere e valorizzare una cultura etica al proprio interno, in un'ottica di correttezza e trasparenza nella conduzione degli affari;
- predisporre un sistema strutturato ed organico di prevenzione e controllo

finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale;

- determinare, in tutti coloro che operano in nome e per conto di Oracle Italia nelle "aree di attività a rischio", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni sia a carico dell'autore della violazione (sul piano civilistico, disciplinare e, in taluni casi, penale) sia a carico della Società (responsabilità amministrativa ai sensi del Decreto);
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di Oracle Italia che la violazione delle prescrizioni contenute nel Modello comporterà l'applicazione di apposite sanzioni oppure la risoluzione del rapporto contrattuale;
- ribadire che Oracle Italia non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui Oracle intende attenersi;
- censurare fattivamente i comportamenti posti in essere in violazione del Modello attraverso la comminazione di sanzioni disciplinari e/o contrattuali;
- garantire ai Destinatari la possibilità di segnalare violazioni del Modello o condotte illecite rilevanti ai sensi del Decreto, in conformità a quanto previsto dal D.lgs. 24/2023.

Il Modello predisposto da Oracle Italia S.r.l. si fonda pertanto su un sistema strutturato ed organico di protocolli e di attività di controllo che:

- individua le aree e i processi potenzialmente a rischio nello svolgimento dell'attività aziendale, vale a dire quelle attività nel cui ambito si ritiene più alta la possibilità che possano essere commessi Reati;
- definisce un sistema normativo interno, finalizzato alla prevenzione dei Reati, nel quale sono tra l'altro ricompresi:
 - un Codice di Comportamento, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali;
 - un sistema di deleghe, poteri e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
 - procedure formalizzate, tese a disciplinare le modalità operative e di controllo nelle aree a rischio;
- trova il proprio presupposto in una struttura organizzativa coerente con l'attività svolta dalla Società e progettata con lo scopo di assicurare da un lato, una corretta gestione strategico-operativa delle attività di business, dall'altro un controllo continuativo dei comportamenti. Tale controllo viene assicurato garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che l'assetto della struttura organizzativa definita sia realmente attuato, attraverso:
 - un organigramma formalmente definito, chiaro, adeguato e

- coerente con l'attività svolta dalla Società;
- una chiara definizione delle funzioni e delle responsabilità attribuite a ciascuna unità organizzativa;
- un sistema di deleghe di funzioni interne e di procure a rappresentare la Società verso l'esterno che assicuri una chiara e coerente segregazione delle funzioni;
- individua i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- attribuisce all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporre l'aggiornamento.

3.2 Destinatari del Modello

Le prescrizioni del Modello sono indirizzate agli organi societari ed i loro componenti, i dipendenti, ivi compresi i dirigenti, i Fornitori, i Consulenti esterni, i Partner, gli Appaltatori, i collaboratori a diverso titolo coinvolti nelle Attività Sensibili (ivi compresi i lavoratori somministrati, gli stagiaires e i lavoratori a progetto), i dipendenti di altre Società del Gruppo coinvolti nelle Attività Sensibili e/o distaccati presso la Società, nonché i membri dell'Organismo di Vigilanza, in quanto non appartenenti alle categorie summenzionate.

I Destinatari del Modello sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

La Società condanna qualsiasi comportamento difforme, oltre che dalla legge, dalle previsioni del Modello, anche qualora il comportamento sia realizzato nell'interesse della Società ovvero con l'intenzione di arrecare ad essa un vantaggio.

3.3 Natura del Modello e rapporti con il Codice di Comportamento

Le prescrizioni contenute nel presente Modello si fondano e si integrano con quelle definite nel "Codice di Etica e Condotta Aziendale" e nel "Employee Handbook", redatto dalla Corporation e tradotto in lingua italiana (che è genericamente applicabile a tutte le Società del Gruppo) e con quelle definite nel Codice di Comportamento che recepisce i principi del "Codice di Etica e Condotta Aziendale" e li rappresenta e li specifica rispetto alle finalità di ragionevole prevenzione dei reati indicati nel Decreto 231/01. Tale Codice di Comportamento è approvato dal Consiglio d'Amministrazione di Oracle Italia S.r.l. contestualmente al Modello di cui ne costituisce un allegato e parte integrante (**Allegato A**).

Si specifica tuttavia che:

- il Codice di Etica e Condotta Aziendale, l'Employee Handbook e il Codice di Comportamento rappresentano strumenti adottati in via autonoma, suscettibili di applicazione sul piano generale da parte della Società allo scopo di esprimere dei principi di "deontologia aziendale" che la stessa riconosce come propri e sui quali richiama l'osservanza di tutti i Destinatari;

- il Modello risponde invece alle specifiche esigenze previste dal Decreto, ed è finalizzato a prevenire la commissione di particolari tipologie di reati per fatti che, in quanto commessi a interesse o a vantaggio della Società, possano comportare una responsabilità amministrativa in base alle disposizioni del Decreto medesimo.

3.4 Adozione, efficace attuazione, modifica e integrazione del Modello

Il Decreto prevede che sia l'organo dirigente ad adottare il Modello, rimettendo ad ogni ente il compito di individuare al proprio interno l'organo cui affidare tale compito.

In coerenza con quanto indicato dalle Linee Guida di Confindustria, Oracle Italia ha individuato nel proprio Consiglio di Amministrazione l'Organo Dirigente deputato all'adozione del Modello. Il compito di vigilare sull'efficace attuazione del Modello è invece affidato, secondo quanto previsto dal Decreto, all'Organismo di Vigilanza (di seguito anche OdV).

Conseguentemente, essendo il presente documento un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6 co. 1 lett. a) del Decreto) le successive modifiche ed integrazioni di carattere sostanziale dello stesso sono rimesse alla competenza dello stesso Consiglio di Amministrazione.

Fra le modifiche di carattere sostanziale rientrano, a titolo esemplificativo e non esaustivo:

- aggiornamento dei Protocolli costituenti la Parte Speciale;
- soppressione di alcune parti del presente documento;
- modifica dei compiti dell'OdV;
- individuazione di un OdV diverso da quello attualmente previsto;
- aggiornamento/modifica/integrazione dei principi di controllo e delle regole comportamentali.

È peraltro riconosciuta all'Amministratore Delegato la facoltà di apportare eventuali modifiche o integrazioni al presente documento di carattere esclusivamente formale, a condizione che il contenuto rimanga invariato nella sostanza, nonché apportare eventuali integrazioni, modifiche ed aggiornamenti agli Allegati. Di tali modifiche o integrazioni dovrà essere prontamente informato il Consiglio di Amministrazione e l'OdV.

3.5 Efficace implementazione del Modello - Ruoli e responsabilità

Il Consiglio di Amministrazione, al fine di garantire un'efficace e concreta attuazione del Modello, delega alle singole LOB/Funzioni ed ai loro responsabili le seguenti responsabilità:

- garantire l'effettiva applicazione delle prescrizioni e dei principi di controllo e di comportamento contenuti nel Modello;
- rivedere, alla luce dei principi di comportamento e di controllo prescritti per la disciplina dei Attività Sensibili, le prassi ed i processi di propria competenza, al fine di renderli adeguati a prevenire comportamenti illeciti;

- monitorare l'effettivo rispetto, da parte dei soggetti impiegati nelle proprie strutture, della normativa interna (Policy, Procedure, disposizioni organizzative, ecc.) che costituisce parte integrante del Modello; monitorare il costante aggiornamento della normativa interna (Policy, Procedure, disposizioni organizzative, ecc.) rispetto alle evoluzioni del business e all'effettiva operatività dei processi;

In particolare, le LOB/altre funzioni, per le attività aziendali sensibili, devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio ad eventuali carenze di normative o di procedure che potrebbero dar luogo a prevedibili rischi di commissione di "illeciti presupposti" nell'ambito delle attività di propria competenza.

L'efficace e concreta attuazione del Modello deve essere altresì garantita dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti e rappresentati nel successivo Capitolo 5.

Specifici ruoli e responsabilità aggiuntive sull'efficace attuazione ed implementazione del Modello sono inoltre attribuiti alle strutture di seguito indicate:

Funzione Legal/Ufficio Legale

La Funzione Legal è responsabile di assicurare assistenza e consulenza legale alle strutture della Società, seguendo l'evolversi della normativa e degli orientamenti giurisprudenziali.

Stanti tali competenze, la Funzione Legal può essere chiamata a collaborare con l'Organismo di Vigilanza per la valutazione delle opportunità/necessità di adeguamento del Modello, per fornire supporto per l'identificazione delle condotte che possano configurare ipotesi di reato e delle condotte comunque in violazione del Modello, per la gestione del sistema disciplinare di cui al Capitolo 7.

La Funzione Legal inoltre si occupa della formalizzazione di un sistema di deleghe e procure coerente con i principi ispiratori stabiliti al Capitolo 4 e per la definizione dei contenuti delle clausole contrattuali c.d. "231" (cfr. par. 8.5).

Funzione Human Resources

Con riferimento al Decreto, la funzione Human Resources, come illustrato rispettivamente nei successivi Capitoli 4, 7 e 8:

- in coordinamento con Oracle University, supporta l'Organismo di Vigilanza per la programmazione di piani di formazione e interventi di sensibilizzazione rivolti a tutti i dipendenti sull'importanza di un comportamento conforme alle regole aziendali, sulla comprensione dei contenuti del Modello, del Codice di Comportamento, nonché specifici corsi destinati al personale che opera nelle aree sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio;

- presidia il processo sanzionatorio per eventuali violazioni del Modello e, a sua volta, fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del Decreto all'Organismo di Vigilanza, il quale le analizza al fine di prevenire la commissione di reati rilevanti ai sensi del Decreto, nonché di monitorare l'adeguatezza del Modello.

Inoltre, al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di *governance* rispetto agli obiettivi perseguiti col Modello, la funzione Human Resources supporta le LOB/Funzioni, in coerenza con le linee guida della Corporation nella:

- definizione delle regole per l'ufficializzazione e la gestione dei processi organizzativi;
- validare procedure definite da altre funzioni, garantendone la coerenza con il disegno organizzativo complessivo;
- diffusione della normativa interna a tutta la struttura della Società attraverso gli appositi strumenti aziendali.

Specifici ruoli e responsabilità nella gestione del Modello sono infine attribuiti alle unità/strutture della Corporation di seguito indicate:

Funzione Governance, Risk and Compliance

Alla Funzione Governance, Risk and Compliance di Oracle Italia compete garantire, nel tempo, la presenza di regole, procedure e prassi operative che prevengano efficacemente violazioni o infrazioni alle norme vigenti nonché delle politiche aziendali.

Con specifico riferimento ai rischi della responsabilità amministrativa introdotta dal Decreto, la Funzione Governance, Risk and Compliance supporta l'Organismo di Vigilanza nello svolgimento delle sue attività di controllo:

- effettuando verifiche sul rispetto delle procedure;
- collaborando all'aggiornamento e alla diffusione del Modello;
- effettuando attività di audit su aree sensibili (business, sicurezza sul lavoro);
- collaborando all'aggiornamento di procedure aziendali; collaborando al monitoraggio sulla coerenza organizzativa;

Funzione Internal Audit di Corporation

La funzione Internal Audit della Corporation assicura in generale una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali.

La funzione Internal Audit della Corporation si coordina con l'Organismo di Vigilanza nel vigilare sul rispetto e sull'adeguatezza delle regole contenute nel Modello, attivando, a fronte delle eventuali criticità riscontrate nel corso della propria attività, le funzioni di volta in volta competenti per le opportune azioni di mitigazione.

3.6 La struttura e l'organizzazione del Modello (Parte Generale e Protocolli)

Il Modello si compone di:

- Parte Generale (il presente documento) - illustra la funzione e i principi del Modello, individua e disciplina le sue componenti essenziali ovvero l'Organismo di Vigilanza, il Sistema Sanzionatorio, nonché la diffusione, l'applicazione e l'adeguatezza del Modello.
- Protocolli a disciplina delle Attività Sensibili, in cui sono contenuti i presidi di controllo attuati dalla Società con riferimento ai processi e alle attività identificate come a rischio di commissione dei reati previsti dal Decreto. I Protocolli sono i seguenti:

01_Rapporti con la PA;
02_Flussi Finanziari;
03_Approvigionamenti;
04_Risorse Umane;
05_Marketing;
06_Actività Commerciale;
07_Contentenzioso;
08_Bilancio e Fiscalità;
09_Rapporti Infragruppo;
10_Sistemi informativi;
11_Salute e Sicurezza;
12_Ambiente.

Le finalità dei **Protocolli** sono di:

- richiamare le Attività Sensibili rilevanti, ovvero l'insieme delle attività e operazioni aziendali organizzate al fine di perseguire un determinato scopo o gestire un determinato ambito aziendale della Società in aree potenzialmente a rischio di commissione reato;
- specificare le componenti che caratterizzano il sistema di controllo preventivo, nonché i principi generali e specifici di comportamento e le regole specifiche di condotta riconducibili alle Attività Sensibili;
- fornire all'Organismo di Vigilanza gli strumenti necessari per esercitare le attività di monitoraggio e di verifica della corretta applicazione del Modello in tutte le sue parti.

L'ambito di applicazione di ogni singolo Protocollo con riferimento alle Attività Sensibili e alle categorie di reato applicabili è riportato nell'**Allegato B**, recante "Tabella Attività Sensibili/Reati/Protocolli".

4. LE COMPONENTI DEL SISTEMA DI CONTROLLO INTERNO

Il Modello predisposto da Oracle Italia si fonda e si integra con un sistema di controllo interno strutturato ed organico composto da protocolli e regole, strumenti di definizione delle responsabilità, nonché da meccanismi e strumenti di monitoraggio dei processi aziendali, preesistente rispetto all'emanazione del Modello.

In particolare, tale sistema trae origine e si integra con un più ampio sistema di controllo di derivazione corporate, esteso e comune a tutte le Società del

Gruppo (ivi inclusa Oracle Italia) e finalizzato a garantire la compliance a diverse normative anticorruzione e antifrode (tra le altre Foreign Corrupt Practices Act del 1977, Sarbanes-Oxley Act del 2002 e United Kingdom Bribery Act del 2010). Di conseguenza, i principi di controllo che ispirano l'architettura del sistema di controllo interno di Oracle Italia e le componenti del sistema stesso, rilevanti ai fini del presente Modello e di seguito descritti, caratterizzano in modo coerente i sistemi di controllo interno attuati dalle altre Società del Gruppo, siano esse direttamente coinvolte nei processi di business siano esse riconducibili ai c.d. Shared Service Center e/o Centri d'eccellenza.

I principi di controllo che ispirano l'architettura del sistema di controllo interno di Oracle Italia, con particolare riferimento alle Attività Sensibili delineati dal Modello e coerentemente con le previsioni di Confindustria, sono di seguito rappresentati:

- **Chiara identificazione di ruoli, compiti e responsabilità** dei soggetti che partecipano alla realizzazione delle attività aziendali (interni o esterni all'organizzazione);
- **Segregazione dei compiti** tra chi esegue operativamente un'attività, chi la controlla, chi la autorizza e chi la registra (ove applicabile);
- **Verificabilità e documentabilità delle operazioni ex-post:** le attività rilevanti condotte (soprattutto nell'ambito delle Attività Sensibili) devono trovare adeguata formalizzazione, con particolare riferimento alla documentazione predisposta nell'ambito della realizzazione delle stesse. La documentazione prodotta e/o disponibile su supporto cartaceo od elettronico, deve essere archiviata in maniera ordinata e sistematica a cura delle funzioni/soggetti coinvolti.
- **Identificazione di controlli preventivi e verifiche ex-post, manuali e automatici:** devono essere previsti dei presidi manuali e/o automatici idonei a prevenire la commissione dei Reati o a rilevare ex-post delle irregolarità che potrebbero contrastare con le finalità del presente Modello. Tali controlli sono più frequenti, articolati e sofisticati nell'ambito di quelle Attività Sensibili caratterizzate da un profilo di rischio di commissione dei Reati più elevato. In tale logica un ambito che deve essere fortemente presidiato è la gestione delle risorse finanziarie. Tra queste tipologie di controllo si richiamano a titolo esemplificativo le seguenti:
 - Protezione dei sistemi automatici (accesso, back-up dei dati etc.);
 - Riconciliazioni/quadrature dati;
 - Monitoraggio/verifica ex-post delle attività più significative/dei dati più sensibili;
 - Reportistica sulle attività svolte e invio al livello gerarchicamente superiore.

Ai fini del presente Modello rilevano in particolare le seguenti **componenti del sistema di controllo interno** come di seguito classificate:

- sistema di principi etici e regole di comportamento;
- sistema organizzativo;

- sistema autorizzativo e decisionale;
- sistema di policy e procedure;
- programma di formazione e informazione;
- sistema disciplinare;
- sistemi informativi e applicativi informatici.

Tali componenti del sistema di controllo (e gli strumenti organizzativi ed operativi in cui si traducono), coerentemente con i principi di controllo ispiratori sopra delineati, sono stati in particolare valutati in occasione delle attività di risk assessment condotte (come anticipato nel Capitolo dedicato alla “Metodologia”) al fine di verificarne la coerenza rispetto alle finalità di prevenzione delle condotte illecite di cui al Decreto.

In tale sede è emerso che alcuni strumenti risultavano già esistenti ed operanti precedentemente all’adozione del presente Modello e sono stati ritenuti validi e immediatamente applicabili anche ai presenti fini.

Alcuni di essi non sono stati valutati idonei o sufficientemente articolati per soddisfare le finalità del presente Modello e, al fine di rispondere in modo più adeguato ai requisiti del D. Lgs. 231/01, sono stati identificati i relativi ambiti di miglioramento. Gli interventi correttivi sono stati esplicitati nell’ambito di un “Action Plan” (di cui al Capitolo 2).

Al fine di completare gli strumenti necessari alla costituzione di un Modello adeguato alla prevenzione dei Reati, sono stati inoltre individuati componenti del sistema, non presenti, da implementare ex-novo, tramite l’attuazione di un relativo intervento correttivo, anch’esso previsto dall’Action Plan (di cui al Capitolo 2).

Si precisa inoltre che le suddette componenti del sistema di controllo interno, anche qualora formalizzate in documentazione distinta rispetto al presente Modello, sono richiamate nel testo del Modello e/o contenute nei relativi Allegati e ne sono, quindi, da considerarsi parte integrante. Ne consegue dunque che il rispetto dei principi e delle prescrizioni in esse contenuti è quindi da considerarsi aspetto imprescindibile per l’attuazione e l’efficacia del presente Modello stesso.

Nei Paragrafi seguenti vengono descritte e dettagliate le singole componenti che costituiscono il sistema di controllo interno di Oracle rilevanti anche ai fini del Modello.

4.1 Sistema di principi etici e regole di comportamento

La Società ritiene indispensabile che i Destinatari rispettino principi etici e regole generali di comportamento nello svolgimento delle proprie attività e nella gestione dei rapporti con colleghi, business partner, outsourcer e parti terze, clienti, fornitori e con la Pubblica Amministrazione.

Tali norme sono formulate in un articolato set di documenti aziendali quali in primis:

- Codice di Comportamento di Oracle Italia S.r.l. (previsto espressamente in Allegato anche al presente Modello);
- Policy di Gruppo.

In particolare le Policy di Gruppo sono riferite a documenti applicabili a tutte le Società del Gruppo, ivi inclusa Oracle Italia S.r.l., che disciplinano le attività di business e sanciscono le regole di comportamento che i dipendenti di Oracle devono osservare nello svolgimento delle proprie attività.

Con riferimento alla disciplina del comportamento di soggetti terzi alla Società ma con i quali la stessa collabora in modo continuativo, sono stati redatti degli appositi documenti di regolamentazione e nello specifico:

- per disciplinare i rapporti con i fornitori è stato formalizzato un apposito documento comportamentale denominato “Supplier Code of Ethics and Business Conduct”,
- con riferimento invece alla disciplina del comportamento dei partner commerciali è stato inoltre formalizzato un apposito documento comportamentale denominato “Partner Code of Conduct and Business Ethics”.

La Società garantisce l'attività di aggiornamento e diffusione dei documenti di cui sopra, individuando le funzioni a ciò preposte ed i canali più opportuni (pubblicazione sul portale internet o comunicazioni via posta elettronica).

I principi e le regole di comportamento formalizzati nei documenti sopra richiamati si integrano con quanto nello specifico è stato formalizzato nel presente Modello, con particolare riferimento alla prevenzione dei Reati come previsto nei Protocolli sviluppati (si rimanda a tale proposito alle relative sezioni “*Principi di comportamento e regole di condotta*”).

4.2 Sistema organizzativo

Il sistema organizzativo di Oracle viene definito attraverso la predisposizione di un organigramma aziendale e l’emanazione di deleghe di funzioni e disposizioni organizzative che forniscono una chiara definizione delle funzioni e delle responsabilità attribuite a ciascuna unità organizzativa locale.

L’organigramma aziendale rappresenta la struttura organizzativa dell’azienda, attraverso l’identificazione e denominazione delle divisioni e funzioni in cui si articola sia con riferimento alla realtà di Oracle Italia sia con riferimento alle linee di riporto funzionali che collegano quest’ultima alla Capogruppo.

La formalizzazione, aggiornamento e diffusione dell’organigramma viene assicurata dalla Funzione Human Resources.

L’assetto organizzativo del Gruppo Oracle prevede inoltre l’esistenza di strutture condivise a livello europeo, dislocate all’esterno del territorio italiano, denominate Shared Service Center e/o Centri d’eccellenza i principali dei quali vengono di seguito riportati:

- **Centro di eccellenza Irlanda:** il centro ha sede a Dublino e svolge principalmente attività di contabilità generale e taxation a supporto delle Country afferenti all’area geografica EMEA;
- **Shared Service Center Romania:** il centro si occupa di gestire le attività di recupero crediti per conto di Oracle Italia e per le altre Legal Entities afferenti all’area geografica EMEA. Gestisce inoltre il calcolo di premi e incentivi ai venditori, controlla e effettua i pagamenti delle note spese di tutti i dipendenti e, supporta i Sales Representative delle varie LOBs

nella predisposizione dei contratti standard di licenza/consulenza ed i rinnovi di supporto. Gestisce inoltre le adesioni ed i rinnovi alla rete di partnership di Oracle.

- **Shared Service Center India:** il centro è situato a Bangalore e, con riferimento all'area geografica EMEA, svolge le attività di account payable, account receivable, cash management, emissione Ordini di Acquisto e order management in generale (sulla base delle richieste effettuate dalle funzioni richiedenti di ciascuna legal entity), apertura e modifica dell'anagrafica dei clienti/fornitori. Il centro si occupa inoltre di svolgere alcune attività di controllo di gestione e analisi degli scostamenti e di generare report standard per il management della legal entity richiedente.

La formalizzazione di job description e deleghe interne trova manifestazione all'interno delle Policy di Gruppo e le Procedure redatte a livello locale che prevedono esplicitamente dei paragrafi dedicati alla rappresentazione delle responsabilità dei soggetti organizzativi coinvolti nel corso dei diversi processi.

Le Policy di Gruppo e le Procedure, rappresentative di ruoli e responsabilità dei soggetti coinvolti nei diversi processi, vengono diffuse attraverso pubblicazione su intranet aziendale.

Nel caso di documentazione di prima redazione e di recente approvazione, la Funzione Legal della Corporation effettua degli invii massivi di mail per comunicare l'entrata in vigore dei diversi documenti.

Al momento dell'assunzione sono inoltre previste delle sessioni di "induction" al fine di trasmettere le regole di comportamento di carattere sia generale che specifico cui tutti i dipendenti Oracle Italia devono attenersi nello svolgimento dell'attività lavorativa. Tali regole di comportamento sono inoltre formalizzate nell'ambito del "Employee Handbook".

La Società assegna la responsabilità di aggiornare tempestivamente l'organigramma ed altre disposizioni relative alla struttura organizzativa alla funzione Human Resources. Tale Funzione collabora con l'Ufficio Legale per l'assegnazione delle deleghe interne in coerenza con la struttura organizzativa delineata. La Società inoltre provvede ad un'adeguata ed efficace diffusione dei suddetti documenti ai Destinatari.

Ad integrazione della diffusione dei suddetti documenti sono inoltre previsti dei programmi di training on-line realizzati ad hoc per tutti i dipendenti della Società.

4.3 Sistema autorizzativo e decisionale

Il sistema autorizzativo e decisionale si traduce in un sistema articolato e coerente di deleghe di poteri e procure della Società fondato sulle seguenti prescrizioni:

- le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire e descrivere in modo specifico e non equivoco i poteri gestionali del delegato ed il soggetto cui il delegato riporta gerarchicamente e funzionalmente;

- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli;
- le procure possono essere conferite esclusivamente a soggetti dotati di delega di poteri o di specifico incarico e devono prevedere l'estensione dei poteri di rappresentanza ed, eventualmente, i limiti di spesa numerici;
- i destinatari di poteri e deleghe nonché le persone direttamente coinvolte/interessate devono essere adeguatamente informate e istruite circa l'estensione e i limiti dei singoli poteri conferiti;
- in particolare tutti coloro che intrattengono per conto di Oracle Italia rapporti con la Pubblica Amministrazione, devono essere dotati di delega/procura in tal senso;
- i destinatari di poteri e deleghe possono esercitare i poteri di firma e di rappresentanza solo una volta completato l'iter di approvazioni e autorizzazioni interne previste per ciascuna attività.

L'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo. Con riferimento a tale aspetto, nell'ipotesi in cui il legale rappresentante sia indagato per un reato-presupposto dell'illecito amministrativo ascritto a carico dell'ente, e si trovi quindi in una situazione di conflitto con gli interessi dell'ente stesso, la nomina del difensore dell'ente deve avvenire per il tramite di un soggetto specificamente delegato a tale attività per i casi di eventuale conflitto con le indagini penali a carico del rappresentante legale (in questo senso, v. Cass. Pen., Sez. III, 13 maggio 2022, n. 35387).

Il processo decisionale afferente alle Attività Sensibili deve ispirarsi ai seguenti criteri:

- ogni decisione riguardante le operazioni nell'ambito delle Attività Sensibili, come di seguito individuati, deve avere una formale evidenza (cartacea o elettronica);
- non potrà comunque mai esservi identità soggettiva tra colui che decide in merito allo svolgimento di un'Attività Sensibile e colui che effettivamente la pone in essere portandola a compimento;
- del pari, non potrà comunque mai esservi identità soggettiva tra coloro che decidono e pongono in essere un'Operazione Sensibile e coloro che risultano investiti del potere di destinarvi le eventuali risorse economiche e finanziarie.

I principi sopra descritti trovano applicazione e formalizzazione nei seguenti documenti:

- delibere del Consiglio di Amministrazione;
- deleghe del Consiglio di Amministrazione, procure speciali e relativa lettera di conferimento;
- "Document Signing Authority Policy Oracle Corporation" e "Signing Authority Matrix" di Oracle Italia, che definiscono le regole per l'esercizio del potere di firma e di rappresentanza con particolare riferimento alla formalizzazione di transazioni/accordi e quindi alla stipula di contratti in nome e per conto di Oracle Italia;

- “Spending Approval Policy” che individua i soggetti organizzativi designati ad autorizzare internamente delle spese e i relativi limiti;
- “Approval Matrix” che individua i soggetti organizzativi designati ad autorizzare internamente le varie attività aziendali;

4.4 Sistema di policy e procedure

Il set procedurale di cui Oracle si è dotata è riconducibile a tre tipologie e livelli di documenti:

- policy/procedure emesse dalla Corporation che sono da ritenersi valide a livello locale;
- procedure locali emesse in recepimento delle policy/procedure della Corporation;
- procedure redatte a livello locale a disciplina di specifiche esigenze (ad esempio, procedure Qualità).

I principali ambiti regolati dal set procedurale sopra descritto sono i seguenti:

- rapporti con esponenti della Pubblica Amministrazione;
- gestione delle visite ispettive;
- attività di partecipazione a gare ad evidenza pubblica o attraverso trattative private;
- attività di tenuta contabile e redazione del Bilancio d'Esercizio;
- attività di approvvigionamento e gestione del ciclo passivo;
- attività di vendita e di gestione del ciclo attivo;
- gestione dei rapporti con i Partner.

Tali documenti consentono in particolare di disciplinare più nel dettaglio le attività oggetto delle Attività Sensibili e di guidare e garantire dunque l'implementazione e l'attuazione nella pratica dei principi di comportamento e di controllo stabiliti nel presente Modello.

A tale scopo, le procedure aziendali relative alle Attività Sensibili garantiscono in particolare l'applicazione dei seguenti principi:

- aderenza con eventuali policy di emanazione della capogruppo che disciplinino gli stessi ambiti di attività del documento aziendale in oggetto;
- chiara formalizzazione di ruoli, compiti e modalità e tempistiche di realizzazione delle attività operative e di controllo disciplinate;
- rappresentazione e disciplina della separazione dei compiti tra il soggetto che assume la decisione (impulso decisionale), il soggetto che ne autorizza la realizzazione, il soggetto che esegue le attività ed il soggetto a cui è affidato il controllo;
- tracciabilità e formalizzazione di ciascuna attività rilevante del processo oggetto della procedura al fine della ripercorribilità a posteriori di quanto realizzato e dell'evidenza dei principi e delle attività di controllo applicate;
- adeguato livello di archiviazione della documentazione rilevante.

Si precisa inoltre che la strutturazione di tale sistema procedurale, ai fini del presente Modello, è in particolare guidata da quanto rilevato in occasione delle attività di risk assessment condotte e formalizzato nell'Action Plan di cui al Capitolo 2.

4.5 Programma di formazione e informazione

Con specifico riferimento alle attività realizzate nell'ambito delle Attività Sensibili, viene previsto e garantito un adeguato programma di informazione e formazione periodico e sistematico rivolto ai Dipendenti e collaboratori coinvolti nelle stesse.

In particolare, per i nuovi assunti è previsto un training obbligatorio di "induction" definito a cura della Funzione Human Resources.

La Società prevede inoltre, per tutte le risorse, un training via web su tematiche specifiche aventi ad oggetto, ad esempio, il Codice di Comportamento, le modalità di utilizzo delle policy/procedure e la compliance normativa (ad esempio FCPA, Sox, salute e sicurezza sul luogo di lavoro, etc.). Tali attività integrano e completano il percorso di informazione e formazione sul tema specifico delle attività poste in essere dalla Società in tema di adeguamento al D. Lgs. 231/2001 previsto e disciplinato specificamente nei Capitoli a ciò dedicati della Parte Generale del Modello.

4.6 Sistema disciplinare

L'esistenza di un sistema di sanzioni applicabili in caso di mancato rispetto delle regole di condotta aziendali e, nello specifico, delle prescrizioni e delle procedure interne previste dal Modello è una componente indispensabile per garantire l'effettività del Modello stesso. In merito a tale aspetto si rimanda a quanto ampiamente descritto di seguito nell'ambito del Capitolo 8 del presente documento. Più in generale il sistema di governance e di regole di compliance definite a livello di Gruppo, che trovano formale manifestazione all'interno di specifiche Policy e Procedure di Gruppo e al cui rispetto sono chiamate tutte le Società appartenenti al Gruppo stesso (ivi inclusa Oracle Italia), prevedono, tra gli altri elementi, un sistema articolato di meccanismi sanzionatori in caso di mancato rispetto delle regole specifiche di condotta e comportamento in esse contenute.

4.7 Sistemi informativi e applicativi informatici

Per la salvaguardia del patrimonio documentale ed informativo aziendale devono essere previste adeguate misure di sicurezza a presidio del rischio di perdita e/o alterazione della documentazione riferita alle Attività Sensibili o di accessi indesiderati ai dati/documenti.

Al fine di presidiare l'integrità dei dati e l'efficacia dei sistemi informativi e/o gli applicativi informatici utilizzati per lo svolgimento di attività operative o di controllo nell'ambito delle Attività Sensibili, o a supporto delle stesse, è garantita la presenza e l'operatività di:

- sistemi di profilazione delle utenze in relazione all'accesso a moduli o ambienti;
- regole per il corretto utilizzo dei sistemi ed ausili informativi aziendali (supporti hardware e software);
- meccanismi automatizzati di controllo accessi ai sistemi;
- meccanismi automatizzati di blocco o inibizione all'accesso.

5. ORGANISMO DI VIGILANZA

L'art. 6 comma 1, lett. b) del Decreto prevede, tra i presupposti indispensabili per l'esonero della responsabilità conseguente alla commissione dei reati da questo indicati, l'istituzione di un Organismo *interno* all'Ente denominato *Organismo di vigilanza* (di seguito "*l'Organismo*" o "*OdV*") dotato di autonomi poteri di iniziativa e controllo con il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

5.1 Requisiti dell'Organismo di Vigilanza

Al fine di soddisfare le funzioni stabilite dal Decreto l'Organismo deve soddisfare i seguenti requisiti:

- **autonomia ed indipendenza:** come anche precisato dalle Linee Guida, la posizione dell'Organismo nell'Ente "*deve garantire l'autonomia dell'iniziativa di controllo da ogni forma di interferenza e/o condizionamento da parte di qualunque componente dell'Ente*" (ivi compreso l'organo dirigente). L'Organismo deve pertanto essere inserito come unità di staff in una posizione gerarchica (la più elevata possibile) con la previsione di un riporto al massimo Vertice operativo aziendale. Non solo, al fine di garantirne la necessaria autonomia di iniziativa ed indipendenza, "*è indispensabile che all'OdV non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni ed attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello*".
- **professionalità:** tale requisito si riferisce alle competenze tecniche specialistiche di cui deve essere dotato l'Organismo per poter svolgere l'attività che la norma gli attribuisce. In particolare, i componenti dell'Organismo devono avere conoscenze specifiche in relazione a qualsiasi tecnica utile per compiere l'attività ispettiva, consulenziale di analisi del sistema di controllo e di tipo giuridico, (in particolare nel settore penalistico e societario), come chiaramente specificato nelle Linee Guida. E', infatti, essenziale la conoscenza delle tecniche di analisi e valutazione dei rischi, del flow-charting di procedure e processi, delle metodologie per l'individuazione di frodi, del campionamento statistico e della struttura e delle modalità realizzative dei reati.
- **continuità di azione:** per garantire l'efficace attuazione del Modello organizzativo, è necessaria la presenza di una struttura dedicata esclusivamente e a tempo pieno all'attività di vigilanza.

Pertanto, l'ODV deve:

- essere indipendente ed in posizione di terzietà rispetto a coloro sui quali dovrà effettuare la vigilanza;
- essere collocato in una posizione gerarchica la più elevata possibile;
- essere dotato di autonomi poteri di iniziativa e di controllo;
- essere dotato di autonomia finanziaria;
- essere privo di compiti operativi;
- avere continuità d'azione;
- avere requisiti di professionalità;
- realizzare un sistematico canale di comunicazione con il CdA nel suo

insieme.

5.2 Identificazione dell'Organismo di Vigilanza

Il Consiglio di Amministrazione di Oracle Italia S.r.l. ha ritenuto opportuno costituire un organo monocratico cui attribuire il ruolo di Organismo di Vigilanza (di seguito anche solo OdV).

In particolare, tale organo è composto da:

- un professionista esterno, esperto in materia di D.lgs. 231/2001.

Le riflessioni formulate alla luce della tipologia e delle peculiarità della Società portano a ritenere che la composizione ottimale dell'OdV sia quella monocratica.

Per una piena aderenza ai dettami del Decreto, l'OdV come sopra identificato è un soggetto che riporta direttamente ai vertici della Società (Consiglio di Amministrazione) e non è legato alle strutture operative da alcun vincolo gerarchico, in modo da garantire la sua piena autonomia ed indipendenza nell'espletamento delle funzioni.

Le attività poste in essere dall'OdV non possono essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che il Consiglio di Amministrazione è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto responsabile ultimo del funzionamento e dell'efficacia del Modello.

A ulteriore garanzia di autonomia e in coerenza con quanto previsto dalle Linee Guida di Confindustria, nel contesto delle procedure di formazione del budget aziendale, il Consiglio di Amministrazione dovrà approvare una dotazione di risorse finanziarie, proposta dall'OdV, della quale l'OdV stesso potrà disporre per ogni esigenza necessaria a garantire un corretto svolgimento dei propri compiti (es. consulenze specialistiche, trasferte, etc.).

Il componente dell'OdV possiede le capacità, conoscenze e competenze professionali nonché i requisiti di onorabilità indispensabili allo svolgimento dei compiti ad essi attribuiti. Infatti l'OdV della Società, così composto, è dotato di idonee capacità ispettive e consulenziali, con particolare riferimento, tra l'altro, alle tecniche di audit, di rilevazione delle frodi, di analisi e rilevazione dei rischi.

Inoltre, l'OdV potrà avvalersi nell'espletamento dei propri compiti del supporto costante di Funzioni della Società specificatamente dedicate al controllo interno per l'individuazione costante dei rischi e delle frodi, al fine di assicurare un'efficace applicazione delle regole del Modello, quali la Funzione Governance Risk & Compliance, la Funzione Legal e la Funzione Human Resources (cfr. anche Par. 3.5 della Parte Generale).

In particolare, l'impegno sistematico e dedicato della Funzione Governance Risk & Compliance, priva di mansioni operative, alla vigilanza sul Modello, garantisce la continuità d'azione dell'OdV, mentre la Funzione Legal garantisce le competenze necessarie per l'interpretazione della normativa e della giurisprudenza rilevante ai fini dell'attuazione del Modello, nonché per l'analisi delle fattispecie di reato rilevanti e la valutazione delle condotte in

violazione del Modello.

L'attribuzione del ruolo di OdV ad un soggetto diversi da quello qui identificato o la modifica della composizione o delle funzioni assegnate all'OdV deve essere deliberata dal Consiglio di Amministrazione.

5.3 Modalità di nomina dell'OdV e durata in carica

L'OdV è nominato dal Consiglio d'Amministrazione con decisione presa all'unanimità dei suoi componenti.

Il perfezionamento della nomina del membro dell'OdV si determina con la dichiarazione di accettazione della carica resa dal componente stesso e verbalizzata dal Consiglio di Amministrazione. Alternativamente è possibile perfezionare la nomina a membro dell'OdV attraverso la sottoscrizione, da parte del componente stesso:

- della copia dell'estratto della delibera di nomina effettuata dal Consiglio di Amministrazione;
- del verbale della prima riunione dell'OdV successiva a detta nomina contenente dichiarazione espressa di accettazione della carica, purché in detto verbale la delibera del Consiglio di Amministrazione sia espressamente richiamata o allegata. Successivamente l'OdV trasmetterà il suddetto verbale della prima riunione o un suo estratto alla Società.

Il Consiglio d'Amministrazione provvede, prima di ogni nuova nomina, a verificare la sussistenza dei requisiti espressamente richiesti dal Decreto per il membro dell'OdV, nonché degli altri requisiti citati nel presente Capitolo.

Il Consiglio di Amministrazione valuta periodicamente l'adeguatezza dell'OdV in termini di struttura organizzativa e di poteri conferiti.

La retribuzione annuale del componente dell'OdV sarà determinata dal Consiglio di Amministrazione e rimarrà invariata per l'intero periodo di durata dell'incarico.

La durata dell'incarico sarà di tre anni ed è ammesso il rinnovo dell'incarico alla scadenza.

È facoltà del componente dell'Organismo di Vigilanza rinunciare in qualsiasi momento all'incarico. In tal caso, egli dovrà darne comunicazione al Consiglio di Amministrazione per iscritto motivando le ragioni che hanno determinato la rinuncia.

La cessazione del componente dell'Organismo di Vigilanza per scadenza del termine ha effetto dal momento in cui l'Organismo di Vigilanza è stato ricostituito con la dichiarazione di accettazione della delibera di nomina dell'Organo Dirigente resa nei modi sopradescritti.

5.4 Cause di ineleggibilità, motivi e poteri di revoca

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza dei requisiti soggettivi di onorabilità, integrità, rispettabilità e professionalità, nonché all'assenza delle seguenti cause di ineleggibilità con la nomina stessa:

- esistenza di relazioni di parentela, coniugio o affinità entro il quarto grado

con il Presidente del Consiglio di Amministrazione e con gli Amministratori Delegati della Società, con soggetti apicali in genere e con revisori incaricati dalla società di revisione;

- sussistenza di conflitti di interesse, anche potenziali, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'Organismo di Vigilanza;
- prestazione di fideiussione o di altra garanzia in favore di uno degli amministratori (o del coniuge), ovvero avere con questi ultimi rapporti - estranei all'incarico conferito - di credito o debito;
- titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza sulla Società;
- esercizio di funzioni di amministratore - nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza - di imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali;
- presenza di sentenza di condanna anche non passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento), in Italia o all'estero, per i delitti richiamati dal Decreto;
- esistenza di condanna, con sentenza anche non passata in giudicato, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
- esistenza di condanna, con sentenza passata in giudicato, ovvero sentenza di applicazione della pena su richiesta (il c.d. patteggiamento) in Italia o all'estero, per reati diversi da quelli richiamati nel decreto, che incidono sulla onorabilità e moralità professionale;
- rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale membro dell'OdV.

Il membro dell'OdV, con l'accettazione della nomina, riconosce implicitamente l'insussistenza di detti motivi di ineleggibilità.

Le regole sopra descritte si applicano anche in caso di nomina di un componente dell'Organismo di Vigilanza in sostituzione di altro membro dell'organismo stesso.

La revoca dei poteri propri del componente dell'Organismo di Vigilanza e l'attribuzione di tali poteri ad altro soggetto, potrà avvenire soltanto per giusta causa, anche legata ad interventi di ristrutturazione organizzativa della Società, mediante un'apposita delibera del Consiglio di Amministrazione presa all'unanimità dei suoi componenti.

A tale proposito, per "giusta causa" di revoca dei poteri connessi con l'incarico di membro dell'Organismo di Vigilanza potrà intendersi, a titolo esemplificativo e non tassativo:

- la perdita dei requisiti soggettivi di onorabilità, integrità, rispettabilità e professionalità presenti in sede di nomina;
- il sopraggiungere di un motivo di ineleggibilità;
- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione della relazione informativa annuale sull'attività svolta al Consiglio di Amministrazione ed al Collegio Sindacale, l'omessa redazione del piano delle attività;

- una sentenza di condanna della Società, anche non passata in giudicato, ovvero un procedimento penale concluso tramite “patteggiamento”, ove risulti dagli atti “l’omessa o insufficiente vigilanza” da parte dell’Organismo di Vigilanza - secondo quanto previsto dall’art. 6, comma 1, lett. d), del Decreto;
- l’attribuzione di funzioni e responsabilità operative all’interno dell’organizzazione aziendale incompatibili con i requisiti di “autonomia e indipendenza” e “continuità di azione” propri dell’Organismo di Vigilanza;
- la mendace dichiarazione circa l’insussistenza dei motivi di ineleggibilità sopra descritti;
- 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, o un’infermità che, comunque, comporti l’assenza dal luogo di lavoro per un periodo superiore a sei mesi.

Nei casi sopra descritti, il Consiglio di Amministrazione provvederà a nominare il nuovo componente dell’Organismo di Vigilanza in sostituzione di quello cui sia stato revocato il mandato.

In casi di particolare gravità e urgenza, il Consiglio di Amministrazione potrà comunque disporre la sospensione dei poteri dell’Organismo di Vigilanza e la nomina di un Organismo *ad interim* prima di provvedere alla revoca dell’OdV.

5.5 Funzioni dell’OdV

L’OdV è completamente autonomo nell’esplicazione dei suoi compiti e le sue determinazioni sono insindacabili. In particolare, l’OdV deve:

- vigilare sull’osservanza del Modello da parte dei Destinatari;
- vigilare sull’efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- proporre e sollecitare l’aggiornamento del Modello laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali, normative o di contesto esterno.

L’OdV, in particolare, deve operare:

- ex-ante (adoperandosi ad esempio per la formazione ed informazione del personale);
- continuativamente (attraverso l’attività di monitoraggio, di vigilanza, di revisione e di aggiornamento);
- ex-post (analizzando cause, circostanze che abbiano portato alla violazione delle prescrizioni del Modello o alla commissione del reato).

Per un efficace svolgimento delle predette funzioni, all’OdV sono affidati i seguenti compiti e poteri:

- vigilare sull’osservanza del Modello stesso nonché raccogliere, elaborare e conservare ogni informazione rilevante ai fini della verifica dell’osservanza del Modello;
- verificare periodicamente l’effettiva applicazione della normativa interna (procedure aziendali di controllo) nelle aree di attività a rischio e sulla loro efficacia;
- effettuare periodicamente verifiche su operazioni o atti specifici posti in essere nell’ambito delle Attività Sensibili;

- vigilare sulla efficacia nel tempo del Modello, con particolare riferimento ai comportamenti riscontrati nell'ambito aziendale;
- proporre al Consiglio di Amministrazione l'aggiornamento del Modello nell'ipotesi in cui si renda necessario e/o opportuno effettuare correzioni e adeguamenti dello stesso, a seguito delle mutate condizioni aziendali e/o legislative;
- verificare periodicamente la mappa delle aree a rischio al fine di garantire l'adeguamento ai mutamenti dell'attività e/o della struttura aziendale;
- segnalare tempestivamente alla funzione aziendale competente ad irrogare le sanzioni disciplinari, o all'Amministratore Delegato, qualsiasi violazione del Modello ritenuta significativa di cui sia venuto a conoscenza nell'ambito dello svolgimento delle proprie attività di vigilanza.
- verificare l'adozione degli interventi a soluzione delle criticità in termini di sistemi di controllo interno rilevate in sede di risk assessment (Action Plan) di cui ai Paragrafi 2.1;
- monitorare l'adeguatezza del sistema disciplinare previsto per i casi di violazione delle regole definite dal Modello;
- coordinarsi con le altre funzioni aziendali, nonché con gli altri organi di controllo (*in primis* la società di revisione e il Collegio Sindacale), anche attraverso apposite riunioni, per il migliore monitoraggio delle attività in relazione alle procedure stabilite dal Modello, o per l'individuazione di nuove aree a rischio, nonché, in generale, per la valutazione dei diversi aspetti attinenti all'attuazione del Modello;
- coordinarsi e cooperare con i soggetti responsabili della tutela della sicurezza e salute dei lavoratori al fine di garantire che il sistema di controllo ai sensi del Decreto sia integrato con il sistema di controllo predisposto in conformità alle normative speciali per la sicurezza sui luoghi di lavoro;
- coordinarsi con i responsabili delle funzioni aziendali al fine di promuovere iniziative per la diffusione della conoscenza (anche in riferimento nello specifico all'organizzazione di corsi di formazione) e della comprensione dei principi del Modello e per assicurare la predisposizione della documentazione organizzativa interna necessaria al funzionamento dello stesso, contenente istruzioni, chiarimenti o aggiornamenti;
- effettuare verifiche periodiche sul contenuto e sulla qualità dei programmi di formazione.

A tal fine l'OdV avrà facoltà di:

- emanare disposizioni ed ordini di servizio intesi a regolare l'attività dell'OdV stesso;
- accedere a qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'OdV ai sensi del Decreto;
- impartire direttive generali e specifiche alle diverse strutture aziendali, anche di vertice, al fine di ottenere da queste ultime le informazioni ritenute necessarie per l'assolvimento dei propri compiti;
- effettuare verifiche periodiche sulla base di un proprio piano di attività o anche interventi spot non programmati in detto piano, ma, comunque,

- ritenuti necessari all'espletamento dei propri compiti;
- sollecitare le strutture preposte per l'applicazione dei provvedimenti disciplinari in caso di violazioni accertate del Modello e dei suoi elementi costitutivi;
 - ricorrere comunque, nello svolgimento dei compiti che gli competono, al supporto di collaboratori esterni all'Organismo, sia identificabili in soggetti appartenenti a qualsiasi funzione aziendale della Società che di volta in volta si rendesse utile coinvolgere per il perseguimento dei fini specificati sia anche in consulenti terzi rispetto alla Società.

I collaboratori dell'OdV, su indicazione dell'OdV stesso, possono, anche individualmente, procedere alle attività di vigilanza ritenute opportune per il funzionamento e l'osservanza del Modello.

I soggetti appartenenti ad una funzione aziendale, nell'espletamento dell'incarico ad essi conferito, in qualità di collaboratori dell'OdV, sono esonerati dallo svolgimento delle loro funzioni operative aziendali e rispondono, gerarchicamente e funzionalmente, esclusivamente all'OdV.

Inoltre, l'OdV dovrà espressamente prevedere dei momenti formalizzati di incontro e confronto, in particolare con:

- il Collegio Sindacale;
- gli attori rilevanti in materia di sistema di controllo interno;
- gli attori rilevanti in materia di sistema di gestione della sicurezza e salute sul luogo di lavoro e in materia di sicurezza informatica;
- la società di revisione contabile.

Obiettivo di detti incontri sarà principalmente il confronto ed il coordinamento con i soggetti coinvolti in c.d. prima linea nell'implementazione del sistema di controllo, ciascuno secondo l'area di propria pertinenza, al fine di consentire all'OdV di cogliere opportunità di miglioramento dei presidi in essere ai fini dell'efficacia del Modello. In tale ottica sarà cura dell'OdV verificare con gli stessi l'efficacia dei flussi informativi nei suoi confronti, così come definiti al Paragrafo 5.6 "Obblighi di informazione verso l'Organismo di Vigilanza".

L'OdV provvederà a disciplinare le modalità operative e la periodicità di organizzazione di detti incontri, individuando i soggetti di volta in volta coinvolti, nonché l'ordine del giorno degli stessi.

L'OdV, inoltre, provvederà a dotarsi di un Piano delle Attività che intende svolgere per adempiere i compiti assegnatigli, da comunicare al Consiglio di Amministrazione.

5.6 Obblighi di informazione verso l'OdV

Al fine di agevolare l'attività di vigilanza sull'effettività e sull'efficacia del Modello, l'OdV è destinatario di informazioni utili e necessarie allo svolgimento dei compiti di vigilanza affidati all'OdV stesso (di seguito classificate in **Informazioni Generali** e **Informazioni Sensibili**).

Deve essere permesso all'OdV di accedere ad ogni tipo di informazione utile al fine dello svolgimento della sua attività. Ne deriva di converso l'obbligo per l'OdV di mantenere segrete tutte le informazioni acquisite.

In ogni caso al fine di agevolare le attività di vigilanza che gli competono, l'OdV deve ottenere tempestivamente le Informazioni Generali ritenute utili a tale

scopo, tra cui, a titolo esemplificativo, ancorché non esaustivo:

- le criticità, anomalie o atipicità riscontrate dalle funzioni aziendali nell'attuazione del Modello;
- 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;
- le comunicazioni interne ed esterne riguardanti qualsiasi fattispecie che possa essere messa in collegamento con ipotesi di reato di cui al Decreto (es. provvedimenti disciplinari avviati/attuati nei confronti di dipendenti);
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario per i Reati;
- le commissioni di inchiesta o le relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al Decreto;
- le notizie relative ai procedimenti disciplinari svolti con riferimento a violazioni del Modello e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le notizie relative a cambiamenti dell'assetto organizzativo;
- gli aggiornamenti del sistema delle deleghe e delle procure (ivi incluso il sistema poteri e deleghe in materia di sicurezza e salute sul lavoro);
- le notizie relative a cambiamenti organizzativi dei ruoli chiave in materia di sicurezza e salute sul luogo di lavoro (es: cambiamenti in merito a ruoli, compiti e soggetti delegati alla tutela dei lavoratori);
- modifiche al sistema normativo in materia di sicurezza e salute sul luogo di lavoro;
- le eventuali comunicazioni della società di revisione riguardanti aspetti che possono indicare carenze nel sistema dei controlli interni, fatti censurabili, osservazioni sul bilancio della Società;
- qualsiasi incarico conferito o che si intende conferire alla società di revisione o a società ad esse collegate, diverso da quello concernente la revisione del bilancio o il controllo contabile;
- copia dei verbali delle adunanze del Consiglio di Amministrazione e del Collegio Sindacale.

Tali Informazioni Generali devono essere fornite all'OdV a cura dei responsabili delle funzioni aziendali secondo la propria area di competenza, fermo restando l'obbligo di ciascun Destinatario di informare immediatamente l'OdV circa eventuali procedimenti penali che lo riguardi direttamente (in qualità di indagato o imputato).

Le Informazioni Generali, salvo quanto specificato di seguito con riferimento alle Informazioni riguardanti le Operazioni Sensibili a cura dei Process Owner, dovranno essere effettuate in forma scritta, utilizzando una casella di e-mail appositamente attivata (odv231_it@oracle.com). Al fine di agevolare l'accesso da parte dell'OdV al maggior numero possibile di informazioni, la Società garantisce la tutela di qualunque segnalante contro ogni forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Inoltre, al fine di consentire il monitoraggio da parte dell'OdV delle attività di

particolare rilevanza svolte nell'ambito delle Attività Sensibili l'Amministratore Delegato o i responsabili di LOB/funzione vengono qualificati come Process Owner e sono tenuti a trasmettere all'OdV le Informazioni su operazioni/attività realizzate nell'ambito delle Attività Sensibili. Tali soggetti sono stati qualificati come Process Owner nell'ambito delle attività di risk assessment condotte e formalizzati nella Matrice Attività Sensibili/Reati/Funzioni di cui all'Allegato B.

Data la natura trasversale delle aree rilevanti in tema di reati in materia di sicurezza e salute sul lavoro, assumono altresì il ruolo di Process Owner, in quanto Destinatari del Modello ai sensi del Paragrafo 3.2, le seguenti figure organizzative, come definite dall'art. 2, D.Lgs. 9 aprile 2008, n. 81:

- il Datore di lavoro;
- il Delegato del Datore di lavoro
- i Dirigenti;
- il Responsabile del Servizio di Prevenzione e Protezione;
- il Medico competente.

L'identificazione delle Informazioni rilevanti relative alle ad operazioni/attività svolte nell'ambito delle Attività Sensibili avviene attraverso la delineazione di criteri di valutazione e parametri definiti con il supporto dell'OdV, in ragione dell'attività di risk assessment condotta, e valutandone l'efficacia ai fini dello svolgimento dei propri compiti, nonché la costante coerenza con l'evoluzione di volumi e delle attività.

L'OdV procederà ad informare opportunamente il CdA circa l'identificazione di detti criteri e parametri. In particolare, i contenuti informativi riguardanti le operazioni/attività relative a ciascuna Attività Sensibile, nonché, in generale, la disciplina dei flussi informativi nei confronti dell'OdV in termini di frequenza, modalità di trasmissione e responsabilità per la trasmissione di suddetti flussi saranno regolamentati in dettaglio in un'apposita Procedura definita dal Responsabile della Funzione Governance, Risk & Compliance (Ufficio Legale) con il supporto dell'OdV stesso. Sarà cura inoltre dell'OdV accertare che tale Procedura sia efficacemente diffusa da parte della Funzione competente secondo le modalità previste dalla Procedura stessa.

Infine, l'OdV dovrà ricevere dal Gestore delle Segnalazioni, come identificato al successivo paragrafo 6.2, tempestivi flussi informativi in merito:

- alla ricezione di Segnalazioni relative a violazioni riconducibili a condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o a violazioni del Modello;
- al progressivo sviluppo del seguito dato a tali Segnalazioni;
- all'esito delle indagini e valutazioni effettuate rispetto alle Segnalazioni rivelatesi fondate;
- alla tipologia e l'oggetto di tutte le Segnalazioni ricevute, anche se non riconducibili a condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o violazioni del Modello, e all'esito delle relative indagini.
- alla tipologia e l'oggetto di tutte le Segnalazioni ricevute, anche se non riconducibili a condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o violazioni del Modello, e all'esito delle relative indagini (il tutto nel rispetto dei principi di riservatezza dell'identità delle persone segnalanti e della esclusiva legittimazione del Gestore delle Segnalazioni a trattare i dati).

5.7 Reporting dell'OdV

L'OdV riferisce in merito all'attuazione del Modello e alle eventuali criticità, direttamente al Consiglio di Amministrazione e al Collegio Sindacale.

L'OdV, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale, ha la responsabilità di:

- comunicare, all'inizio di ciascun esercizio, il Piano delle Attività, che intende svolgere per adempiere ai compiti assegnatigli;
- comunicare periodicamente, con cadenza almeno annuale, lo stato di avanzamento del Piano delle Attività, ed eventuali cambiamenti apportati allo stesso, motivandoli;
- segnalare tempestivamente qualsiasi violazione del Modello oppure condotte illegittime e/o illecite, di cui sia venuto a conoscenza nell'ambito delle proprie attività istituzionali di vigilanza;
- redigere, almeno ogni dodici mesi, una relazione riepilogativa delle attività svolte nei precedenti dodici mesi e dei risultati delle stesse, degli elementi di criticità e delle violazioni del Modello, nonché delle proposte relative ai necessari aggiornamenti del Modello da porre in essere.

Il Consiglio di Amministrazione e il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'OdV, il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti e di particolare gravità.

L'OdV potrà, inoltre, comunicare i risultati dei propri accertamenti ai responsabili delle LOB/funzioni qualora dalle verifiche svolte scaturiscano carenze, comportamenti o azioni non in linea con il Modello. In tal caso, sarà necessario che l'OdV ottenga dai responsabili dei processi medesimi un piano delle azioni da intraprendere, con relativa tempistica, al fine di impedire il ripetersi di tali circostanze.

L'OdV ha l'obbligo di informare immediatamente il Collegio Sindacale, nonché il Consiglio di Amministrazione, qualora la violazione riguardi i vertici dell'Azienda.

5.8 Conservazione delle informazioni

Tutte le Informazioni, rapporti e altri documenti raccolti e/o predisposti in applicazione del presente Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo), gestito dall'OdV, per un periodo di 6 anni.

L'accesso all'archivio è consentito esclusivamente ai membri dell'OdV e al Consiglio di Amministrazione.

Si precisa inoltre che anche la documentazione prodotta nell'ambito delle attività di predisposizione e aggiornamento del Modello (risk assessment, etc.) e raccolta in uno specifico Archivio (di cui al Capitolo 2), è custodita a cura dell'OdV.

6. SEGNALAZIONI DI ILLECITI O DI VIOLAZIONI DEL MODELLO

6.1 Principi generali

La Società è consapevole del fatto che, al fine di incoraggiare le segnalazioni di illeciti o di violazioni del Modello, è necessario creare un sistema *ad hoc* di gestione delle stesse, che tuteli attraverso idonee misure tecniche e organizzative la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione e che sia affidato a un soggetto autonomo e specificamente formato.

La Società si è quindi dotata, in conformità con la normativa applicabile¹, di specifici canali di segnalazione, definendo altresì, in una apposita Procedura denominata "Il sistema di segnalazioni - Whistleblowing" (di seguito «Procedura Whistleblowing»), da intendersi integralmente richiamata nel Modello e che ne costituisce parte integrante, le modalità operative e le responsabilità per il ricevimento, la valutazione, la gestione e la chiusura delle segnalazioni.

6.2 Sistema di segnalazione

Ai sensi dell'art. 6, comma 2-bis D.Lgs. 231/2001, come modificato dal D.Lgs 24/2023, la Società ha istituito i canali di segnalazione interna (di seguito i «**Canali**») di cui all'art. 4 del suddetto decreto (di seguito il «**Decreto Whistleblowing**»), affidandone la gestione ad un apposito comitato nominato ai sensi del predetto art. 4, comma 2 (di seguito il «**Gestore delle Segnalazioni**»).

Il Gestore delle Segnalazioni è formato dal Responsabile della Funzione Governance Risk & Compliance EMEA e dal Responsabile della Funzione Governance Risk & Compliance di Oracle Italia S.r.l. quali soggetti espressamente autorizzati a trattare i dati di cui al presente processo ai sensi dell'art. 29 e 32 del GDPR e dell'art. 2-quaterdecies del Codice Privacy.

In particolare, i Canali consentono, alle persone espressamente indicate dal Decreto Whistleblowing e dalla Procedura Whistleblowing (a titolo esemplificativo: dipendenti, collaboratori, azionisti, consulenti ecc., di seguito i «**Segnalanti**»), di presentare, a tutela dell'integrità della Società, segnalazioni relative a condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 o a violazioni del Modello, nonché relative alle violazioni del diritto dell'Unione europea e della normativa nazionale di recepimento richiamate dal Decreto Whistleblowing², tutte apprese nell'ambito del proprio contesto lavorativo (di seguito le «**Segnalazioni**»):

- **in forma scritta** - tramite una apposita piattaforma denominata EthicsPoint (di seguito "EthicsPoint" o anche "Piattaforma WB"), fornita dalla società Navex Global contrattualizzata da Oracle Inc. e nominata responsabile ex art. 28 GDPR, accessibile tramite il seguente link presente nel sito di Oracle Italia S.r.l.,

¹ Il riferimento è al D.Lgs. 24/2023, recante "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali"

² Il riferimento è all'art. 2, comma 1, lett. a), nn. 3), 4), 5) e 6) D.Lgs. 24/2023.

[\(<https://secure.ethicspoint.com/domain/media/en/gui/31053/index.html>\)](https://secure.ethicspoint.com/domain/media/en/gui/31053/index.html)

oppure all'interno della intranet aziendale (sezione "Global Legal, Compliance and Ethics >" Oracle's Integrity Helpline).³;

- in forma scritta tramite corrispondenza indirizzata al Gestore delle Segnalazioni da inviare presso la sede di Oracle Italia S.r.l.;
- in forma orale, contattando il numero telefonico: EU Helpline: (800-786-907) oppure mediante richiesta di un incontro diretto con il Gestore delle Segnalazioni, veicolata tramite uno dei canali citati in precedenza.

Tutte le informazioni relative alla identificazione dei Segnalanti e delle violazioni segnalabili, ai Canali ed alle modalità per accedervi, ai presupposti per effettuare le Segnalazioni interne ed esterne, all'iter di gestione delle Segnalazioni, sono specificate nella Procedura Whistleblowing, pubblicata nel sito Internet della Società nonché affissa presso le sedi aziendali e comunque accessibili ai possibili Segnalanti.

6.3 Divieto di ritorsioni

Inoltre, la Società, nel garantire ai Segnalanti il diritto di effettuare le Segnalazioni - peraltro alle sole condizioni previste nel Decreto Whistleblowing e nella Procedura Whistleblowing - vieta rigorosamente qualsiasi ritorsione nei confronti dei Segnalanti stessi.

Per ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione di una Segnalazione (o una denuncia all'Autorità giudiziaria o divulgazione pubblica), che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto.

A titolo esemplificativo si fa riferimento alle fattispecie dell'art. 17, co. 4, del Decreto ed alle specificazioni della Procedura Whistleblowing.

Tale tutela si applica anche:

- ai soggetti che assistono i Segnalanti nel processo di segnalazione ("facilitatori");
- alle persone del medesimo contesto lavorativo del Segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del Segnalante, che lavorano nel medesimo contesto lavorativo dello stesso e che hanno con il Segnalante un rapporto abituale e corrente;
- agli enti di proprietà del Segnalante o per i quali lo stesso lavora nonché agli enti che operano nel medesimo contesto lavorativo del Segnalante.

7. DIFFUSIONE DEL MODELLO

Ai fini dell'efficacia e comprensione del Modello, è di primaria importanza la piena conoscenza delle regole di condotta e delle componenti del sistema di controllo preventivo che vi sono contenute sia da parte delle risorse già presenti nell'azienda, che di quelle che ne entreranno a fare parte in futuro, con differente grado di approfondimento a seconda del diverso grado di coinvolgimento nelle Attività Sensibili.

³ In conformità agli artt. 4, co. 1, e 12 del D.Lgs. 24/2023 e delle corrispondenti prescrizioni delle Linee Guida ANAC (Delibera n. 311 del 12 luglio 2023).

7.1 Attività informativa

Per garantire un'effettiva conoscenza ed applicazione, l'adozione del Modello viene comunicata formalmente dal Consiglio di Amministrazione alle diverse categorie di Destinatari.

In particolare, successivamente all'approvazione del Modello, i dipendenti della Società ed in seguito tutti i nuovi assunti, sono tenuti a sottoscrivere, una dichiarazione di presa visione del Modello stesso e di impegno ad osservarne le prescrizioni.

Per quanto attiene invece i Fornitori, nonché i Consulenti esterni, i Partner gli Appaltatori, la lettera di incarico od il contratto che comporti la costituzione di una forma di collaborazione con essi deve esplicitamente contenere clausole (ad es. clausole risolutive espresse) che facciano esplicito riferimento al rispetto delle prescrizioni del Modello e/o del Codice di Comportamento.

I lavoratori interinali/somministrati, i collaboratori a progetto e gli stagiaires saranno altresì tenuti a sottoscrivere, una dichiarazione di presa visione del Modello e del Codice di Comportamento e di impegno ad osservarne le prescrizioni.

In caso di revisioni e/o aggiornamenti significativi del Modello la Società provvederà a darne debita comunicazione ai Destinatari.

Il Modello è inoltre reso disponibile secondo le modalità e gli strumenti che il Consiglio di Amministrazione riterrà opportuno adottare, quale, a titolo esemplificativo la diffusione su sito internet della Società.

7.2 Formazione del personale

La formazione del personale ai fini dell'attuazione del Modello è di competenza del Consiglio di Amministrazione che individua le risorse interne od esterne alla Società cui affidarne l'organizzazione.

In particolare, l'Organismo di Vigilanza è responsabile della gestione della formazione del personale, come anticipato al precedente Paragrafo 3.5, ed ha la facoltà di avvalersi del supporto della Funzione Human Resources e della funzione Oracle University.

Le risorse afferenti alle suddette funzioni procedono in coordinamento con l'OdV, che valuta l'efficacia dell'azione formativa in termini di pianificazione, contenuti, aggiornamento, tempistiche, modalità e identificazione dei partecipanti.

La partecipazione alle suddette attività formative da parte dei soggetti individuati deve essere ritenuta obbligatoria: conseguentemente, la mancata partecipazione sarà sanzionata ai sensi del Sistema Disciplinare contenuto nel Modello.

La formazione deve fornire informazioni almeno in riferimento:

- al quadro normativo di riferimento (D. Lgs. 231/2001 e Linee Guida di Confindustria);
- al Modello adottato dalla Società;
- al Codice di Comportamento della Società;
- a casi aziendali di applicazione della normativa;

- alla struttura del sistema di controllo interno, presidi e controlli introdotti.

La formazione dovrà essere differenziata in relazione alle diverse aree aziendali di appartenenza dei destinatari della formazione stessa.

Viene innanzitutto prevista una formazione d'aula iniziale rivolta alle persone in organico presso la Società al momento dell'adozione del Modello che risultino operare nelle Attività Sensibili come sopra definiti. Per la restante parte del personale, e nei casi di nuovi ingressi in organico successivi all'adozione del Modello, è prevista un'apposita edizione del corso (anche eventualmente con modalità on-line).

Della formazione effettuata dovrà essere tenuta puntuale registrazione.

Infine, la pianificazione della formazione deve prevedere delle sessioni periodiche che garantiscano un costante programma di aggiornamento.

8. SISTEMA DISCIPLINARE

Il Decreto prevede che sia predisposto un "*sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*" sia per i soggetti in posizione apicale sia per i soggetti sottoposti ad altrui direzione e vigilanza.

L'esistenza di un sistema di sanzioni applicabili in caso di mancato rispetto delle regole di condotta, delle prescrizioni e delle procedure interne previste dal Modello è, infatti, indispensabile per garantire l'effettività del Modello stesso.

L'applicazione delle sanzioni in questione deve restare del tutto indipendente dallo svolgimento e dall'esito di eventuali procedimenti penali o amministrativi avviati dall'Autorità Giudiziaria o Amministrativa, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto ovvero una fattispecie penale o amministrativa rilevante ai sensi della normativa in materia di tutela della salute e della sicurezza sui luoghi di lavoro. Infatti, le regole imposte dal Modello sono assunte dalla Società in piena autonomia, indipendentemente dal fatto che eventuali condotte possano costituire illecito penale o amministrativo e che l'Autorità Giudiziaria o Amministrativa intenda perseguire tale illecito.

La verifica dell'adeguatezza del sistema disciplinare, il costante monitoraggio degli eventuali procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'OdV, il quale procede anche alla segnalazione delle infrazioni di cui venisse a conoscenza nello svolgimento delle funzioni che gli sono proprie.

Fatto salvo quanto previsto dal Paragrafo 5.4 ("Cause di ineleggibilità, motivi e poteri di revoca"), il sistema disciplinare definito potrà essere applicato anche ai componenti dell'OdV, relativamente alle funzioni ad essi attribuite dal presente Modello (si veda sul punto il successivo Paragrafo).

8.1 Violazioni del Modello

Costituiscono violazioni del Modello:

1. comportamenti che integrino le fattispecie di reato contemplate nel Decreto;
2. comportamenti che, sebbene non configurino una delle fattispecie di reato contemplate nel Decreto, siano diretti in modo univoco alla loro commissione;
3. comportamenti non conformi alle procedure richiamate nel Modello;
4. comportamenti non conformi al Codice di Comportamento, al Codice di Etica e Condotta Aziendale e all'Employee Handbook;
5. comportamenti non conformi alle disposizioni previste nel Modello o richiamate dal Modello e, in particolare, non conformi ai presidi di controllo nella Parte Speciale e alle Procedure richiamate dal Modello stesso,
6. comportamento non collaborativo nei confronti dell'OdV, consistente, a titolo esemplificativo e non esaustivo, nel rifiuto di fornire le informazioni o la documentazione richiesta, nel mancato rispetto delle direttive generali e specifiche rivolte dall'OdV al fine di ottenere le informazioni ritenute necessarie per l'assolvimento dei propri compiti, nella mancata partecipazione senza giustificato motivo alle visite ispettive programmate dall'OdV, nella mancata partecipazione agli incontri di formazione.
7. violazione degli obblighi di informazione verso l'OdV indicati nel precedente paragrafo 5.6;
8. le violazioni inerenti al sistema di segnalazione di cui al precedente paragrafo 6.2 "Sistema di Segnalazione"; con riferimento a tali violazioni e correlate sanzioni, si rimanda al successivo par. 8.6 "Sistema disciplinare per le violazioni del sistema di segnalazione.

8.2 Misure nei confronti dei dipendenti

La violazione delle singole regole comportamentali previste dal presente Modello da parte dei dipendenti della Società (quadri, impiegati, operai), costituisce illecito disciplinare ai sensi del vigente Contratto Collettivo Nazionale del Lavoro (CCNL) di riferimento, ossia il "Contratto Collettivo Nazionale di Lavoro per i dipendenti dalle industrie metalmeccaniche private e della installazione di impianti" nella versione attualmente vigente.

Qualsiasi tipo di violazione delle regole comportamentali contenute nel Modello autorizza comunque l'OdV a richiedere alla funzione aziendale competente l'avvio del procedimento di contestazione disciplinare e l'eventuale irrogazione di una delle sanzioni di seguito elencate, determinata sulla base della gravità della violazione commessa alla luce dei criteri indicati nel Paragrafo 8.1 e del comportamento tenuto prima (e.g. eventuali precedenti violazioni commesse) e dopo il fatto (e.g. comunicazione all'OdV dell'avvenuta irregolarità) dall'autore della violazione.

I provvedimenti disciplinari irrogabili nei riguardi di detti lavoratori nel rispetto delle procedure previste dall'articolo 7 commi 2 e 3 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e secondo quanto disposto dal "Contratto Collettivo Nazionale di Lavoro per i dipendenti dalle industrie metalmeccaniche private e della installazione di impianti" nonché delle altre

disposizioni di legge applicabili, sono quelli previsti dal seguente apparato sanzionatorio:

- a) richiamo verbale;
- b) ammonizione scritta;
- c) multa fino a tre ore di retribuzione oraria calcolata sul minimo tabellare;
- d) sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
- e) licenziamento per mancanze ai sensi dell'art.10 del CCNL - Sezione IV – titolo VII.

Ai fini della graduazione interna delle sanzioni della multa non superiore a 3 ore della retribuzione oraria e della sospensione fino a un massimo di 3 giorni, si terrà conto della **gravità delle violazioni, la quale sarà valutata sulla base dei seguenti criteri:**

- la presenza e l'intensità dell'elemento intenzionale;
- la presenza e intensità della condotta negligente, imprudente, imperita;
- la presenza e intensità della condotta recidiva;
- l'entità del pericolo e/o delle conseguenze della violazione per le persone destinatarie della normativa in materia di tutela della salute e della sicurezza sui luoghi di lavoro, nonché per la Società;
- la prevedibilità delle conseguenze;
- i tempi e i modi della violazione;
- le circostanze nelle quali la violazione ha avuto luogo.

Le sanzioni sopra descritte saranno applicate dal dirigente responsabile della struttura al quale il dipendente è assegnato nel momento in cui si verifica l'infrazione, di concerto con il Responsabile della Funzione Human Resources, previa consultazione con l'Organismo di Vigilanza; nel caso di applicazione delle sanzioni di cui ai punti d) ed e) che precedono ne viene data tempestiva comunicazione all'Amministratore Delegato.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate la funzione aziendale competente terrà sempre informato l'OdV.

In particolare, con riferimento alle violazioni del Modello realizzate dal dipendente che riveste la qualifica di quadro, impiegato o operaio, si prevede che:

1. incorre nei provvedimenti di **richiamo verbale o ammonizione scritta** secondo la gravità della violazione, il dipendente che violi le procedure interne previste dal presente Modello o adottati, nell'espletamento di attività nelle aree a rischio, un comportamento in violazione delle prescrizioni del Modello stesso, purché tale condotta non determini l'applicazione di misure previste dal Decreto;
2. incorre nel provvedimento della **multa** il lavoratore che violi più volte le procedure interne previste dal Modello o adottati più volte, nell'espletamento di attività delle aree a rischio, un comportamento in violazione alle prescrizioni del Modello stesso, purché tale condotta non determini l'applicazione di misure previste dal Decreto;
3. incorre nel provvedimento di **sospensione dal servizio e dalla**

retribuzione fino ad un massimo di tre giorni il dipendente che nel violare le procedure interne previste dal Modello o adottando nell'espletamento di attività nelle aree a rischio un comportamento in violazione delle prescrizioni dello stesso, arrechi danno alla Società o la esponga a una situazione oggettiva di pericolo alla integrità dei beni della stessa, purché tali condotte non siano comunque dirette in modo univoco alla commissione del Reato o non determinino l'applicazione di misure previste dal Decreto;

4. incorre nel provvedimento di **licenziamento per mancanze** il dipendente che adotti un comportamento non conforme alle prescrizioni del presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, nonché il dipendente che adotti un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto.
In ogni caso, con riferimento al rischio di commissione dei reati in violazione della normativa in materia di salute e sicurezza sul lavoro previsti dall'art. 25 septies del Decreto, in ossequio anche a quanto stabilito dalla Circolare del Ministero del Lavoro del 11 Luglio 2011 n. 15816 avente ad oggetto "Modelli di organizzazione e gestione ex art. 30 D.Lgs. 81/2008", si indicano di seguito le possibili violazioni, graduate in ordine crescente di gravità:
5. incorre nel provvedimento dell'**ammonizione scritta** il dipendente che non rispetta il Modello, nel caso in cui la violazione comporti il determinarsi di una situazione di eventuale pericolo per l'integrità fisica di una o più persone, compreso l'autore della violazione, e sempre che non sia integrata una delle ipotesi previste nei successivi punti 6, 7 e 8;
6. incorre nel provvedimento della **multa** il dipendente che non rispetta il Modello, nel caso in cui la violazione comporti il determinarsi di una situazione di eventuale pericolo per l'integrità fisica di una o più persone, compreso l'autore della violazione (con riferimento a un comportamento di recidiva che abbia già causato l'irrogazione di ammonizioni scritte), oppure una lesione all'integrità fisica di uno o più soggetti, compreso l'autore della violazione, e sempre che non sia integrata una delle ipotesi previste nei successivi punti 7 e 8;
7. incorre nel provvedimento della **sospensione dal lavoro e dalla retribuzione fino a un massimo di tre giorni** il dipendente che non rispetta il Modello, nel caso in cui la violazione cagioni una lesione all'integrità fisica di uno o più soggetti, compreso l'autore dell'infrazione, e sempre che non sia integrata una delle ipotesi previste nel successivo punto 8;
8. incorre nel provvedimento del **licenziamento per mancanze** il lavoratore che adotti un comportamento in violazione alle prescrizioni del presente Modello tale da esporre la Società al rischio concreto ed immediato di applicazione di misure previste dal Decreto (trattasi, a mero titolo esemplificativo, della condotta negligente, imprudente od imperita suscettibile di provocare un infortunio a se stesso ovvero ad altre persone).

Per i dipendenti di altre Società del Gruppo distaccati presso Oracle Italia S.r.l., gli opportuni provvedimenti saranno valutati e adottati dalla società di

provenienza, nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori), previa circostanziata comunicazione da parte delle funzioni aziendali competenti di Oracle Italia S.r.l.

Le accertate violazioni delle disposizioni del Modello e del Codice di Comportamento, così come l'inerzia da parte della società distaccante costituiranno cause di incompatibilità con la prosecuzione del distacco e Oracle Italia S.r.l. potrà comunicare alla società distaccante la cessazione immediata del distacco medesimo.

Infine, con riferimento alle violazioni inerenti al sistema di segnalazione di cui al precedente paragrafo 6.2 "Segnalazioni di illeciti o di violazioni del Modello", si rimanda al successivo par. 8.6 "Sistema disciplinare per le violazioni del sistema di segnalazione".

8.3 Misure nei confronti dei dirigenti

Per quanto attiene alle violazioni delle singole regole di cui al presente Modello poste in essere da lavoratori della Società aventi qualifica di 'dirigente', anche queste costituiscono illecito disciplinare.

Qualsiasi tipo di violazione delle regole comportamentali contenute nel Modello autorizza comunque l'OdV a richiedere alla funzione aziendale competente l'irrogazione di una delle sanzioni di seguito elencate, determinata sulla base della gravità della violazione commessa alla luce dei criteri indicati nel Paragrafo 8.2 e del comportamento tenuto prima (ad esempio le eventuali precedenti violazioni commesse) e dopo il fatto (ad esempio la comunicazione all'OdV dell'avvenuta irregolarità) dall'autore della violazione.

I provvedimenti disciplinari irrogabili nei riguardi dei 'dirigenti' - nel rispetto delle procedure previste dall'articolo 7 commi 2 e 3 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e del Contratto Collettivo Nazionale di Lavoro per i dirigenti di aziende industriali, sono quelli previsti dal seguente apparato sanzionatorio:

- a) censura scritta;
- b) sospensione disciplinare;
- c) licenziamento per giustificato motivo;
- d) licenziamento per giusta causa.

Le sanzioni della "censura scritta" e della "sospensione disciplinare" sono applicate dal responsabile della struttura al quale il dirigente è assegnato nel momento in cui si verifica l'infrazione, di concerto con il responsabile della Funzione Human Resources previa consultazione con l'Organismo di Vigilanza; dell'applicazione di tali sanzioni ne viene data tempestiva comunicazione all'Amministratore Delegato.

Le sanzioni del "licenziamento per giustificato motivo" e il "licenziamento per giusta causa" sono applicate dall'Amministratore Delegato, previa consultazione con l'Organismo di Vigilanza.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate, la funzione aziendale competente terrà sempre informato l'OdV.

In particolare, con riferimento alle violazioni del Modello poste in essere dai dirigenti della Società, si prevede che:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nella **censura scritta** consistente nel richiamo all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di violazione non grave, ma reiterata, di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel provvedimento della **sospensione disciplinare**;
- in caso di grave violazione di una o più regole procedurali o comportamentali previste nel Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del **licenziamento per giustificato motivo**;
- laddove la violazione di una o più regole procedurali o comportamentali previste nel Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il dirigente incorre nel provvedimento del **licenziamento per giusta causa**.

Inoltre, per i lavoratori della Società aventi qualifica di 'dirigente' costituisce grave violazione delle prescrizioni del Modello:

- l'inosservanza dell'obbligo di direzione o vigilanza sui lavoratori subordinati circa la corretta ed effettiva applicazione del Modello stesso.
- l'inosservanza dell'obbligo di direzione e vigilanza sugli altri lavoratori che, sebbene non legati alla Società da un vincolo di subordinazione (trattasi, ad esempio, di lavoratori autonomi, consulenti, collaboratori coordinati e continuativi etc.), sono comunque soggetti alla direzione e vigilanza del 'Dirigente' ai sensi dell'art. 5 comma 1 lett. b) del D.lgs. 231/01.

Infine, con riferimento alle violazioni inerenti al sistema di segnalazione di cui al precedente paragrafo 6.2 "Segnalazioni di illeciti o di violazioni del Modello", si rimanda al successivo par. 8.6 "Sistema disciplinare per le violazioni del sistema di segnalazione".

8.4 Misure nei confronti dei membri del Consiglio di Amministrazione, del Collegio Sindacale, dei membri dell'OdV

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione della Società, l'OdV informerà l'intero Consiglio di Amministrazione e il Collegio Sindacale che prenderanno gli opportuni provvedimenti coerentemente con la gravità della violazione commessa, alla luce dei criteri indicati nel Paragrafo 8.2 e conformemente ai poteri previsti dalla legge e/o dallo Statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, etc.).

I provvedimenti irrogabili nei riguardi di uno o più membri del Consiglio di Amministrazione, previa delibera del Consiglio di Amministrazione da adottare con l'astensione dell'interessato e, ove previsto dalla legge e dallo Statuto, con delibera dell'Assemblea dei soci sono quelli previsti dal seguente apparato sanzionatorio:

- a. richiamo scritto;
- b. sospensione temporanea dalla carica;
- c. revoca dalla carica.

In particolare, con riferimento alle violazioni del Modello poste in essere da uno o più membri del Consiglio di Amministrazione, si prevede che:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il membro del Consiglio di Amministrazione incorre nel **richiamo scritto** consistente nel richiamo all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave violazione di una o più regole procedurali o comportamentali previste nel Modello, il membro del Consiglio di Amministrazione incorre nel provvedimento della **sospensione temporanea dalla carica**;
- in caso di grave violazione di una o più regole procedurali o comportamentali previste nel Modello tale da ledere irreparabilmente il rapporto di fiducia, il membro del Consiglio di Amministrazione incorre nella **revoca dalla carica**.

In caso di violazione del Modello da parte dell'intero Consiglio di Amministrazione della Società, l'OdV informerà il Collegio Sindacale affinché questo convochi senza indugio l'Assemblea dei Soci per gli opportuni provvedimenti.

In caso di violazione del Modello da parte di uno o più membri del Collegio Sindacale della Società, l'OdV informerà il Consiglio di Amministrazione il quale prenderà gli opportuni provvedimenti coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto (dichiarazioni nei verbali delle adunanze, richiesta di convocazione o convocazione dell'Assemblea con all'ordine del giorno adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, etc.).

Qualora il Consiglio di Amministrazione fosse informato in merito a violazioni del Modello da parte dell'OdV, il Consiglio di Amministrazione provvederà ad assumere le iniziative ritenute più idonee coerentemente con la gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto.

In particolare, qualora la violazione sia commessa da un componente dell'OdV che sia anche un dipendente ovvero un dirigente della Società, si applicheranno rispettivamente le sanzioni di cui ai Paragrafi 8.2 e 8.3.

In ogni caso, delle sanzioni irrogate e/o delle violazioni accertate il Consiglio di Amministrazione ed il Collegio Sindacale terranno sempre informato l'OdV.

Infine, con riferimento alle violazioni inerenti al sistema di segnalazione di cui al precedente paragrafo 6.2 “Segnalazioni di illeciti o di violazioni del Modello”, si rimanda al successivo par. 8.6 “Sistema disciplinare per le violazioni del sistema di segnalazione”.

8.5 Misure nei confronti dei collaboratori coinvolti nelle Attività Sensibili, dei Consulenti esterni, dei Fornitori, dei Partner, degli Appaltatori

Ogni violazione posta in essere dai collaboratori coinvolti nelle Attività Sensibili, dai Consulenti, dai Fornitori, dai Partner, dagli Appaltatori potrà determinare, secondo quanto previsto dalle specifiche clausole inserite nel contratto che disciplina i rapporti con la Società, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento, qualora da tale comportamento derivino danni a Oracle come nel caso di applicazione da parte del Giudice delle misure previste dal Decreto.

8.6 Sistema disciplinare per le violazioni del sistema di segnalazione

La Società adotta il presente Sistema Disciplinare per le violazioni del sistema di segnalazione, ai sensi dell'art. 6, co. 2, D.lgs. 231/2001 e dell'art. 21, co. 2, del Decreto Whistleblowing, prevedendo sanzioni disciplinari per le seguenti categorie di infrazioni sanzionabili:

- (I) Commissione di Ritorsioni;
- (II) Ostacolo alla presentazione di Segnalazioni;
- (III) Violazione dell'obbligo di riservatezza dell'identità dei Segnalanti, dei Segnalati, delle persone comunque menzionate nella Segnalazione e dei Facilitatori, nonché del contenuto delle Segnalazioni e della relativa documentazione;
- (IV) Mancato svolgimento dell'attività di verifica e analisi delle Segnalazioni ricevute;
- (V) Segnalazioni, denunce, divulgazioni infondate delle quali sia accertata l'effettuazione con dolo e colpa grave;
- (VI) adozione di procedure non conformi a quelle di cui agli articoli 4 e 5 del Decreto Whistleblowing.

A tali categorie di infrazioni disciplinari saranno applicabili le sanzioni specificate nei paragrafi precedenti, in funzione della natura del rapporto con la Società e secondo un criterio generale di corrispondenza progressiva tra categoria di infrazioni e genere di sanzione.

Nell'ambito di tale criterio sistematico generale, la sanzione applicata in concreto dovrà tenere in specifica considerazione, caso per caso aggravante o attenuante secondo il principio di proporzionalità, la gravità della fattispecie oggettiva; il tipo e l'intensità dell'elemento soggettivo (dolo o colpa, grave, media o lieve); la circostanza che l'infrazione sia rimasta tentata od invece effettivamente compiuta; le conseguenze dannose eventualmente provocate, l'eventuale ravvedimento operoso; il ricorso di precedenti riconducibili alle suddette categorie disciplinari, anche laddove non integrante gli estremi della recidiva; il grado di diligenza e fiducia esigibili in ragione delle mansioni e/o della qualifica professionale e/o del ruolo aziendale dell'autore; ed ogni altra circostanza concreta altrimenti rilevante ai fini della graduazione della sanzione tra quelle astrattamente applicabili.

In ogni caso le sanzioni disciplinari saranno applicate indipendentemente:

- dalla determinazione o meno di danni come conseguenza della realizzazione delle corrispondenti infrazioni disciplinari;
- dalla mancata applicazione, da parte dell'ANAC, delle sanzioni amministrative pecuniarie previste per le stesse ipotesi dall'art. 21, co. 1, del Decreto Whistleblowing.

Per contro, salvo il rilievo di altre particolarità del caso concreto, saranno considerate una notevole aggravante:

- la circostanza che l'infrazione abbia determinato l'applicazione alla Società di una sanzione amministrativa pecuniaria ai sensi dell'art. 21, co. 1, del Decreto Whistleblowing;
- La commissione dell'infrazione da parte del Gestore delle Segnalazioni;
- il fatto che la violazione della riservatezza abbia determinato provvedimenti sanzionatori da parte dell'Autorità Garante per la protezione dei dati personali.

Infine, nei casi di segnalazioni, denunce o divulgazioni infondate delle quali sia accertata l'effettuazione con dolo o colpa grave, la determinazione di un danno per la Società sarà considerata massima aggravante. In tali casi, inoltre, la Società si riserva di richiedere al responsabile il conseguente risarcimento.

Le sanzioni disciplinari saranno applicate nel rispetto dell'art. 7 della L. 20 maggio 1970, n. 300 e delle disposizioni in materia del CCNL applicato, all'esito del procedimento di contestazione e ricezione delle giustificazioni, laddove queste ultime non risultassero fondate o sufficienti ai fini esimenti.

Laddove i responsabili delle infrazioni suddette fossero lavoratori distaccati o somministrati, l'esercizio del potere disciplinare nei loro confronti avverrà nelle forme e con la distribuzione di competenze datoriali proprie del corrispondente rapporto di lavoro.

9. INTRODUZIONE ALLA PARTE SPECIALE

Come già evidenziato al capitolo "Struttura del Modello" ai sensi di quanto disposto dall'art. 6, comma 1, lett. a) del Decreto, la Società ha proceduto all'identificazione delle Attività Sensibili (control and risk self assessment).

La Società ha conseguentemente identificato e effettivamente implementato nel sistema di controllo adeguati presidi al fine di rendere lo stesso idoneo a diminuire il rischio di commissione dei reati. Tali presidi sono riportati nei Protocolli che costituiscono la Parte Speciale del Modello.

Nei Protocolli sono riportati:

- le Attività Sensibili con riferimento a ciascuna delle categorie di reato identificate come rilevanti per la Società;
- per ogni Attività Sensibile, i presidi di controllo in essere, finalizzati o comunque idonei a diminuire il rischio di commissione dei reati-presupposto. Tali presidi di controllo sono contenuti e trovano attuazione nelle procedure aziendali e nelle altre componenti del sistema di controllo interno.

Nel citato **Allegato B** del Modello è riportata una “Matrice attività sensibili/protocolli/reati” per facilitare l’associazione tra ciascuna delle attività sensibili, i protocolli a disciplina delle stesse e i reati astrattamente rilevanti in tali attività.