

TELEBIT S.p.A.

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO EX D. LGS. N.
231/2001**

ESTRATTO DELLA PARTE GENERALE

Versione	Approvazione
Prima adozione	Approvato dal Consiglio di Amministrazione in data 05.07.2024
Aggiornamento 01	Approvato dal Consiglio di Amministrazione in data 18.09.2026

INDICE DELLA PARTE GENERALE

DEFINIZIONI.....	4
1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI EX D.LGS. N. 231/2001 E LA SUA.....	7
EVOLUZIONE	7
1.1. Il Decreto Legislativo n. 231 dell'8 giugno 2001	7
1.2. I reati presupposto.....	7
1.3. Le sanzioni.....	9
2. L'ADOZIONE E L'ATTUAZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO EX ART. 6 DEL D.LGS. N. 231/2001 E ART. 30 DEL D.LGS. N. 81/2008	11
2.1. Le previsioni del Decreto 231	11
2.2. L'integrazione della norma: le Linee Guida delle Associazioni di Categoria e le <i>best practice</i> a cui il Decreto 231 è stato ispirato	13
2.3. Il Codice Antimafia per le imprese	14
3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI TELEBIT S.P.A. EX ART. 6 DEL DECRETO 231 E ART. 30 DEL D.LGS. 81/2008 IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO	14
3.1. Telebit S.p.A. e la sua <i>mission</i>	14
3.2. I lavori preparatori alla redazione e all'aggiornamento del Modello. L'attività del Gruppo di Lavoro ed i presupposti del Modello	16
3.3. La struttura del Modello	17
4. IL MODELLO DI GOVERNANCE E LA STRUTTURA ORGANIZZATIVA DI TELEBIT.....	19
4.1. Il modello di <i>governance</i> e di controllo.....	19
4.2. La struttura organizzativa.....	19
4.2.1. Definizione dell'organigramma aziendale e dei compiti.....	19
4.3. La Struttura organizzativa in materia di Salute e Sicurezza sul Lavoro.....	20
5. IL SISTEMA DI DELEGHE E PROCURE	20
5.1. I principi generali.....	20
5.2. La struttura del sistema di deleghe e procure in TELEBIT	21
5.3. Rappresentanza in giudizio e nomina del difensore di fiducia della Società	21

6. PROCEDURE MANUALI E INFORMATICHE (IL SISTEMA DI GESTIONE INTEGRATO)	22
7. IL BUDGET E IL CONTROLLO DI GESTIONE	22
8. IL SISTEMA DI CONTROLLO SULLA SALUTE E SICUREZZA SUL LAVORO	23
9. L'ORGANISMO DI VIGILANZA	24
9.1. La nomina, la composizione dell'Organismo di Vigilanza e i suoi requisiti	24
9.2. I casi di ineleggibilità e decadenza	24
9.3. La durata dell'incarico e le cause di cessazione	24
9.4. Le risorse dell'Organismo di Vigilanza	24
9.5. I compiti e i poteri	25
9.6. Il Regolamento dell'OdV	25
9.7. Il riporto informativo verso l'Organismo di Vigilanza	25
9.8. Il riporto informativo dell'Organismo di Vigilanza verso gli organi sociali	25
10. IL SISTEMA WHISTLEBLOWING	25
11. IL CODICE ETICO ed il CODICE CONDOTTA FORNITORI	28
12. IL SISTEMA DISCIPLINARE DI TELEBIT	29
12.1. L'elaborazione e l'adozione del Sistema Disciplinare	29
12.2. La struttura del Sistema Disciplinare	29
12.2.1. I destinatari del Sistema Disciplinare	29
12.2.2. Le condotte rilevanti ai sensi dell'applicazione del Sistema Disciplinare	30
12.2.3. Le sanzioni	30
12.2.4. Il procedimento di irrogazione delle sanzioni	32
13. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI	32
13.1. La comunicazione e il coinvolgimento sul Modello e sui Protocolli connessi	32
13.2. La formazione e l'addestramento sul Modello e sui Protocolli connessi	33
14. AGGIORNAMENTO DEL MODELLO	34

DEFINIZIONI

Le definizioni di seguito indicate trovano applicazione nella presente Parte Generale, nonché nelle singole Parti Speciali, fatte salve le ulteriori definizioni contenute in queste ultime.

Amministratori	I componenti del Consiglio di Amministrazione della Società.
Aree a Rischio reato	Le aree di attività della Società, o fasi delle stesse, nell'ambito del cui svolgimento può determinarsi l'insorgere di un rischio di commissione di Reati.
Aree Strumentali	Le aree nell'ambito delle quali sono gestiti strumenti di tipo finanziario e/o mezzi sostitutivi che possessione dei reati corruttivi nelle Aree a Rischio.
API	Addetti alla Prevenzione degli Incidenti.
APS	Addetti al Primo Soccorso.
ASPP	Addetti al Servizio di Prevenzione e Protezione dai rischi per la salute e sicurezza sul lavoro.
Attività Sensibili	Le attività della Società al cui svolgimento è collegato il rischio, anche potenziale, di commissione di Reati.
CCNL	I Contratti Collettivi Nazionali di Lavoro applicati dalla Società.
Codice Etico	Il documento interno, predisposto e approvato dal Consiglio di Amministrazione, che definisce l'insieme dei principi e delle regole di condotta volti a promuovere un elevato livello di professionalità e a vietare comportamenti in contrasto con le disposizioni legislative, con i principi deontologici, nonché con i valori e la <i>mission</i> della Società.
Comitato Whistleblowing o CWB	Comitato incaricato di gestire le segnalazioni e verificarne la fondatezza, composto dai componenti dell'OdV, dal Responsabile dell'Ufficio Legale e dalla Funzione FCPC.
Consiglio di Amministrazione o CdA	L'organo amministrativo della Società.
D.Lgs. n. 231/2001, il Decreto o Decreto 231	Il D.Lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni.
Decreto Whistleblowing	Il D.Lgs. n. 24 del 2023, che recepisce la 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 europea e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali”.

Destinatari	I Soggetti Apicali, i Dipendenti ed i Terzi Destinatari.
Dipendenti	I soggetti aventi un rapporto di lavoro subordinato con la Società, a prescindere dalla tipologia ed inquadramento contrattuale
Gruppo di Lavoro	Gruppo formato da risorse aziendali individuate dalla Società, assistite da consulenti esterni specializzati in materia penale.
Gruppo Telebit o Gruppo	La Società e le sue Società Controllate.
Linee Guida	Le linee guida adottate da associazioni rappresentative degli enti per la predisposizione dei modelli di organizzazione, gestione e controllo ai sensi dell’art. 6, comma terzo, del D.Lgs. n. 231/2001 (e.g., Confindustria, ANCE, ABI, Assonime, ecc.).
Manuale MGI o MGI	Il documento che descrive sinteticamente il Sistema SGI della Società e ne definisce politiche, organizzazione, processi, responsabilità e modalità di svolgimento delle attività aziendali fondamentali.
MC	Medico Competente.
Modello	Il modello di organizzazione, gestione e controllo previsto dal D.Lgs. n. 231/2001.
Organismo di Vigilanza, OdV o Organismo	Ai sensi di quanto previsto dall’art. 6 del D.Lgs. n. 231/2001, l’organismo della Società dotato di autonomi poteri di iniziativa e di controllo a cui è affidato il compito di (i) vigilare sul funzionamento e sull’osservanza del Modello, nonché (ii) indirizzare le proposte di aggiornamento dello stesso agli organi/funzioni competenti, supervisionando le attività funzionali a tale scopo.
Protocollo Antimafia	Documento che riassume organicamente i controlli svolti dalla Società sui soggetti che intervengono nella catena esecutiva, al fine di prevenire infiltrazioni della criminalità organizzata.
Reati o Reati Presupposto	Le fattispecie di reato che costituiscono presupposto della responsabilità amministrativa dell’ente prevista dal Decreto.
RLS	Rappresentante dei Lavoratori per la Sicurezza.

RSPP	Responsabile del Servizio di Prevenzione e Protezione in materia di salute e sicurezza sul lavoro.
Sistema Disciplinare	Il sistema volto a sanzionare le violazioni dei principi, delle norme e delle misure previste dal Modello e dai relativi Protocolli.
Sistema SGI o SGI	Il Sistema di Gestione Integrato della Società, formalizzato nel Manuale MGI e in procedure gestionali, istruzioni operative, moduli e documenti.
Società o Telebit	Telebit S.p.A.
Soggetti Apicali	Persone che (i) rivestono funzioni di rappresentanza (sia organica che volontaria), di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o che (ii) esercitano, anche di fatto, la gestione e il controllo della Società.
SSL	Salute e Sicurezza sul Lavoro.
Terzi Destinatari	I soggetti tenuti al rispetto del Modello in ragione della funzione svolta o perché operano, direttamente o indirettamente, per la Società.
TU SSL	Testo Unico Salute e Sicurezza sul Lavoro.
Whistleblowing	Il sistema di gestione delle segnalazioni attraverso il quale è possibile segnalare condotte illecite rilevanti ai sensi D.lgs. 24/2023, incluse le violazioni del Decreto 231 e del Modello.

1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI EX D.LGS. N. 231/2001 E LA SUA EVOLUZIONE

1.1. Il Decreto Legislativo n. 231 dell'8 giugno 2001

Il Decreto Legislativo dell'8 giugno 2001 n. 231, recante la *“Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica”* (**Decreto 231**), in attuazione della delega legislativa contenuta nell'art. 11 della legge 29 settembre 2000, n. 300, ha introdotto a carico degli enti un regime di responsabilità amministrativa, assimilabile ad una responsabilità penale, nell'ipotesi in cui alcune specifiche fattispecie di reato vengano commesse nell'interesse o a vantaggio degli enti stessi da parte di:

- a) persone che rivestono funzioni di rappresentanza, sia organica che volontaria, di amministrazione o di direzione dell'ente o di una sua unità organizzativa (dotata di autonomia finanziaria e funzionale) o che esercitano, anche di fatto, la gestione e il controllo dell'ente (soggetti c.d. “apicali”)¹;
- b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (soggetti c.d. “subordinati”).

È stato così superato l'antico principio *societas delinquere non potest*² ed enucleata una responsabilità autonoma della persona giuridica.

Quanto ai soggetti destinatari della nuova forma di responsabilità, il Decreto 231 specifica che si tratta di *“enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica”*. Sono invece esclusi dal novero dei soggetti destinatari, lo Stato, gli enti pubblici territoriali (Regioni, Province, Comuni e Comunità montane), gli enti pubblici non economici e, in generale, tutti gli enti che svolgano funzioni di rilievo costituzionale (Camera dei deputati, Senato della Repubblica, Corte costituzionale, Segretariato generale della Presidenza della Repubblica, C.S.M., CNEL).

1.2. I reati presupposto

Al fine di configurare la responsabilità amministrativa ex Decreto 231, nella Sezione III del Capo I del Decreto 231, sono individuate, come rilevanti, solo specifiche tipologie di reato (i c.d. reati presupposto)³, meglio indicate nell'**Allegato n. 1**.

¹ Possono essere qualificati come apicali i componenti degli organi di amministrazione e controllo dell'ente, quale che sia il sistema prescelto tra quelli indicati dal Legislatore (amministratore unico, consiglio di amministrazione, amministrazione congiunta o disgiunta). Nel novero dei soggetti in c.d. “posizione apicale”, oltre agli amministratori e ai sindaci vanno, inoltre, ricompresi, alla stregua dell'art. 5 del Decreto 231, il direttore generale, i direttori esecutivi dotati di autonomia finanziaria e funzionale, nonché i preposti alle sedi secondarie ed ai siti/stabilimenti, i quali possono anche assumere la qualifica di “datori di lavoro” ai sensi della normativa prevenzionistica vigente in materia di salute e sicurezza sul lavoro. Tali soggetti possono essere legati alla società sia da un rapporto di lavoro subordinato, sia da altri rapporti di natura privatistica (ad es., mandato, agenzia, preposizione institoria, ecc.).

² Era escluso che una società potesse comparire nella veste di imputato nell'ambito di un processo penale.

³ Il “catalogo” dei reati presupposto rilevanti ai sensi del Decreto 231 è in continua espansione. Se, da un lato, vi è una forte spinta da parte degli organi comunitari, dall'altro, anche a livello nazionale, sono stati presentati numerosi disegni di legge diretti ad inserire ulteriori fattispecie.

Il presente Modello prende in considerazione le fattispecie di reato per le quali, a seguito dell'attività di *risk assessment*, è stato rilevato un potenziale rischio rispetto alle attività esercitate dalla Società (**reati presupposto rilevanti**), in particolare:

- Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24);
- Delitti informatici e trattamento illecito di dati (art. 24-bis);
- Delitti di criminalità organizzata (art. 24-ter);
- Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione (art. 25);
- 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 (art. 25-ter);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quater);
- Delitti contro la personalità individuale, inclusi del reato di intermediazione illecita e sfruttamento del lavoro (art. 25-quinquies);
- Reati di omicidio colposo o lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies);
- Reati di 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);
- Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-octies.2);
- Reati 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 transnazionali in materia di associazioni criminali, riciclaggio, traffico di migranti, intralcio alla giustizia (Legge 16 marzo 2006, n. 146, artt. 3 e 10);
- Reati ambientali (art. 25-undecies);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies);
- Razzismo e Xenofobia (art. 25-terdecies);
- Reati tributari (art. 25-quinquiesdecies);
- Delitti contro il patrimonio culturale (art. 25-septiesdecies);
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-octiesdecies);
- Contrabbando (art. 25-sexiesdecies);
- Delitti contro gli animali (art. 25-undevicies);
- Reati commessi con l'uso di sistemi di intelligenza artificiale (art. 25 – vicies).

Per quanto concerne i reati di cui agli artt. 25-quater.1 (pratiche di mutilazione degli organi genitali

femminili); 25-sexies (abuso di informazioni privilegiate e manipolazione del mercato); 25-quaterdecies (frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati), l'esito delle attività di *risk assessment* svolte hanno portato a ritenere che la loro commissione possa essere stimata non significativa in relazione all'ambito di attività della Società. In ogni caso, il rischio ad esse connesso risulta essere adeguatamente presidiato alla luce dei principi generali di comportamento descritti nel Codice Etico.

1.3. Le sanzioni

Ai sensi dell'art. 9 del Decreto 231 le sanzioni applicabili agli enti, a seguito della commissione del reato sono:

- i. sanzioni pecuniarie: hanno natura afflittiva (sanzionatoria) e non risarcitoria, sono calcolate in base a un sistema per quote (in un numero non inferiore a cento né superiore a mille) e vengono determinate dal giudice sulla base della gravità del fatto e del grado di responsabilità dell'ente, nonché dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto illecito e per prevenire la commissione di ulteriori illeciti. L'importo di ciascuna quota va da un minimo di 258,23 € ad un massimo di 1.549,37 € e viene determinato dal giudice tenendo in considerazione le condizioni economiche e patrimoniali dell'ente. L'ammontare della sanzione pecuniaria, pertanto, viene determinato per effetto della moltiplicazione del primo fattore (numero di quote) per il secondo (importo della quota).

Per alcune tipologie di reati, l'ente può incorrere sistema basato sul fatturato globale totale dell'ente. In tali casi, la sanzione pecuniaria è determinata in relazione alla specifica percentuale, prevista per ciascun reato presupposto, del fatturato globale totale dell'ente relativo all'esercizio finanziario precedente quello in cui è stato commesso il Reato, ovvero, se inferiore, all'esercizio precedente l'applicazione della sanzione pecuniaria. Qualora non sia possibile accertare il fatturato globale totale dell'ente, la sanzione pecuniaria è applicata nell'importo determinato in relazione a ciascun Reato;

- ii. sanzioni interdittive (art. 9, comma II):
 - l'interdizione dall'esercizio dell'attività;
 - la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
 - il divieto di contrattare con la pubblica amministrazione, salvo che per l'ottenimento di un servizio pubblico (tale divieto può essere limitato anche a determinati tipi di contratto o a determinate amministrazioni);
 - l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
 - il divieto di pubblicizzare beni o servizi;

- iii. confisca (sanzione obbligatoria conseguente all'eventuale sentenza di condanna);
- iv. pubblicazione della sentenza.

Le sanzioni interdittive hanno la caratteristica di limitare o condizionare l'attività sociale, e nei casi più gravi arrivano a paralizzare l'ente (interdizione dall'esercizio dell'attività); esse hanno altresì la finalità di prevenire comportamenti connessi alla commissione di reati.

Tali sanzioni si applicano, come detto, nei casi espressamente previsti dal Decreto 231 quando ricorrono almeno una delle seguenti condizioni:

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

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni; è possibile l'applicazione in via definitiva delle sanzioni interdittive, nelle situazioni più gravi descritte nell'art. 16 del Decreto 231.

Deve essere evidenziato che il Decreto 231 prevede all'art. 15 che, in luogo dell'applicazione della sanzione interdittiva che determina l'interruzione dell'attività dell'ente, se sussistono particolari presupposti, il giudice può nominare un commissario per la prosecuzione dell'attività dell'ente per un periodo pari alla durata della pena interdittiva.

Appare opportuno indicare che l'art. 45 del Decreto 231 prevede l'applicazione delle sanzioni interdittive indicate nell'art. 9, comma II, anche in via cautelare quando vi sono gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per il quale si procede.

Deve, infine, osservarsi che l'Autorità Giudiziaria può, altresì, disporre:

- il sequestro preventivo delle cose di cui è consentita la confisca (art. 53);
- il sequestro conservativo dei beni mobili e immobili dell'ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54).

2. L'ADOZIONE E L'ATTUAZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO QUALE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA DA REATO EX ART. 6 DEL D.LGS. N. 231/2001 E ART. 30 DEL D.LGS. N. 81/2008

2.1. Le previsioni del Decreto 231

Il Legislatore riconosce, agli artt. 6 e 7 del Decreto 231, forme specifiche di esonero della responsabilità amministrativa dell'ente.

In particolare, l'art. 6, comma I, prescrive che, nell'ipotesi in cui i fatti di reato siano ascrivibili a soggetti in posizione apicale, l'ente non è ritenuto responsabile se prova che:

- a) ha adottato ed attuato, prima della commissione del fatto, un modello di organizzazione, gestione e controllo ("**Modello**") idoneo a prevenire reati della specie di quello verificatosi;
- b) ha nominato un organismo, indipendente e con poteri autonomi, che vigili sul funzionamento e l'osservanza del Modello e ne curi l'aggiornamento ("**Organismo di Vigilanza**", "**OdV**" o "**Organismo**");
- c) il reato è stato commesso eludendo fraudolentemente le misure previste nel Modello;
- d) non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Il contenuto del Modello è individuato dallo stesso art. 6, il quale, al comma II, prevede che l'ente debba:

- a) individuare le attività nel cui ambito possono essere commessi i reati;
- b) prevedere specifici protocolli volti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee a prevenire i reati;
- d) prevedere obblighi di informazione nei confronti dell'OdV;
- e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate dal Modello.

Ai sensi dell'art. 6, comma II bis, "*i modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)*".

Nel caso dei soggetti in posizione subordinata, l'adozione e l'efficace attuazione del Modello comportano che l'ente sarà chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza (combinato di cui ai commi I e II dell'art. 7).

I successivi commi III e IV introducono due principi che, sebbene siano collocati nell'ambito della norma sopra rammentata, appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'ente per entrambe le ipotesi di reato di cui all'art. 5, lett. a) e b). Segnatamente, è previsto che:

- il Modello deve prevedere misure idonee sia a garantire lo svolgimento dell'attività nel rispetto della legge, sia a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;
- l'efficace attuazione del Modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione o normativi; assume rilevanza, altresì, l'esistenza di un idoneo sistema disciplinare (condizione, invero, già prevista dalla lett. e), sub art. 6, comma II).

Deve aggiungersi, inoltre, che con specifico riferimento alla efficacia preventiva del Modello con riferimento ai reati (colposi) in materia di salute e sicurezza sul lavoro, l'**art. 30 del D.Lgs. n. 81/2008 ("TU SSL")** stabilisce che:

"Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, 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".*

Sempre secondo la lettera dell'art. 30: *"Il modello organizzativo e gestionale [...] deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello 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. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o alla norma UNI EN ISO 45001:2023+A1:2024 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione [consultiva permanente per la salute e sicurezza sul Lavoro]".

Come noto, sotto un profilo formale, l'adozione ed efficace attuazione di un Modello non costituiscono un obbligo, ma unicamente una facoltà per gli enti, i quali ben potrebbero decidere di non conformarsi al disposto del Decreto 231 senza incorrere, per ciò solo, in alcuna sanzione. Tuttavia, l'adozione e l'efficace attuazione di un Modello idoneo sono, per gli Enti, un presupposto molto importante per poter beneficiare dell'esimente prevista dal Legislatore.

È importante, inoltre, tenere in conto che il Modello non è da intendersi quale strumento statico, ma deve essere considerato, di converso, un apparato dinamico che permette all'ente di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze che, al momento della sua creazione, non era possibile individuare.

2.2. L'integrazione della norma: le Linee Guida delle Associazioni di Categoria e le *best practice* a cui il Decreto 231 è stato ispirato

Il Legislatore – consapevole della svolta epocale correlata all'emanazione del Decreto 231 che, di fatto, fa venire meno il tradizionale principio *societas delinquere non potest* – ha ritenuto importante precisare, al comma III dell'art. 6, che i modelli di organizzazione e gestione possono essere adottati sulla base dei codici di comportamento redatti dalle Associazioni rappresentative degli enti e comunicati al Ministero di Giustizia che, se del caso, può formulare osservazioni.

Così disponendo, il Legislatore ha inteso fornire agli enti interessati specifiche "Linee Guida", aprioristicamente valutate come corrette e corrispondenti alle finalità della disciplina in questione, a cui attenersi nell'elaborazione dei propri "modelli".

La prima Associazione a redigere un documento di indirizzo per la costruzione dei modelli è stata Confindustria che, nel marzo del 2002, ha emanato delle Linee Guida, poi parzialmente modificate e aggiornate prima nel maggio 2004, nel marzo 2008, nel marzo 2014 e, da ultimo, nel giugno 2021 ("**Linee Guida**")⁴.

Successivamente, molte Associazioni settoriali hanno redatto le proprie linee guida tenendo in considerazione i principi enucleati da Confindustria le cui Linee Guida costituiscono, dunque, l'imprescindibile punto di partenza per la costruzione del Modello.

Come è evidente, le Linee Guida considerano come rilevante l'effettiva implementazione di misure

⁴ Tutte le versioni delle Linee Guida di Confindustria sono state poi giudicate adeguate dal Ministero di Giustizia (con riferimento alle Linee Guida del 2002, cfr. la "Nota del Ministero della Giustizia" del 4 dicembre 2003; con riferimento agli aggiornamenti del 2004 e del 2008, cfr. la "Nota del Ministero della Giustizia" del 28 giugno 2004 e la "Nota del Ministero della Giustizia" del 2 aprile 2008; con riferimento all'aggiornamento del marzo 2014, cfr. la "Nota del Ministero della Giustizia" del 21 luglio 2014, con riferimento all'ultimo aggiornamento del giugno 2021, cfr. la "Nota del Ministero della Giustizia" dell'8 giugno 2021).

preventive quale parametro di riferimento per la *compliance* al Decreto 231 e ciò indipendentemente dal “nome” che a questo sistema di controllo voglia darsi (sia esso “modello” o “manuale” o “procedure” o qualsivoglia altro).

Infatti, il punto nodale della verifica circa la bontà o meno del sistema di controllo interno non è quello relativo all’esistenza o meno di un documento denominato “Modello” ma, al contrario, all’adozione e all’implementazione di sistemi preventivi del rischio.

2.3. Il Codice Antimafia per le imprese

Ai fini della prevenzione di episodi di infiltrazione di criminalità organizzata, come sarà meglio specificato nel Protocollo predisposto ad hoc (Cfr. All. 2, “**Protocollo Antimafia**”), la Società ha anche considerato le best practice in materia rappresentate, tre le altre, dal Codice Antimafia per le imprese di Pier Luigi Vigna, Giovanni Fiandaca, Donato Masciandaro ponendo particolare attenzione all’iter di qualifica e monitoraggio delle terze parti con le quali la Società intrattiene rapporti contrattuali. Tale Protocollo ha lo scopo di riassumere in modo organico i controlli che la Società svolge sui soggetti che, a vario titolo, intervengono nella catena esecutiva, estratti dalle relative procedure aziendali di riferimento.

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI TELEBIT S.P.A. EX ART. 6 DEL DECRETO 231 E ART. 30 DEL D.LGS. 81/2008 IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

3.1. Telebit S.p.A. e la sua *mission*

Telebit S.p.A. (“**Telebit**” o “**Società**”) è una società italiana, capogruppo dell’omonimo Gruppo. Inizialmente la Società si è occupata principalmente di telecomunicazioni fisse, sia in centrali pubbliche di commutazione, che presso utenti privati. Successivamente, seguendo l’evolversi del settore, la Società si è ingrandita ed ha ampliato il proprio ambito di attività. Attualmente Telebit è parte integrante di un gruppo di società che opera come System Integrator a livello nazionale, avendo rafforzato la propria presenza su tutto il territorio italiano.

Le attività operative di Telebit risultano organizzate principalmente nelle aree Field Operation Unit e Digital Services Unit.

L’area **Field Operation Unit** è responsabile delle attività operative svolte sul territorio nazionale relative a executive design, delivery e maintenance di reti, infrastrutture ed impianti nei settori in cui il gruppo opera. Gli ambiti di attività sono i seguenti:

- **Mobile Networks:** presidia la progettazione, la realizzazione, l’integrazione e la manutenzione delle reti e delle infrastrutture radio, con responsabilità diretta sull’execution del relativo perimetro operativo.
- **Fixed Access Networks:** presidia la progettazione, la costruzione e la manutenzione delle reti e delle infrastrutture di accesso fisso in fibra e rame, inclusi delivery degli abbonati e decommissioning delle centrali di telefonia.

- **Data Center & Industrial Systems:** presidia la progettazione, la realizzazione e la manutenzione di data center, centrali di telefonia e POP, comprese le opere civili e gli impianti tecnologici, speciali e meccanici.
- **Network & Transport Infrastructure:** presidia la progettazione, la realizzazione e la gestione delle reti e delle infrastrutture di trasporto, core e IP.
- **Renewables & E-Mobility:** presidia la progettazione, la realizzazione e la gestione di soluzioni e infrastrutture per energie rinnovabili e sistemi di ricarica.

L'area **Digital Services Unit** è responsabile della progettazione, realizzazione e governo di soluzioni e servizi ICT, soluzioni Smart/IoT e managed services. La struttura presidia l'intero ciclo di vita tecnico delle soluzioni, dal Solution Design (in supporto alle attività di Pre-Sales) al dettaglio ingegneristico — inclusi HLD, LLD, MoP e scripting — fino al provisioning e alla conduzione operativa dei servizi. Le attività sono erogate attraverso un modello di Remote Delivery centralizzato, affiancato, ove necessario, da presidi specialistici dedicati e da attività di campo localizzate in situ. Tali attività integrano i processi di Service Assurance tecnica, assicurando la compliance normativa e contrattuale.

Per lo svolgimento delle proprie attività nel settore delle telecomunicazioni TELEBIT è inoltre **qualificata all'esecuzione di Lavori Pubblici** nelle seguenti categorie di opere generali e specializzate:

- Categoria OG 1 (Edifici Civili e Industriali) – Classificazione: II (fino a 516.000,00 euro);
- Categoria OG 10 (Impianti per la trasformazione/distribuzione di energia elettrica e di pubblica illuminazione) – Classificazione: V (fino a 5.165.000,00 euro);
- Categoria OG 11 (Impianti Tecnologici) – Classificazione: V (fino a 5.165.000,00 euro);
- Categoria OG 3 (Strade, autostrade, ponti, viadotti, ferrovie, metropolitane) – Classificazione IV bis: (fino a 3.500.000,00 euro);
- Categoria OG 6 (Acquedotti, gasdotti, oleodotti, opere di irrigazione e di evacuazione) – Classificazione III-bis (fino a 1.500.000 euro);
- Categoria OS 1 (lavori in terra) – Classificazione V: (fino a 5.165.000,00 euro);
- Categoria OS 17 (linee telefoniche ed impianti di telefonia) – Classificazione VIII: (oltre 15.494.000,00 euro);
- Categoria OS 19 (impianti di reti di telecomunicazioni e di trasmissioni e trattamento) – Classificazione: VIII (oltre a 15.494.000,00 euro);
- Categoria OS 30 (impianti interni elettrici, telefonici, radiotelefonici e televisivi) – Classificazione IV bis: (fino a 3.500.000,00 euro);
- Categoria OS 35 (interventi a basso impatto ambientale) – Classificazione III bis: (fino a 1.500.000,00 euro).

La TELEBIT è, inoltre, **abilitata ai sensi del Decreto del Ministero dello Sviluppo Economico n. 37 del 22/1/2008** per le seguenti attività:

- impianti di produzione, trasformazione, trasporto, distribuzione, utilizzazione dell'energia elettrica, impianti di protezione contro le scariche atmosferiche, nonché gli impianti per l'automazione di porte, cancelli e barriere [art. 1, lett. a) D.M. 37/2008];
- impianti radiotelevisivi, le antenne e gli impianti elettronici in genere [art. 1, lett. b) D.M. 37/2008];
- impianti di riscaldamento, di climatizzazione, di condizionamento e di refrigerazione di qualsiasi natura o specie, comprese le opere di evacuazione dei prodotti della combustione e delle condense, e di ventilazione ed aerazione dei locali [art. 1, lett. c) D.M. 37/2008];
- impianti idrici e sanitari di qualsiasi natura o specie [art. 1, lett. d) D.M. 37/2008];
- impianti di protezione antincendio [art. 1, lett. g) D.M. 37/2008] .

La *mission* aziendale è garantita da un sistema di *corporate governance* conforme alla dimensione e alla struttura aziendale (sul punto, vedi *infra*, paragrafo 4).

3.2. I lavori preparatori alla redazione e all'aggiornamento del Modello. L'attività del Gruppo di Lavoro ed i presupposti del Modello

Telebit, sempre tesa al proprio miglioramento, ha proceduto alla formalizzazione del proprio Modello, previa l'esecuzione di un'analisi sull'intera struttura organizzativa aziendale e sul proprio sistema di controlli, onde verificarne l'adeguatezza rispetto ai fini di prevenzione dei reati rilevanti, nonché al periodico aggiornamento del Modello stesso.

Ai fini dell'ultimo aggiornamento del Modello, la Società ha programmato l'attuazione di un piano di intervento volto a sottoporre a una approfondita e complessa analisi l'organizzazione e l'attività della Società. A tal fine, è stato costituito un gruppo di lavoro formato da risorse aziendali individuate dalla Società assistite da consulenti esterni specializzati in materia penale (di seguito, "**Gruppo di Lavoro**").

La metodologia seguita dal Gruppo di Lavoro per la predisposizione del Modello è articolata nelle seguenti fasi:

- a) analisi della documentazione preliminare richiesta alla Società;
- b) individuazione delle "persone chiave" con cui svolgere i necessari approfondimenti;
- c) svolgimento delle interviste con le "persone chiave";
- d) formalizzazione delle interviste in appositi *report* poi condivisi con le funzioni aziendali;
- e) identificazione, per ciascuna processo aziendale, delle aree di rischio, delle attività sensibili e dei controlli esistenti con riferimento alle specifiche aree individuate ed eventuali aspetti suscettibili di miglioramento;
- f) individuazione di possibili modalità di commissione dei reati.

In particolare, con riferimento ai **reati dolosi**:

- a) è stato messo a punto un dettagliato e completo elenco dei **processi aziendali rilevanti**, correlate **aree “a rischio reato”** ed **“attività sensibili”**, ossia un elenco dei settori della Società per i quali è stato ritenuto astrattamente sussistente, sulla base dei risultati dell’analisi, il rischio di commissione dei reati teoricamente riconducibili alla tipologia dei c.d. reati presupposto, previsti dal Decreto 231 e rilevanti per la Società; sono state individuate le c.d. aree “strumentali”, ossia le aree nelle quali è prevista la gestione di strumenti di tipo finanziario e/o mezzi sostitutivi che possono supportare la commissione dei reati nelle “aree a rischio reato”;
- b) per ciascuna “area a rischio reato”, inoltre, sono state individuate le **fattispecie di reato astrattamente ipotizzabili e alcune delle possibili modalità di commissione dei reati** presi in considerazione;
- c) sono stati individuati i **controlli in essere** adottati dalla Società.

Successivamente, sono stati identificati i punti di miglioramento, con la formulazione di appositi suggerimenti, nonché dei piani di azione per l’implementazione dei principi di controllo.

Come suggerito dalle Linee Guida, con riferimento ai **reati colposi in materia di salute e sicurezza sui luoghi di lavoro**, l’analisi è stata condotta sull’intera struttura aziendale, poiché, rispetto ai reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione delle norme di tutela della salute e sicurezza sul lavoro (anche “**SSL**”), non è possibile escludere aprioristicamente alcun ambito di attività, atteso che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali. Il Gruppo di Lavoro ha, quindi, provveduto a raccogliere e analizzare la documentazione rilevante in materia di SSL (tra cui organigrammi, documenti di valutazione dei rischi, verbali delle riunioni previste ai sensi di legge, ecc.) necessaria alla comprensione sia della struttura organizzativa della Società sia degli ambiti relativi alla SSL.

A seguito di tale attività è stata redatta apposita Parte Speciale B sulla scorta di quanto previsto dall’art. 30 del D.lgs. 81/2001.

Il risultato del lavoro svolto è riportato nel presente Modello (Parte Generale, Parte Speciale e relativi Allegati).

3.3. La struttura del Modello

Una volta concluse le attività preparatorie sopra indicate, si è provveduto alla progettazione ed alla predisposizione dei documenti rappresentativi del Modello.

In particolare, il Modello della Società è costituito da una **Parte Generale e da una Parte Speciale (suddivisa in Parte Speciale A e Parte Speciale B)**, nonché da ulteriori documenti che, rappresentativi di alcuni protocolli di controllo, completano il quadro.

Nella **Parte Generale**, oltre all’illustrazione dei contenuti del Decreto 231 e della funzione del Modello, nonché alla regolamentazione dell’Organismo di Vigilanza, sono rappresentati sinteticamente i protocolli sottoindicati (“**Protocolli**”), che – in conformità a quanto previsto dalle Associazioni di categoria – compongono il Modello:

- il modello di *governance*;
- la struttura organizzativa, anche in materia di salute e sicurezza sul lavoro;
- il sistema di procure e deleghe;
- le procedure manuali e informatiche;
- il sistema di *budget* e controllo di gestione;
- il sistema di controllo sulla salute e sicurezza sul lavoro;
- la regolamentazione dell'Organismo di Vigilanza;
- il Sistema di whistleblowing;
- il Codice Etico;
- il Sistema disciplinare;
- la comunicazione e la formazione;
- l'aggiornamento del Modello.

Inoltre, è allegato alla Parte Generale l'**elenco dei reati presupposto** (Allegato 1) ed il **Protocollo Antimafia** (Allegato 2).

La **Parte Speciale A** è strutturata in diversi capitoli in relazione ai vari processi aziendali (esclusa la gestione della salute e sicurezza sui luoghi di lavoro). In relazione a ciascun processo vengono individuate: (i) le aree di rischio e le relative attività "sensibili", cioè le attività che sono state considerate dalla Società a rischio di reato, in esito alle analisi dei rischi condotte, ai sensi del Decreto, (ii) le funzioni aziendali coinvolte; (iii) i reati ipotizzabili; (iv) i principi generali di comportamento; (v) i principali presidi di controllo volti alla prevenzione o alla mitigazione degli illeciti, estratti dalle procedure aziendali.

Con riferimento alla gestione della salute e sicurezza sui luoghi di lavoro è stata predisposta apposita **Parte Speciale B** in linea con le previsioni di cui all'art. 30 del D.lgs. 81/2008.

Costituiscono inoltre parte integrante del Modello:

- il **Risk Assessment** finalizzato all'individuazione delle aree a rischio;
- il **Codice Etico**, che definisce i principi e le norme di comportamento della Società;
- il **Codice di Condotta Fornitori**, che contiene i principi e le regole di comportamento che i fornitori devono osservare nello svolgimento delle attività per Telebit;
- il **Sistema di gestione delle segnalazioni Whistleblowing**;
- tutte le disposizioni, i provvedimenti interni, gli atti o le procedure operative aziendali che costituiscono gli strumenti di attuazione del Modello ivi incluso il Manuale di Gestione Integrato e relative procedure ed istruzioni operative.

Tali atti e documenti sono reperibili, secondo le modalità previste per la loro diffusione, all'interno

dell'azienda e sulla intranet aziendale.

È opportuno precisare che il presente documento individua e riassume il contenuto descrittivo ed i principi generali di adozione del Modello, essendo l'individuazione dei sistemi di prevenzione dei rischi concretamente definita anche attraverso il rinvio agli strumenti di controllo utilizzati nella realtà operativa aziendale (tra cui procedure, istruzioni operative, policies, sistemi autorizzativi, struttura organizzativa, sistema delle deleghe e delle procure, norme di comportamento, modalità di gestione delle risorse finanziarie, strumenti di tracciabilità e documentazione, etc.), da intendersi integralmente richiamati nel presente Modello. E infatti, ragioni di "praticabilità" e funzionalità dello stesso Modello impongono di non trascrivere pedissequamente e materialmente all'interno del presente documento l'intero sistema delle procedure e degli ulteriori controlli in essere, tanto più ove si consideri che tali strumenti di controllo operativo costituiscono un "corpo vivo", dinamico ed in costante evoluzione, soggetto ad esigenze di aggiornamento proprio allo scopo di garantirne l'efficacia e l'attualità. Cionondimeno, tali procedure e sistemi di controllo devono intendersi qui richiamati quale parte integrante ed essenziale del Modello, del quale costituiscono il nucleo "operativo".

Anche le azioni di miglioramento del sistema di controllo interno attuate successivamente all'adozione del Modello costituiscono a tutti gli effetti parte integrante del Modello Organizzativo stesso, nonché del sistema dei protocolli preventivi adottati a presidio delle diverse aree e attività a rischio.

4. IL MODELLO DI GOVERNANCE E LA STRUTTURA ORGANIZZATIVA DI TELEBIT

Il modello di *governance* di Telebit e, in generale, tutto il suo sistema organizzativo, è interamente strutturato in modo da assicurare alla Società l'attuazione delle strategie e il raggiungimento degli obiettivi.

La struttura di Telebit, infatti, è stata creata tenendo conto della necessità di dotare la Società di una organizzazione tale da garantirle la massima efficienza ed efficacia operativa.

4.1. Il modello di *governance* e di controllo

OMISSIS

4.2. La struttura organizzativa

4.2.1. Definizione dell'organigramma aziendale e dei compiti

La struttura organizzativa della Società è orientata a garantire, da un lato, la separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, dall'altro, la massima efficienza possibile.

Al fine di rendere immediatamente chiaro il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale, TELEBIT ha messo a punto un prospetto sintetico nel quale è

schematizzata l'intera struttura organizzativa (organigramma) nonché apposita disposizione organizzativa volta a descrivere in dettaglio le attività svolta dalle singole aree aziendali (ai quali si rimanda per un'analisi di dettaglio della struttura organizzativa). Tali documenti sono oggetto di puntuale aggiornamento in funzione dei cambiamenti intervenuti nella struttura organizzativa.

OMISSIS

4.3. La Struttura organizzativa in materia di Salute e Sicurezza sul Lavoro

Fermo restando l'approfondimento che sarà svolto nella Parte Speciale, deve intanto osservarsi che, in materia di salute e sicurezza sul lavoro, la Società si è dotata di una struttura organizzativa conforme a quella prevista dalla normativa prevenzionistica vigente, nell'ottica di eliminare ovvero, laddove ciò non sia possibile, ridurre – e, quindi, gestire – i rischi lavorativi per i lavoratori.

OMISSIS

I compiti e le responsabilità in materia SSL dei soggetti sopra indicati sono definiti formalmente in coerenza con lo schema organizzativo e funzionale della Società, con particolare riferimento alle figure specifiche operanti in tale ambito. A tale proposito, la Società esplicita, in sede di definizione dei compiti organizzativi e operativi dell'intero ente, anche quelli relativi alle attività di sicurezza di rispettiva competenza, nonché le responsabilità connesse all'esercizio delle attività stesse.

5. IL SISTEMA DI DELEGHE E PROCURE

5.1. I principi generali

Così come richiesto dalla buona pratica aziendale e specificato anche nelle Linee Guida di Confindustria, l'Organo Amministrativo è l'organo preposto a conferire ed approvare formalmente le deleghe ai singoli consiglieri; i poteri di firma poi sono assegnati in coerenza con le responsabilità organizzative e gestionali definite e, ove attribuito il relativo potere, con una puntuale indicazione delle soglie di approvazione delle spese.

Ai sensi dello Statuto, la firma e la rappresentanza legale della Società, di fronte ai terzi ed in giudizio, spettano:

- all'Amministratore Unico;
- al Presidente e al Vicepresidente del Consiglio di Amministrazione;
- al Presidente del Comitato esecutivo, nelle materie delegate dal Consiglio di Amministrazione a tale organo collegiale;
- agli Amministratori delegati, nei limiti e alle condizioni di esercizio dei poteri ad essi

conferiti dal Consiglio di Amministrazione.

Il livello di autonomia, il potere di rappresentanza e i limiti di spesa assegnati ai vari titolari di deleghe e procure all'interno della Società devono essere sempre individuati. Essi devono essere fissati in modo coerente con il ruolo o con il livello gerarchico del destinatario della delega o della procura nei limiti di quanto strettamente necessario all'espletamento dei compiti e delle mansioni da assegnare.

I poteri così conferiti vengono periodicamente aggiornati in funzione dei cambiamenti organizzativi che intervengono nella struttura della Società.

5.2. La struttura del sistema di deleghe e procure in TELEBIT

Il Consiglio di Amministrazione può delegare tutte o parte delle sue attribuzioni, in quanto delegabili, a un Comitato Esecutivo o ad uno o più Consiglieri.

OMISSIS

5.3. Rappresentanza in giudizio e nomina del difensore di fiducia della Società

Ai sensi dell'art. 39 del Decreto 231, *“l'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo”*.

A tal riguardo, la Società, al fine di scongiurare il verificarsi di possibili situazioni di conflitto di interessi, riconosce formalmente una condizione di incompatibilità in capo ai propri legali rappresentanti, come identificati dal sistema di delega e procure in essere, a rappresentare la Società in giudizio, nonché a procedere alla nomina del difensore di fiducia della stessa, qualora lo stesso legale rappresentante risulti sottoposto a indagini o imputato in procedimento penale per i medesimi reati ascritti alla Società ai sensi del Decreto 231.

A tal fine, TELEBIT ha ritenuto opportuno adottare i seguenti presidi:

- ai legali rappresentanti è fatto obbligo di segnalare tempestivamente il proprio coinvolgimento, a titolo personale, in procedimenti penali relativi a contestazioni potenzialmente rilevanti ai sensi del Decreto 231 e connesse alle attività della Società, così come laddove sia riscontrata una situazione di incompatibilità o conflitto di interessi, nei termini sopra descritti, in relazione a qualsiasi procedimento di cui sia parte la Società ai sensi del Decreto 231;
- al legale rappresentante coinvolto è fatto divieto di rappresentare la Società in giudizio, nonché di nominare il difensore di fiducia della Società, nelle situazioni sopra descritte;
- nel caso di coinvolgimento della Società in un procedimento ai sensi del Decreto 231 e quando non vi siano altri soggetti dotati dei necessari poteri di rappresentanza generale e di nomina di avvocati e procuratori speciali esenti da conflitti di interessi, come nelle

situazioni sopra descritte, l'Organo Amministrativo conferisce apposita procura speciale a uno dei membri del Consiglio di Amministrazione medesimo o ad altro procuratore speciale della Società ai fini della rappresentanza in giudizio della Società e per procedere alla nomina del difensore dell'ente;

- l'Organo Amministrativo verifica preventivamente che il difensore di fiducia della Società e del legale rappresentante corrispondano a due distinte personalità.

6. PROCEDURE MANUALI E INFORMATICHE (IL SISTEMA DI GESTIONE INTEGRATO)

Telebit ha sempre orientato la propria attività in un'ottica di crescita aziendale intesa come "miglioramento" nel senso più ampio del termine. Nel suo "percorso" di crescita la Società ha conseguito una serie di certificazioni secondo i seguenti standards normativi:

- UNI EN ISO 9001:2015, relativa al sistema di gestione per la qualità;
- **UNI ISO 45001:2023, relativa al sistema di gestione per la salute e sicurezza dei lavoratori;**
- **UNI EN ISO 14001:2015, relativa al sistema di gestione ambientale;**
- UNI EN ISO 22301:2019, relativa al sistema di gestione della continuità operativa;
- UNI EN ISO 27001:2013, relativa al sistema di gestione della sicurezza delle informazioni;
- UNI/PdR 125:2022, relativa al sistema di gestione per la parità di genere;
- Certificazione F-GAS, ai sensi del Regolamento CE n. 303/2008, certificato n. IR011155, relativa ai gas fluorurati ad effetto serra;
- SA8000:2014, relativa alla responsabilità sociale d'impresa;
- UNI EN ISO 30415:2021, relativa alla gestione delle risorse umane in materia di diversità e inclusione;
- Modello EASI — Ecosistema Aziendale Sostenibile Integrato, versione E1 del 6 giugno 2022;
- ISO 50001:2018, relativa al sistema di gestione dell'energia;
- **UNI EN ISO 37001:2016, relativa ai sistemi di gestione per la prevenzione della corruzione.**

OMISSIS

7. IL BUDGET E IL CONTROLLO DI GESTIONE

Il sistema di controllo di gestione della Società prevede meccanismi di verifica della gestione delle risorse che devono garantire, oltre che la verificabilità e tracciabilità delle spese, l'efficienza e l'economicità delle attività aziendali, mirando ai seguenti obiettivi:

- definire in maniera chiara, sistematica e conoscibile tutte le risorse a disposizione delle funzioni aziendali nonché l'ambito in cui le stesse possono essere impiegate, attraverso la programmazione e definizione del budget;
- garantire la predisposizione del budget sulla base di obiettivi di *business* "ragionevoli",

previa adeguata analisi dei risultati degli anni precedenti;

- rilevare gli eventuali scostamenti rispetto a quanto predefinito in sede di budget, analizzarne le cause e riferire i risultati delle valutazioni ai livelli gerarchicamente responsabili al fine di predisporre i più opportuni interventi di adeguamento, attraverso la relativa consuntivazione.

8. IL SISTEMA DI CONTROLLO SULLA SALUTE E SICUREZZA SUL LAVORO

La gestione delle questioni connesse alla salute e alla sicurezza sul lavoro è effettuata con l'obiettivo di provvedere in via sistematica:

- all'identificazione dei rischi e alla loro valutazione;
- all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati, affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo – e, quindi, gestiti – in relazione alle conoscenze acquisite in base al progresso tecnico;
- alla limitazione al minimo del numero di lavoratori esposti a rischi;
- alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde;
- al controllo sanitario dei lavoratori in funzione dei rischi specifici;
- alla programmazione della prevenzione, mirando a un complesso che integri in modo coerente le condizioni tecniche e produttive dell'azienda con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro, nonché alla successiva realizzazione degli interventi programmati;
- alla formazione, all'addestramento, alla comunicazione ed al coinvolgimento adeguati dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL;
- alla regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Le modalità operative per il concreto svolgimento delle attività e il raggiungimento degli obiettivi sopra indicati sono definite nella documentazione aziendale in materia, redatta in conformità alla normativa prevenzionistica vigente, la quale assicura l'adeguata tracciabilità dei processi e delle attività svolte (si veda anche la Parte Speciale).

9. L'ORGANISMO DI VIGILANZA

9.1. La nomina, la composizione dell'Organismo di Vigilanza e i suoi requisiti

L'Organo Amministrativo di TELEBIT nomina, con apposita delibera, un Organismo di Vigilanza, nel rispetto delle previsioni di cui alle Linee Guida.

Con la medesima delibera, l'Organo Amministrativo fissa il compenso spettante ai membri dell'OdV per l'incarico a ciascuno assegnato. La nomina dell'OdV, i suoi compiti e i suoi poteri, sono oggetto di tempestiva comunicazione all'intera popolazione aziendale.

L'OdV di TELEBIT, in ossequio a quanto previsto dalle Linee Guida, risponde ai seguenti requisiti, che si riferiscono all'Organismo in quanto tale e caratterizzano la sua azione:

- autonomia e indipendenza: è previsto che l'OdV sia privo di compiti operativi, i quali potrebbero ledere l'obiettività di giudizio e non sia soggetto al potere gerarchico e disciplinare di alcun organo o funzione societari;
- professionalità: intesa come insieme di strumenti e tecniche necessarie allo svolgimento dell'attività assegnata;
- continuità di azione: l'OdV è provvisto di un adeguato budget e di adeguate risorse ed è dedicato esclusivamente all'attività di vigilanza in modo che sia garantita una efficace e costante attuazione del Modello;
- onorabilità ed assenza di conflitti di interessi: negli stessi termini previsti dalla legge con riferimento ad amministratori e membri del Collegio Sindacale.

OMISSIS

9.2. I casi di ineleggibilità e decadenza

OMISSIS

9.3. La durata dell'incarico e le cause di cessazione

OMISSIS

9.4. Le risorse dell'Organismo di Vigilanza

OMISSIS

9.5. I compiti e i poteri

OMISSIS

9.6. Il Regolamento dell'OdV

OMISSIS

9.7. Il riporto informativo verso l'Organismo di Vigilanza

OMISSIS

In relazione ai flussi informativi sopra descritti, sono attivi gli opportuni canali di comunicazione dedicati e, precisamente, una apposita casella di posta elettronica: organismodivigilanza@telebit.it.

OMISSIS

9.8. Il riporto informativo dell'Organismo di Vigilanza verso gli organi sociali

OMISSIS

10. IL SISTEMA WHISTLEBLOWING

La Società ha attivato un sistema di gestione delle segnalazioni ("**Whistleblowing**"), previo coinvolgimento delle rappresentanze sindacali, conforme ai requisiti di cui al D.lgs. 24/2023 attraverso il quale è possibile inviare anche segnalazioni di condotte illecite rilevanti ai sensi della normativa (ivi inclusa la violazione del Decreto e del Modello).

In linea con la preferenza espressa dall'ANAC, Telebit ha optato per l'utilizzo di piattaforma informatica dedicata, capace di assicurare la richiesta riservatezza.

La gestione e la verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate ad un comitato appositamente costituito (**Comitato Whistleblowing – CWB**) composto dall'Internal Audit, dal responsabile della funzione Legal & Corporate Affairs, dal responsabile

della Funzione Management System & Sustainability, dalla Funzione FCPC (Funzione di conformità per la prevenzione della corruzione) i quali sono dotati dei necessari requisiti di indipendenza ed imparzialità, nonché destinatari di specifica formazione in materia sia di privacy che di whistleblowing.

La segnalazione tramite canale interno costituisce la modalità prioritaria e può essere presentata con le seguenti modalità, a scelta del segnalante:

- a) in **modalità telematica**, utilizzando la piattaforma dedicata, mediante l'utilizzo del software denominato "*whistleblower software by Formalize*" utilizzando il link: [Telebit Spa Sistema degli informatori | Home](#)

Nella piattaforma, la segnalazione può essere fatta per iscritto oppure in forma orale tramite sistema di messaggistica. Si può scegliere di segnalare:

- in forma anonima: l'identità del segnalante non è rivelata a nessuna delle persone coinvolte nella procedura;
 - in forma confidenziale: in questo caso l'identità del segnalante sarà nota solo al personale incaricato di gestire la segnalazione ed apparirà anonima e confidenziale agli altri durante il trattamento della segnalazione.
- b) in **modalità cartacea tramite busta chiusa** recapitata presso la sede delle Società, avendo cura di specificare sulla busta stessa la dicitura "**SEGNALAZIONE WHISTLEBLOWING**", all'attenzione del Comitato Whistleblowing. Laddove tale busta sia stata indirizzata per errore a soggetto diverso dal Comitato, la busta va trasmessa a quest'ultimo entro 7 giorni dal suo ricevimento con contestuale notizia della trasmissione al segnalante;
- c) in **forma orale** mediante richiesta di incontro diretto con il Comitato Whistleblowing tramite una delle due modalità sopra indicate.

Il CWB provvede a trattare la segnalazione nel rispetto dei principi di imparzialità e riservatezza, effettuando ogni attività ritenuta opportuna e si confrontano con il Responsabile dell'Ufficio Risorse Umane per ogni caso in cui sia necessario avviare un procedimento disciplinare.

Immediatamente o, comunque, entro 7 giorni dal ricevimento della segnalazione, è inviato al segnalante un avviso di ricevimento della segnalazione tramite il sistema di messaggistica dell'applicativo o, se la segnalazione è presentata in forma orale, tramite apposita ricevuta consegnata al termine dell'incontro.

Successivamente, il Comitato, sulla base del contenuto della segnalazione, effettua una valutazione della rilevanza della medesima e della sua fondatezza. Se il gestore considera che la segnalazione necessiti di ulteriori accertamenti, avvia un'istruttoria, al termine della quale viene deciso se archiviare la segnalazione (informando il segnalante) o adottare opportune misure (es. eventuali procedimenti disciplinari).

Inoltre, nell'ipotesi in cui il Comitato riceva segnalazioni rilevanti ai sensi del Decreto coinvolgerà nelle proprie attività relative alla gestione della segnalazione anche l'OdV, dando apposite

informative, garantendo la riservatezza del soggetto che effettua la segnalazione salvo eventuali obblighi di legge.

In particolare l'OdV dovrà ricevere:

- immediata informativa su segnalazioni rilevanti ai sensi del D.lgs. 231/2001 e del Modello affinché, nell'esercizio della sua attività di vigilanza, possa condividere le proprie eventuali osservazioni e partecipare all'istruttoria o comunque seguirne l'andamento;
- un aggiornamento periodico sull'attività complessiva di gestione delle segnalazioni, al fine di verificare il funzionamento del sistema whistleblowing e proporre all'ente eventuali necessità di suo miglioramento.

In ottemperanza alle disposizioni normative, Telebit garantisce:

- la riservatezza dell'identità del segnalante, nei modi indicati nella procedura
- la protezione del segnalante da qualsiasi forma di ritorsione o di discriminazione, diretta o indiretta, per motivi collegati, direttamente o indirettamente, alla segnalazione. A tal fine, è previsto l'avvio di procedimenti disciplinari a carico dei soggetti che, in qualsiasi modo, pongano in essere condotte discriminatorie, dirette o indirette, nei confronti del segnalante
- la protezione dalle ritorsioni anche ai facilitatori; a coloro che nel medesimo contesto lavorativo sono legati al segnalante da uno stabile legame affettivo o di parentela entro il quarto grado; ai colleghi di lavoro che intrattengono un rapporto abituale e corrente con il segnalante; agli enti (con particolare riferimento ai rapporti di "partnership") di proprietà del segnalante e agli enti collegati allo stesso che operano nel medesimo contesto lavorativo.

Rappresentano un esempio non esaustivo di atti ritorsivi:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni reputazionali, i pregiudizi economici o finanziari.

Qualsiasi violazione del divieto di porre in essere comportamenti ritorsivi può dar luogo a procedimenti disciplinari e alla conseguente irrogazione di sanzioni (cfr. paragrafo 12).

Per tutti gli ulteriori dettagli sul processo di invio e gestione delle segnalazioni rilevanti ai sensi del Decreto Whistleblowing, si rinvia alla Procedura Whistleblowing, parte integrante del presente Modello.

11. IL CODICE ETICO ed il CODICE CONDOTTA FORNITORI

Così come previsto dalle Linee Guida delle maggiori Associazioni di categoria, il Codice Etico è uno dei Protocolli fondamentali per la costruzione di un valido Modello, idoneo a prevenire i reati presupposto indicati dal Decreto 231.

TELEBIT ha adottato un Codice Etico ("**Codice Etico**") che contiene l'insieme dei diritti, dei doveri e delle responsabilità dell'Ente nei confronti dei "portatori d'interesse" (dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario ecc.).

I valori di TELEBIT sono i principi fondamentali in cui la Società crede ossia:

- **Rispetto:** *rispettando veniamo rispettati, agendo responsabilmente verso le persone e l'ecosistema che ci circonda, senza alcuna distinzione e discriminazione;*
- **Spirito di Squadra:** *uniamo talenti per fare cose straordinarie: siamo lavoro di squadra;*
- **Integrità:** *ci comportiamo ed agiamo in modo da essere fieri di quello che facciamo e di come lo facciamo;*
- **Intraprendenza:** *agiamo con audacia e spirito di iniziativa anche nelle sfide più complesse e rischiose per creare un valore duraturo;*
- **Affidabilità:** *manteniamo gli impegni assunti con concretezza e coscienza;*
- **Competenza:** *uniamo conoscenza ed abilità per trasformare i problemi in soluzioni;*
- **Progresso:** *crediamo nell'evoluzione come impulso per uno sviluppo sociale, ambientale ed economico sostenibile nel tempo;*
- **Passione:** *lavoriamo soddisfacendo le nostre ambizioni con entusiasmo e positività;*
- **Perseveranza:** *non ci arrendiamo di fronte alle difficoltà, agendo con costanza e tenacia, senza cedere;*
- **Dirompenza creativa:** *modifichiamo velocemente e radicalmente gli schemi con cui operiamo, siamo disruptive.*

L'osservanza del Codice Etico è responsabilità personale di tutti coloro che operano nel contesto della Società, tenuti ad agire in conformità con i suoi principi e regolamenti nello svolgimento delle attività quotidiane. In caso di violazione del Codice, la Società si riserva il diritto di intraprendere azioni disciplinari nei confronti dei soggetti interessati nel rispetto della normativa applicabile e del sistema disciplinare previsto dal Modello (cfr. paragrafo 12).

Telebit, inoltre, presta particolare attenzione alla filiera dei fornitori avvalendosi soltanto di fornitori qualificati che si attengono ai medesimi standard etici della Società. A tal fine, la Società

ha adottato apposito **Codice di Condotta Fornitori**, pubblicato sul sito internet, con il quale la Società richiede ai propri fornitori l'adozione dei medesimi comportamenti su temi quali diritti umani, condizioni di lavoro, parità di genere, diversità ed inclusione, salute e sicurezza sul luogo di lavoro, tutela dell'ambiente, risparmio energetico, lotta alla corruzione ed alla criminalità organizzata, protezione dei dati, *business continuity* e sulla sostenibilità ed il trasferimento degli stessi nella catena di fornitura.

12. IL SISTEMA DISCIPLINARE DI TELEBIT

12.1. L'elaborazione e l'adozione del Sistema Disciplinare

Ai sensi degli artt. 6 e 7 del Decreto 231, il Modello può ritenersi efficacemente attuato, ai fini dell'esclusione di responsabilità della Società, se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate.

TELEBIT ha, quindi, adottato un sistema disciplinare ("**Sistema Disciplinare**") precipuamente volto a sanzionare la violazione dei principi, delle norme e delle misure previste nel Modello e nei relativi Protocolli, nel rispetto delle norme previste dalla contrattazione collettiva nazionale, nonché delle norme di legge o di regolamento vigenti.

Sulla scorta di tale Sistema Disciplinare, sono passibili di sanzione sia le violazioni del Modello e dei relativi Protocolli commesse dai soggetti posti in posizione "apicale" – in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero titolari del potere, anche solo di fatto, di gestione o di controllo della Società stessa – sia le violazioni perpetrate dai soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto della Società.

Nel rispetto di quanto previsto anche dalla Linee Guida, l'instaurazione di un procedimento disciplinare, così come l'applicazione delle relative sanzioni, prescindono dall'eventuale instaurazione e/o dall'esito di eventuali procedimenti penali aventi ad oggetto le medesime condotte rilevanti ai fini del Sistema Disciplinare.

12.2. La struttura del Sistema Disciplinare

Il Sistema Disciplinare, unitamente al Modello di cui costituisce uno fra i principali Protocolli, è consegnato, anche per via telematica o su supporto informatico, ai soggetti in posizione apicale e ai dipendenti.

12.2.1. I destinatari del Sistema Disciplinare

I Soggetti Apicali

OMISSIS

I dipendenti

OMISSIS

Gli altri soggetti tenuti al rispetto del Modello

Il presente Sistema Disciplinare ha, inoltre, la funzione di sanzionare le violazioni del Modello commesse da soggetti anche diversi da quelli sopra indicati.

Si tratta, in particolare, di tutti i soggetti (collettivamente, “**Terzi Destinatari**”) che sono comunque tenuti al rispetto del Modello in virtù della funzione svolta in relazione alla struttura societaria e organizzativa della Società, ad esempio in quanto funzionalmente soggetti alla direzione o vigilanza di un Soggetto Apicale, ovvero in quanto operanti, direttamente o indirettamente, per TELEBIT.

Nell’ambito di tale categoria, possono farsi rientrare:

- tutti coloro che intrattengono con la Società un rapporto di lavoro di natura non subordinata (es., gli appaltatori, subappaltatori, i collaboratori a progetto, i consulenti, i lavoratori somministrati, i collaboratori in virtù di contratto di servizi);
- i collaboratori a qualsiasi titolo;
- i procuratori, gli agenti e tutti coloro che agiscono in nome e/o per conto della Società;
- i soggetti cui sono assegnati, o che comunque svolgono, funzioni e compiti specifici in materia di salute e sicurezza sul lavoro;
- i contraenti e i partner.

I membri del Collegio Sindacale, i Revisori ed i membri dell'OdV

OMISSIS

12.2.2. Le condotte rilevanti ai sensi dell’applicazione del Sistema Disciplinare

OMISSIS

12.2.3. Le sanzioni

Il Sistema Disciplinare prevede con riguardo a ognuna delle condotte rilevanti le sanzioni astrattamente comminabili per ciascuna categoria di soggetti tenuti al rispetto del Modello.

In ogni caso, ai fini dell’applicazione delle sanzioni si deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata, nonché delle seguenti

circostanze:

- a) la gravità della condotta o dell'evento che quest'ultima ha determinato;
- b) la tipologia della violazione;
- c) le circostanze nel cui ambito si è sviluppata la condotta;
- d) l'intensità del dolo o il grado della colpa.

Ai fini dell'eventuale aggravamento della sanzione, sono inoltre considerati i seguenti elementi:

- i. l'eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
- ii. l'eventuale concorso di più soggetti nella commissione della violazione;
- iii. l'eventuale recidività del suo autore.

Le sanzioni nei confronti dei Soggetti Apicali

OMISSIS

Le sanzioni nei confronti dei Dipendenti

OMISSIS

Le sanzioni nei confronti dei Terzi Destinatari

Qualora sia accertata la commissione di una delle violazioni indicate nel paragrafo 12.2.2. da parte di un Terzo Destinatario, saranno applicate le seguenti sanzioni:

- la diffida al puntuale rispetto del Modello, pena l'applicazione di una penale ovvero la sospensione o risoluzione del rapporto negoziale intercorrente con la Società;
- l'applicazione di una penale, convenzionalmente prevista;
- la sospensione del rapporto contrattuale in essere e del pagamento del relativo corrispettivo;
- la risoluzione immediata del rapporto negoziale intercorrente con la Società.

Le clausole e le relative sanzioni possono variare in base alla tipologia del soggetto qualificabile come Terzo Destinatario (a seconda del caso che agisca in nome e per conto della Società o meno).

Nel caso in cui le violazioni previste del paragrafo 12.2.2., siano commesse da lavoratori somministrati ovvero nell'ambito di contratti di appalto di opere o di servizi, le sanzioni verranno applicate, all'esito dell'accertamento positivo delle violazioni da parte del lavoratore, nei confronti del somministratore o dell'appaltatore.

Nell'ambito dei rapporti con i Terzi Destinatari, la Società inserisce, nelle lettere di incarico e/o negli accordi negoziali relativi, apposite clausole volte a prevedere, in caso di violazione del Modello, l'applicazione delle misure sopra indicate.

Sindaci, Revisori ed Organismo di Vigilanza

OMISSIS

12.2.4. Il procedimento di irrogazione delle sanzioni

OMISSIS

13. COMUNICAZIONE E FORMAZIONE SUL MODELLO E SUI PROTOCOLLI

13.1. La comunicazione e il coinvolgimento sul Modello e sui Protocolli connessi

Al fine di assicurare un corretto ed efficace funzionamento del Modello, la Società si impegna a implementare la divulgazione dello stesso, adottando le più opportune iniziative per promuoverne e diffonderne la conoscenza differenziando i contenuti a seconda dei Destinatari. In particolare, garantendo la comunicazione formale dello stesso a tutti i dipendenti della Società mediante idonei strumenti divulgativi e l'affissione in luogo accessibile a tutti (pubblicazione sulla rete intranet aziendale).

Inoltre, nei confronti dei dipendenti:

- copia del Modello e dei relativi allegati è inviata via e-mail al momento dell'assunzione;
- viene fatta sottoscrivere al momento dell'assunzione apposita dichiarazione di presa visione del contenuto del Modello e dei relativi allegati.

Per i Terzi Destinatari tenuti al rispetto del Modello, una sintesi dello stesso è messa a disposizione su richiesta e pubblicata sul sito. Il Codice Etico ed il Codice Condotta Fornitori sono pubblicati sul sito internet. Sotto tale ultimo aspetto, al fine di formalizzare l'impegno al rispetto dei principi del Modello nonché dei Protocolli ad esso connessi da parte di Terzi Destinatari, è previsto l'inserimento nel contratto di riferimento di una apposita clausola, ovvero, per i contratti già in essere, la sottoscrizione di una specifica pattuizione integrativa in tal senso.

L'OdV promuove, anche mediante la predisposizione di appositi piani implementati dalla Società, e monitora tutte le ulteriori attività di informazione che dovesse ritenere necessarie o opportune.

La Società promuove adeguati sistemi di comunicazione e coinvolgimento dei destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL, con particolare riguardo ai seguenti profili:

- i rischi per la sicurezza e la salute connessi all'attività aziendale;

- le misure e le attività di prevenzione e protezione adottate;
- i rischi specifici cui ciascun lavoratore è esposto in relazione all'attività svolta;
- le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori;
- la nomina dei soggetti cui sono affidati specifici compiti in materia di SSL (ad esempio, RSPP, APS, API, RLS, MC).

Il coinvolgimento dei soggetti interessati può essere assicurato anche mediante la loro consultazione preventiva in occasione di apposite riunioni periodiche.

13.2. La formazione e l'addestramento sul Modello e sui Protocolli connessi

In aggiunta alle attività connesse alla informazione dei Destinatari, l'OdV ha il compito di promuovere e monitorare la periodica e costante formazione, ovvero di promuovere e monitorare l'implementazione, da parte della Società, delle iniziative volte a favorire una conoscenza ed una consapevolezza adeguate del Modello e dei Protocolli ad esso connessi, al fine di incrementare la cultura di eticità all'interno della Società.

In particolare, è previsto che i principi del Modello, e in particolare quelli del Codice Etico che ne è parte integrante, siano illustrati alle risorse aziendali attraverso apposite attività formative (ad es. corsi, seminari, questionari, ecc.) a cui è posto obbligo di partecipazione e le cui modalità di esecuzione sono pianificate mediante predisposizione di specifici piani, approvati dalle competenti funzioni aziendali.

La Società potrà prevedere, peraltro, che i corsi e le altre iniziative di formazione sui principi del Modello siano differenziati in base al ruolo e alla responsabilità delle risorse interessate, ovvero mediante la previsione di una formazione più intensa e caratterizzata da un più elevato grado di approfondimento per i soggetti operanti nelle aree qualificabili come "a rischio" ai sensi del Modello con focus differenziato in base ai rischi ai quali sono sottoposti.

La Società promuove, inoltre, la formazione e l'addestramento dei Destinatari del Modello, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL, al fine di assicurare un'adeguata consapevolezza circa l'importanza sia della conformità delle azioni rispetto al Modello, sia delle possibili conseguenze connesse a violazioni dello stesso; in quest'ottica, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti in materia di SSL.

A tali fini, è definito, documentato, implementato, monitorato e aggiornato, da parte della Società, un programma di formazione e addestramento periodici dei Destinatari del Modello – con particolare riguardo ai lavoratori neoassunti, per i quali è necessaria una particolare qualificazione – in materia di SSL, anche con riferimento alla sicurezza aziendale e ai differenti profili di rischio (ad esempio, squadra antincendio, pronto soccorso, preposti alla sicurezza, ecc.). In particolare, si prevede che la formazione e l'addestramento siano differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del

trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro, di nuove tecnologie, di nuove sostanze e preparati pericolosi.

14. AGGIORNAMENTO DEL MODELLO

L'OdV ha il compito di monitorare il necessario e continuo aggiornamento e adeguamento del Modello, ivi incluso il Codice Etico, eventualmente suggerendo mediante comunicazione scritta all'Organo Amministrativo, o alle funzioni aziendali di volta in volta competenti, le correzioni e gli adeguamenti necessari o opportuni.

Il Consiglio di Amministrazione è responsabile, unitamente alle funzioni aziendali eventualmente interessate, dell'aggiornamento del Modello e del suo adeguamento in conseguenza di un mutamento degli assetti organizzativi o dei processi operativi, di significative violazioni del Modello stesso, di integrazioni legislative.

Eventuali modifiche non sostanziali potranno essere appartate all'AD ed oggetto di successiva ratifica da parte del Consiglio di Amministrazione.