Modello di Organizzazione, Gestione e Controllo

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

PARTE GENERALE

Aggiornato in data 22/04/2026

Matrice delle revisioni:
1ª edizione: 20/12/2023
2ª edizione: 30/10/2024
3ª edizione: 27/11/2024
4ª edizione: 20/01/2025
5ª edizione: 9/04/2025
6ª edizione: 22/04/2026

Indice

Allegato A	Codice Etico di Gruppo
Allegato B	Lista dei reati presupposto *ex* Decreto 231 astrattamente applicabili alla Società
Allegato C	Rappresentazione grafica dell'Assetto di *Governance* della Società
Allegato D	Matrice Identificazione Attività sensibili a Rischio-reato (MIAR)

Glossario

ATTIVITÀ SENSIBILE	Attività che potrebbe esporre, anche solo potenzialmente, la Società al rischio di commissione di uno dei reati contemplati nel Decreto a proprio interesse o vantaggio, con conseguente configurabilità della responsabilità amministrativa da reato in capo alla stessa.
AUTORITÀ GIUDIZIARIA	Il complesso degli organi che esercitano la giurisdizione ordinaria (i.e. organi giudicanti e organi 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.
COMPLIANCE	Presidio che, in ambito Affari Legali, Societari e Compliance assicura l'aggiornamento del 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.
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, 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., conformemente alle previsioni dell'art. 154-*bis* del D.Lgs. n. 58/1998.
ENTE	Ente dotato di personalità giuridica, società e associazioni anche prive di personalità giuridica, a cui si applicano le disposizioni di cui al Decreto (*i.e.* società di capitali, società di persone, associazioni, fondazioni, consorzi con attività esterna ecc.).
ENTE PRIVATO RILEVANTE	Enti privati, anche privi di personalità giuridica, che operano in modo indipendente nell'interesse generale e la cui attività professionale/istituzionale si traduce in valutazioni/giudizi/attestazioni che possono incidere sull'attività e/o influenzare l'apprezzamento di FS Security SpA e/o delle Società del Gruppo FS Italiane dall'esterno, ovvero dal cui mancato svolgimento possa derivare un vantaggio per FS Security SpA e/o delle Società del Gruppo FS (per esempio, agenzie di *rating*, analisti finanziari, organismi di certificazione e di valutazione di conformità, 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).
FS SECURITY o SOCIETÀ	FS Security S.p.A. con sede legale in Via Marsala, 27 - 00185 Roma.
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*". Anche un privato può essere qualificato come Incaricato di pubblico servizio quando svolge 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 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 S.p.A.
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.
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 attività sensibili identificate 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*" e 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	L'insieme di strumenti, strutture organizzative, norme e regole aziendali volte a consentire una conduzione dell'impresa sana, sostenibile, corretta e coerente con gli obiettivi aziendali definiti dal CdA, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, così come attraverso la strutturazione di adeguati flussi informativi volti a garantire la circolazione di informazioni idonee a consentire ai diversi attori coinvolti nel SCIGR di svolgere il ruolo loro affidato.

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*", 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], 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, nell'interesse o a vantaggio dell'Ente.

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

1) la commissione di un reato espressamente previsto nel catalogo dei c.d. reati presupposto indicati tassativamente nello stesso Decreto (artt. 24 e ss.). Successivamente all'emanazione del Decreto, il catalogo dei reati presupposto è stato negli anni integrato con nuove ipotesi criminose introdotte nel Decreto o in normativa speciale[3].

---

[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 categorie di reato attualmente previste dal Decreto:

- i reati commessi nei rapporti con la Pubblica Amministrazione, di cui agli artt. 24 e 25 del Decreto;
- i reati informatici, di cui all'art. 24-*bis* del Decreto;
- i delitti di criminalità organizzata, di cui all'art. 24-*ter* del Decreto;
- i reati in tema di falsità in moneta, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, di cui all'art. 25-*bis* del Decreto;
- i delitti contro l'industria e il commercio, di cui all'art. 25-*bis*.1 del Decreto;
- i reati societari, di cui all'art. 25-*ter* del Decreto;
- i delitti con finalità di terrorismo o di eversione dell'ordine democratico, di cui all'art. 25-*quater* del Decreto;
- pratiche di mutilazione degli organi genitali femminili, di cui all'art. 25-*quater*.1 del Decreto;
- i delitti contro la personalità individuale, di cui all'art. 25-*quinquies* del Decreto;
- i reati di abuso di mercato, di cui all'art. 25-*sexies* del Decreto;
- i delitti di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela della salute e sicurezza sul lavoro, di cui all'art. 25-*septies* del Decreto;
- i reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio, di cui all'art. 25-*octies* del Decreto;
- i delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori, di cui all'art. 25-*octies*.1 del Decreto;
- i reati in materia di violazione di misure restrittive dell'Unione europea, di cui all'art. 25-*octies*.2 del Decreto;
- i delitti in materia di violazione del diritto d'autore, di cui all'art. 25-*novies* del Decreto;

L'**Allegato B** contiene il testo completo e aggiornato delle fattispecie di reato ritenute applicabili ad FS Security SpA, nonché il testo di ciascuno degli articoli rilevanti del Decreto 231.

2) La commissione di un reato presupposto da parte di persone dell'Ente o funzionalmente legate all'Ente.
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[4];
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 consulenti, *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 più facilmente il rischio del coinvolgimento in concorso del dipendente e, quindi, ricorrendone i presupposti, di interesse e/o vantaggio dell'Ente.

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. In tale caso, l'*extraneus* risponderà in concorso del medesimo reato previsto a carico del soggetto qualificato. In ogni caso, non può escludersi che un soggetto dell'Ente o funzionalmente legato all'Ente, nell'esercizio di determinate attività, possa essere qualificato come Incaricato di Pubblico Servizio e, dunque, possa rispondere direttamente della commissione di un reato "proprio" al di fuori delle sopraindicate ipotesi di concorso. Ciò potrebbe verificarsi, ad esempio,

---

- il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, di cui all'art. 25-*decies* del Decreto;
- i reati ambientali, di cui all'art. 25-*undecies* del Decreto;
- i reati c.d. transnazionali (previsti dagli artt. 3-10 della Legge 16 marzo 2006, n. 146, per i quali introduce la responsabilità amministrativa dell'Ente, ai sensi del Decreto, l'art. 10 di suddetta legge);
- il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, di cui all'art. 25-duodecies del Decreto;
- i delitti di razzismo e xenofobia, di cui all'art 25-*terdecies* del Decreto;
- i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, di cui all'art. 25-*quaterdecies* del Decreto;
- i reati tributari, di cui all'art. 25–*quinquiesdecies* del Decreto;
- i reati di contrabbando, di cui all'art. 25–*sexiesdecies* del Decreto;
- i reati contro il patrimonio culturale, di cui all'art. 25-*septiesdecies* del Decreto;
- i reati di Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici, di cui all'art. 25-duodevicies del Decreto;
- i delitti contro gli animali, di cui all'art. 25-*undevicies* del Decreto.

Altre fattispecie di reato potranno in futuro essere inserite dal legislatore nel Decreto.

[4] L'art. 39 del Decreto prevede una presunzione di conflitto di interesse del legale rappresentante indagato di un reato presupposto ai fini del conferimento della nomina al difensore dell'Ente responsabile dell'illecito amministrativo. In particolare, affinché l'Ente possa validamente partecipare al procedimento penale, la procura al difensore dell'Ente dovrà essere conferita da un soggetto diverso dal legale rappresentante indagato del reato presupposto che sia munito dei relativi poteri.

nel caso in cui lo svolgimento di determinate attività sia disciplinato da una normativa pubblicistica o tali attività perseguano finalità pubbliche, pur se con gli strumenti privatistici propri delle società per azioni (assumono qualifica pubblicistica, ad es., i componenti della commissione di una gara di appalto a evidenza pubblica indetta dall'Ente di cui sono dipendenti).

3) La commissione di un reato presupposto 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 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[5], 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

[5] 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.

interdittiva).

Ai sensi dell'art. 10 del Decreto, le **sanzioni pecuniarie** vengono sempre applicate e si determinano attraverso un sistema basato su "quote", ovvero sul "fatturato globale totale" dell'Ente.
Nel primo caso, 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.

Nel secondo caso, ai sensi del comma 3 *bis* dell'art. 10, nei casi previsti dalla legge, la sanzione pecuniaria è determinata in relazione alla specifica percentuale, indicata per ciascun illecito, del fatturato globale totale dell'Ente relativo all'esercizio finanziario precedente quello in cui è stato commesso il reato o, se inferiore, all'esercizio finanziario precedente l'applicazione della sanzione pecuniaria. Qualora non sia possibile accertate il fatturato globale totale dell'Ente, la sanzione pecuniaria è applicata nell'importo determinato in relazione a ciascun illecito.

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 nonché dall'art. 25 *octies* 2. del Decreto, per i quali le sanzioni interdittive possono essere applicate per una durata massima di sei 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, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione - 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 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,[6] 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.

---

6 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.

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).
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 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 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 nelle 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;
g) attività e servizi di sicurezza logica in genere, tra cui: progettazione, realizzazione e gestione di sistemi di protezione; consulenza e formazione in materia di sicurezza informatica; monitoraggio e controllo del livello di sicurezza dei sistemi informatici; contrasto agli attacchi informatici; protezione dei sistemi informatici; supporto nello sviluppo sicuro delle applicazioni e dei sistemi informatici.

La Società può inoltre fornire:
- servizi amministrativi in materia di processi di qualificazione dei fornitori;
- servizi di gestione di banche dati fornitori;
- 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

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 Capofila di *Business Unit* e delle altre Società controllate Dirette, con l'obiettivo di svolgere funzioni di indirizzo strategico generale e di coordinamento attuativo e finanziario del comune disegno imprenditoriale del Gruppo[7].

Inoltre, relativamente ai processi trasversali o di *staff*, FS esercita il proprio ruolo anche tramite una gestione per "Comunità Professionali", 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 quattro 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.

2.2. LA STRUTTURA ORGANIZZATIVA

La struttura organizzativa di FS Security si articola in Strutture macro e 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*.

L'Allegato C contiene la rappresentazione grafica della struttura organizzativa e di *governance* di FS Security SpA.

---

7 L'attività di direzione e coordinamento della *Holding* riguarda elettivamente i seguenti ambiti: strategie generali d'impresa e di investimento; finanza; presidio e sviluppo dei mercati esteri; modifiche dei perimetri di business; innovazione e sviluppo tecnologico e digitale; legale, *governance* e assetti societari; operazioni straordinarie; linee guida metodologiche per i modelli di controllo interno e gestione dei rischi; macro-disegni organizzativi; relazioni istituzionali; modelli di compliance normativa (non tecnico-operativa o ambientale); linee guida metodologiche per i modelli di security; modelli e linee guida nei processi di *procurement*; modelli di budget, pianificazione e processi di reporting e amministrativi; politiche di gestione/sviluppo delle risorse umane di Gruppo; comunicazione e immagine.

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 SERVIZIO

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.

2.4. IL SISTEMA DI DELEGHE E PROCURE

L'Organo Amministrativo è l'organo preposto a conferire ed approvare formalmente 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, sin dal 2023, ritenuto conforme alle proprie politiche aziendali procedere all'adozione di un Modello nel tempo costantemente aggiornato in relazione agli intervenuti mutamenti nell'organizzazione e nelle attività condotte, alle novità legislative, all'evoluzione della giurisprudenza e alle best practice nazionali ed internazionali in materia.

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'aggiornamento 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 dell'Organo Amministrativo di FS Security.

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 Sensibili correlabili a tali rischi-reato;
   ii. delle Strutture aziendali responsabili di tali attività;
   iii. delle 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 uno specifico documento di *risk assessment*.

   Le attività di cui sopra sono state svolte all'esito di una preliminare analisi dell'assetto di *governance*, organizzativo e operativo della Società, nonché della storia pregressa di FS Security, anche mediante analisi della documentazione societaria e 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, contesto naturalistico, ecc.) in cui opera FS Security.

2. ***Gap analysis*** del sistema di controllo interno tramite:
   i. l'analisi del disegno del sistema di controlli esistenti ("*as is*") a presidio delle Attività Sensibili identificate;
   ii. la comparazione del sistema di controllo esistente rispetto ai requisiti identificati nella *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 le Attività Sensibili a rischio-reato, vale a dire quelle attività 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) presidi di controllo collegati alle Attività Sensibili nonché principi di comportamento a cui i destinatari del Modello devono attenersi;
  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
- 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 Sensibili;
- 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, un sistema normativo interno che identifica i principali controlli/procedure, disposizioni e norme comportamentali al fine di prevenire e minimizzare il rischio di commissione di reati presupposto.

Tali documenti sono adeguatamente diffusi all'interno di FS Security attraverso specifici meccanismi di comunicazione interna, fra cui la loro pubblicazione sull'intranet di Gruppo, il loro inoltro – via e-mail – 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** predisposte per le diverse categorie di reato previste dal Decreto.

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 categorie di reato considerate nel Decreto, sono analizzati: *(i)* le **fattispecie di reato astrattamente applicabili** alla Società in relazione alla specifica categoria di reato; *(ii)* 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; (*iii*) le **funzioni aziendali** coinvolte nell'esecuzione delle Attività Sensibili e che, astrattamente, potrebbero commettere i reati previsti dal Decreto 231; (*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

i Destinatari del Modello al fine di prevenire la commissione dei reati previsti dal Decreto.

In particolare, la Parte Speciale si compone delle seguenti sezioni:

Parte Speciale A.	Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del Decreto)
Parte Speciale B.	Delitti informatici e trattamento illecito di dati (art. 24-bis del Decreto)
Parte Speciale C.	Delitti di criminalità organizzata (art. 24-ter del Decreto) ed i reati c.d. "transnazionali" (previsti ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146)
Parte Speciale D.	Reati societari e di corruzione tra privati (art. 25-ter del Decreto)
Parte Speciale E.	Delitti contro la personalità individuale (art. 25-quinquies del Decreto)
Parte Speciale F.	Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies del Decreto)
Parte Speciale G.	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies del Decreto)
Parte Speciale H.	Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1 del Decreto)
Parte Speciale I.	Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)
Parte Speciale J.	Delitti in materia di violazione del diritto d'autore (art. 25-novies del Decreto)
Parte Speciale K.	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 25-decies del Decreto)
Parte Speciale L.	Reati ambientali (art. 25-undecies del Decreto)
Parte Speciale M.	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-duodecies del Decreto)
Parte Speciale N.	Reati tributari (art. 25-quinquiesdecies del Decreto)
Parte Speciale O.	Delitti contro il patrimonio culturale (art. 25-septiesdecies del Decreto) e riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies del Decreto)

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.

La funzione Compliance assicura l'aggiornamento del Modello 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 A), 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.

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.

In particolare, il Sistema Normativo Interno costituisce 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.

In linea con il percorso intrapreso, FS Security ha adottato in via di autoregolamentazione un insieme di documenti organizzativi che definisce l'architettura dell'intero sistema anticorruzione della Società e risponde all'esigenza di approcciare in via sistematica ed unitaria l'attività di prevenzione della corruzione nel suo complesso, promuovendo sinergie tra i diversi presidi anticorruzione. Tale sistema documentale, inoltre, supporta la Società nell'impegno verso lo sviluppo sostenibile e concorre al rafforzamento di una reputazione aziendale solida e credibile verso l'esterno, anche attraverso una normativa interna conforme a specifici standard anticorruzione e coerente con le best practice internazionali in materia.

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 (per le attività ed i presidi relativi alle fattispecie penali rilevanti in materia di corruzione);
- Modello di Gestione *Anti-Corruption.*

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 l'insieme di norme e regole aziendali volte a consentire

una conduzione dell'impresa sana, sostenibile, corretta e coerente con gli obiettivi aziendali definiti dall'Organo Amministrativo di FS Security SpA, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, così come attraverso la strutturazione di adeguati flussi informativi volti a garantire la circolazione delle informazioni idonee a consentire ai diversi attori coinvolti nel SCIGR di svolgere il ruolo loro affidato.

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.

La Società utilizza il Modello "*Controls – Integrated Framework*" emesso dal *Committee of Sponsoring Organizations of the Tradeway Commission* nel 2013 (c.d. CoSO Report[11]) quale *framework* di riferimento, internazionalmente riconosciuto, per l'implementazione, l'analisi e la valutazione del SCIGR.

Il SCIGR attualmente si articola in 3 livelli di controllo:

MANAGEMENT		
PRIMO LIVELLO	**SECONDO LIVELLO**	**TERZO LIVELLO**
Il **Management** si occupa di condurre verifiche periodiche dell'efficacia e dell'efficienza del disegno e dell'effettiva operatività dei controlli al fine di identificare e gestire e/o prevenire i rischi inerenti.	**Le funzioni aziendali preposte** (a titolo esemplificativo e non esaustivo, le strutture: Affari Legali, Societari e Compliance, *Risk & Anti-Corruption* e Dirigente Preposto) forniscono supporto al primo livello nella definizione e implementazione di adeguati sistemi di controllo e di gestione dei principali rischi inerenti.	**Audit** si occupa di fornire assurance indipendente e obiettiva sull'adeguatezza ed effettiva operatività del primo e secondo livello di controllo e in generale sul SCIGR nel suo complesso.

I 3 livelli di controllo comunicano, collaborano e si coordinano attraverso appositi flussi informativi, nel rispetto dei propri ruoli e delle proprie responsabilità, con l'obiettivo di massimizzare l'efficacia ed efficienza dei sistemi di controllo al fine di ottimizzare la gestione del rischio e, per l'effetto, di accrescere il valore della Società sul mercato.

5.3.1. 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.

- **Modello di Controllo Interno e Gestione dei Rischi sull'Informativa Economica Finanziaria e sull'informativa di sostenibilità**

  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*). Parallelamente, anche tenendo conto del mutato contesto normativo (D.Lgs. n. 125 del 6 settembre 2024), è stato definito il Modello di controllo interno sull'informativa di sostenibilità (Modello di sostenibilità), il quale, per ragioni di efficacia ed efficienza del sistema complessivo dei controlli interni, si basa e si integra con il suddetto Modello 262. Tali sistemi supportano la completezza, correttezza e accuratezza delle informazioni finanziarie e di sostenibilità, tutelando investitori, enti di controllo e *Stakeholder*.

- **Modello data protection**

  In ottemperanza a quanto previsto dal Regolamento (UE) 2016/679 (*General Data Protection Regulation* – c.d. GDPR), il Gruppo FS ha adottato ed applica un proprio modello gestionale per la protezione dei dati personali costituito dall'insieme di regole e metodi definiti dal sistema delle norme organizzative, i ruoli e le responsabilità delle funzioni coinvolte, i processi e i sistemi informativi, i flussi informativi (da e verso il CdA, i vertici aziendali, le strutture che partecipano alla realizzazione del *Framework di Data Protection* e quelle coinvolte nel trattamento), il sistema dei controlli e della loro tracciabilità rivolto alla gestione e mitigazione dei rischi per i diritti e le libertà delle persone fisiche legati al trattamento di dati personali.

  Il Gruppo FS 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*.

- ***Framework* di Compliance**

  Il *Framework* di Compliance definisce l'architettura del Sistema di Gestione della Compliance nel Gruppo FS e individua gli obiettivi e i principi di riferimento per la gestione del rischio di Compliance. Tale *Framework* è costituito dall'insieme dei documenti che contengono i principi, gli indirizzi e le regole in materia di Compliance, quali:

  - la *Policy* di Compliance, che indica i principi di riferimento per la gestione del rischio di compliance e definisce la relativa governance, attribuendo ruoli e responsabilità del processo di compliance ed evidenziando il ruolo di leadership del CdA;
  - il Modello di Compliance, che descrive e disciplina le attività attraverso le quali le funzioni societarie attuano la gestione dei rischi di compliance;
  - la Tassonomia degli ambiti di Compliance, che costituisce la mappa degli Ambiti di Compliance rilevanti per il Gruppo.

  La funzione Compliance & 231 di *Holding*, collocata a diretto riporto della struttura "*Anti-Corruption, Risk & Compliance*", assicura la definizione di strategie, indirizzi, politiche, linee guida e standard di Gruppo in materia di conformità normativa.

  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.

- **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 DI FS SECURITY

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

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 funzioni aziendali nonché l'ambito in cui le stesse possono essere impiegate, attraverso la programmazione e definizione del *budget*;
- garantire la predisposizione del *budget* sulla base di obiettivi di *business* "ragionevoli", previa adeguata analisi dei risultati degli anni precedenti;
- rilevare gli eventuali scostamenti rispetto a quanto predefinito in sede di *budget*, analizzarne le cause e riferire i risultati delle valutazioni ai livelli gerarchicamente responsabili al fine di predisporre i più opportuni interventi di adeguamento, attraverso la relativa consuntivazione.

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, 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

L'Organismo è un organo collegiale composto da tre membri, di cui (i) almeno due sono soggetti di provenienza esterna al Gruppo, uno dei quali – in possesso di specifiche competenze sul Decreto – viene altresì nominato presidente, e (ii) il terzo è un altro soggetto di provenienza esterna al Gruppo o come alternativa è il Responsabile della struttura Audit in carica. Un componente esterno al Gruppo che non ricopre l'incarico di presidente può essere individuato in un membro del Collegio Sindacale. I componenti esterni al Gruppo devono possedere le necessarie competenze per lo svolgimento dell'incarico (di natura giuridica e/o economico-aziendale). Almeno uno di essi deve possedere competenze giuridiche. Qualora l'OdV si componga esclusivamente di membri esterni, il medesimo OdV, al fine di favorire l'integrazione e la sinergia tra gli attori del sistema di controllo interno, con propria delibera stabilisce se (i) il Responsabile della struttura Audit in carica partecipi stabilmente come uditore alle riunioni dello stesso con funzioni consultive e di supporto, ovvero se (ii) il predetto responsabile venga di volta in volta convocato dall'OdV per partecipare a singole riunioni o alla trattazione di specifici argomenti, sempre con funzioni consultive e di supporto.

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 dovrà 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

Il soggetto incaricato a ricoprire la carica di membro dell'Organismo di Vigilanza possiede 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 e che sia garantita l'onerosità dell'incarico conferito, al fine di estendere l'indipendenza e l'autonomia dell'OdV anche all'aspetto finanziario.
- 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. A tal fine, l'OdV si riunisce periodicamente sulla base di apposita calendarizzazione delle riunioni, così assicurando la continuità e l'effettività dell'attività di vigilanza.

La continuità di azione impone inoltre di fare in modo che l'Organismo di Vigilanza sia a conoscenza dei processi aziendali e possa avere un diretto contatto con le funzioni societarie relative alle attività sensibili, in modo da ricevere riscontri sull'efficacia del sistema di controllo di cui al Modello.

- 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

L'incarico dell'OdV è conferito per la durata di tre anni e può essere rinnovato per non più di tre mandati consecutivi.

In ogni caso, l'OdV 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'Organo Amministrativo 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, debitore assoggettato a liquidazione giudiziale 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.

La **revoca** dell'OdV quale organo può avvenire solo per giusta causa, anche al fine di garantirne l'assoluta indipendenza.

Per giusta causa di revoca si intendono in via esemplificativa e non esaustiva: (i) una grave negligenza nell'espletamento dei compiti connessi all'incarico (ii) il possibile coinvolgimento dell'Ente in un procedimento, penale o civile, che sia connesso ad una omessa o insufficiente vigilanza.
La revoca per giusta causa è disposta con delibera dell'Organo Amministrativo.
In caso di scadenza, revoca o rinuncia, l'Organo Amministrativo nomina senza indugio il nuovo OdV.
In caso di rinuncia di tutti i componenti dell'OdV, sarà trasmessa apposita comunicazione scritta all'Organo Amministrativo.
Al di fuori delle ipotesi riguardanti l'intero OdV, la cessazione dell'incarico di un singolo componente può avvenire: (i) a seguito di revoca per giusta causa dell'incarico da parte dell'Organo Amministrativo, sentito il parere del Collegio Sindacale; (ii) a seguito di rinuncia all'incarico, formalizzata mediante apposita comunicazione scritta inviata all'Organo Amministrativo; (iii) qualora sopraggiunga una delle cause di decadenza.

Per giusta causa di revoca devono intendersi, oltre alle ipotesi sopra previste per l'intero OdV, a titolo esemplificativo, anche le seguenti ipotesi: 1) il caso in cui il singolo componente sia coinvolto in un processo penale avente ad oggetto la commissione di un delitto doloso; 2) il caso in cui sia riscontrata la violazione degli obblighi di riservatezza previsti a carico dei membri dell'OdV; 3) il caso di assenza ingiustificata per più di tre volte consecutive alle riunioni dell'OdV.

Il Consiglio di Amministrazione di FS Security, in caso di cessazione dalla carica, per qualsiasi ragione, di un componente dell'OdV, nomina senza indugio un nuovo componente. 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 Vertice Aziendale, ai fini degli opportuni provvedimenti, di quelle violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo all'ente;
- predisposizione, su base almeno semestrale, di una relazione informativa all'Organo Amministrativo riguardante le attività svolte nel periodo di riferimento e le altre notizie ritenute di rilievo;
- 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 Amministrativo 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.

6.5. MODALITÀ DI FUNZIONAMENTO E SUPPORTO ALL'ODV

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

In ogni caso, il Presidente può convocare l'Organismo di Vigilanza anche al di fuori delle riunioni schedulate e l'Amministratore Delegato, il Consiglio di Amministrazione o organo equivalente e il Collegio Sindacale possono in qualsiasi momento chiedere al Presidente di convocare l'OdV.

L'OdV, al fine di svolgere le proprie funzioni di vigilanza, può avvalersi del supporto operativo della struttura *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.

Le violazioni degli obblighi di informazione nei confronti dell'OdV potranno comportare l'applicazione di sanzioni disciplinari di cui al seguente paragrafo 7.
I flussi informativi periodici attivati con i *Process Owner* sono riportati in apposito documento.

All'OdV, infine, deve essere comunicato, ovvero messo comunque a disposizione, il sistema di deleghe adottato da FS Security SpA ed ogni successiva modifica allo stesso.

6.8. SEGNALAZIONI

I Destinatari informano 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 e con la normativa di riferimento.

Come previsto dalla "*Procedura per la gestione delle segnalazioni*", le segnalazioni sono indirizzate al Comitato Etico e Segnalazioni e/o all'Organismo di Vigilanza di Società e sono gestite con il supporto della struttura Audit della Società.

In particolare, devono essere indirizzate all'Organismo di Vigilanza della Società, tramite i canali informativi dedicati istituiti ai sensi del D.Lgs. n. 24/2023 di seguito richiamati, le segnalazioni relative a condotte illecite rilevanti ai sensi del Decreto o a violazione del Modello e/o delle procedure che ne costituiscono attuazione.

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.

In attuazione delle disposizioni di cui all'art. 6, comma 2-bis, del Decreto, (così come modificato dal D. Lgs. 24/2023), ai sensi del quale 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.

FS Security si è dotata dei seguenti canali di segnalazione interna:

- piattaforma informatica: accessibile tramite il sito internet di FS Security SpA www.fsitalianesecurity.it nella sezione Chi siamo – Etica, compliance e integrità – Gestione delle segnalazioni – Whistleblowing/Ordinarie o dalla rete intranet aziendale. 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;
- linea telefonica con sistema automatico di risposta (*Interactive Voice Response*): accessibile al numero di telefono dedicato alle segnalazioni *Whistleblowing* per FS Security S.p.A. +39 0682950720, che prevede: i) la registrazione della chiamata dietro consenso espresso del Segnalante; ii) la contraffazione della voce registrata del Segnalante al fine di renderla non riconoscibile; iii) l'inserimento della segnalazione all'interno della piattaforma informatica per la gestione delle segnalazioni;
- 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 garantire la riservatezza dell'identità del segnalante a partire dalla ricezione della segnalazione (fatti salvi gli obblighi di legge) e vieta ogni forma diretta o indiretta di provvedimenti e comportamenti ritorsivi o discriminatori adottati nei confronti del segnalante in conseguenza della segnalazione, ovvero di condotte volte a ostacolare o tentare di ostacolare il segnalante nell'effettuazione della segnalazione medesima.
Le tutele sopra descritte sono garantite ai segnalanti anche nel caso in cui la segnalazione non si sia poi rivelata fondata, salvo il caso di segnalazione effettuata con dolo o colpa grave.

La Società tutela altresì i diritti delle persone coinvolte assicurandone la riservatezza.

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.
Per il dettaglio sulle modalità di ricezione e gestione delle segnalazioni, si rimanda alla "*Procedura per la gestione delle segnalazioni*" emanata dalla Società.

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 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, ovvero quando la segnalazione è stata ostacolata o che si è tentato di ostacolarla;
  - 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 o a terzi

(rispetto ai quali la Società possa essere ritenuta responsabile) ovvero l'abbia esposta ad un procedimento per responsabilità amministrativa ai sensi del Decreto; altre particolari circostanze soggettive e/o oggettive 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 e dall'art. 66 del CCNL della Mobilità – Area Attività Ferroviarie vigente.

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

Si tratta di:

a) rimprovero verbale o scritto;
b) multa;
c) sospensione dal servizio e dalla retribuzione (graduate in 3 livelli di gravità);
d) licenziamento con o senza preavviso.

Salvo che le singole violazioni non possano essere valutate in termini di maggiore gravità, secondo i criteri sopra descritti da considerare ai fini di tale valutazione e confermata la possibilità – qualora ne ricorrano i presupposti – dell'applicazione dell'istituto della c.d. "recidiva", 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 paragrafo7.1.

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 applicabili le seguenti sanzioni nel rispetto del principio di proporzionalità, avuto riguardo alla gravità dell'infrazione commessa:

a) richiamo/nota riservata di censura: 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 ed istantaneamente il rapporto di fiducia, non consentendo la prosecuzione neppure temporanea del rapporto di lavoro.

Il procedimento disciplinare è regolato dall'art. 7 della legge n. 300/1970, dalle norme del CCNL della Mobilità – Area Attività Ferroviarie 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 dal soggetto che la rileva.

In caso di violazione del Modello da parte di uno o più Amministratori, l'OdV informa 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. Nel caso in cui le violazioni del Modello siano concretizzate da parte di uno o più Amministratori, che siano - allo stesso tempo - dirigenti con rapporto di lavoro subordinato, si procederà – altresì – all'adozione delle misure di cui al precedente paragrafo 7.3.

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 dell'OdV, uno qualsiasi tra i membri del Collegio Sindacale o del Consiglio di Amministrazione, informa 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 (i.e. Collaboratori, Fornitori e Consulenti), 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 funzioni 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 prevede che nel sistema disciplinare adottato ai sensi dell'art. 6, comma 2, lettera e) del Decreto siano previste 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, 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, con riferimento ai rapporti contrattuali con soggetti terzi, la Società prevede l'inserimento, nei relativi contratti, di apposite "clausole di integrità" volte a richiamare il rispetto del Codice Etico di Gruppo, del Modello e della *Policy Anti-Corruption*.
Tali clausole sono formulate tenendo conto del contesto negoziale, delle caratteristiche del rapporto e della natura della controparte e possono pertanto essere previste e/o declinate in modo coerente con le esigenze sottese al singolo rapporto e con il livello di rischio rilevante nel caso concreto. Le clausole di integrità contemplano inoltre l'adozione di rimedi contrattuali proporzionati in caso di violazione, fino alla risoluzione del contratto nei casi di maggiore gravità.
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.

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 del Modello di Gestione *Anti-Corruption* e di osservanza dei contenuti ivi descritti.

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

Il sito *intranet* di FS Security, 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, ivi incluso il Codice Etico.

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 promuove le iniziative finalizzate al continuo rafforzamento del Modello (es. iniziative formative e di comunicazione), monitorandone l'attuazione e, tramite la competente struttura aziendale, predispone un piano annuale specifico di formazione sul Decreto ("Piano Annuale") 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 Annuale 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 Annuale.
Le modalità formative adottate consistono:

- in via principale in corsi e-learning erogati sulla piattaforma informatica di Gruppo attraverso la intranet aziendale;
- in sessioni formative in aula / seminari, secondo le indicazioni del Piano Annuale.

In particolare, con riferimento ai fabbisogni formativi individuati nel Piano Annuale, sono previste le seguenti attività formative:

- Tutto il personale di FS Security SpA: formazione e-learning, avente ad oggetto i principali contenuti della normativa di riferimento - con particolare approfondimento dei reati-presupposto della responsabilità amministrativa degli enti - e le componenti generali del Modello e del Codice Etico;
- Dirigenti e quadri che operano in particolari aree sensibili e che per il ruolo rivestito sono coinvolti in attività esposte a rischi di reato: formazione attraverso interventi formativi in aula / seminari aventi ad oggetto l'approfondimento degli aspetti più rilevanti del Decreto e del Modello, anche con riferimento alle attività gestite. Gli interventi formativi in aula prevedono la trattazione di argomenti oggetto di periodici aggiornamenti appositamente pianificati.

Detti soggetti provvedono al proprio continuo aggiornamento, ad esempio anche tramite partecipazione a *workshop* sulla materia.

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 può comportare l'applicazione delle sanzioni disciplinari di cui al precedente paragrafo 7.

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.