Modello di Organizzazione, Gestione e Controllo

ai sensi del Decreto Legislativo
8 giugno 2001, n° 231

PARTE GENERALE

Aggiornato in data 20/1/2025

Matrice delle revisioni:

1ª edizione: 20/12/2023

2ª edizione: 30/10/2024

3ª edizione: 27/11/2024

4ª edizione: 20/1/2025

Indice

Allegato 1	Lista dei reati presupposto *ex* Decreto 231 astrattamente applicabili alla Società
Allegato 2	Rappresentazione grafica dell'Assetto di *Governance* della Società
Allegato 3	Codice Etico di Gruppo
Allegato 4	Flussi informativi da parte delle Strutture aziendali competenti all'OdV
Allegato 5	Procedura per la gestione delle segnalazioni (*Whistleblowing*)

Glossario

AUTORITÀ GIUDIZIARIA	Il complesso degli organi che esercitano la giurisdizione ordinaria, comprendente sia gli organi giudicanti sia quelli requirenti.
CCNL	Contratto Collettivo Nazionale di Lavoro.
CDA o ORGANO AMMINISTRATIVO	Il Consiglio di Amministrazione di FS Security S.p.A.
CODICE ETICO DI GRUPPO	Documento che rappresenta i valori fondamentali e la "carta dei diritti e dei doveri" attraverso cui il Gruppo FS enuncia e chiarisce le proprie responsabilità e impegni etico/sociali verso gli *stakeholder*, interni ed esterni, e detta i principi di comportamento e il relativo sistema sanzionatorio anche ai fini della prevenzione e del contrasto a possibili illeciti. Costituisce parte integrante del presente Modello.
COLLABORATORI	Le persone fisiche che collaborano con FS Security S.p.A., in virtù di un rapporto di collaborazione autonoma, coordinata e continuativa o in altre forme di collaborazione assimilabili di natura non subordinata.
COMITATO ETICO E SEGNALAZIONI	Comitato istituito con il compito di: a) chiarire, mediante pareri consultivi, il significato e l'applicazione del Codice Etico; b) coordinarsi con l'Organismo di Vigilanza nelle attività afferenti alla gestione delle segnalazioni; c) coordinarsi e mantenere flussi informativi con l'Organismo di Vigilanza per gli aspetti di reciproco interesse; d) informare periodicamente il Consiglio di Amministrazione di FS Security sulle attività svolte.
CORPORATE GOVERNANCE	Il complesso dei criteri, dei processi e delle norme di gestione, organizzazione e controllo di FS Security S.p.A., che esprimono l'azione di governo d'impresa.
DECRETO	Il Decreto Legislativo dell'8 giugno 2001, n. 231 e le successive integrazioni e modifiche.
DESTINATARI	I componenti degli Organi Sociali e dell'Organismo di Vigilanza, i Dipendenti, i Collaboratori, i revisori dei conti, i Fornitori, i *Business Partner,* i Consulenti e Promotori Commerciali e, più in generale, tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, intrattengono rapporti con FS Security S.p.A.
DIPENDENTI	Tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato.

DIRIGENTE PREPOSTO	Il Dirigente Preposto alla redazione dei documenti contabili societari di Ferrovie dello Stato S.p.A., nominato conformemente alle previsioni dell'art. 154-*bis* del D.Lgs. n. 58/1998.
ENTE	Tutti gli enti dotati di personalità giuridica, società e associazioni anche prive di personalità giuridica, a cui si applicano le disposizioni di cui al Decreto (*i.e.* società, associazioni, fondazioni, consorzi con attività esterna ecc.).
FORNITORI	Le persone fisiche o giuridiche che eseguono lavori e/o forniscono beni e/o prestano servizi a favore di FS Security S.p.A. e loro collaboratori (da intendersi come soggetti che supportano il fornitore nell'esecuzione dei lavori, erogazione del bene o servizio).
FRAMEWORK ANTI-CORRUPTION	Insieme dei documenti che contengono i principi, indirizzi e le regole in materia di anticorruzione.
FS S.P.A. o FS o HOLDING	Ferrovie dello Stato Italiane S.p.A., con sede legale in Piazza della Croce Rossa, n. 1 - 00161 Roma (RM) e tutte le sue strutture organizzative, Holding del Gruppo FS.
FS SECURITY o SOCIETÀ	FS Security S.p.A.
FUNZIONE COMPLIANCE	Funzione preposta alla gestione e aggiornamento del Modello di *compliance* nella Società, in coerenza con il *framework* definito a livello di Gruppo, e aggiorna il Modello 231 in relazione all'evoluzione della normativa di riferimento e a modifiche organizzative e di processo intervenute, garantendo il monitoraggio dell'andamento delle eventuali azioni correttive.
GRUPPO o GRUPPO FS	Ferrovie dello Stato Italiane S.p.A. e le altre società dalla medesima controllate, direttamente e indirettamente, ai sensi dell'art. 2359, comma 1, numeri 1) e 2) del codice civile.

INCARICATI DI PUBBLICO SERVIZIO	Persona che, pur non essendo un Pubblico Ufficiale con le funzioni proprie di tale *status* (certificative, autorizzative, deliberative), a qualunque titolo esercita un pubblico servizio, incluso quello per un'agenzia nazionale o internazionale, così come definito dalle singole legislazioni nazionali cui il pubblico servizio afferisce. Ai sensi dell'art. 358 c.p. "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*". Possono essere qualificati come Incaricati di pubblico servizio anche i privati che svolgano attività oggettivamente finalizzate al conseguimento di finalità pubblicistiche (ad es. i componenti della commissione di una gara di appalto ad evidenza pubblica indetta dalla Società di cui sono dipendenti), nonché i membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri, assimilati agli incaricati di un pubblico servizio, qualora esercitino funzioni corrispondenti, *ex* art. 322-*bis* c.p.
LINEE GUIDA DI CONFINDUSTRIA	Linee Guida emanate da Confindustria per la predisposizione dei Modelli di organizzazione, gestione e controllo di cui al Decreto, elaborate nel 2002 e il cui ultimo aggiornamento è stato approvato a giugno 2021.
MODELLO DI GESTIONE *ANTI-CORRUPTION*	Modello societario per la prevenzione delle ipotesi delittuose di corruzione e delle condotte corruttive "in senso ampio" (riferite a situazioni di *maladministration*).
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO o MODELLO	Il presente documento, ivi compresi gli allegati, che illustra il Modello di organizzazione, gestione e controllo *ex* D.Lgs. n. 231/2001 vigente in FS Security.
ORGANI SOCIALI	Il Consiglio di Amministrazione della Società, il Collegio Sindacale e i loro componenti.
ORGANISMO DI VIGILANZA o ODV	Organismo previsto dall'art. 6 del Decreto, dotato di autonomi poteri di iniziativa e di controllo e avente il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché di curarne l'aggiornamento.

***POLICY ANTI-CORRUPTION* GRUPPO FS**	*Policy* obbligatoria per tutte le Società del Gruppo, italiane ed estere, che uniforma ed integra in un quadro unitario per tutte le Società del Gruppo FS, italiane ed estere, i princìpi e i presìdi di prevenzione e contrasto alla corruzione, individuando le regole e i comportamenti che tutti i destinatari, compresi i terzi esterni al Gruppo con cui si instaurano relazioni professionali e d'affari, sono chiamati ad applicare.
PROCEDURE AMMINISTRATIVO CONTABILI o PAC	Procedure amministrativo-contabili, emanate a cura del Dirigente Preposto di FS ai sensi della L. n. 262/2005, volte a regolamentare le attività e i controlli amministrativo-contabili sui processi collegati all'informativa economica e finanziaria al fine di prevenire i rischi di una errata/non corretta rappresentazione del bilancio di esercizio, del bilancio consolidato e delle altre comunicazioni economiche e finanziarie destinate agli *stakeholder*.
***PROCESS OWNER* 231**	Responsabile di uno o più aree a rischio reato/processi mappati all'interno della Società nell'ambito del *risk assessment* 231.
PUBBLICA AMMINISTRAZIONE	Ai fini del Modello, si considera Pubblica Amministrazione: a) Soggetti, ivi comprese le persone giuridiche, nazionali, centrali e locali, in Italia o all'estero, sovranazionali e internazionali, che operano per il perseguimento di interessi pubblicistici e che svolgono attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi; b) Autorità di Vigilanza, Regolazione e Controllo, ossia autorità amministrative indipendenti, istituite per legge, dotate di autonomia, indipendenza e imparzialità, la cui missione è la tutela di interessi pubblici e della collettività in specifici settori economici e di rilevanza sociale (ad es. ART, AGCM, ANAC, Garante per la protezione dei dati personali, etc.); c) Pubblici Ufficiali; d) Incaricati di un Pubblico Servizio. Ai fini del presente documento si considerano i soggetti che possono essere qualificati Pubblica Amministrazione in base alla vigente legislazione ed alle correnti interpretazioni dottrinali e giurisprudenziali.

PUBBLICI UFFICIALI	Persone che esercitano una pubblica funzione legislativa, amministrativa o giudiziaria, indipendentemente dal fatto che la funzione derivi da nomina, elezione o successione, nonché soggetti assimilati ai sensi della normativa nazionale applicabile. Ai sensi dell'art. 357 c.p. "*sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*", nonché i membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri, assimilati ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, *ex* art. 322-*bis* c.p.
SISTEMA NORMATIVO INTERNO	Il complesso di disposizioni, comunicazioni, istruzioni, procedure, linee guida e *policy*, societari e di Gruppo, che regolamenta le attività aziendali.
STAKEHOLDER	Soggetto (o gruppo di soggetti) che, in quanto portatore di un interesse rispetto all'impresa, direttamente o indirettamente, può influenzare le attività della Società o esserne influenzato.
SISTEMA DI CONTROLLO E GESTIONE DEI RISCHI AZIENDALE o SCIGR	Insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società.
SLA	*Service Level Agreement*. Strumenti contrattuali attraverso i quali si definiscono le metriche di servizio che devono essere rispettate da un fornitore di servizi nei confronti dei propri clienti/utenti.
VERTICE AZIENDALE	Il Presidente del Consiglio di Amministrazione e l'Amministratore Delegato della Società.

1. IL DECRETO LEGISLATIVO N. 231/2001

1.1. IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DEGLI ENTI

Il Decreto Legislativo n. 231 dell'8 giugno 2001, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito anche il "**Decreto**"), ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa a carico degli enti dotati di personalità giuridica, delle società e delle associazioni anche prive di personalità giuridica[1] (di seguito anche "**Ente/i**"), che va ad aggiungersi alla responsabilità della persona fisica che ha commesso materialmente i reati e che mira a coinvolgere, nella punizione degli stessi, gli Enti nel cui interesse o vantaggio tali reati siano stati compiuti. Dall'entrata in vigore del Decreto, al pari delle persone fisiche, gli Enti possono essere quindi soggetti a un procedimento penale e possono essere destinatari di sanzioni, pecuniarie e interdittive.

FS Security S.p.A. rientra tra i destinatari della disciplina prevista dal Decreto.

La responsabilità amministrativa prevista dal Decreto può configurarsi a fronte della commissione, in Italia o all'estero[2], da parte di determinati soggetti, di alcuni reati specificamente indicati nel Decreto stesso, nell'interesse o a vantaggio dell'Ente.

I presupposti sulla base dei quali l'Ente può essere ritenuto responsabile ai sensi del Decreto, includono:

1) che sia stato commesso un reato espressamente previsto nel catalogo dei c.d. **reati presupposto** indicati tassativamente nello stesso Decreto (artt. 24 e ss.)[3]. A decorrere dall'emanazione del Decreto, il catalogo dei

---

[1] Con esclusione dello Stato, degli enti pubblici territoriali, degli enti che svolgono funzioni di rilievo costituzionale e degli altri enti pubblici non economici.

[2] Al verificarsi di certe condizioni, l'art. 4 del Decreto prevede che gli enti aventi la sede principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero, purché per gli stessi non proceda lo Stato in cui è stato commesso il reato. I presupposti sui quali si fonda la responsabilità della società per i reati commessi all'estero sono i seguenti:

a) il reato deve essere commesso da un soggetto funzionalmente legato alla società (soggetto apicale o sottoposto);

b) la società deve avere la propria sede principale nel territorio dello Stato italiano;

c) la società può rispondere solo nei casi e alle condizioni previste dalla normativa italiana;

d) lo Stato del luogo in cui è stato commesso il fatto non proceda in autonomia nel perseguire il reato.

Vale la pena evidenziare che tali norme si applicano esclusivamente nel caso in cui il reato sia stato commesso interamente all'estero, in quanto, per le condotte criminose avvenute anche solo in parte in Italia, in base al principio di territorialità ex art. 6 del Codice penale "*il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione*".

[3] Si riportano sinteticamente le tipologie di reato attualmente previste dal Decreto:

- Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o 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, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (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*);
- Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-*quater*);
- Pratiche di mutilazione degli organi genitali femminili (Art. 25-*quater*.1);
- Delitti contro la personalità individuale (Art. 25-*quinquies*);
- Reati di abuso di mercato (Art. 25-*sexies*);
- Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-*septies*);

reati presupposto è stato negli anni integrato con nuove ipotesi criminose introdotte nel Decreto o in normativa speciale.

L'**Allegato 1** contiene la lista completa e aggiornata di tutti i reati per i quali gli Enti possono essere chiamati a rispondere, con indicazione delle fattispecie di reato ritenute applicabili a FS Security S.p.A., nonché il testo di ciascuno degli articoli rilevanti del Decreto seguiti dal testo dei vari reati presupposto riferibili a FS Security S.p.A. e indicati nella Parte Speciale del Modello;

2) che il reato sia stato commesso da persone dell'Ente o funzionalmente legate allo stesso. In particolare, si può trattare di:

   i. **soggetti in posizione apicale**, ovvero i soggetti che rivestono funzioni di rappresentanza, amministrazione o direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, ovvero persone che esercitano, anche in via di fatto, la gestione e il controllo dello stesso;

   ii. **soggetti in posizione subordinata**, ovvero coloro i quali sono sottoposti ai poteri di direzione o vigilanza dei soggetti apicali.

   Il Decreto non richiede che tra l'Ente e la persona fisica sussista un rapporto di lavoro subordinato, ma è sufficiente la sottoposizione alla direzione e coordinamento di un apicale, il che può facilmente accadere anche in relazione a numerose categorie di collaboratori esterni, ivi compresi gli agenti, i distributori, *partner* commerciali, etc.

   La responsabilità dell'Ente può, infine, sussistere anche laddove il dipendente autore dell'illecito abbia concorso nella sua realizzazione con altri soggetti estranei all'organizzazione dell'Ente medesimo. Diversi possono essere i settori di *business* o le occasioni nei quali può annidarsi il rischio del coinvolgimento in concorso del dipendente e, quindi, ricorrendone i presupposti, di interesse e/o vantaggio dell'Ente. Rilevano, in particolare, i rapporti connessi agli appalti e, in generale, i contratti di *partnership*.

   Il concorso nel reato può rilevare, peraltro, ai fini della responsabilità dell'Ente anche nell'ipotesi del cd. concorso dell'*extraneus* nel reato "proprio". Nella specie, la responsabilità in concorso può ricorrere laddove l'esponente aziendale, consapevole della particolare qualifica soggettiva della controparte (es. pubblico ufficiale, sindaco, *etc.*), concorra nella condotta a quest'ultimo ascrivibile (es. abuso d'ufficio). In tale caso, l'*extraneus* risponderà in concorso del medesimo reato previsto a carico del soggetto qualificato;

- 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 (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*);
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-*duodecies*);
- Razzismo e xenofobia (Art. 25-*terdecies*);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-*quaterdecies*);
- Reati Tributari (Art. 25-*quinquiesdecies*);
- Contrabbando (Art. 25-*sexiesdecies*);
- Delitti contro il patrimonio culturale (Art. 25-*septiesdecies*);
- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-*duodevicies*);
- Responsabilità degli enti che operano nell'ambito della filiera degli oli vergini di oliva, per gli illeciti amministrativi dipendenti da reato (L. n. 9/2013);
- Reati transnazionali (L. n. 146/2006).

3) che la condotta criminosa sia realizzata nell'**interesse** o a **vantaggio** dell'Ente. Quest'ultimo, quindi, non risponde dell'illecito se le persone indicate al precedente punto 2) hanno agito nell'interesse esclusivo proprio o di terzi.

In merito ai menzionati criteri dell'interesse e del vantaggio, la giurisprudenza ha evidenziato che l'interesse dell'Ente ricorre quando il soggetto agente abbia commesso il reato presupposto con la finalità di favorire l'Ente di appartenenza, a prescindere dal raggiungimento o meno di tale obiettivo. Si tratta di un criterio da valutarsi *ex ante* al momento della realizzazione della condotta. L'interesse dell'autore del reato può coincidere con quello dell'Ente ma la responsabilità dello stesso può sussistere anche quando, perseguendo il proprio autonomo interesse, l'agente obiettivamente realizzi (ovvero la sua condotta illecita appaia *ex ante* in grado di realizzare) quello proprio dell'Ente.

Il vantaggio, invece, ha una connotazione essenzialmente oggettiva e consiste nel beneficio (soprattutto patrimoniale e da valutarsi sempre *ex post* rispetto alla realizzazione dello stesso) che l'Ente ha tratto, dal compimento del reato. Per quanto riguarda i reati colposi ricompresi nel catalogo dei reati presupposto del Decreto, la mancanza di volontà del soggetto agente rispetto all'evento conseguente alla condotta criminosa (ovvero la mancanza di volontà del fatto offensivo che si esaurisce nella condotta, nei casi di reati colposi di mera condotta), implicita nel reato stesso, mal si concilia con i predetti criteri di imputazione per gli Enti, *i.e.* il perseguimento dell'interesse o del vantaggio dell'Ente. Sul punto, oltre al costante dibattito dottrinale, si è pronunciata la Corte di Cassazione[4], la quale ha stabilito che, nei casi di reato colposo, i criteri di imputazione oggettiva rappresentati dall'interesse e dal vantaggio dell'Ente devono essere riferiti alla condotta del soggetto agente (autore/persona fisica) e non all'evento (ove previsto dalla fattispecie penale). Devono essere riferiti, dunque, alle circostanze di fatto che hanno dato origine al suddetto evento.

L'ascrizione della responsabilità *ex* Decreto in capo alla società avverrà solo quando l'autore dell'illecito, nel perpetrare la condotta colposa, abbia "*violato la normativa cautelare con il consapevole intento di conseguire un risparmio di spesa per l'ente, indipendentemente dal suo effettivo raggiungimento (criterio dell'interesse dell'Ente), e/o qualora l'autore del reato abbia violato (…) le norme (...) ricavandone oggettivamente un qualche vantaggio per l'ente, sotto forma di risparmio di spesa (e/o tempi) o di massimizzazione della produzione, indipendentemente dalla volontà di ottenere il vantaggio stesso (criterio del vantaggio dell'Ente)*".

Il Decreto inoltre sancisce il principio di autonomia della responsabilità dell'Ente da quella della persona fisica, precisando che la responsabilità dell'Ente sussiste anche quando:

i. l'autore del reato non è stato identificato o non è imputabile;

ii. il reato si estingue per una causa diversa dall'amnistia.

1.2. LE SANZIONI PREVISTE DAL DECRETO

Le sanzioni previste dal Decreto per l'Ente sono le seguenti:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca del profitto che l'Ente ha tratto dal reato (anche nella forma per equivalente);
- pubblicazione della sentenza (disposta quando nei confronti dell'Ente viene applicata una sanzione interdittiva).

Ai sensi dell'art. 10 del Decreto, le **sanzioni pecuniarie** vengono sempre applicate e si determinano attraverso un sistema basato su "quote".

[4] Cass. Pen., Sez. IV, sentenza 9/12/2019, n. 49775. *Ex multis*, in tema di responsabilità degli enti derivante da reati colposi di evento in violazione della normativa antinfortunistica, si vedano Cass. pen., sez. IV, 28/10/2019, n. 43656, Cass. pen. Sez. IV Sent., 23/05/2018, n. 38363 e Cass. Pen. Sez. IV Sent., 16/04/2018, n. 16713.

In relazione a ciascun reato viene, infatti, stabilita una quota, che deve necessariamente rispettare un *quantum* minimo e massimo (che si assesta tra le 100 e le 1.000 quote), ciascuna delle quali può, a sua volta, avere un valore che oscilla dai 258,00 euro ai 1.549,00 euro.

Il giudice è, quindi, chiamato a commisurare la sanzione pecuniaria al caso concreto, dovendo determinare per ogni ipotesi di responsabilità della società sia il numero delle quote da applicare che il valore di ogni singola quota, potendo in concreto graduare la sanzione da una soglia minima di 25.800,00 euro ed una massima di 1.549.000,00 euro.

Nella commisurazione della sanzione il giudice determina il numero delle quote tenendo 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.

Per quanto riguarda, invece, l'importo da attribuire a ciascuna quota assumono una rilevanza peculiare le condizioni economiche e patrimoniali dell'Ente, e ciò allo scopo di assicurare l'efficacia della sanzione.

È prevista la riduzione della sanzione della metà (e comunque non superiore a 103.291,00 euro) se:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e la società non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità.

È prevista, inoltre, la riduzione della sanzione da un terzo alla metà se:

- la società ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato, ovvero si sia comunque efficacemente adoperata in tal senso;
- è stato adottato e reso operativo un Modello idoneo a prevenire reati della specie di quello verificatosi.

Nel caso in cui concorrano entrambe le condizioni sopra previste, la sanzione è ridotta dalla metà ai due terzi. In ogni caso, la sanzione pecuniaria non può essere inferiore a 10.329,00 euro.

Le principali **sanzioni interdittive** consistono in:

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

Diversamente dalle sanzioni pecuniarie, le sanzioni interdittive si applicano in relazione ai soli reati per i quali sono espressamente previste, qualora ricorra almeno una delle seguenti condizioni:

a) 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 e vigilanza, e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

b) in caso di reiterazione degli illeciti.

Le sanzioni interdittive possono essere applicate congiuntamente e hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'Ente. Il giudice ne determina il tipo e la durata (da tre mesi a due anni, ad eccezione di alcuni illeciti previsti dall'art. 25 comma 5 del Decreto, per i quali le sanzioni interdittive possono essere applicate per una durata massima di sette anni), sulla base dei criteri indicati con riferimento alle sanzioni pecuniarie, tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso.

Come anticipato, ai sensi dell'art. 25 del Decreto, inerente ai reati di *peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio* e modificato dal Legge 9 gennaio 2019, n. 3, nei casi di condanna per uno dei delitti indicati nei commi 2 e 3 del medesimo articolo (*i.e.* gli artt. 317, 319, 319-*ter*, comma 1, 319, aggravato ai sensi dell'articolo 319-*bis* quando dal fatto l'ente abbia conseguito un profitto di rilevante entità, 319-*ter*, comma 2, 319-*quater* e 321, 322, commi 2 e 4 del codice penale), le sanzioni interdittive previste dal Decreto si applicano per una durata "*non inferiore a quattro anni e non superiore a sette anni*" ove il reato presupposto sia stato commesso da un soggetto apicale, ovvero per una durata "*non inferiore a due anni e non superiore a quattro anni*" ove il reato presupposto sia stato, invece, commesso da un soggetto sottoposto alla direzione e controllo del soggetto apicale.

D'altro canto, sempre ai sensi del novellato art. 25 del Decreto, se prima della sentenza di primo grado l'Ente si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili, ovvero per il sequestro delle somme o altre utilità trasferite, e abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi, le sanzioni interdittive hanno la durata stabilita dall'articolo 13, comma 2 (ovvero non inferiore a tre mesi e non superiore a due anni).

Ai sensi dell'art. 16 del Decreto, le sanzioni dell'interdizione dell'esercizio dell'attività, del divieto di contrarre con la Pubblica Amministrazione e del divieto di pubblicizzare beni o servizi, in alcuni casi,[5] possono essere applicate in via definitiva.

In luogo dell'applicazione di una misura interdittiva che comporti l'interruzione dell'attività, il Giudice può nominare un commissario giudiziale ai sensi dell'art. 15 del Decreto per un periodo pari alla durata della misura che sarebbe stata applicata, qualora l'Ente oggetto del procedimento svolga un pubblico servizio la cui interruzione possa determinare un grave pregiudizio per la collettività o nel caso la medesima interruzione possa provocare rilevanti ripercussioni sull'occupazione.

Qualora sussistano gravi indizi di colpevolezza o vi siano fondati e specifici elementi che fanno ritenere concreto il rischio di reiterazione del reato, il giudice può disporre l'applicazione delle misure interdittive di cui sopra anche in via cautelare.

L'art. 17 del Decreto stabilisce, invece, che le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni:

a) l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;

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

c) l'Ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Il Decreto prevede, inoltre, all'art. 23, uno specifico reato riferito all'eventuale inosservanza delle sanzioni interdittive disposte nei confronti dell'Ente, ossia di trasgressione agli obblighi o ai divieti inerenti a tali sanzioni o misure. Ove tale reato sia commesso da un esponente aziendale nell'interesse o a vantaggio dell'Ente, il Decreto prevede la responsabilità amministrativa dell'Ente medesimo, con applicazione delle sanzioni amministrative pecuniarie ed eventualmente delle sanzioni interdittive.

Il Decreto prevede, ancora, che nei confronti dell'Ente sia sempre disposta, con la sentenza di condanna, la **confisca** del prezzo o del profitto che l'Ente ha tratto dal reato (salvo che per la parte che può essere restituita al danneggiato). Quando non è possibile eseguire la confisca sul prezzo o sul profitto del reato, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore ad essi equivalente (cd. confisca per equivalente).

[5] Se l'Ente ha tratto dal reato un profitto di rilevante entità e/o è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni e/o l'Ente stesso o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità.

La **pubblicazione della sentenza**, invece, può essere disposta quando nei confronti della società viene applicata una sanzione interdittiva.

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

- il **sequestro preventivo** delle cose di cui è consentita la confisca (Art. 53 del Decreto);
- 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 del Decreto).

1.3. CONDIZIONI ESIMENTI DALLA RESPONSABILITÀ AMMINISTRATIVA

Il Decreto prevede forme specifiche di esonero dalla responsabilità amministrativa dell'Ente per i reati commessi nel suo interesse o a suo vantaggio. I casi di esonero della responsabilità dell'Ente variano a seconda che il reato presupposto sia stato commesso da soggetti che rivestono posizioni apicali oppure da soggetti sottoposti all'altrui direzione e vigilanza (soggetti in posizione subordinata).

In particolare, nel caso di reati commessi da soggetti in posizione apicale l'art. 6 prevede l'esonero qualora l'Ente stesso dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di curarne e proporne l'aggiornamento sia stato affidato ad un Organismo di Vigilanza dell'Ente, dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il suddetto Modello;

d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Inoltre, a seguito delle modifiche normative intervenute con il Decreto Legislativo n. 24 del 10 marzo 2023 ("*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*") i Modelli devono espressamente contenere la disciplina del *Whistleblowing*, così come disposto dalla predetta norma.

Costituiscono, in particolare, ulteriori requisiti del Modello:

- l'istituzione di canali di segnalazione interna;
- la previsione del divieto di ritorsione;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

Per quanto concerne i soggetti in posizione subordinata, l'art. 7 prevede la responsabilità dell'Ente solo nel caso in cui la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. È esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto, inoltre, nel delineare il contenuto minimo del modello di organizzazione, gestione e controllo, prevede che tale documento debba:

a) individuare le attività nel cui ambito esiste la possibilità che siano commessi i reati presupposto;

b) prevedere specifici protocolli diretti 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 impedire la commissione di tali reati;

d) prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;

e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Il Modello deve inoltre prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

Lo stesso Decreto prevede che i Modelli possano essere adottati, garantendo le esigenze di cui sopra, tenendo conto dei codici di comportamento redatti dalle associazioni rappresentative di categoria, comunicati al Ministero della Giustizia, nel caso specifico da Confindustria nelle "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo *ex* D.lgs. 231/2001" (le "**Linee Guida di Confindustria**").

La mera adozione di un Modello non è sufficiente ad escludere la responsabilità dell'Ente, essendo necessario che il Modello sia effettivamente ed efficacemente attuato. In particolare, l'efficace attuazione del Modello richiede, in aggiunta alla concreta applicazione del sistema disciplinare, anche una verifica periodica sul Modello stesso e l'aggiornamento/modifica dello stesso nel caso siano scoperte significative violazioni delle sue prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività dell'Ente.

2. LA SOCIETÀ E IL SUO SISTEMA ORGANIZZATIVO

FS Security, società con socio unico soggetta alla direzione e coordinamento di Ferrovie dello Stato S.p.A., ha per oggetto principale la prestazione di servizi di sicurezza e vigilanza privata.

La Società, come previsto dal suo Statuto, può svolgere, in via esemplificativa e non esaustiva, le seguenti attività:

a) servizi di sicurezza sussidiaria di cui al D.M. n. 154/2009 e s.m.i.;

b) attività di progettazione e consulenza in materia di sicurezza;

c) servizi di controllo, vigilanza, custodia e guardiania di beni mobili ed immobili e misure di gestione dei flussi di persone e dei mezzi autorizzati all'accesso in aree, impianti, stabili, strutture aperte al pubblico e mezzi di trasporto, anche tramite sistemi e impianti di videosorveglianza, antintrusione e allarme;

d) servizi specialistici in materia di sicurezza del patrimonio;

e) attività di formazione nel settore della sicurezza;

f) ogni altra attività strumentale, complementare o connessa a quelle di cui sopra.

La Società può inoltre fornire servizi di controllo e monitoraggio delle aree di cantiere.

FS Security presta i propri servizi prevalentemente ma non esclusivamente nei confronti delle società del Gruppo FS.

2.1. IL MODELLO DI GOVERNANCE

A seguito dell'adozione, da parte dell'Amministratore Unico pro tempore della Società, con determina del 9 febbraio 2023, del Regolamento del Gruppo Ferrovie dello Stato, FS Security S.p.A. ha confermato, con Comunicazione Organizzativa n. 1/AU del 15 marzo 2023, "Atto di recepimento del Modello di Governance di Gruppo", l'adozione della Disposizione di Gruppo n. 304/AD del 18 maggio 2022, "Modello di Governance del Gruppo FS Italiane", emanata da FS S.p.A.

Il Modello di Governance del Gruppo è impostato con un'articolazione funzionale a realizzare il progetto strategico unitario proprio di un gruppo che opera in più settori tra loro complementari e ad assicurare, al contempo, l'autonomia della gestione di ciascun settore e dell'operatività delle società controllate.

Nell'ambito del Modello di Governance, a FS è attribuito il ruolo di direzione e coordinamento nei confronti delle Società Capogruppo di settore e delle altre Società controllate previste dal Regolamento di Gruppo, con l'obiettivo di svolgere funzioni di indirizzo strategico generale e di coordinamento attuativo e finanziario del comune disegno imprenditoriale del Gruppo[6].

Inoltre, relativamente ai processi trasversali o di *staff*, FS esercita il proprio ruolo anche tramite una gestione per "Famiglie Professionali"[7], che attribuisce a ciascuna di queste ultime una responsabilità diretta a livello di Gruppo sul funzionamento efficace ed efficiente delle funzioni di rispettiva competenza, al fine di favorire lo sviluppo e la valorizzazione di sinergie e di presidiare in maniera unitaria e omogenea lo sviluppo delle competenze e conoscenze, anche attraverso la condivisione di modelli di lavoro e delle esperienze e l'ordinata compartecipazione al *know-how* disponibile nel Gruppo.

Le funzioni delle Società del Gruppo che afferiscono alle famiglie professionali sono dunque soggette a un doppio coordinamento:

- "di famiglia professionale", da parte dei *Process Owner* di Gruppo di FS[8], che effettuano indirizzo e coordinamento della famiglia professionale di riferimento;
- "operativo", da parte dell'Amministratore Delegato della rispettiva società, in coerenza con i poteri e deleghe attribuiti.

FS Security adotta una struttura di *corporate governance* articolata secondo il sistema tradizionale: il sistema di *governance* prevede che l'Assemblea nomini un Consiglio di Amministrazione, attualmente composto da cinque amministratori, e un Collegio Sindacale, composto da tre sindaci effettivi e due supplenti. La revisione legale è esercitata da una Società di Revisione incaricata dall'Assemblea su proposta motivata del Collegio Sindacale.

Il Consiglio di Amministrazione, i cui componenti, scelti secondo criteri di professionalità e competenza tra persone di comprovata esperienza, durano in carica per il periodo di tempo che determina l'Assemblea all'atto della loro nomina, che non può essere superiore a tre esercizi, elegge tra i suoi membri il Presidente, ai sensi dell'art. 2380-*bis* c.c., e nomina l'Amministratore Delegato.

L'Allegato 2 riporta una rappresentazione grafica dell'Assetto di *Governance* di FS Security.

2.2. LA STRUTTURA ORGANIZZATIVA

La struttura organizzativa di FS Security si articola in Strutture macro in Strutture micro[9]. L'assetto organizzativo, le missioni e le aree di responsabilità delle singole Strutture aziendali sono definiti e individuati mediante apposite Disposizioni Organizzative, nel rispetto del principio di segregazione delle funzioni, così come degli altri principi di *compliance* e di *governance*.

La formalizzazione, aggiornamento, diffusione, pubblicazione sulla *intranet* e archiviazione dei documenti organizzativi vengono assicurati dalla struttura competente in materia di organizzazione e processi.

---

[6] L'attività di direzione e coordinamento di FS riguarda elettivamente i seguenti ambiti: i) strategie generali d'impresa e investimento; ii) finanza; iii) presidio e sviluppo dei mercati esteri; iv) modifiche del perimetro di *business*; v) innovazione e sviluppo tecnologico e digitale; vi) *governance* e assetti societari; vi) linee guida metodologiche per i modelli di controllo interno e di gestione dei rischi; vii) macrodisegni organizzativi; viii) relazioni istituzionali; ix) modelli di *compliance* normativa (non tecnico-operativa o ambientale); ix) modelli di *budget*, controllo, pianificazione e processi amministrativi e di *reporting*; x) politiche di gestione/sviluppo delle risorse umane di Gruppo; xi) comunicazione e immagine.

[7] Le famiglie professionali individuate dall'Allegato 3 al citato Regolamento di Gruppo sono: i) Strategie e Sostenibilità; ii) *International*; iii) *Technology, Innovation & Digital*; iv) *Legal & Compliance*; v) *Security*; vi) *Risk Management*; vii) Comunicazione & Immagine; viii) Risorse Umane e Organizzazione; ix) Affari Istituzionali e Regolatori; x) Amministrazione, Pianificazione, Controllo di Gestione e Fiscale; xi) *Finance*; xii) *Internal Audit;* xiii) *Anti-Corruption;* xiv) *Procurement*.

[8] Si intendono i Responsabili di primo riporto del Presidente/AD di FS, come individuati nelle relative disposizioni organizzative.

[9] Sono definite "macro" le Strutture affidate a dirigenti o a quadri in sviluppo e "micro" quelle affidate a quadri.

2.3. CONTRATTI DI SERVIZI

La Società ha stipulato contratti di servizi per la regolamentazione dei rapporti con altre società facenti parte del Gruppo, che forniscono servizi in favore della stessa, prevedendone l'esternalizzazione totale o parziale. Tali contratti prevedono:

- la definizione puntuale delle attività prestate, le modalità di esecuzione delle stesse ed i relativi corrispettivi;
- la nomina di un referente responsabile della gestione del contratto;
- che il fornitore dia adeguata esecuzione alle attività esternalizzate nel rispetto della normativa vigente e delle disposizioni della Società;
- che il fornitore informi tempestivamente la Società di qualsiasi fatto che possa incidere in maniera rilevante sulla propria capacità di eseguire le attività esternalizzate in conformità alla normativa vigente e in maniera efficiente ed efficace;
- che il fornitore garantisca la riservatezza dei dati relativi alla Società.

Relativamente a tali rapporti, rimane sotto la responsabilità propria della Società, nel rispetto della legge applicabile e delle prescrizioni del presente Modello, la verifica dell'adempimento degli obblighi contrattuali e del corretto esercizio dei correlati poteri eventualmente delegati.

In particolare, FS Security ha affidato a Ferservizi S.p.A., il "Centro Servizi Integrato" del Gruppo FS, i seguenti servizi: i) servizi di acquisti trasversali; ii) servizio di gestione acquisti *on line* sul sistema di "*e-requisitioning"*; iii) servizio di acquisti a richiesta; iv) servizio di gestione della banca dati di Gruppo; v) acquisti specifici; vi) contabilità fornitori; vii) contabilità clienti; viii) servizi integrati di contabilità generale; ix) adempimenti fiscali; x) assistenza fiscale; xi) gestione del personale amministrato; xii) manutenzione continuativa; xiii) pulizia continuativa; xiv) ricevimento e accoglienza Villa Patrizi; xv) *business travel*; xvi) gestione ristorazione; xii) gestione *smart card* multiservizi; xiii) prestazioni a richiesta (ASFB).

Inoltre, la Società ha affidato a FS Technology, *Digital factory* centralizzata del Gruppo, i servizi di *Information and Communication Technology*.

2.4. IL SISTEMA DI DELEGHE E PROCURE

Il Consiglio di Amministrazione e l'Amministratore Delegato conferiscono e approvano formalmente - in base alla ripartizione dei poteri del Consiglio di Amministrazione, Presidente e Amministratore Delegato deliberata dal Consiglio di Amministrazione di FS Security - le deleghe e i poteri di firma assegnati in coerenza con le responsabilità organizzative e gestionali definite, con una puntuale indicazione delle soglie di approvazione delle spese.

Nell'ambito del proprio sistema organizzativo, la Società ha adottato un sistema di deleghe e procure volto a strutturare, in modo analitico e coerente con la realtà organizzativa, lo svolgimento delle attività societarie.

Nelle deleghe e procure vigenti sono, tra l'altro, individuati e fissati, in modo coerente con la posizione organizzativa e il livello gerarchico del destinatario delle stesse:

- il livello di autonomia,
- il potere di rappresentanza,
- i limiti di spesa assegnati,
- nei limiti di quanto necessario all'espletamento dei compiti e delle mansioni oggetto di delega.

3. IL MODELLO ADOTTATO DA FS SECURITY

3.1. L'ADOZIONE DEL MODELLO

FS Security, al fine di assicurare condizioni sempre maggiori di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali e sensibili alle esigenze di *compliance* aziendale, ha ritenuto opportuno procedere all'adozione di un Modello di Organizzazione, Gestione e Controllo ex D.lgs. n. 231/2001 (di seguito anche "Modello").

Il Modello si ispira ai principi ed alle best practice più avanzate nel campo della lotta alla criminalità d'impresa e si uniforma ai principi di controllo elaborati dalle Linee Guida di Confindustria.

Nel presente documento, FS Security ha proceduto all'adozione del Modello al fine di renderlo rispondente alla situazione aziendale di FS Security, alle novità legislative, all'evoluzione della giurisprudenza e delle best practice nazionali ed internazionali.

Il presente Modello entra in vigore a decorrere dalla data della sua approvazione da parte del Consiglio di Amministrazione di FS Security.

La Società avrà cura di procedere, ove necessario, all'aggiornamento del Modello, al fine di renderlo rispondente alla situazione aziendale, alle novità legislative, all'evoluzione della giurisprudenza e delle *best practice* nazionali e internazionali.

Il Modello è rivolto a tutti i Destinatari e le eventuali violazioni dello stesso potranno dar luogo all'applicazione di specifiche misure, così come previsto al capitolo 7 della presente Parte Generale.

3.2. METODOLOGIA

La costruzione del presente Modello si è articolata nelle seguenti fasi:

1. **Individuazione e analisi dei processi e attività** di potenziale rilevanza ai fini della commissione dei reati presupposto richiamati dal Decreto e **mappatura dei rischi-reato**, con annessa individuazione:
    i. dei processi e attività a rischio;
    ii. delle Strutture aziendali che presidiano tali attività;
    iii. delle famiglie e fattispecie di reato rilevanti *ex* Decreto potenzialmente applicabili allo specifico contesto societario;
    iv. delle ipotetiche modalità di commissione dei reati *ex* Decreto;
    v. dei presidi di controllo esistenti.

    Tale analisi è riportata all'interno di specifiche Schede di *Risk Assessment*.

    Le attività di cui sopra sono state svolte all'esito di una preliminare analisi e comprensione dell'assetto di *governance*, organizzativo e operativo della Società, nonché della storia pregressa di FS Security, mediante l'esame della documentazione societaria e lo svolgimento di interviste con i referenti aziendali e le figure interne alla Società rilevanti ai fini dell'analisi.

    Si è altresì tenuto conto delle possibili modalità attuative concrete dei reati nei diversi processi aziendali, così da individuare quali condotte potrebbero astrattamente compromettere gli obiettivi indicati dal Decreto. L'analisi dei rischi ha ricompreso una valutazione in merito alle modalità con cui le fattispecie di reato potrebbero essere attuate rispetto al contesto operativo interno (struttura organizzativa, articolazione territoriale, dimensioni, ecc.) ed esterno (settore economico, area geografica, ecc.) in cui opera FS Security, nonché una verifica dei singoli reati ipoteticamente collegabili alle specifiche attività della Società considerate a rischio.

2. ***Gap analysis*** del sistema di controllo interno tramite:

   i. l'analisi del disegno del sistema di controlli esistenti ("*as is*") a presidio dei processi e attività a rischio identificati;

   ii. la comparazione del sistema di controllo esistente rispetto ai requisiti identificati nella metodologia applicata e nelle Linee Guida/*Best Practice* di riferimento e la contestuale valutazione di adeguatezza degli stessi;

   iii. la definizione di un piano di azioni da implementare per il rafforzamento del sistema di controllo interno in ottica di miglioramento continuo del Modello per la prevenzione dei rischi-reato di cui al Decreto, anche tramite la modifica, integrazione e/o evoluzione del *corpus* normativo aziendale.

3.3. STRUTTURA DEL MODELLO

Il Modello di FS Security si fonda su un sistema strutturato e organico di principi, procedure ed attività di controllo che nella sostanza:

- individua i processi e le attività a rischio-reato nell'attività aziendale, nel cui ambito si ritiene sussista la possibilità che siano commessi i reati previsti dal Decreto;
- definisce un sistema normativo interno diretto a regolare i processi attraverso i quali le decisioni di FS Security vengono adottate e a dettare regole di comportamento nell'ottica di prevenzione dei rischi/reato attraverso:
  a) il Codice Etico di Gruppo, che fissa i valori ed i principi di riferimento;
  b) i protocolli contenenti principi di prevenzione e di controllo collegati ai processi e attività mappati come "a rischio";
  c) procedure formalizzate, tese a disciplinare in dettaglio le modalità operative nei processi e attività sensibili;
  d) un sistema di deleghe di funzioni 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;
  e) la *Policy Anti-Corruption* del Gruppo FS, che rappresenta un apparato organico di strumenti e regole comportamentali per la prevenzione e il contenimento del rischio corruzione.
- determina una struttura organizzativa coerente volta a ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando il principio di segregazione delle funzioni e assicurando che gli assetti della struttura organizzativa definiti siano realmente attuati;
- 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 curarne e proporne l'aggiornamento.

Pertanto, in aggiunta all'adozione del Modello, FS Security ha definito e adottato, con riferimento ai processi e attività sensibili, un sistema normativo interno che identifica i principali controlli/procedure, disposizioni e norme comportamentali, adottate dalla Società al fine di prevenire e minimizzare il rischio di commissione di reati, volte a regolare e rendere verificabili le fasi rilevanti dei processi e attività sensibili individuate in relazione ai reati rilevanti ai sensi del Decreto.

Tali documenti sono adeguatamente diffusi all'interno di FS Security attraverso specifici meccanismi di comunicazione interna il loro inoltro a liste di Destinatari interessati, nonché attraverso programmi di informazione/formazione *ad hoc*, al fine di garantire la conoscibilità e la piena comprensione degli stessi.

FS Security, per garantire l'effettività e un'efficace attuazione di quanto previsto nel Modello, ha altresì adottato un sistema di sanzioni, disciplinari o contrattuali, rivolto ai Destinatari.

Il Modello è suddiviso in una **Parte Generale** e in una **Parte Speciale**.

Nella **Parte Generale**, dopo un sintetico richiamo alla normativa contenuta nel Decreto, vengono riportate la natura, la metodologia e la struttura del Modello, i suoi elementi fondamentali, gli allegati, compreso il Codice Etico, vengono indicati i Destinatari, nonché il sistema di controllo interno e di gestione dei rischi adottato da FS Security di cui il presente Modello è parte integrante e vengono infine illustrate le componenti essenziali del Modello, con particolare riferimento all'OdV (con indicazione della sua struttura e funzionamento), al sistema disciplinare e alle misure da adottare in caso di mancata osservanza delle prescrizioni del Modello, alla formazione del personale e alla diffusione del Modello nel contesto aziendale.

Nell'ambito della **Parte Speciale** del Modello suddivisa in sezioni per processi sensibili, sono analizzati: *(i)* i **processi a rischio** e le relative **attività sensibili** nell'ambito delle quali è stato riscontrato il rischio di potenziale commissione dei reati previsti dal Decreto; (*ii*) le **funzioni/ruoli aziendali e i soggetti terzi** che agiscono in nome e per conto della Società (es. *outsourcer* o soggetti a cui è stata esternalizzata un'attività) coinvolti nell'esecuzione delle attività "sensibili" e che, astrattamente, potrebbero commettere i reati previsti dal Decreto 231; *(iii)* le **fattispecie di reato astrattamente applicabili** alla Società in relazione alla specifica famiglia di reato; (*iv*) le **modalità esemplificative** e non esaustive di commissione del reato; (*v*) i **presidi di controllo** adottati dalla Società, nonché (*vi*) i **principi di comportamento** che specificano le regole di condotta che devono ispirare il comportamento dei Destinatari del Modello al fine di prevenire la commissione dei singoli gruppi di reati.

In particolare, la Parte Speciale analizza le seguenti attività sensibili:

i. Selezione, assunzione, gestione, valutazione, remunerazione e incentivazione del personale

ii. Amministrazione del personale, gestione delle trasferte e dei rimborsi spese

iii. Contenzioso e rapporti con l'Autorità Giudiziaria

iv. Conferimento, gestione e revoca delle procure aziendali

v. Omaggi, ospitalità e spese di rappresentanza

vi. Gestione degli aspetti connessi alla salute e sicurezza sul lavoro

vii. Gestione degli aspetti ambientali

viii. Valutazione, approvazione e gestione delle operazioni ordinarie e straordinarie

ix. Contabilità generale, bilancio e altre comunicazioni sociali

x. Finanza a tesoreria

xi. Gestione degli adempimenti fiscali

xii. Approvvigionamenti di beni, servizi e lavori

xiii. Conferimento di incarichi di consulenza

xiv. *Demand Management* e monitoraggio attuazione progetti

xv. Affari societari

xvi. Gestione della contrattualistica

xvii. Contrasto frodi

xviii. Controlli e protezione degli *asset*

xix. Supporto alle Forze dell'Ordine, all'Autorità Giudiziaria, agli Enti e Istituzioni pubbliche

xx. Ottenimento di autorizzazioni, licenze e certificazioni connesse alla gestione del *business* e/o altre attività connesse all'esercizio del *business* che comportino interlocuzioni con la Pubblica Amministrazione

xxi. Progettazione, realizzazione e manutenzione di impianti di *security*

xxii. Gestione e utilizzo dei sistemi informativi, di *software* e delle attività connesse al diritto d'autore

3.4. AGGIORNAMENTO, MODIFICHE E INTEGRAZIONI DEL MODELLO E SUA ATTUAZIONE

L'art. 7, comma 4, lett. a) del Decreto precisa che l'efficace attuazione del Modello richiede "*una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività*".

In aggiunta a tali due casi, l'aggiornamento del Modello è altresì imposto anche quando siano intervenute modifiche del Decreto (*i.e.* quando il legislatore introduce nuovi reati presupposto o modifica alcune prescrizioni del Decreto) o comunque interventi della giurisprudenza, tali da segnare nuovi orientamenti interpretativi della disciplina prevista dal Modello.

Infine, la revisione del Modello è necessaria nel caso di verificata inadeguatezza del Modello (*i.e.* nel caso in cui fosse accertata una non piena effettività del Modello ovvero incoerenza tra lo stesso e i comportamenti concreti dei Destinatari).

Essendo il presente Modello un "*atto di emanazione dell'organo dirigente*" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a) del Decreto), la sua adozione, le successive modifiche e integrazioni sono sottoposte, previo esame dell'Organismo di Vigilanza, all'approvazione del Consiglio di Amministrazione di FS Security.

Invero, 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 o modifiche legislative.

In particolare, sono demandate al Consiglio di Amministrazione di FS Security:

- l'attività di verifica in merito alla necessità di aggiornamento del Modello;
- la responsabilità di modificare o integrare il Modello stesso, a seguito della suddetta verifica o comunque a seguito di segnalazione di proposte e/o esigenze di adeguamento o aggiornamento del Modello da parte dell'Organismo di Vigilanza.

Le modifiche di carattere meramente formale del Modello e dei suoi allegati sono approvate dall'Amministratore Delegato e vengono portate a conoscenza del Consiglio di Amministrazione con apposita informativa, alla prima riunione utile.

Nell'attuale assetto societario la Struttura Affari Legali, Societari e Compliance è deputata a promuovere l'aggiornamento del Modello di Organizzazione, Gestione e Controllo di FS Security S.p.A., in relazione all'evoluzione della normativa di riferimento e a modifiche organizzative e di processo intervenute, garantendo il monitoraggio dell'andamento delle eventuali azioni correttive.

Tutte le modifiche e le integrazioni di cui sopra sono tempestivamente comunicate ai Destinatari.

Al fine di dare concreta attuazione al Modello e assicurare il costante allineamento con il contesto organizzativo e operativo di riferimento, nonché l'adeguamento e l'attualizzazione dei presidi di controllo e prevenzione ai rischi reato *ex* Decreto applicabili, ciascun *Process Owner 231* ha il compito di definire e tenere aggiornati i documenti organizzativi che normano i processi di propria competenza, d'intesa con la struttura competente in materia di organizzazione e processi, che dovrà assicurare la valutazione delle ricadute organizzative, l'orientamento delle azioni conseguenti, l'adozione di un linguaggio e di un approccio metodologico comune, la coerenza con l'assetto

organizzativo, con la documentazione normativa vigente o in via di emissione e con il sistema di procure e deleghe vigenti.

I *Process Owner 231* sono altresì tenuti alla compilazione e trasmissione periodica dei flussi informativi verso l'OdV, attraverso cui possono segnalare eventuali criticità riscontrate nell'attuazione del Modello e possibili aree di miglioramento.

4. IL CODICE ETICO

Il Codice Etico di Gruppo (Allegato 3), costituisce parte integrante del presente Modello. Esso rappresenta i valori fondamentali e la "carta dei diritti e dei doveri" attraverso la quale il Gruppo FS enuncia e chiarisce le proprie responsabilità ed impegni etico/sociali verso gli *stakeholder* interni ed esterni, ai fini della prevenzione e del contrasto di possibili illeciti, e detta i principi, raccoglie i valori e gli standard di comportamento.

Il Codice Etico di Gruppo deve guidare i comportamenti dei Destinatari del Modello.

Il Codice Etico di Gruppo evidenzia in modo chiaro ed esplicito che la realizzazione di comportamenti ad esso non conformi determina una personale assunzione di responsabilità da parte del loro autore. Al Codice Etico di Gruppo è data ampia diffusione sui siti *intranet* e *internet* aziendali e lo stesso è richiamato nei contratti stipulati dalla Società.

5. PROCEDURE MANUALI E INFORMATICHE E SISTEMI DI CONTROLLO INTERNI

5.1. PROCEDURE MANUALI E INFORMATICHE

Nell'ambito del proprio sistema organizzativo, FS Security si è impegnata a mettere a punto un complesso di procedure, sia manuali sia informatiche, volto a regolamentare lo svolgimento delle attività aziendali, nel rispetto dei principi indicati dalle Linee Guida di Confindustria.

Le procedure approntate dalla Società, sia manuali sia informatiche, costituiscono le regole da seguire in seno ai processi aziendali interessati, prevedendo anche i controlli da espletare al fine di garantire la correttezza, l'efficacia e l'efficienza delle attività aziendali.

La definizione, attuazione e continuo aggiornamento dei documenti normativi interni assicurano un'adeguata regolamentazione dei processi a rischio.

5.2. IL FRAMEWORK ANTI-CORRUPTION

Il Gruppo FS è impegnato a prevenire e contrastare ogni forma di pratica corruttiva nello svolgimento delle proprie attività, secondo il principio "*zero tolerance for corruption",* in coerenza con il Codice Etico di Gruppo e con l'adesione al *Global Compact* delle Nazioni Unite, il cui principio impegna le imprese a contrastare la corruzione in ogni sua forma.

Nel suo ruolo di indirizzo e coordinamento, nel 2023 la Holding ha emanato la *policy* "*Framework Anti-Corruption* del Gruppo Ferrovie dello Stato Italiane" che definisce l'architettura dell'intero sistema anticorruzione del Gruppo e risponde all'esigenza di assicurare in via sistematica ed unitaria l'attività di prevenzione della corruzione, supportando l' impegno del Gruppo verso lo sviluppo sostenibile e concorrendo alla creazione di valore, anche attraverso la diffusione e il rafforzamento della cultura dell'integrità, della legalità e della correttezza nell'agire.

Il *Framework Anti-Corruption* è costituito dall'insieme dei documenti che contengono i princìpi, gli indirizzi e le regole in materia di anticorruzione e in particolare:

- Codice Etico di Gruppo;

- *Policy Anti-Corruption* del Gruppo Ferrovie dello Stato Italiane;
- Modello di Organizzazione Gestione e Controllo *ex* D.lgs. 231/2001;
- Modello di Gestione *Anti-Corruption.*

In linea con il percorso intrapreso, FS Security ha recepito il "*Framework Anti-Corruption* del Gruppo Ferrovie dello Stato Italiane" garantendo la corretta e costante applicazione di quanto definito, nel rispetto delle proprie prerogative di autonomia e indipendenza.

5.3. IL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI AZIENDALE (SCIGR) DI FS SECURITY

Il Sistema di controllo interno e gestione rischi (SCIGR) è costituito dall'insieme delle regole, procedure e strutture organizzative finalizzate ad una effettiva ed efficace identificazione, misurazione, gestione e monitoraggio dei principali rischi, al fine di contribuire al successo sostenibile della società.

Un efficace SCIGR favorisce l'assunzione di decisioni consapevoli e concorre ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità dell'informativa finanziaria, il rispetto di leggi e regolamenti, dello Statuto sociale e degli strumenti normativi interni.

5.3.1. COMPITI E RESPONSABILITÀ

Ferma restando la centralità del *management* e delle strutture di presidio specialistico nelle attività di gestione e monitoraggio del rischio (come responsabili del monitoraggio di linea o "I livello di controllo"), FS Security ha strutturato diversi presidi di "II livello" che supportano il *management* nella definizione e nell'implementazione di adeguati sistemi di gestione e monitoraggio dei principali rischi e controlli. Ad essi si aggiunge, attualmente, la funzione di *Internal Audit* di FS S.p.A.

Di seguito una descrizione dei compiti e delle responsabilità dei principali soggetti coinvolti nel SCIGR.

Risk & Anti-Corruption. Il *Risk & Anti-Corruption* assicura, a livello societario, in coerenza con le strategie, gli indirizzi e le politiche di Gruppo e societarie:

- l'attuazione e diffusione di strategie, politiche e indirizzi di gestione del rischio emanati dalla competente struttura di Holding, il monitoraggio dell'evoluzione normativa e delle *best practice* di riferimento e la diffusione di una cultura orientata alla valutazione del rischio, collaborando nello sviluppo di metodi e strumenti per la raccolta, analisi e condivisione dai dati e delle informazioni sui rischi;
- l'implementazione e la gestione del *Framework* di *Risk Management* per la gestione e misurazione dei rischi aziendali in una logica di *Enterprise Risk Management* (ERM) e il monitoraggio dei rischi aziendali, con particolare focalizzazione sui rischi operativi, fornendo reportistica periodica agli organi di *governance* e controllo societari e alla competente struttura di Holding;
- la gestione del processo di identificazione, analisi, misurazione, definizione dei relativi strumenti di prevenzione anticorruzione, valutazione e monitoraggio dei rischi, supportando i *Process Owner* societari e collaborando con la competente struttura di Holding nell'esecuzione delle analisi sulle tematiche presidiate direttamente dalla stessa;
- l'implementazione e la gestione del *Framework Anti-Corruption*, curando la definizione della proposta del modello di gestione *Anti-Corruption* di FS Security e il monitoraggio dello stesso, al fine di segnalare eventuali esigenze di aggiornamento e di proporre le iniziative da adottare con approccio *risk based*, sulla base degli esiti delle attività delle strutture aziendali interessate e delle attività di audit svolte dalla competente struttura, a tal fine istituendo e gestendo appositi flussi informativi;
- il monitoraggio sull'attuazione del modello di gestione *Anti-Corruption* e i relativi aggiornamenti, in

coerenza con l'evoluzione dell'assetto normativo e organizzativo e del piano strategico societario, segnalando eventuali esigenze di aggiornamento;

- l'elaborazione della reportistica periodica agli organi di *governance* e controllo societari ed alla competente struttura di Holding prevista dal sistema di gestione anticorruzione;
- per le materie di competenza, l'individuazione delle esigenze formative e la definizione del piano degli eventi formativi e comunicativi per la diffusione della cultura della legalità e dell'integrità in ambito societario.

DPO e *Data Protection Department*. In ottemperanza a quanto previsto dal Regolamento UE 2016/679 (*General Data Protection Regulation* – "GDPR"), il Gruppo FS Italiane si è dotato di un proprio modello gestionale per la protezione dei dati personali (*Framework* di *Data Protection*), il quale definisce il set di regole interne, le metodologie, i ruoli e le responsabilità attribuiti a tutte le strutture coinvolte nel trattamento di dati personali.

Il Gruppo ha individuato, per la *data protection*, un modello organizzativo di Gruppo "distribuito", che prevede, laddove ne sussistano le condizioni, la nomina di un *Data Protection Officer* (DPO) societario, demandando al DPO di FS l'attività di indirizzo e coordinamento.

In considerazione della rilevanza delle attività di trattamento dati personali connesse alle funzioni assolte da FS Security, è prevista la nomina di un DPO societario da parte del Consiglio di Amministrazione su proposta dell'AD. Il DPO riporta funzionalmente allo stesso CdA ed è supportato dalla funzione *Data Protection* societaria, collocata all'interno della funzione legale e, precisamente, nel *Data Protection Department*.

Il DPO societario è incaricato almeno dei compiti di cui all'art. 39 GDPR ed è membro "permanente" del Team Tecnico *Data Protection* nell'ambito del quale proporrà il piano *data protection* societario e il piano DPIA annuale.

Il *Data Protection Department*, in raccordo con il DPO, assicura:

- assistenza al Titolare nel recepimento e nell'attuazione del sistema di norme di Gruppo in materia di *data protection* definito da FS S.p.A., coordinandosi con lo stesso per le verifiche di coerenza e per ogni necessario supporto consulenziale;
- supporto al Titolare e/o ai *Data Controller Manager*/*Data Manager* nelle attività operative di adempimento normativo;
- il coinvolgimento del DPO e della Struttura *Data Protection Department* di FS S.p.A. nei casi previsti dal *Framework* di *Data Protection*;
- il monitoraggio delle attività di competenza e l'elaborazione della relativa reportistica societaria, inclusa la reportistica verso FS S.p.A.

Affari Legali, Societari e Compliance. A partire dal 2019 è stato definito e diffuso il "Modello di *Compliance* del Gruppo FS Italiane" descrivendone gli aspetti organizzativi e i processi che ne regolano il funzionamento. In coerenza con le soluzioni organizzative adottate da altre funzioni di controllo di II e III livello che compongono il più generale SCIGR è previsto un Modello di *Compliance* di Gruppo "decentrato", che vede nella Holding, la presenza di una struttura *Compliance* quale Responsabile Funzionale di Gruppo e di strutture/presidi di *Compliance* nelle società controllate.

Le strutture/presidi di *Compliance* delle società controllate del Gruppo, sulla base delle proprie specificità organizzative e di *business*, nonché della complessità operativa delle attività, assicurano l'applicazione di metodologie e modalità operative coerenti con quelle rappresentate nell'ambito del Modello di *Compliance* di Gruppo.

In coerenza con gli indirizzi e le politiche aziendali e di Gruppo assicura il presidio delle attività di *Compliance* mediante:

- l'aggiornamento del Modello 231 di FS Security in relazione all'evoluzione della normativa di riferimento e/o a modifiche organizzative e di processo intervenute, garantendo il monitoraggio dell'andamento delle eventuali azioni correttive;

- l'adozione, la gestione e l'aggiornamento del Modello di *compliance* societario, in coerenza con il *framework* definito a livello di Holding;
- il monitoraggio della normativa a cui il sistema delle regole aziendali deve essere conforme, assicurando e fornendo alle strutture interessate il necessario supporto, per la definizione delle azioni da adottare per garantire uniforme interpretazione/applicazione delle nuove disposizioni di legge e regolamentari, nonché delle conseguenti implicazioni organizzative, strategiche e di *business*.

Dirigente Preposto di FS S.p.A. La L. n. 262 del 28 dicembre 2005, "*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*", ha introdotto l'art. 154-*bis* del D. Lgs. n. 58/1998 (c.d. "Testo Unico della Finanza" o "TUF"), prevedendo, per gli emittenti quotati aventi l'Italia come Stato membro d'origine, la nomina di un "Dirigente preposto alla redazione dei documenti contabili societari" (il "Dirigente Preposto").

In FS l'introduzione della figura del Dirigente Preposto, istituita su base volontaria nel 2007, è diventata nel 2013 a tutti gli effetti obbligatoria *ex lege*, ricadendo a pieno nell'ambito di applicazione dell'art. 154 bis del TUF, a seguito dell'emissione dei prestiti obbligazionari quotati sul mercato irlandese (Programma EMTN *Euro Medium Term Notes*) in conseguenza della quale FS ha assunto la configurazione di Ente di interesse Pubblico (EIP), di cui all'art.16 del D. Lgs. n. 39/2010, in quanto società "Emittente Strumenti finanziari quotati".

A livello di Gruppo, è stato implementato il "Modello di Controllo Interno e Gestione dei Rischi sull'Informativa Economica Finanziaria del Gruppo Ferrovie dello Stato Italiane", adottato da FS Security con Comunicazione Organizzativa n. 33/AD del 3 novembre 2023.

Giova precisare che, in considerazione della complessità organizzativa ed operativa del Gruppo FS, con lo scopo di ottenere un rafforzamento e una migliore efficacia nell'applicazione della norma nonché del sistema di controllo interno e gestione del rischio di Gruppo, il CdA di FS ha ritenuto opportuno promuovere la nomina dei Dirigenti Preposti anche nelle principali società controllate.

In FS Security non è stato nominato un Dirigente Preposto, ma è stato demandato alla Struttura Amministrazione, Finanza e Controllo il compito di curare la redazione dei documenti contabili societari ai sensi della L. n. 262/2005.

Società di Revisione. L'Assemblea di FS Security ha conferito a una società esterna, per la durata di tre esercizi, l'incarico di revisione legale dei conti, su proposta motivata del Collegio Sindacale.

La Società di Revisione documenta l'attività svolta in apposito libro, tenuto presso la sede della Società.

5.3.2. SISTEMI DI GESTIONE E CONTROLLO DI RISCHI SPECIFICI

Sul piano più propriamente operativo non possono essere sottaciuti, in quanto fondamentali strumenti di prevenzione di cui il Modello si avvale per le proprie finalità cautelari, i vari Sistemi di Gestione e controllo di rischi specifici adottati in azienda.

Tali sistemi, operanti rispetto a categorie di rischio più ampie del Modello qui rappresentato, costituiscono una fondamentale matrice di controllo atta a prevenire i rischi-reato connessi ai relativi specifici processi.

Modello di Controllo Interno e Gestione dei Rischi sull'Informativa Economica Finanziaria. Il Modello adottato da FS Security, nel rispetto della propria autonomia societaria, è definito da FS in coerenza con l'evoluzione degli assetti del Gruppo e del contesto di riferimento, nel rispetto delle previsioni del TUF (art. 154 bis e seguenti) e degli standard di riferimento comunemente accettati a livello internazionale in tema di controllo interno ("*Internal Control – Integrated Framework*" c.d. *Coso Report pubblicato dal Committee of Sponsoring Organizations of the Treadway Commission*).

Modello di gestione della salute e sicurezza sul lavoro adottato ai sensi del D.lgs. n. 81/2008. FS Security ha formalmente adottato le linee generali in materia di Salute e Sicurezza sul lavoro emanate da FS e destinate alle Società del Gruppo, le quali individuano i requisiti minimi che devono soddisfare i sistemi di gestione in materia per essere conformi alla norma UNI ISO 45001/2018.

5.4. ALTRI PRESIDI DI CONTROLLO

Nell'ambito di FS Security, è stato altresì costituito il Comitato Etico e Segnalazioni, composto dai titolari *pro tempore* delle Strutture Risorse Umane e Organizzazione, Amministrazione, Finanza e Controllo e Affari Legali, Societari e *Compliance* (in funzione di Coordinatore).

Il Comitato, in coerenza con quanto previsto dal vigente Codice Etico di Gruppo, ha il compito di:

- chiarire, mediante pareri consultivi, il significato e l'applicazione del Codice Etico;
- coordinarsi con l'Organismo di Vigilanza nelle attività afferenti alla gestione delle segnalazioni di cui al paragrafo 6.8;
- coordinarsi e mantenere flussi informativi con l'Organismo di Vigilanza per gli aspetti di reciproco interesse;
- informare periodicamente il Consiglio di Amministrazione di FS Security sulle attività svolte.

Per lo svolgimento della propria attività, il Comitato può avvalersi del supporto operativo delle competenti Strutture aziendali.

5.5. BUDGET E 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 Strutture 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.

6. ORGANISMO DI VIGILANZA

In ottemperanza a quanto previsto dal Decreto, il Consiglio di Amministrazione di FS Security nomina un Organismo di Vigilanza con il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento.

Gli aspetti strutturali dell'OdV (es. modalità di nomina, durata in carica, riunioni, voto e delibere, ecc.) sono precisati in uno statuto approvato dal Consiglio di Amministrazione della Società.

Gli aspetti relativi al funzionamento sono disciplinati da un Regolamento interno, autonomamente approvato dall'Organismo.

L'OdV può avvalersi del supporto operativo delle altre Strutture Organizzative della Società per gli approfondimenti/verifiche ritenuti necessari. L'Organismo può, inoltre, decidere di delegare a propri singoli membri – sulla base delle rispettive competenze – uno o più specifici adempimenti, con l'obbligo per il delegato di operare nei limiti dei poteri e del budget assegnato e di riferire in merito all'Organismo. In ogni caso, anche in ordine alle funzioni delegate dall'Organismo a singoli membri, permane la responsabilità collegiale dell'Organismo

medesimo.

Di seguito sono descritti i principali aspetti relativi alla costituzione e al funzionamento dell'Organismo.

6.1. COMPOSIZIONE E NOMINA

La composizione dell'Organismo di Vigilanza è individuata nell'ambito del Regolamento interno approvato dallo stesso OdV.

L'OdV è nominato, previa verifica del possesso dei requisiti soggettivi previsti dal paragrafo 6.2. del presente Modello, da parte del Consiglio di Amministrazione di FS Security, che ne indica anche il Presidente. La nomina si perfeziona con la formale accettazione dell'incarico espressa da ciascun componente dell'OdV. All'atto del conferimento dell'incarico, ogni individuo designato a ricoprire la carica di membro dell'OdV deve rilasciare una dichiarazione nella quale si attesti l'assenza di cause di ineleggibilità (si veda paragrafo 6.3 del presente Modello).

6.2. REQUISITI DELL'ORGANISMO DI VIGILANZA

I componenti dell'Organismo nominato da FS Security hanno i requisiti di:

- Autonomia e indipendenza. Come precisato dalle Linee Guida di Confindustria, tali requisiti sono assicurati riconoscendo all'OdV una posizione autonoma e imparziale, prevedendo il "riporto" al massimo vertice operativo aziendale, vale a dire al Consiglio di Amministrazione, nonché la dotazione di un *budget* annuale a supporto delle attività di verifica tecniche necessarie per lo svolgimento dei compiti ad esso affidati dal legislatore. Per assicurare la necessaria autonomia di iniziativa e l'indipendenza è poi indispensabile che all'OdV non siano attribuiti compiti operativi, nonché garantire l'onerosità dell'incarico conferito alle persone che compongono l'Organismo, al fine di estendere l'indipendenza e l'autonomia dell'OdV anche all'aspetto finanziario.
- Professionalità. A prescindere dalla qualificazione del componente dell'OdV quale interno od esterno, la professionalità si caratterizza come insieme delle conoscenze, degli strumenti e delle tecniche necessari per lo svolgimento dell'attività assegnata, sia di carattere ispettivo che consulenziale. I compiti propri dell'OdV presuppongono competenze specifiche in ambito giuridico e, segnatamente, penale e societario nonché in materia di *auditing* e *risk management*.
- Continuità d'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 un'efficace e costante attuazione del Modello. La continuità di azione impone inoltre di fare in modo che i componenti dell'Organismo di Vigilanza siano a conoscenza dei processi aziendali e possano avere un diretto contatto con le Strutture societarie relative alle aree sensibili al rischio reato, in modo da ricevere riscontri sull'efficacia del sistema di controllo di cui al modello organizzativo.
- Onorabilità e assenza di conflitti di interessi: i requisiti dell'onorabilità e dell'assenza di conflitto di interessi sono assicurati con la previsione di specifiche cause di ineleggibilità e decadenza legate a specifici requisiti e che, tra l'altro, garantiscono la mancanza di qualsiasi interesse economico e/o personale in capo ai componenti dell'OdV, interferente con gli interessi della Società.

6.3. DURATA DELL'INCARICO, CAUSE DI INELEGGIBILITÀ, DECADENZA E REVOCA

I componenti dell'OdV possono restare in carica per tre anni e possono essere rieletti per non più di tre mandati consecutivi. In ogni caso, ciascun componente rimane in carica fino alla nomina del successore, a eccezione dei casi di decadenza e revoca, di seguito descritti.

La **rinuncia** da parte dei componenti dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata

all'OdV per iscritto, unitamente alle motivazioni che l'hanno determinata.

Ai fini di assicurare i requisiti di autonomia, indipendenza e onorabilità, costituiscono cause di **ineleggibilità e decadenza** da membro dell'OdV di FS Security:

a) avere rapporti di coniugio, parentela o di affinità entro il quarto grado, o di unione civile con gli amministratori della Società e/o delle altre società del Gruppo;

b) ricoprire, o avere ricoperto nell'ultimo triennio, incarichi in organi di amministrazione di FS Security e/o delle altre società del Gruppo;

c) salvo che per l'espletamento di funzioni di *audit* e/o di membro del Collegio Sindacale, essere legati a qualsivoglia titolo o in qualsiasi modo, alla Società o a soggetti in posizione apicale della Società da interessi o rapporti economici (es. partecipazioni azionarie, rapporti di fornitura di beni e servizi, rapporti di consulenza) ritenuti rilevanti dal Consiglio di Amministrazione, o essersi trovati nelle predette condizioni nei tre anni precedenti la nomina;

d) essere legati a società controllate da interessi o rapporti economici, ritenuti rilevanti dall'Organo Amministrativo;

e) essere membri di Organismi di Vigilanza di società controllate dalla Società che provvede alla nomina e/o di Società che la controllano;

f) in qualità di dipendente di pubbliche amministrazioni, esercitare o aver esercitato negli ultimi tre anni di servizio, poteri autoritativi o negoziali per conto delle stesse nei confronti di FS Security e/o altre società del Gruppo;

g) trovarsi nella condizione giuridica di interdetto, inabilitato, fallito o condannato, anche con sentenza non definitiva, a una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi; la sentenza di patteggiamento è da considerarsi equivalente ad una sentenza di condanna;

h) avere riportato una condanna, anche non definitiva, per uno dei reati previsti dal Decreto (la sentenza di patteggiamento è da considerarsi equivalente ad una sentenza di condanna);

i) essere destinatario di misure cautelari personali, coercitive o interdittive, per uno dei reati previsti dal Decreto;

j) essere destinatario di misure di prevenzione personali o patrimoniali, di cui al D.lgs. n. 159/2011 e s.m.i.;

k) avere riportato una condanna, anche non definitiva, alla pena della reclusione per un reato contro il patrimonio, la Pubblica Amministrazione, la fede pubblica, l'ordine pubblico, l'economia pubblica, per un delitto doloso contro la personalità individuale, per un reato societario, tributario, bancario, finanziario o per uno dei delitti previsti dal R.D. 16 marzo 1942, n. 267 (la sentenza di patteggiamento a tali fini è da considerarsi equivalente ad una sentenza di condanna).

I membri dell'OdV sono tenuti a comunicare al Consiglio di Amministrazione (e informare gli altri componenti dell'OdV) ogni sopravvenuta causa di ineleggibilità/decadenza o eventuale situazione di incompatibilità, ulteriore rispetto a quelle sopra elencate, che possa assumere rilievo ai fini della nomina o della permanenza in carica.

Il Consiglio di Amministrazione di FS Security, sentito il Collegio Sindacale, potrà inoltre **revocare** in ogni momento i componenti dell'OdV qualora ricorra una giusta causa.

Per giusta causa di revoca dovranno intendersi:

a) un grave inadempimento dei propri doveri;

b) una sentenza di condanna della Società o una sentenza di patteggiamento, passate in giudicato, per reati previsti dagli articoli 24 e seguenti del Decreto ove risulti dagli atti la "*omessa o insufficiente vigilanza*" da

parte dell'Organismo, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto 231;

c) la violazione degli obblighi di riservatezza;

d) l'assenza, senza giustificato motivo, ad almeno tre riunioni dell'OdV.

Il Consiglio di Amministrazione di FS Security, in caso di cessazione dalla carica, per qualsiasi ragione, di un componente dell'OdV, si impegna a nominare un nuovo componente dell'OdV senza indugio. Il componente così nominato scade insieme con quelli in carica all'atto della sua nomina.

In caso di cessazione per qualunque causa del Presidente, la funzione è assunta dal membro più anziano, il quale rimane in carica fino alla data della nomina del nuovo Presidente dell'Organismo.

6.4. FUNZIONI, POTERI E BUDGET

Allo scopo di assolvere alle funzioni indicate dal Decreto, all'OdV di FS Security sono demandate le seguenti attività:

- esame dell'adeguatezza del Modello, ovvero la sua idoneità a prevenire il verificarsi di comportamenti illeciti, nonché ad evidenziarne l'eventuale realizzazione;
- vigilanza sull'effettività del Modello, cioè sulla coerenza tra i comportamenti concreti e il Modello istituito;
- cura del necessario aggiornamento in senso dinamico del Modello, proponendo, se necessario, al Consiglio di Amministrazione o alle funzioni dell'ente eventualmente competenti l'adeguamento dello stesso;
- segnalazione al Consiglio di Amministrazione, ai fini degli opportuni provvedimenti, di quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
- predisposizione, su base almeno semestrale, di una relazione informativa riguardante le attività di verifica e controllo compiute e l'esito delle stesse per il Consiglio di Amministrazione;
- trasmissione al Collegio Sindacale della relazione di cui al punto precedente.

Inoltre, è previsto che:

- le attività poste in essere dall'OdV non possano essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che l'organo dirigente vigila sull'adeguatezza del suo intervento, poiché ad esso compete la responsabilità ultima del funzionamento (e dell'efficacia) del Modello;
- l'OdV deve avere libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal Decreto 231;
- l'OdV possa avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le Strutture della Società, ovvero di consulenti esterni.

L'OdV ha un'autonomia di mezzi finanziari e logistici adeguati che ne garantiscono la piena ed autonoma operatività nell'espletamento delle proprie funzioni. A tal fine, il CdA di FS Security provvede annualmente a dotare l'OdV, su proposta dello stesso, di un **fondo adeguato**, approvato in sede di formazione del *budget* aziendale, di cui l'Organismo potrà disporre in piena autonomia per ogni esigenza necessaria al corretto svolgimento dei propri compiti e funzioni, ivi compresi gli eventuali supporti consulenziali, redigendo apposito rendiconto.

La definizione degli aspetti attinenti alla continuità dell'azione dell'Organismo di Vigilanza (*i.e.* calendarizzazione dell'attività, verbalizzazione delle riunioni e la disciplina dei flussi informativi dalle strutture aziendali all'OdV) è rimessa all'OdV stesso al fine di garantirne l'indipendenza, il quale provvede a disciplinare il proprio funzionamento tramite un **Regolamento interno** delle proprie attività che definisce, a titolo di esempio, la determinazione delle

cadenze temporali dei controlli e l'individuazione dei criteri e delle procedure di analisi.

6.5. MODALITÀ DI FUNZIONAMENTO E SUPPORTO ALL'ODV

L'Organismo di Vigilanza si riunisce con la frequenza prevista dal Regolamento interno.

L'OdV, al fine di svolgere le proprie funzioni di vigilanza, può avvalersi del supporto operativo della funzione *Internal Audit* della Holding (nelle more della nomina di apposita funzione *Internal Audit* societaria), nonché del supporto operativo di altri organi societari e funzioni di controllo della Società ogni qualvolta lo ritenga opportuno ai fini dell'efficace ed efficiente adempimento dei compiti a esso assegnati.

6.6. FLUSSI INFORMATIVI DELL'ODV

Annualmente, l'OdV presenta il piano di vigilanza al Consiglio di Amministrazione e al Collegio Sindacale di FS Security S.p.A.

L'OdV trasmette al Consiglio di Amministrazione e al Collegio Sindacale di FS Security S.p.A., con cadenza semestrale, una relazione in cui vengono illustrate tutte le attività e le verifiche svolte dall'OdV nel periodo di riferimento, le modalità operative impiegate, nonché le eventuali criticità riscontrate e le altre notizie ritenute di rilievo.

A prescindere da questi obblighi informativi periodici, l'OdV riferisce tempestivamente e su base continuativa al Consiglio di Amministrazione e all'Amministratore Delegato della Società, relativamente a violazioni del Modello, accertate o tali da generare l'opportunità di determinazioni urgenti, di cui sia venuto a conoscenza tramite segnalazione da parte dei Destinatari o che abbia accertato durante lo svolgimento delle proprie attività.

In ogni caso, l'OdV può rivolgersi al Consiglio di Amministrazione ogni qualvolta lo ritenga opportuno ai fini dell'efficace ed efficiente adempimento dei compiti ad esso assegnati.

6.7. FLUSSI INFORMATIVI VERSO L'ODV

I flussi informativi verso l'OdV sono diretti ad agevolarne l'attività di vigilanza o a segnalare eventi che abbiano generato o possano generare violazioni o tentata elusione del Modello o del Codice Etico di Gruppo che hanno o potrebbero avere rilievo ai sensi del Decreto.

Dovrà essere portata a conoscenza dell'OdV ogni informazione, di qualsiasi tipo, proveniente anche da terzi e attinente all'attuazione del Modello nelle aree sensibili nonché qualsiasi informazione utile per valutare l'adeguatezza e l'efficacia del Modello.

I Destinatari devono informare l'OdV in relazione ai fatti e alle circostanze che potrebbero generare responsabilità ai sensi del Decreto e garantiscono che le segnalazioni siano circostanziate e fondate su elementi di fatto precisi e concordanti.

Le violazioni degli obblighi di informazione nei confronti dell'OdV potranno comportare l'applicazione di sanzioni disciplinari di cui al seguente paragrafo.

L'Allegato 4 al presente Modello individua nel dettaglio i flussi informativi che i *Process Owner* 231 competenti sono tenuti a trasmettere all'OdV, definendone i contenuti e la periodicità.

6.8. SEGNALAZIONI – WHISTLEBLOWING

I Destinatari sono tenuti a informare tempestivamente l'OdV di ogni violazione o presunta violazione dei principi di cui al Modello, o comunque comportamenti non in linea con le previsioni del Modello.

Il Comitato Etico e Segnalazioni e l'OdV garantiscono l'inoltro reciproco delle segnalazioni ricevute a seconda

della competenza. In particolare, il Comitato Etico e Segnalazioni trasmette all'Organismo di Vigilanza di FS Security tutte le segnalazioni ricevute relative a FS Security, anche se coinvolta unitamente ad altre società del gruppo, affinché l'OdV a proprio insindacabile giudizio possa valutarne la potenziale rilevanza ai sensi del decreto e, di conseguenza, decidere la relativa competenza alla gestione.

Ai sensi dell'art. 6 del Decreto, comma 2-*bis* (così come modificato dal D. Lgs. 24/2023), la Società deve dotarsi di un Modello che preveda:

a) dei canali di segnalazione interna;

b) il divieto di ritorsione e

c) il sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

A tal proposito, FS Security ha implementato i seguenti canali di segnalazione interna:

- piattaforma informatica: accessibile all'indirizzo internet segnalazione-whistleblowing.fssecurity.openblow.it. Questo canale è da considerarsi preferenziale in quanto maggiormente idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del Segnalante e adeguate misure di sicurezza delle informazioni;
- posta ordinaria: all'indirizzo FS Security S.p.A., Segreteria Tecnica Comitato Etico e Segnalazioni di FS Security S.p.A. – Via Marsala, 27 – 00185 Roma;
- posta elettronica: agli indirizzi di posta elettronica comitatoetico@fsitalianesecurity.it , ovvero odv@fsitalianesecurity.it , entrambi accessibili ai soli componenti, rispettivamente, del Comitato Etico e Segnalazioni e dell'OdV;
- verbalmente: mediante dichiarazione rilasciata dal Segnalante, in apposita audizione fissata entro un termine ragionevole, al Comitato Etico e Segnalazioni di FS Security S.p.A., riportata a verbale e sottoscritta dal Segnalante.

FS Security si impegna a far sì che i segnalanti vengano garantiti contro qualsiasi forma, diretta o indiretta, di ritorsione, discriminazione o penalizzazione, per motivi collegati direttamente o indirettamente alla segnalazione, assicurando altresì la riservatezza dell'identità del segnalante (fatti salvi gli obblighi di legge) e la tutela delle persone accusate erroneamente e/o in mala fede.

Il trattamento dei dati personali raccolti nell'ambito del procedimento di segnalazione viene svolto nel pieno rispetto della normativa in materia di protezione dei dati personali e nel rispetto di quanto prescritto dalla normativa in materia di *Whistleblowing*.

Qualora le segnalazioni ricevute risultino circostanziate ai sensi della "Procedura per la gestione delle segnalazioni", verrà avviata l'attività istruttoria e di accertamento, attraverso verifiche interne, come previsto dall'apposita "Procedura per la gestione delle segnalazioni", di tempo in tempo vigente, affinché possano essere assunte, ove necessarie, opportune azioni correttive, avviati eventuali procedimenti disciplinari ovvero intraprese altre iniziative che, a seconda dei casi, saranno considerate adeguate. Ad ogni modo, gli esiti dovranno essere comunicati all'OdV il quale, laddove ritenuto opportuno, formulerà le dovute osservazioni.
Le segnalazioni possono essere inviate ai canali di segnalazione interna sopra indicati.

Con riferimento alla ricezione e gestione delle segnalazioni, si rimanda alla "Procedura per la gestione delle segnalazioni" (Allegato 5 al presente Modello).

6.9. RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI

L' Organismo di Vigilanza deve curare la tracciabilità e la conservazione della documentazione delle attività svolte (verbali, relazioni, schede di flussi informativi, segnalazioni, report inviati e ricevuti).

Presso l'OdV è conservata copia (cartacea e/o informatica) dei documenti relativi alle sue attività operative.

Le segnalazioni ricevute e tutta la documentazione relativa all'attività espletata dall'OdV vengono conservate, nel rispetto della normativa in materia di protezione dei dati personali, in un apposito archivio, il cui accesso è consentito ai soli componenti dell'OdV e al personale che assicura il servizio di segreteria tecnica. L'accesso da parte di soggetti diversi deve essere preventivamente autorizzato dall'OdV e deve svolgersi secondo modalità dallo stesso stabilite.

7. SISTEMA DISCIPLINARE E SANZIONATORIO

7.1. PRINCIPI GENERALI E VIOLAZIONI

La predisposizione di un adeguato sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per assicurare l'efficacia del Modello stesso.

Al riguardo, infatti, l'articolo 6 comma 2, lettera e) del Decreto prevede che i *modelli di organizzazione e gestione* debbano *«[…] introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello […]».*

La mancata osservanza delle norme e delle disposizioni, contenute nel presente Modello e nel Codice Etico di Gruppo, lede, di per sé sola, il rapporto in essere con FS Security e comporta azioni di carattere sanzionatorio e disciplinare a prescindere dall'eventuale instaurazione o dall'esito di un giudizio penale, nei casi in cui la violazione costituisca reato.

A titolo generale, costituiscono "violazione" del presente Modello:

- condotte omissive o commissive non conformi alla legge e alle prescrizioni contenute nel presente Modello e nel Codice Etico di Gruppo, sia che comportino o meno la consumazione di uno dei reati contemplati dal Decreto, sia che comportino o meno una situazione di rischio di consumazione di uno dei reati contemplati dal Decreto;
- in caso di segnalazioni (come previste dal paragrafo 6.8):
  - le condotte omissive o commissive non conformi alla legge e alle prescrizioni contenute nel presente Modello e nelle procedure che ne costituiscono attuazione, che comportino una privazione o riduzione di tutela del segnalante, anche in termini di riservatezza della sua identità, nonché dei soggetti e/o dei fatti indicati nella segnalazione;
  - la minaccia o l'adozione nei confronti del segnalante di misure ritorsive e/o discriminatorie (ad esempio licenziamento, *mobbing*, demansionamento, ecc.), dirette o indirette, per motivi collegati, direttamente o indirettamente, alla segnalazione effettuata;
  - l'effettuazione, con dolo o colpa grave, da parte dei Destinatari del Modello, di segnalazioni che si rivelano infondate;
  - l'omissione volontaria di rilevare o riportare eventuali violazioni di una o più norme o prescrizioni previste dal Modello.

L'elenco delle possibili violazioni, graduate secondo un ordine crescente di gravità, è il seguente:

i) violazioni di una o più norme o prescrizioni previste dal Modello, che costituiscono inosservanze di minor rilievo;
ii) violazioni di una o più norme o prescrizioni previste dal Modello, che costituiscono inosservanze gravi o danno luogo ad ipotesi di recidiva;
iii) violazioni di una o più norme o prescrizioni previste dal Modello, che determinano la commissione di uno dei reati sanzionati dal Decreto.

Ai fini della valutazione della gravità delle violazioni sono tenute in considerazione: le concrete modalità di realizzazione della violazione; l'intenzionalità del comportamento e il grado di colpa; le funzioni/mansioni

dell'autore della violazione in ambito aziendale; il comportamento dell'autore della violazione prima e dopo la realizzazione della stessa; la circostanza che la violazione abbia provocato un grave danno alla Società ovvero l'abbia esposta ad un procedimento per responsabilità amministrativa ai sensi del Decreto; altre particolari circostanze che accompagnano la violazione.

7.2. MISURE NEI CONFRONTI DEI DIPENDENTI

I comportamenti tenuti dal lavoratore in violazione delle norme di cui al Decreto, del presente Modello, del Codice Etico di Gruppo, nonché di tutti i protocolli/procedure aziendali di cui al Modello, sono da considerarsi mancanze ai sensi del vigente Contratto Collettivo Nazionale di Lavoro applicato da FS Security.

Con riferimento alle sanzioni disciplinari nei riguardi di detti lavoratori, queste vengono irrogate nel rispetto delle procedure previste dall'art. 7 della legge 20 maggio 1970 n. 300.

In particolare, ai Dipendenti (non dirigenti) sono comminabili le sanzioni previste dal vigente CCNL della Mobilità/Area contrattuale Attività Ferroviarie, nel rispetto del principio della gradualità della sanzione e della proporzionalità alla gravità dell'infrazione.

Le sanzioni previste dal predetto CCNL sono le seguenti, graduate in base alla gravità:

a) rimprovero verbale e rimprovero scritto;
b) multa mediante ritenuta sulla retribuzione non superiore a quattro ore della retribuzione giornaliera spettante;
c) sospensione dal servizio e dalla retribuzione da uno a dieci giorni, senza perdita di anzianità;
d) licenziamento con o senza preavviso.

Le sanzioni di cui alle lettere a) e b) sono comminabili per le violazioni indicate al punto i) del precedente paragrafo 7.1. La sanzione di cui alla lettera c) è comminabile per le violazioni indicate al punto ii) del precedente paragrafo 7.1. Le sanzioni di cui alla lettera d) sono comminabili per le violazioni indicate al punto iii) del precedente paragrafo 7.1.

Il procedimento disciplinare è regolato dalle norme del CCNL di riferimento ed è di competenza della struttura Risorse Umane e Organizzazione.

7.3. MISURE NEI CONFRONTI DEI DIRIGENTI

In caso di violazione delle norme di cui al Decreto, del Modello, del Codice Etico di Gruppo o dei protocolli/procedure aziendali di cui al Modello da parte dei Dirigenti, sono comminabili le sanzioni previste dal vigente CCNL per i Dirigenti di aziende produttrici di beni e servizi nel rispetto del principio di proporzionalità, avuto riguardo alla gravità dell'infrazione commessa.

In particolare:

a) richiamo: per le violazioni del Modello di cui al punto i) del precedente paragrafo 7.1;
b) licenziamento con preavviso: laddove si tratti di una violazione di cui al punto ii) del precedente paragrafo 7.1 tale da ledere il vincolo fiduciario;
c) licenziamento senza preavviso: laddove si tratti di una violazione di cui al punto iii) del precedente paragrafo 7.1 tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione neppure temporanea del rapporto di lavoro.

Il procedimento per l'applicazione delle sanzioni è regolato dalle norme del CCNL della Mobilità/Area contrattuale Attività Ferroviarie in base al richiamo operato dall'art. 27 del CCNL per i Dirigenti di Aziende Produttrici di beni e servizi ed è di competenza della Struttura Risorse Umane e Organizzazione.

7.4. MISURE NEI CONFRONTI DEGLI ORGANI SOCIALI

La violazione delle norme di cui al Decreto, del Modello e del Codice Etico di Gruppo o dei protocolli/procedure aziendali di cui al Modello da parte di uno o più Amministratori, dei membri degli Organi Sociali va segnalata senza indugio all'OdV da parte di chi la rileva.

In particolare, in caso di violazione del Modello da parte di uno o più Amministratori, l'OdV informa tempestivamente Consiglio di Amministrazione e il Collegio Sindacale.

Il Consiglio di Amministrazione, con l'astensione del soggetto coinvolto, procede ad assumere, sentito il parere obbligatorio del Collegio Sindacale, una delle seguenti iniziative tenendo conto della gravità della violazione e conformemente ai poteri previsti dalla legge e/o dallo Statuto:

- dichiarazione nei verbali delle adunanze;
- diffida formale;
- revoca dei poteri delegati dal Consiglio di Amministrazione o dell'incarico affidato;
- convocazione dell'Assemblea con, all'ordine del giorno, l'adozione di adeguati provvedimenti nei confronti dei soggetti responsabili della violazione, ivi compreso l'esercizio di azioni legali volte al riconoscimento della responsabilità dell'amministratore nei confronti della Società e al ristoro dei danni patiti. Nel caso in cui le violazioni del Modello siano ritenute tali da compromettere il rapporto di fiducia con l'amministratore ovvero sussistano comunque gravi ragioni connesse alla tutela dell'interesse e/o dell'immagine della Società, il Consiglio di Amministrazione convoca l'Assemblea per deliberare in merito alla eventuale revoca dell'amministratore.

Sono in ogni caso salve le ipotesi di decadenza per giusta causa, senza diritto al risarcimento dei danni, dalle funzioni di Amministratore, di cui all'art. 14, comma 4, dello Statuto di FS Security.

In caso di violazione delle norme di cui al Decreto, del Modello, del relativo Codice Etico o dei protocolli/procedure aziendali di cui al Modello da parte di uno o più Sindaci, l'OdV, con esclusione delle ipotesi in cui gli accertamenti siano stati condotti a seguito di una segnalazione dallo stesso Collegio Sindacale o dal Consiglio di Amministrazione ai sensi della procedura interna sulle segnalazioni, ne informa il Consiglio di Amministrazione ed il Collegio Sindacale che, con l'astensione del soggetto coinvolto, per le valutazioni di competenza e affinché si proceda tempestivamente a convocare, sulla scorta di quanto previsto dalla legge e dallo Statuto, l'Assemblea, che potrà adottare le delibere opportune e conseguenti, ivi compresa la revoca per giusta causa nel rispetto della disciplina di cui all'art. 2400, comma 2, c.c.

7.5. MISURE NEI CONFRONTI DEI COMPONENTI DELL'ODV

In caso di violazioni del presente Modello da parte di uno o più componenti dell'OdV, gli altri componenti dell'OdV, ovvero uno qualsiasi tra i membri del Collegio Sindacale o del Consiglio di Amministrazione, informano immediatamente il Collegio Sindacale e il CdA della Società.

Tali Organi, previa contestazione della violazione e preso atto delle argomentazioni difensive eventualmente addotte, assumono gli opportuni provvedimenti ivi compresa, in presenza dei relativi presupposti, la revoca dell'incarico.

7.6. MISURE NEI CONFRONTI DEGLI ALTRI DESTINATARI

La violazione e l'inosservanza dei principi e delle disposizioni di cui al Decreto, del Modello, ivi incluso il Codice Etico di Gruppo, da parte degli altri Destinatari (quali, a titolo esemplificativo, Collaboratori, Fornitori, *Business*

Partner, Consulenti e Promotori Commerciali), come previsto da apposite clausole inserite nei relativi contratti, potrà costituire inadempimento delle obbligazioni contrattuali e comportare la risoluzione del contratto e in ogni caso legittimerà la Società a richiedere il risarcimento dei danni, secondo quanto previsto nelle clausole contrattuali che le competenti strutture aziendali cureranno, elaboreranno, aggiorneranno e inseriranno nei contratti, nelle lettere di incarico o negli accordi di *partnership.*

Inoltre, in tutti i contratti la controparte dovrà assumere l'impegno a risarcire, manlevare e tenere indenne FS Security rispetto a ogni costo, spesa, perdita, passività od onere, sostenuto e dimostrato che non si sarebbe verificato ove le dichiarazioni e garanzie rilasciate dalla controparte contenute nel contratto fossero state veritiere, complete, corrette ed accurate e gli impegni sopra descritti fossero stati puntualmente adempiuti.

7.7. MISURE RELATIVE ALLE SEGNALAZIONI

L'articolo 21, comma 2 del Decreto Legislativo n. 24 del 10 marzo 2023 ("*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")* prevede che nel sistema disciplinare adottato ai sensi dell'art. 6, comma 2, lettera e) del Decreto siano inserite delle sanzioni nei confronti di coloro che si accertano essere responsabili di alcuni illeciti, tra cui, a titolo esemplificativo, aver commesso delle ritorsioni, aver ostacolato (o tentato di ostacolare) una segnalazione o aver violato l'obbligo di riservatezza di cui all'articolo 12 del Decreto Legislativo n. 24 del 10 marzo 2023.

Pertanto, le misure e le sanzioni previste ai punti che precedono si applicano anche nei confronti dei Destinatari che siano responsabili degli illeciti di cui all' articolo 21 del Decreto Legislativo n. 24 del 10 marzo 2023.

8. COMUNICAZIONE, DIFFUSIONE E FORMAZIONE

La Società è consapevole dell'importanza della diffusione e comunicazione del Modello e del Codice Etico di Gruppo, nonché delle attività di formazione e si impegna a dare ampia divulgazione ai principi e alle regole di condotta contenuti nel presente Modello e nel Codice Etico di Gruppo, adottando le più opportune iniziative per promuoverne e diffonderne la conoscenza.

L'OdV monitora le iniziative volte a promuovere la comunicazione, la diffusione e la formazione sul Modello.

8.1. DIFFUSIONE

Le competenti funzioni aziendali provvederanno a curare la diffusione del contenuto del Modello e del Codice Etico di Gruppo nei confronti dei Destinatari.

I Destinatari sono tenuti ad avere piena conoscenza del contenuto del Modello e del Codice Etico di Gruppo, degli obiettivi di correttezza e trasparenza che si intendono perseguire con gli stessi, nonché delle modalità attraverso le quali FS Security intende perseguirli, e sono inoltre tenuti ad osservarli ed a contribuire alla loro efficace attuazione.

Ai Collaboratori, *Business Partner,* Fornitori e alle controparti delle attività di *business* è garantita la possibilità di accedere e consultare in qualsiasi momento sul sito *internet* di FS Security il Codice Etico di Gruppo e un estratto del Modello.

Inoltre, in merito alla comunicazione verso i soggetti terzi, sono inserite nei contratti tra questi ultimi e la Società apposite "clausole di integrità" volte a garantire il rispetto del Codice Etico di Gruppo, del Modello e della *Policy Anti-Corruption*, per quanto applicabili, con la previsione di rimedi contrattuali che ne sanzionino le violazioni, anche con la risoluzione del contratto nei casi più gravi.

È fatto obbligo a tutti i Dipendenti e ai componenti degli Organi Sociali di prendere visione del presente Modello e del Codice Etico di Gruppo pubblicati sui siti *intranet* ed *internet.*

In tutti i nuovi contratti di assunzione di FS Security o al momento della nomina quale membri degli Organi Sociali è previsto l'inserimento di un'informativa concernente l'adozione del Modello e del Codice Etico di Gruppo e contenente l'ultima versione adottata dalla Società di tali documenti; sarà inoltre fatta loro sottoscrivere una dichiarazione specifica attestante l'avvenuta conoscenza ed accettazione del Codice Etico di Gruppo, del Modello e della *Policy Anti-Corruption* e di osservanza dei contenuti ivi descritti.

Le procedure interne vigenti sono pubblicate e facilmente accessibili nell'*intranet* aziendale.

Il sito *intranet*, infine, assicura la diffusione di principi e valori nonché delle più importanti evoluzioni di legge, della normativa e dell'organizzazione interna.

8.2. FORMAZIONE

Ai fini dell'attuazione del Modello e per garantirne l'effettivo funzionamento, FS Security diffonde la conoscenza della normativa di cui al Decreto e promuove la sensibilizzazione e la formazione del personale sui principi e i contenuti del Modello.

L'attività di formazione è obbligatoria, capillare, efficace, autorevole, chiara e dettagliata, nonché periodicamente ripetuta ed è finalizzata a far acquisire, consolidare e aggiornare le conoscenze sul Modello e sulle procedure interne.

La formazione è indirizzata a tutto il personale ed è differenziata nei contenuti e nelle modalità di attuazione in funzione della tipologia dei destinatari cui si rivolge, della qualifica e del ruolo organizzativo ricoperto nella Società e del livello di rischio dell'area in cui questi operano.

FS Security propone le iniziative finalizzate al continuo rafforzamento del Modello (es. iniziative formative e di comunicazione), monitorandone l'attuazione e, tramite la competente funzione e struttura, predispone un piano annuale specifico di formazione sul Decreto nell'ambito della definizione del piano formativo di FS Security, sulla base dei fabbisogni formativi raccolti e delle proposte di iniziative formative.

Inoltre, il piano di formazione è trasmesso all'OdV, così da mettere tale organismo nella condizione di monitorare tale attività di formazione. Sono inoltre comunicati all'OdV eventuali aggiornamenti del piano.

8.2.1. PARTECIPAZIONE, REGISTRAZIONE, VERIFICA E MONITORAGGIO

La partecipazione alla formazione è obbligatoria e prevede la verifica della partecipazione in aula, in presenza o da remoto. La documentazione relativa alla formazione viene archiviata a cura delle competenti funzioni aziendali e messa a disposizione dell'OdV.

L'assenza non giustificata alle sessioni formative costituisce illecito disciplinare e comporta l'applicazione delle sanzioni disciplinari di cui al precedente paragrafo 7.2.

La tracciabilità della formazione è assicurata, indipendentemente dalla modalità scelta, dalla registrazione sul "libretto formativo" della risorsa, che viene archiviato nel sistema informativo aziendale.

La verifica di apprendimento della formazione è realizzata tramite specifici *test* a conclusione del percorso o dei singoli moduli formativi.

Viene, inoltre, effettuato un monitoraggio volto a verificare che il percorso formativo (*e-learning* e in aula) sia fruito da tutto il personale interessato e fornisce all'OdV evidenza delle attività svolte, dell'adesione ai corsi e dell'esito dei *test* di apprendimento.

Le risorse che non hanno superato i *test* di apprendimento sono sottoposte a nuovi cicli formativi.