Il Chief Legal Officer

International Compliance Program

Tipologia documento:
Policy

ID: n° 56_v.02

Ambito di applicazione:
Gruppo

Processo:

Sistema del Controllo Interno e Gestione dei Rischi/Compliance e 231

Data: 30/06/2025

INDICE

DISCLAIMER

I principi e le regole di comportamento definiti nel presente documento costituiscono presidi di controllo anche ai fini anticorruzione e di prevenzione dei rischi di compliance e dei rischi-reato ex D. Lgs. 231/2001 dando attuazione a quanto previsto dal Modello di Organizzazione, Gestione e Controllo adottato dalle Società ai sensi del d.lgs. 231/2001 (Modello 231), dal Codice Etico del Gruppo FS Italiane, dalla Policy Anti-Corruption del Gruppo FS Italiane e dal Modello di Gestione Anti-Corruption [1], dal Framework di Data Protection e dal Framework di classificazione e protezione della riservatezza della informazione del Gruppo FS Italiane.

Si raccomanda ai Responsabili delle strutture coinvolte il costante monitoraggio del presente documento al fine di garantirne la corretta applicazione ed il costante adeguamento ai fini della sua efficacia. Chiunque venisse a conoscenza di eventuali violazioni o tentata elusione del presente documento è tenuto ad informare tempestivamente l'Organismo di Vigilanza e/o il Comitato Etico e Segnalazioni di Società, secondo le modalità previste dalla Procedura per la Gestione delle Segnalazioni e dal Modello 231.

PRESIDI DI CONTROLLO

- ☑ D. Lgs. 231/2001
- ☑ Anti-Corruption

Quanto disciplinato nel presente documento è da intendersi in coerenza con quanto previsto dal Modello di Governance del Gruppo FS Italiane e dal Regolamento di Gruppo. Ove mai dal testo si possano ricavare elementi teoricamente riferibili alle tematiche inerenti e/o funzionali alle attività escluse dalla direzione e coordinamento della Holding, prevale l'esclusiva competenza di ciascuna singola Società del Gruppo.

[1] Ove adottato dalla Società. Il modello è stato pubblicato nella sua prima edizione con la denominazione "Anti-Bribery&Corruption management system" (DdG n. 247 P/AD del 23/02/2018 e corrispondenti documenti societari). Nel rispetto delle proprie peculiarità, Anas SpA e QMU SpA hanno adottato un proprio modello volontaristico di organizzazione e gestione per la prevenzione della corruzione e trasparenza.

INTRODUZIONE

Il Gruppo FS Italiane (di seguito anche Gruppo FS) ha una consolidata presenza a livello internazionale garantita dall'impegno diretto delle proprie Società Controllate Estere, che operano in settori/mercati diversi e complementari.

Negli ultimi anni, molti Paesi in cui il Gruppo FS opera hanno istituito un regime di responsabilità per le persone giuridiche in relazione a comportamenti illeciti commessi da rappresentanti, dipendenti o terzi che agiscono nel loro interesse. La maggior parte di queste normative incoraggia le Società ad adottare strutture di *corporate governance* e sistemi di prevenzione dei rischi, prevedendo, talvolta, un'esenzione o un'attenuazione delle sanzioni applicabili ove siano state adottate adeguate misure di prevenzione.

In tale contesto, il Gruppo FS conferma l'impegno a prevenire e contrastare le attività illecite nel proprio *business*.

Il presente documento si inserisce come pilastro per il potenziamento del Sistema di Controllo Interno e di Gestione dei Rischi a livello di Gruppo, in conformità alle principali e più recenti *best practice* e normative in materia di programmi di compliance[2], al fine di armonizzare i principi da applicare per fornire un approccio condiviso, coerente e globale contro i comportamenti illeciti o elusivi della normativa applicabile.

[2] Gli esempi includono, ma non si limitano a, quanto segue:
- il D. Lgs. dell'8 giugno 2001, n. 231, e successivi aggiornamenti, che disciplina il regime di responsabilità amministrativa (assimilabile ad una responsabilità penale) delle persone giuridiche derivante dalla commissione di determinati reati nell'interesse o vantaggio delle stesse;
- il "*Codice di Corporate Governance*" delle società quotate promosso da Borsa Italiana S.p.A.;
- il "*Federal Sentencing Guidelines Manual & Supplement*", adottato dalla United States Sentencing Commission il 1° novembre 2010;
- il "*Foreign Corruption Practice Act*" ("FCPA") del 1977 e i successivi aggiornamenti;
- il "*UK Bribery Act*" del 2010 e successivi aggiornamenti;
- la "*Good Practise Guidance on Internal Controls, Ethics, and Compliance*" adottata dal Consiglio dell'OCSE il 18 febbraio 2010;
- la "*Resource Guide to the U.S. Foreign Corrupt Practices Act*" emanata dalla Criminal Division of the U.S. Department of Justice ("DOJ") e dalla Enforcement Division of the U.S. Securities and Exchange Commission del 2012 e successivi aggiornamenti;
- l'"*Evaluation of Corporate Compliance Programs*" del DOJ del 2017 e successivi aggiornamenti;
- l' "*Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide*" adottato dall'United Nations Office of Drugs and Crime ("UNODC") nel settembre 2013;
- le raccomandazioni adottate dal Financial Action Task Force – Gruppo d'Azione Finanziaria Internazionale ("FATF-GAFI" o "GAFI") sul riciclaggio e sul finanziamento del terrorismo del 2012 e successivi aggiornamenti;
- i Regolamenti europei in materia di riciclaggio, ricerca, sequestro e confisca dei proventi da reato e sul finanziamento del terrorismo (tra cui la Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 e il Regolamento delegato (UE) 2016/1675 e successivi aggiornamenti).

SCOPO

L'International Compliance Program rappresenta un'opportunità per rafforzare il Sistema di Controllo Interno e Gestione dei Rischi ed è concepito per promuovere comportamenti basati sui principi di lealtà, correttezza, onestà, integrità e rispetto di leggi, normative, standard e *best practice*.

L'International Compliance Program mira a prevenire il rischio di compliance, ossia il rischio di incorrere in violazioni di norme (legislative o regolamentari), nazionali o internazionali, o di autoregolamentazione (ad es., statuti, codici di condotta, codici di autodisciplina) che, oltre a poter arrecare danni alla reputazione delle Società e del Gruppo, possono comportare sanzioni, comminate da autorità giudiziarie o amministrative, nazionali, estere o sovranazionali, anche con provvedimenti restrittivi e interdittivi (ad es., sospensione o cessazione dell'attività, divieto di contrattare con la Pubblica Amministrazione, inserimento in *black list*, interdizione, *etc.*) in grado di compromettere la continuità aziendale nonché di generare significative perdite economiche e finanziarie.

In questo contesto, l'International Compliance Program identifica gli Standard Generali di Controllo, gli Ambiti di Compliance, le Aree a Rischio e gli Standard Specifici di Comportamento al fine di fornire ai destinatari un insieme di regole standard volto a prevenire la responsabilità della Società.

Ogni Società Estera è responsabile in via esclusiva della prevenzione dei rischi di reato nell'ambito della propria organizzazione.

Ogni Società Estera è tenuta, per quanto ritenuto necessario e opportuno, ad introdurre ogni presidio di controllo, nonché ad integrare, adottare o sviluppare i principi e le indicazioni riportate nel presente documento.

Inoltre, ogni Società Estera è in ogni caso tenuta ad identificare ulteriori Ambiti di Compliance, Aree a Rischio e Standard Specifici di Comportamento riconducibili al proprio contesto operativo e alla normativa locale di riferimento e ad adottare, se necessario, ulteriori strumenti di prevenzione e controllo per far fronte agli specifici rischi individuati, anche in attuazione della normativa di Gruppo.

Le previsioni contenute nell'International Compliance Program sono integrate dalle disposizioni contenute:

- nel Codice Etico del Gruppo;
- nella Policy Anti-Corruption del Gruppo e nei Modelli di Gestione Anti-Corruption societari;
- nella Sanction Policy di Gruppo;
- nel Programma di Compliance Antitrust di Gruppo;
- Framework Data Protection di Gruppo;

- nella Strategia Fiscale del Gruppo;
- nel Regolamento per la gestione interna e comunicazione all'esterno delle informazioni privilegiate e per il trattamento delle informazioni riservate;
- nel Modello di Controllo Interno e Gestione dei Rischi sull'Informativa Economica Finanziaria del Gruppo Ferrovie dello Stato Italiane;
- nelle linee guida, nelle procedure e nei documenti organizzativi societari e di Gruppo.

AMBITO DI APPLICAZIONE

- Ferrovie dello Stato Italiane SpA
- FS International SpA e FS Logistix SpA
- Società Estere del Gruppo FS Italiane[3]

ATTO DI DIREZIONE E COORDINAMENTO ☑

MODALITÀ DI ADOZIONE SOCIETARIA

Il presente documento è un atto di direzione e coordinamento.

FS International SpA, FS Logistix e le Società controllate estere[4] adottano, nel rispetto delle proprie prerogative di autonomia ed indipendenza, il presente documento, nonché assicurano la corretta e costante applicazione di quanto definito, la massima diffusione al proprio interno ed il relativo controllo attuativo, nel rispetto degli obblighi di riservatezza e delle prerogative di autonomia e indipendenza di ciascuna Società.

- ☑ Applicabilità diretta
- ☐ Applicabilità con caratterizzazione organizzativa
- ☐ Applicabilità con integrazione
- ☐ Applicabilità con definizione di processo

[3] Per Società Estere del Gruppo FS si intendono le Società estere controllate da FS SpA ai sensi dell'art. 2359, comma 1, numeri 1) e 2) del codice civile.

[4] Le Società estere adottano i principi disciplinati in coerenza con l'ordinamento giuridico ove la Società ha la sede legale

RUOLI E RESPONSABILITÀ

Funzione compliance di FS SpA

La funzione compliance di FS SpA assicura:

- la predisposizione e l'aggiornamento dell'International Compliance Program;
- la promozione, interfacciandosi con le competenti funzioni aziendali, di opportune e specifiche campagne di informazione e comunicazione volte a garantire la conoscenza dell'International Compliance Program con il supporto della funzione human resources di FS International SpA;
- l'informativa periodica ai vertici aziendali e agli organi di controllo sullo stato di adozione dell'International Compliance Program, con il supporto della funzione human resources di FS International SpA.

Funzione human resources di FS International SpA

La funzione human esources di FS International SpA:

- monitora lo stato di adozione dell'International Compliance Program da parte delle Società Estere, interfacciandosi con le competenti funzioni aziendali;
- supporta la funzione compliance di FS SpA nella predisposizione dell'informativa periodica ai vertici aziendali e agli organi di controllo sullo stato di adozione dell'International Compliance Program;
- supporta la funzione compliance di FS SpA e le competenti funzioni aziendali nella promozione di opportune e specifiche campagne di informazione e comunicazione volte a garantire la conoscenza dell'International Compliance Program.

Funzione compliance di Società Estera (o Focal Point Compliance)

La funzione compliance di ciascuna Società Estera (o Focal Point Compliance), in relazione al contesto operativo e nel rispetto della normativa locale di riferimento, ha il compito di:

- valutare l'adeguatezza dell'International Compliance Program rispetto al contesto operativo e alla normativa locale di riferimento;
- identificare eventuali ulteriori Ambiti di Compliance, Aree a Rischio e/o Standard Specifici di Comportamento e valutare l'adozione/aggiornamento di ulteriori strumenti di prevenzione e controllo per far fronte agli specifici rischi individuati, anche in attuazione della normativa di Gruppo;
- supportare le strutture aziendali competenti nella definizione e/o nell'aggiornamento degli strumenti normativi interni a presidio degli Ambiti di Compliance;

- promuovere, interagendo con le strutture aziendali competenti, adeguate e specifiche campagne di formazione, informazione e comunicazione volte a garantire la conoscenza dell'International Compliance Program;
- assicurare, nell'ambito dei flussi informativi periodici verso i vertici aziendali e gli Organi di controllo previsti dal Modello di Compliance di Gruppo, un'informativa in merito allo stato di adozione dell'International Compliance Program.

AMBITI DI COMPLIANCE

Il perimetro del documento ricomprende i seguenti Ambiti di Compliance:

a) Reati di corruzione;
b) Altri reati contro la Pubblica Amministrazione;
c) Frodi contabili;
d) Reati fiscali;
e) Criminalità organizzata;
f) Finanziamento del terrorismo e c.d. reati di riciclaggio di denaro;
g) Abusi di mercato;
h) Reati contro la personalità individuale;
i) Reati in materia di salute e sicurezza;
j) Reati ambientali;
k) Reati informatici;
l) Reati in materia di violazione del diritto d'autore;
m) Contrabbando;
n) Reati contro il patrimonio culturale.

L'elenco degli Ambiti di Compliance, così come le Aree a Rischio e i relativi Standard Specifici di Comportamento individuati nel documento Allegato, sono la base di partenza per le Società Estere per effettuare una propria valutazione del contesto operativo e della normativa locale di riferimento volta ad individuare ulteriori Ambiti di Compliance, Aree a Rischio e/o Standard Specifici di Comportamento (*Risk Assessment*) e valutare l'adozione/aggiornamento di strumenti di prevenzione e controllo (*Gap Analysis*).

MONITORAGGIO

Il compito di monitorare l'adeguatezza e l'osservanza dell'International Compliance Program è affidato alla funzione compliance di Società Estera (o Focal Point Compliance), che in relazione al contesto operativo e

nel rispetto della normativa locale di riferimento, è responsabile di:

- valutare l'adeguatezza dell'International Compliance Program;
- identificare eventuali ulteriori Ambiti di Compliance, Aree a Rischio e/o Standard Specifici di Comportamento e valutare l'adozione/aggiornamento di ulteriori strumenti di prevenzione e controllo per far fronte agli specifici rischi individuati;
- supportare le strutture aziendali competenti nella definizione e/o nell'aggiornamento degli strumenti normativi interni a presidio degli Ambiti di Compliance.

Inoltre, la funzione human resources di FS International SpA monitora lo stato di adozione dell'International Compliance Program da parte delle Società Estere, interfacciandosi con le competenti funzioni aziendali.

REPORTING

Nell'ambito dei flussi informativi periodici previsti dal Modello di Compliance di Gruppo, la funzione compliance di Società Estera (o Focal Point Compliance) riferisce ai vertici aziendali e agli organi di controllo in merito allo stato di adozione dell'International Compliance Program..

Inoltre, la funzione compliance di FS SpA, con il supporto della funzione human resources di FS International SpA, fornisce un'informativa periodica ai vertici aziendali e agli organi di controllo di FS sullo stato di adozione dell'International Compliance Program nel Gruppo in occasione dei flussi informativi periodici previsti dal Modello di Compliance di Gruppo.

FORMAZIONE E COMUNICAZIONE

FS SpA e ciascuna Società Estera promuovono la conoscenza del contenuto dell'International Compliance Program.

Ciascuna Società Estera pianifica e gestisce le attività di formazione sui contenuti dell'International Compliance Program e/o degli ulteriori strumenti di prevenzione e controllo eventualmente previsti per far fronte agli specifici rischi individuati e monitora che il percorso formativo pianificato sia fruito da tutto il personale interessato.

In linea con le più recenti best practice, la formazione deve essere "*real life scenario based*", ossia misurata sui casi pratici delle possibili modalità di violazione degli Standard Generali di Controllo e degli Standard Specifici di Comportamento previsti all'interno di ciascuna Area a Rischio e delle possibili condotte da adottare per garantire il rispetto dell'International Compliance Program, nonché istruzioni per individuare e gestire le

potenziali "*red flags*".

La partecipazione alle attività di formazione è obbligatoria.

Al fine di garantire la massima diffusione dei contenuti dell'International Compliance Program e l'efficacia delle regole di condotta e delle misure di prevenzione in esso contenute, l'International Compliance Program deve essere reso disponibile attraverso canali di comunicazione interni (intranet aziendale) e esterni (sito web).

I principi e i contenuti del presente documento sono portati a conoscenza dei Terzi attraverso clausole contrattuali che, in base all'attività regolata dal contratto, vincolino la controparte al rispetto delle previsioni ad essa direttamente applicabili.

SISTEMA DISCIPLINARE E RIMEDI CONTRATTUALI

La violazione dell'International Compliance Program da parte del personale delle Società del Gruppo può comportare sanzioni disciplinari secondo le misure definite da ciascuna Società.

La violazione da parte di Terzi dei principi o delle previsioni dell'International Compliance Program può comportare, sulla base di specifiche valutazioni della Società del Gruppo interessata, la mancata instaurazione o la risoluzione dei rapporti contrattuali.

Firmato
Mario Antonio Scino

GLOSSARIO

Ambiti di Compliance: categorie di reato la cui prevenzione nel Gruppo FS deve essere considerata una priorità per gestire la propria attività con onestà e integrità.

Area a Rischio: aree/attività nel cui ambito può essere più specificamente considerato il rischio di commissione dei reati individuati negli Ambiti di Compliance.

Destinatari: i componenti degli Organi Sociali e dell'Organismo di Vigilanza, i dipendenti e i collaboratori a qualsiasi titolo di Società Estere del Gruppo FS e i Terzi.

FS SpA o la Holding: Ferrovie dello Stato Italiane SpA.

Gruppo FS Italiane o Gruppo FS o Gruppo: FS e le società da essa controllate ai sensi dell'articolo 2359, codice civile.

Società Controllata Estera o **Società Estera**: indica le società estere controllate da FS SpA ai sensi dell'articolo 2359, comma 1, numeri 1) e 2), del Codice Civile.

Standard Generali di Controllo: standard generali di controllo che devono essere adottati da ciascuna Società Controllata Estera al fine di consentire una conduzione dell'impresa sana, corretta e coerente con i propri obiettivi.

Standard Specifici di Comportamento: standard minimi di comportamento che tutte le Società Controllate Estere sono tenute a seguire in relazione a ciascuna Area a Rischio.

Terzi: tutti coloro che, stabilmente o temporaneamente, intrattengono rapporti contrattuali con Società estere del Gruppo FS (ad es., fornitori, business partner, consulenti e promotori commerciali, revisori dei conti, *etc.*).

RUOLO	DATA	STRUTTURA ORGANIZZATIVA	DOCUMENTO DI RIFERIMENTO
funzione compliance di FS SpA		Struttura **COMPLIANCE** in ambito **LEGAL AFFAIRS**	DOr n.153 /LEG-COA del 08/10/2021
funzione human resources di FS International SpA		Struttura **HUMAN RESOURCES** a riporto dell'AU	DOr n.10/AU del 1° maggio 2025
funzione organizzazione		Struttura **GROUP ORGANIZATION** in ambito PEOPLE, CULTURE & TRANSFORMATION	DOr n. 150/AD del 16/04/2025

RIFERIMENTI NORMATIVI

- Codice Etico del Gruppo;
- Modello di Governance del Gruppo;
- Modello di Compliance del Gruppo FS Italiane;
- Policy Anti-Corruption del Gruppo e Modelli di Gestione Anti-Corruption societari;
- Framework di Data Protection del Gruppo;
- Sanction Policy di Gruppo;
- Programma di Compliance Antitrust di Gruppo;
- Strategia Fiscale del Gruppo Ferrovie dello Stato Italiane;
- Regolamento per la gestione interna e comunicazione all'esterno delle informazioni privilegiate e per il trattamento delle informazioni riservate;
- Modello di Controllo Interno e Gestione dei Rischi sull'Informativa Economica Finanziaria del Gruppo Ferrovie dello Stato Italiane.

ALLEGATO - STANDARD GENERALI DI CONTROLLO, AREE A RISCHIO E STANDARD SPECIFICI DI COMPORTAMENTO

Documento allegato[5] che individua, per ciascun ambito di compliance nel perimetro del documento, gli Standard Generali di Controllo, le Aree a Rischio e gli Standard Specifici di Comportamento che ogni Società Estera è tenuta a rispettare.

[5] L'allegato, che costituisce parte integrante del presente documento, in caso di successive modifiche normative e/o per esigenze operative, sarà aggiornato e reso disponibile sulla intranet aziendale, nella sezione contenente i documenti organizzativi, a cura della funzione compliance di FS SpA, con il supporto della funzione organizzazione di FS SpA, senza necessità di riemettere il presente documento.

VERSIONE/DATA	DOCUMENTO	MOTIVO DELLA REVISIONE
1.0 del 19/12/2023	*GR_PY_ International Compliance Program _n.56_V.01*	Prima Emissione
2.0 del 30/06/2025	*GR_PY_ International Compliance Program _n.56_V.02*	Seconda Emissione – rivisitazione dei ruoli e delle responsabilità nell'ambito delle attività di monitoraggio e reporting e allineamento al nuovo Modello di Governance del Gruppo

Policy di Gruppo
"International Compliance Program"

Allegato "Standard Generali di Controllo, Aree a Rischio e Standard Specifici di Comportamento"

INDICE

INTRODUZIONE

Il presente documento individua gli Standard Generali di Controllo, le Aree a Rischio e gli Standard Specifici di Comportamento per ciascuno degli Ambiti di Compliance individuati nel perimetro dell'International Compliance Program e di seguito rappresentati:

a) Reati di corruzione;
b) Altri reati contro la Pubblica Amministrazione;
c) Frodi contabili;
d) Reati fiscali;
e) Criminalità organizzata;
f) Finanziamento del terrorismo e c.d. reati di riciclaggio di denaro;
g) Abusi di mercato;
h) Reati contro la personalità individuale;
i) Reati in materia di salute e sicurezza;
j) Reati ambientali;
k) Reati informatici;
l) Reati in materia di violazione del diritto d'autore;
m) Contrabbando;
n) Reati contro il patrimonio culturale.

STANDARD GENERALI DI CONTROLLO

Di seguito si riportano gli Standard Generali di Controllo, trasversalmente applicabili ai diversi Ambiti di Compliance, che ogni Società Estera è tenuta a rispettare:

- *Segregazione dei compiti e delle responsabilità*: assicurare la segregazione dei compiti tra chi esegue, chi controlla e/o chi autorizza, anche attraverso una profilazione delle utenze nell'ambito dei sistemi IT, conforme al sistema di deleghe e procure;
- *Ruoli e responsabilità*: formalizzare un corpo normativo articolato che descriva compiti, responsabilità e modalità operative per lo svolgimento delle attività rilevanti/operative;
- *Sistema di deleghe e procure:* definire un sistema di deleghe e procure che individui, in modo coerente con la posizione organizzativa e il livello gerarchico del destinatario delle stesse, il livello di autonomia, il potere di rappresentanza e i limiti di spesa assegnati;

- *Tracciabilità e Conservazione*: garantire la tracciabilità e verificabilità delle attività e dei controlli tramite adeguati supporti documentali e/o informatici e relativa conservazione nel rispetto della normativa vigente e delle policy di Gruppo;
- *Imparzialità e assenza di conflitti di interessi*: assicurare che i soggetti coinvolti nelle Aree a Rischio descritte nel presente documento, operino con professionalità e imparzialità, nel rispetto delle leggi e delle normative applicabili, evitando e segnalando tempestivamente ogni situazione dalla quale possa scaturire un conflitto di interessi;
- *Corretta gestione dei rapporti con i Terzi*: garantire nei rapporti con i Terzi, secondo un approccio risk based:
  (i) la verifica dell'affidabilità, reputazione e adeguatezza dei Terzi con i quali ciascuna Società Estera intenda instaurare un rapporto professionale e d'affari;
  (ii) la previsione di specifiche disposizioni contrattuali che impongano ai Terzi il rispetto dei principi contenuti nel presente International Compliance Program;
  (iii) la verifica dei servizi resi e la congruità degli importi da erogare.

AREE A RISCHIO E STANDARD SPECIFICI DI COMPORTAMENTO

Di seguito si riportano, per ciascun Ambito di Compliance, le Aree a Rischio e gli Standard Specifici di Comportamento che ogni Società Estera è tenuta a rispettare.

REATI DI CORRUZIONE

Per la definizione dei reati di corruzione, l'identificazione delle Aree a Rischio e degli Standard Specifici di Comportamento si rimanda alla Policy Anti-Corruption del Gruppo FS.

ALTRI REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

La commissione di questa tipologia di reati presuppone l'instaurazione di rapporti con enti pubblici. Ai fini dell'International Compliance Program, è tipicamente considerato "ente pubblico" qualsiasi ente dotato di personalità giuridica, a cui sia affidata la cura di interessi pubblici, e che svolga attività legislative, giudiziarie o amministrative in forza di norme di diritto pubblico e di atti autoritativi, o che sia principalmente finanziato dallo Stato, da enti pubblici territoriali, o da altri organismi di diritto pubblico, o sia soggetto al controllo gestionale di questi ultimi.

Questi reati riguardano principalmente le frodi ai danni di enti pubblici e si verificano quando una società mette in atto una o più azioni o schemi illeciti al fine di frodare un ente pubblico per ottenere un qualsiasi vantaggio economico attraverso rappresentazioni, promesse o pretesti falsi o fraudolenti.

Questa tipologia di reati è spesso correlata a finanziamenti pubblici, sovvenzioni e gare d'appalto e si verifica

quando una società richiede finanziamenti pubblici o sovvenzioni a cui non ha diritto o ne fa un uso improprio e diverso da quello indicato nella richiesta di sovvenzione ovvero fornisce all'ente pubblico informazioni non veritiere al fine di ottenere l'aggiudicazione della gara stessa nella predisposizione di documenti o dati per la partecipazione a procedure di gara pubbliche per l'aggiudicazione di un servizio.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) partecipazione a procedure di aggiudicazione di contratti pubblici di appalti e di concessione;
b) svolgimento di procedure di aggiudicazione di contratti pubblici di appalti e di concessione;
c) richiesta di finanziamenti pubblici, sovvenzioni, sussidi o garanzie rilasciate da enti pubblici;
d) gestione dei finanziamenti pubblici ricevuti, delle sovvenzioni o delle garanzie ottenute;
e) gestione dei rapporti con gli enti pubblici (ad es., con riferimento ai requisiti di salute, sicurezza e ambiente, alla gestione del personale, al pagamento delle imposte).

STANDARD SPECIFICI DI COMPORTAMENTO

I rapporti con gli enti pubblici devono ispirarsi a principi di correttezza, professionalità, lealtà e piena collaborazione, etica, integrità, trasparenza e rispetto delle leggi applicabili e devono essere tenuti dalle funzioni aziendali a ciò formalmente delegate e/o da soggetti formalmente autorizzati.

Nel rispetto dei principali Standard Specifici di Comportamento indicati nella Policy Anti-Corruption del Gruppo FS, a cui si rimanda, le Società Estere si astengono, in particolare:

- dal fornire agli enti pubblici informazioni o consegnare documenti con contenuti imprecisi, errati, incompleti e/o falsi;
- dal destinare le somme ricevute da enti pubblici, come fondi, sovvenzioni o prestiti, a scopi diversi da quelli a cui erano destinati;
- dal tenere un comportamento reticente o ingannevole che possa indurre, anche attraverso l'omissione di informazioni dovute, il soggetto pubblico in errore al fine di orientare le decisioni a favore delle Società del Gruppo o di Terzi.

FRODI CONTABILI

La frode contabile è la manipolazione intenzionale dei bilanci per creare una falsa rappresentazione della situazione economico-finanziaria di una società (ad es., una società può falsificare i propri bilanci sovrastimando le entrate o le attività, non registrando le spese e sottostimando le passività).

Le frodi contabili possono avere luogo per una serie di motivi a vantaggio della società, tra cui, a titolo

esemplificativo e non esaustivo:

- continuare a ottenere un finanziamento da una banca in assenza dei necessari requisiti;
- dichiarare profitti inesistenti o nascondere le perdite;
- nascondere circostanze che potrebbero influire negativamente sulla società;
- omettere fatti rilevanti che possano indurre in errore le parti interessate;
- mascherare la creazione di fondi neri.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) redazione di documenti da rilasciare agli azionisti o al pubblico (ad es., bilanci, relazioni finanziarie periodiche) riguardanti la situazione economico-patrimoniale o finanziaria di una Società Estera, anche se tali documenti sono diversi da quelli predisposti ai fini dell'informativa contabile periodica;
b) gestione delle registrazioni contabili;
c) gestione dei flussi monetari e finanziari;
d) gestione dei rapporti con i revisori esterni.

STANDARD SPECIFICI DI COMPORTAMENTO

Nel rispetto dei principali Standard Specifici di Comportamento indicati nelle Direttive e Procedure amministrativo-contabili di Gruppo, a cui si rimanda, le Società Estere si astengono, in particolare, dal porre in essere le seguenti condotte:

- rappresentare o trasmettere dati falsi, imprecisi, lacunosi o, comunque, non corrispondenti alla reale situazione economica, patrimoniale e finanziaria della Società, per l'elaborazione e la rappresentazione in bilanci, relazioni o altre comunicazioni sociali previste dalla legge;
- omettere o alterare dati e informazioni rilevanti sulla situazione economica, patrimoniale e finanziaria della Società da utilizzare nei bilanci, nelle relazioni o in altre comunicazioni sociali previste dalla legge;
- porre in essere comportamenti che, mediante l'occultamento di documenti o l'utilizzo di altre misure fraudolente, impediscano materialmente o comunque ostacolino lo svolgimento delle attività di controllo o di revisione della gestione sociale da parte dei soci, del Collegio Sindacale o organo equivalente o di revisori esterni.

Ogni operazione o transazione della Società Estera deve essere correttamente e tempestivamente registrata nel sistema contabile della Società secondo i criteri indicati dalla legge e dai principi contabili applicabili.

Ogni operazione e transazione della Società Estera deve essere verificabile, legittima, coerente e congrua.

Affinché la contabilità risponda ai requisiti di veridicità, completezza e trasparenza, per ogni transazione deve essere conservata un'adeguata e completa documentazione di supporto dell'attività svolta, in modo da consentire quanto segue:

- un'accurata e completa rappresentazione delle transazioni economiche dell'azienda;
- l'immediata determinazione delle caratteristiche e delle motivazioni alla base della transazione;
- l'agevole ricostruzione formale e cronologica dell'operazione;
- i controlli interni e le verifiche da parte del revisore esterno.

Ogni registrazione contabile deve riflettere fedelmente le informazioni contenute nella documentazione di supporto. Pertanto, sarà responsabilità di ciascun dipendente assicurarsi che la documentazione di supporto sia facilmente reperibile e ordinata.

REATI FISCALI

I reati fiscali possono essere definiti da ciascuna giurisdizione in modo generale per ricomprendere un'ampia gamma di attività e possono verificarsi per una serie di motivi a vantaggio della Società, tra cui, a titolo esemplificativo e non esaustivo:

- emissione di documenti per operazioni inesistenti;
- la mancata registrazione ai fini fiscali o tenuta di registri non corretti;
- mancato pagamento, anche attraverso la compensazioni con crediti non spettanti;
- presentazione di una falsa dichiarazione in materia fiscale;
- evasione di imposte o ricezione di rimborsi mediante frode o pratiche illegali;
- riduzione intenzionale dell'imposta utilizzando documenti falsi e/o fittizi (incluse, ad es., le fatture);
- ostacolo al funzionario dell'Autorità fiscale.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) gestione della fiscalità d'impresa;
b) gestione delle registrazioni contabili e della documentazione che deve essere conservata a fini fiscali;
c) gestione delle attività di raccolta, conservazione, registrazione ed emissione di fatture o altri documenti che devono essere conservati a fini fiscali;
d) attività di raccolta e valutazione dei dati contabili necessari per la redazione del bilancio;
e) gestione delle dichiarazioni fiscali;

f) gestione delle attività relative alla liquidazione e al pagamento delle imposte.

STANDARD SPECIFICI DI COMPORTAMENTO

Nel rispetto della Strategia Fiscale del Gruppo Ferrovie dello Stato Italiane, a cui si rimanda, ogni Società Estera deve:

- rispettare le normative e, più in generale, tutte le disposizioni applicabili ai fini fiscali;
- adottare una condotta basata sul principio della massima prudenza;
- assicurare che l'onere fiscale sia correttamente determinato e indicato nelle dichiarazioni fiscali in conformità alla normativa vigente e alle istruzioni fornite dalle autorità fiscali;
- mantenere una corretta, completa e trasparente tenuta delle registrazioni e dei libri contabili, al fine di garantire che riflettano le operazioni aziendali;
- monitorare le scadenze e gli adempimenti fiscali, nonché il recepimento delle nuove normative fiscali;
- svolgere attività di aggiornamento/formazione periodica per i soggetti coinvolti nei processi di definizione/controllo delle imposte.

CRIMINALITÀ ORGANIZZATA

La criminalità organizzata si riferisce a una forma di criminalità associata che presuppone un'organizzazione stabile di più persone allo scopo di commettere più reati. Sono incluse nel termine "criminalità organizzata" le attività criminali complesse su larga scala portate avanti da gruppi organizzati di persone, in modo indefinito o con strutture complesse, con lo scopo di ottenere profitti per i suoi partecipanti a scapito della comunità e dei suoi membri.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) selezione, assunzione, gestione e incentivazione del personale;
b) selezione degli operatori economici per l'affidamento di lavori, servizi e forniture;
c) gestione dei rapporti con Terzi;
d) operazioni societarie straordinarie e/o operazioni finanziarie di investimento e/o impiego di liquidità propria della Società;
e) attività di investimento e accordi di joint venture o altre forme di partnership con controparti locali o estere.

STANDARD SPECIFICI DI COMPORTAMENTO

Per quanto riguarda le Aree a Rischio individuate ogni Società Estera deve considerare vietato:

- instaurare rapporti commerciali o porre in essere operazioni di erogazione liberale con Terzi qualora vi sia il fondato sospetto che detti Terzi possano essere collegati a esponenti della criminalità organizzata;
- sottostare a richieste di qualsiasi tipo contrarie alla legge ovvero associarsi ad altri allo scopo di commettere più illeciti;
- associarsi con Terzi, mettendo a disposizione di tale associazione conoscenze o mezzi propri, di Terzi o dell'Azienda stessa, al fine di porre in essere comportamenti, atti od operazioni non in linea con le disposizioni del presente documento, delle procedure aziendali e del Codice Etico del Gruppo, o che siano comunque idonei, anche solo potenzialmente, a configurare ipotesi di reato.

Inoltre, ai fini dell'attuazione dei suddetti principi di condotta:

- il processo di selezione degli operatori economici per l'affidamento di lavori, servizi e forniture deve essere ispirato ai principi di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità;
- ogni transazione deve essere svolta attraverso il sistema bancario, richiedendo anche ai clienti di effettuare i pagamenti esclusivamente attraverso questo sistema, che consente la tracciabilità dei movimenti finanziari;
- ogni operazione, anche di natura straordinaria anche all'interno del Gruppo di appartenenza (trasformazioni, fusioni, scissioni, *etc.*), deve essere autorizzata, verificabile, legittima, coerente e congrua, oltre che correttamente registrata;
- è richiesto di svolgere un costante monitoraggio dei flussi finanziari aziendali (anche in relazione alla gestione dei pagamenti intercompany);
- devono essere stabiliti e attuati specifici controlli da effettuare sulla controparte al fine di verificarne l'identità, la sede legale, la natura giuridica, la reputazione e l'affidabilità, anche con riferimento alla presenza in eventuali Liste di Riferimento e Black List nazionali e internazionali per la prevenzione del riciclaggio, del finanziamento del terrorismo e della criminalità organizzata.

FINANZIAMENTO DEL TERRORISMO E C.D. REATI DI RICICLAGGIO DI DENARO

Per finanziamento del terrorismo si intende la fornitura o la raccolta di fondi, con qualsiasi mezzo, direttamente o indirettamente, con l'intenzione di utilizzarli per sostenere atti o organizzazioni terroristiche.

Ai fini dell'International Compliance Program, il fenomeno dei c.d. reati di riciclaggio di denaro può comprendere tre diversi comportamenti: (i) la conversione o il trasferimento di fondi di cui è nota la provenienza illecita; (ii) l'occultamento o la dissimulazione della vera natura, della fonte, dell'ubicazione, della proprietà o di altri diritti sui beni di cui è nota la provenienza illecita; (iii) l'acquisizione, il possesso o l'uso di beni, di cui è nota la provenienza illecita al momento della ricezione.

Quando i proventi di un reato sono creati dalla stessa persona che ne occulta l'origine illecita, tale condotta è punita in alcuni Paesi come autoriciclaggio. Il riciclaggio di denaro e il finanziamento del terrorismo presentano spesso caratteristiche transazionali simili, per lo più legate all'occultamento.

I soggetti che pongono in essere attività di riciclaggio di denaro inviano fondi illeciti attraverso canali legali per nascondere la loro origine criminale, mentre coloro che finanziano il terrorismo trasferiscono fondi che possono essere di origine legale o illecita in modo tale da nascondere la loro fonte e il loro uso finale, ossia il sostegno al terrorismo.

Questo tipo di condotte può avvenire a vantaggio di una società, a titolo esemplificativo e non esaustivo per:

- ottenere proventi o qualsiasi altro vantaggio derivante da attività illegali svolte dalle organizzazioni terroristiche che sono state finanziate (gli altri vantaggi possono consistere nella protezione degli affari, nei Paesi in cui tali organizzazioni sono piuttosto influenti);
- mascherare l'origine illegale dei proventi di reato.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) rapporti contrattuali con operatori economici affidatari di lavori, servizi e forniture, *partners* e altre entità giuridiche controllate direttamente o indirettamente dai soggetti sopra citati, aventi residenza o sede legale in un Paese che rappresenta una giurisdizione ad alto rischio e non cooperativa;
b) gestione dei flussi monetari e finanziari.

STANDARD SPECIFICI DI COMPORTAMENTO

Al fine di evitare ogni possibile comportamento volto, anche indirettamente, ad agevolare reati quali la ricettazione, il riciclaggio e l'impiego di denaro, beni o qualsiasi altra utilità di provenienza illecita, il finanziamento del terrorismo, nonché qualsiasi uso improprio di strumenti finanziari e/o operazioni volte a nascondere la provenienza dei fondi della Società, ciascuna Società Estera:

- deve avvalersi del sistema bancario per effettuare le transazioni, richiedendo anche ai clienti di effettuare i pagamenti esclusivamente attraverso questo sistema, che consente la tracciabilità dei movimenti finanziari, astenendosi dal proporre o accettare richieste di pagamento "fuori piazza", ossia su conti di Paesi diversi rispetto a quello della sede/residenza legale o dei Paesi indicati nel contratto;
- deve utilizzare le carte di credito aziendali, le carte prepagate e/o altri strumenti di pagamento in modo appropriato e conforme alle finalità della Società, avendo cura di salvaguardare e proteggere i relativi dati;
- deve mantenere aggiornati tutti i dati relativi alle controparti commerciali per consentire una valida valutazione dei relativi profili economico-finanziari;

- non deve intrattenere rapporti commerciali con soggetti (persone fisiche o giuridiche) di cui sia nota o sospetta l'appartenenza a organizzazioni criminali o comunque illegali;
- deve garantire che ogni operazione, anche di natura straordinaria anche all'interno del Gruppo di appartenenza (trasformazioni, fusioni, scissioni, *etc.*), sia autorizzata, verificabile, legittima, coerente e congrua, oltre che correttamente registrata;
- deve rispettare le regole per la corretta, completa e trasparente registrazione delle scritture contabili legate alla gestione della Società;
- deve monitorare costantemente i flussi finanziari conformemente alle diverse attività svolte nell'ambito dell'operatività della Società;
- deve identificare il personale incaricato della gestione delle carte di credito, i criteri di assegnazione delle carte di credito aziendali e le modalità di utilizzo delle stesse;
- deve stabilire e attuare specifici controlli da effettuare sulla controparte al fine di verificarne l'identità, la sede legale, la natura giuridica, la reputazione e l'affidabilità, anche con riferimento alla presenza in eventuali Liste di Riferimento e Black List nazionali e internazionali per la prevenzione del riciclaggio, del finanziamento del terrorismo e della criminalità organizzata.

ABUSO DI MERCATO

I reati di abuso di mercato possono riferirsi a vari modelli di comportamento quali:

- possesso di informazioni privilegiate al fine di compiere o indurre altri a compiere operazioni (acquisti, vendite, *etc.*) su strumenti finanziari;
- comunicazione ad altri di tali informazioni privilegiate;
- diffusione di informazioni false al fine di provocare una variazione significativa del prezzo degli strumenti finanziari;
- l'effettuazione di operazioni simulate o altri espedienti per provocare una variazione significativa del prezzo degli strumenti finanziari.

Questi comportamenti possono essere finalizzati a un vantaggio di una società per diversi motivi, tra cui, a titolo esemplificativo e non esaustivo:

- abbattere il prezzo degli strumenti finanziari di una società *target* prima di un'acquisizione;
- indebolire la reputazione di una società concorrente;
- alterare il prezzo di un determinato strumento finanziario in portafoglio prima di effettuare qualsiasi attività di *trading* ad esso relativa.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) gestione delle informazioni divulgate al pubblico (rapporti con investitori, analisti finanziari, agenzie di *rating*, giornalisti e altri rappresentanti dei *mass media*, compresa la gestione di campagne pubblicitarie; organizzazione e partecipazione a incontri, in qualsiasi forma, con i suddetti soggetti);

b) gestione delle informazioni privilegiate in grado di influenzare l'andamento degli strumenti finanziari quotati (ad es., informazioni strettamente connesse a nuovi servizi e mercati, dati contabili di periodo, dati previsionali e obiettivi quantitativi relativi all'andamento della gestione, comunicazioni relative a fusioni/scissioni e a nuove iniziative di particolare rilevanza o a trattative e/o accordi relativi all'acquisizione e/o alla cessione di asset significativi, attività di M&A);

c) redazione dei documenti contabili e dei prospetti informativi da comunicare al pubblico per legge o per decisione aziendale;

d) qualsiasi tipo di operazione relativa agli strumenti finanziari in portafoglio.

STANDARD SPECIFICI DI COMPORTAMENTO

Nel rispetto degli strumenti normativi di Gruppo in materia di Market Abuse, a cui si rimanda, ogni Società Estera è espressamente tenuta ad astenersi da:

- comunicare a Terzi informazioni privilegiate, salvo i casi in cui tale comunicazione sia imposta da disposizioni legislative o regolamentari, dall'Autorità Giudiziaria o Amministrativa, da disposizioni o da specifici accordi contrattuali, se tali informazioni sono finalizzate a favorire o comunque a ottenere un vantaggio per la Società Estera;
- raccomandare o indurre Terzi ad effettuare acquisti, vendite o altre operazioni su strumenti finanziari sulla base di informazioni privilegiate (ottenute da esponenti aziendali in ragione della loro posizione all'interno del Gruppo o da Terzi in virtù dei loro rapporti d'affari con il Gruppo), qualora l'esecuzione di tali operazioni sia finalizzata a favorire o comunque ad ottenere un vantaggio per la Società Estera;
- comunicare o diffondere, attraverso qualsiasi canale comunicativo, informazioni privilegiate o su strumenti finanziari false o fuorvianti, ovvero notizie di cui non sia certa la veridicità, suscettibili di alterare il valore di uno strumento finanziario;
- compiere operazioni idonee a fornire falsi segnali sul valore di uno strumento finanziario, così da indurre altri operatori a porre in essere azioni idonee a produrre ulteriori variazioni sui prezzi.

REATI CONTRO LA PERSONALITÀ INDIVIDUALE

I reati contro la personalità individuale possono essere commessi mediante il reclutamento, l'assunzione e

l'impiego di lavoratori in condizioni di sfruttamento e approfittamento del loro stato di bisogno. Inoltre, tra i reati contro la personalità individuale possono includersi tutte le azioni che violano il rispetto delle persone e dei diritti umani in tutte le loro forme, comprese le differenze etniche, culturali, religiose, razziali e di genere.

L'esistenza di una o più delle seguenti condizioni può costituire un indicatore di sfruttamento a vantaggio della Società:

- la ripetuta corresponsione di compensi con modalità palesemente diverse da quelle indicate dalla legge o comunque sproporzionate rispetto alla quantità e qualità del lavoro svolto;
- la reiterata violazione della legislazione in materia di orari di lavoro, pause, ferie e permessi obbligatori;
- le violazioni delle norme di sicurezza e igiene nei luoghi di lavoro;
- la sottoposizione del lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti.

AREE A RISCHIO

In relazione a questa tipologia di reati, le Aree a Rischio sono da considerarsi le seguenti:

a) selezione, assunzione e gestione del personale, con particolare riguardo alla determinazione dell'orario di lavoro, della retribuzione, degli impatti sulla salute e sulla sicurezza e delle condizioni di lavoro in generale;
b) assegnazione di attività che prevedono l'utilizzo di manodopera di Terzi per la fornitura di personale e/o servizi, anche con riferimento ad operatori economici che operano in Paesi in cui i diritti individuali non sono pienamente tutelati dalla legislazione internazionale o locale.

STANDARD SPECIFICI DI COMPORTAMENTO

Le Società Estere sono tenute a rispettare i seguenti principi:

- verificare, per l'assunzione diretta del personale, il rispetto delle norme giuslavoristiche per il processo di assunzione e il rapporto di lavoro in generale;
- richiedere agli operatori economici affidatari di contratti di lavori, servizi e forniture e ai loro subappaltatori di rispettare qualsiasi legislazione internazionale e locale applicabile in materia di lavoro forzato, protezione del lavoro minorile e delle donne e conformità delle condizioni igienico-sanitarie;
- stabilire e attuare specifici controlli sulla controparte al fine di verificarne la reputazione e l'affidabilità;
- tutelare l'integrità morale e personale degli individui, offrendo condizioni di lavoro rispettose della dignità individuale e ambienti di lavoro salubri e sicuri;
- garantire il massimo rispetto delle persone e dei diritti umani in tutte le loro forme, compreso il rispetto delle differenze etniche, culturali, razziali e religiose.

REATI IN MATERIA DI SALUTE E SICUREZZA

I reati in materia di salute e sicurezza riguardano principalmente l'inosservanza delle legislazioni locali e degli *standards* lavorativi idonei a garantire sul luogo di lavoro la prevenzione di infortuni e malattie, anche mortali o che comportino lesioni gravi o gravissime in danno dei dipendenti, commessi in violazione delle norme in materia di salute e sicurezza sul lavoro.

Questi comportamenti possono avvenire a vantaggio di una società per una serie di motivi, tra cui, a titolo esemplificativo e non esaustivo:

- la riduzione dei costi derivanti dalla mancata adozione delle misure di sicurezza necessarie a garantire la salute e la sicurezza sui luoghi di lavoro;
- l'aumento della produttività, posto che lo svolgimento delle attività lavorative, senza tenere conto di procedure e politiche precauzionali, potrebbe accelerare i processi di lavoro.

AREE A RISCHIO

In relazione a questo tipo di reati, le seguenti aree devono essere considerate a rischio:

a) rispetto delle normative applicabili in materia di salute e sicurezza.

STANDARD SPECIFICI DI COMPORTAMENTO

Ogni Società Estera deve adottare un sistema di gestione della salute e della sicurezza sul lavoro idoneo a controllare i propri rischi in materia, tenendo sempre in considerazione la sicurezza dei lavoratori in ogni fase dell'attività e adottando tutte le misure ritenute necessarie per tutelare l'integrità fisica e morale dei propri lavoratori, dei Terzi e della comunità in cui la Società opera, promuovendo un'efficace cultura della protezione della sicurezza sul luogo di lavoro volta a favorire la consapevolezza in merito ai rischi e alle responsabilità delle condotte dei singoli.

In particolare, il sistema di gestione della salute e della sicurezza sul lavoro adottato ed efficacemente attuato dalla Società Estera deve:

- considerare il rispetto delle previsioni di legge in materia di salute e sicurezza dei lavoratori sul luogo di lavoro quale una priorità;
- eliminare alla fonte i rischi per la salute e la sicurezza dei lavoratori, e, ove ciò non sia possibile, ridurre gli stessi al minimo, attraverso le conoscenze acquisite e il progresso tecnologico;
- svolgere costantemente le attività di valutazione dei rischi specifici, anche al fine di valutare l'introduzione di conseguenti misure di prevenzione e protezione;
- comunicare agli affidatari, nel caso di concessioni o appalto di lavori, servizi o forniture da parte della

Società, i rischi presenti negli ambienti di lavoro nei quali sono destinati ad operare;

- svolgere attività di monitoraggio ed analisi di ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali carenze nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere;
- eseguire periodiche attività di informazione e formazione dei dipendenti;
- svolgere verifiche per assicurare l'applicazione e l'efficacia delle procedure e delle istruzioni di sicurezza sul lavoro da parte dei lavoratori e degli appaltatori.

Al fine di mantenere un adeguato monitoraggio delle Aree a Rischio, ciascuna Società Estera dovrà destinare risorse organizzative, strumentali ed economiche per assicurare, da un lato, il pieno rispetto delle vigenti disposizioni di legge in materia di prevenzione degli infortuni sul lavoro e, dall'altro, il miglioramento continuo della situazione di salute e sicurezza sul lavoro, anche attraverso l'attuazione e l'aggiornamento delle relative misure di prevenzione.

REATI AMBIENTALI

I reati ambientali comprendono gli atti illeciti che causano danni all'ambiente. Tali reati si riferiscono ad un ampio elenco di attività illecite, come i reati contro la fauna selvatica, il commercio e lo smaltimento illecito di sostanze pericolose e molte altre condotte che potrebbero danneggiare l'ambiente.

Ad esempio, tali reati potrebbero essere commessi nell'ambito delle seguenti attività:

- gestione delle attività di raccolta, stoccaggio, trasporto e smaltimento dei rifiuti, anche attraverso l'affidamento delle attività a Terzi;
- gestione delle emissioni derivanti dall'esercizio delle attività industriali;
- gestione e manutenzione degli impianti/dispositivi che impiegano sostanze dannose per l'ambiente.

I reati ambientali potrebbero essere commessi nell'interesse di una società per una serie di motivi, tra cui:

- ridurre i costi, derivanti dalla mancata adozione delle misure necessarie per la salvaguardia dell'ambiente;
- aumentare la produttività, dato che lo svolgimento di attività di impresa, senza considerare le questioni ambientali, potrebbe accelerare il processo produttivo.

AREE A RISCHIO

In relazione a questa tipologia di reati, le seguenti aree devono essere monitorate in quanto considerate a rischio:

a) rispetto della normativa applicabile in materia ambientale anche in occasione della progettazione, costruzione, gestione e manutenzione di infrastrutture;

b) selezione dei Terzi che devono svolgere attività specifiche che possono avere un impatto sull'ambiente (ad es., la gestione e lo smaltimento dei rifiuti).

STANDARD SPECIFICI DI COMPORTAMENTO

Ogni Società Estera, nell'ambito della propria attività, considera prioritario il rispetto e la tutela dell'ambiente, in particolare attraverso:

- la valutazione dei potenziali rischi e sviluppo di adeguati programmi di prevenzione a tutela dell'ambiente e della pubblica incolumità;
- l'istituzione di procedure specifiche in conformità con la legislazione ambientale vigente;
- la diffusione all'interno della Società di informazioni sulla tutela dell'ambiente, promuovendo la consapevolezza su questo tema e assicurando che le attività siano svolte in conformità con la legislazione applicabile in materia;
- l'adozione di strumenti adeguati volti ad evitare che le proprie attività causino qualsiasi forma di danno e pregiudizio all'ecosistema.

REATI INFORMATICI

I reati informatici comprendono un'ampia gamma di attività trasversali a tutte le aree aziendali. In generale, tali reati possono essere suddivisi in due categorie: (i) reati che hanno come obiettivo una rete o un dispositivo informatico; (ii) reati facilitati dall'utilizzo di reti o dispositivi informatici.

I reati informatici considerati nel presente documento consistono ad esempio: (i) nell'intrusione non autorizzata in una rete informatica protetta; (ii) nell'introduzione di virus in un sistema informatico; (iii) nell'intercettazione di dati da una rete informatica; (iv) nell'interruzione di un sistema informatico attraverso il danneggiamento, la cancellazione, l'alterazione o la soppressione di dati informatici; (v) nell'interferenza illegittima con il funzionamento di un sistema informatico; (vi) nella frode informatica e nell'uso fraudolento di dati informatici al fine di ottenere un ingiusto vantaggio patrimoniale.

I reati informatici possono essere commessi nell'interesse di una società per una serie di motivi, tra cui:

- accedere al segreto industriale di una società concorrente;
- ottenere informazioni riservate sulle strategie di mercato delle aziende concorrenti;
- mettere a rischio o danneggiare il sistema informatico di una società concorrente;
- compromettere sistemi informatici critici di una società concorrente, come quelli legati all'infrastruttura essenziale o alla produzione, per causare danni significativi.

AREE A RISCHIO

In relazione a questa tipologia di reati, devono essere considerate Aree a Rischio le seguenti:

a) attività aziendali svolte utilizzando qualsiasi strumento informatico (ad es., il sistema di posta elettronica);
b) attività di gestione e protezione di postazioni di lavoro, laptop, cellulari e dispositivi di archiviazione;
c) definizione delle misure di sicurezza fisica e logica da adottare sul sistema informatico, ivi inclusa la classificazione e il trattamento delle informazioni e dei dati e la gestione dei profili degli amministratori di sistema;
d) attività per la messa in sicurezza delle reti aziendali, compresa la crittografia delle comunicazioni e la difesa contro attacchi di rete, fondamentali per prevenire l'accesso non autorizzato e la compromissione dei dati.

STANDARD SPECIFICI DI COMPORTAMENTO

Come principio generale di prevenzione applicabile a tutti i processi aziendali a rischio di commissione di reati informatici, ogni Società Estera deve garantire che l'accesso e il trattamento dei dati contenuti nei sistemi informatici avvenga in conformità alle disposizioni di legge vigenti.

Ciascuna Società Estera deve assicurare un monitoraggio periodico, in conformità con la legge locale applicabile, delle attività svolte dal personale sul sistema informatico aziendale, al fine di rilevare comportamenti insoliti e potenziali vulnerabilità nei sistemi aziendali.

Inoltre, le Società Estere devono svolgere campagne di sensibilizzazione, anche attraverso sessioni di formazione specifiche ove necessario, sull'importanza di un uso corretto e appropriato degli strumenti informatici in uso nell'ambito delle attività aziendali.

Per quanto riguarda l'utilizzo e la gestione di sistemi, strumenti, documenti o dati informatici, le Società Estere devono attenersi ai seguenti principi di controllo:

- rispetto delle procedure di gestione della sicurezza informatica;
- predisposizione e implementazione di una politica aziendale per la gestione e il controllo della sicurezza fisica degli ambienti e delle risorse informatiche;
- adozione di misure specifiche per garantire la separazione dei ruoli nel processo di *change management* (nuovi sviluppi, manutenzione evolutiva, manutenzione correttiva e manutenzione ordinaria) dei sistemi informatici (software applicativo o di base, hardware e sistemi);
- previsione e implementazione di processi e meccanismi di *disaster recovery* che garantiscano il ripristino di determinati sistemi e dati in caso di indisponibilità temporanea o perdita permanente;
- adozione di misure specifiche per garantire che l'uso di beni eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge o contrattuali;

- implementazione di un sistema di protezione idoneo ad identificare e autenticare gli utenti precedentemente autorizzati che accedono a un sistema di elaborazione o trasmissione;
- predisposizione di strumenti tecnologici e livelli di protezione contro spam, spyware, malware ecc.;
- attivazione di filtri idonei ad impedire l'accesso a siti non pertinenti all'attività lavorativa o vietati;
- revoca dell'autorizzazione all'utilizzo di un sistema/applicazione informatica al termine del rapporto di lavoro, al cambio di ruolo aziendale o in conseguenza del mancato utilizzo per un periodo prolungato;
- implementazione di soluzioni di monitoraggio avanzato del traffico di rete e delle attività degli utenti sui sistemi informatici, incluso l'utilizzo di sistemi di rilevamento delle anomalie e registri dettagliati delle attività degli utenti, al fine di individuare comportamenti insoliti, attività sospette o accessi non autorizzati;
- conduzione di audit periodici della sicurezza informatica per valutare l'efficacia delle misure di sicurezza implementate, identificare potenziali vulnerabilità e apportare miglioramenti continuativi;
- conduzione di test di sicurezza regolari e simulazioni di attacchi per valutare la preparazione dell'organizzazione, identificare punti deboli e migliorare la risposta agli incidenti.

REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

I reati in materia di violazione del diritto d'autore possono consistere nell'utilizzo di opere protette dalla legge sul diritto d'autore e dalla legge sul diritto della proprietà intellettuale/industriale senza autorizzazione, ovvero in violazione di determinati diritti esclusivi spettanti al titolare del diritto d'autore e/o del diritto della proprietà intellettuale/industriale, come il diritto di riprodurre, distribuire, mostrare o eseguire l'opera protetta, o di farne opere derivate.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) l'installazione, la gestione, l'utilizzo e la riproduzione di software protetti da diritto d'autore e/o dal diritto della proprietà intellettuale/industriale nell'ambito dei sistemi informatici aziendali;
b) utilizzo di testi, immagini, musiche e video protetti da diritto d'autore e/o dal diritto della proprietà intellettuale/industriale nell'ambito dei sistemi informatici aziendali;
c) gestione dei diritti di proprietà intellettuale e industriale in relazione a marchi, brevetti, invenzioni, disegni e modelli di utilità.

STANDARD SPECIFICI DI COMPORTAMENTO

Le Società Estere adottano adeguate misure tecniche, fisiche e organizzative al fine di evitare:

- qualsiasi uso illegale o diffusione al pubblico, anche attraverso reti informatiche o attraverso connessioni di qualsiasi altro tipo, dell'opera originale protetta dal diritto d'autore e/o dal diritto della proprietà intellettuale/industriale o di parte di essa;
- l'impiego per finalità aziendali di beni tutelati da diritti acquisiti in elusione degli obblighi imposti dal diritto d'autore e/o dal diritto della proprietà intellettuale/industriale o con modalità difformi da quelle previste dal titolare;
- il download illegale di qualsiasi software senza un'adeguata documentazione contrattuale a supporto.

Inoltre, quando una Società Estera stipula un contratto con appaltatori esterni per l'esecuzione di attività che potrebbero potenzialmente essere considerate a rischio di violazione di diritti d'autore/proprietari, tale contratto deve prevedere clausole mediante le quali l'appaltatore si impegna a rispettare le leggi e le normative applicabili in materia.

CONTRABBANDO

I reati di contrabbando si verificano quando una persona (fisica o giuridica) sottrae, o tenta di sottrarre, beni di origine straniera al pagamento dei diritti di frontiera. In termini generali, il contrabbando consiste nell'importare o esportare illegalmente merci o nell'esportazione di merci in violazione delle disposizioni doganali e delle leggi di uno Stato che ne vietano o tassano l'ingresso, l'uscita e la circolazione.

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) gestione degli adempimenti doganali (predisposizione e trasmissione della documentazione prevista dalla legge, gestione dei rapporti con le Autorità doganali, anche con il supporto di Terzi, *etc.*);
b) pagamento dei dazi doganali e consegna dei documenti relativi all'importazione/esportazione dei materiali alle Autorità doganali;
c) selezione degli operatori economici fornitori di beni e negoziazione, conclusione e gestione dei relativi contratti;
d) gestione del magazzino.

STANDARD SPECIFICI DI COMPORTAMENTO

In aggiunta a quanto previsto nella Sanction Policy del Gruppo FS a cui si rimanda, le Società Estere devono:

- assicurare che tutte le attività e le operazioni svolte siano improntate al massimo rispetto della normativa vigente in materia;
- definire le procedure operative per effettuare, direttamente o indirettamente, le operazioni doganali e il

relativo monitoraggio.

REATI CONTRO IL PATRIMONIO CULTURALE

I reati contro il patrimonio culturale consistono in tutti i reati che hanno per oggetto il patrimonio culturale, quale bene giuridico collettivo o a proprietà diffusa, tutelato non solo da un punto di vista strettamente privatistico-materiale, ma anche e soprattutto come valore in sé, per quella componente pubblicistica che rappresenta uno strumento di cultura funzionale alla formazione intellettuale di tutti gli individui.

A titolo esemplificativo, i seguenti reati possono essere inclusi nella categoria dei reati contro il patrimonio culturale:

- le condotte di dispersione (ad es., furto e appropriazione indebita di beni culturali);
- le condotte di circolazione illegale (ad es., le violazioni relative all'alienazione di beni culturali, all'importazione e all'esportazioni illegali di beni culturali);
- le condotte di falsificazione (falsificazione di scritture private relative a beni culturali e contraffazione di opere d'arte);
- le condotte di dissimulazione dell'origine illecita (ricettazione e riciclaggio di beni culturali);
- le condotte di distruzione (distruzione, dispersione, deterioramento, deturpamento e uso illecito di beni culturali o paesaggistici, devastazione e saccheggio di beni culturali o paesaggistici).

AREE A RISCHIO

In relazione a questa tipologia di reati, è necessario monitorare le seguenti Aree a Rischio:

a) gestione del patrimonio culturale, sia mobiliare che immobiliare.

STANDARD SPECIFICI DI COMPORTAMENTO

Ogni Società Estera deve:

- rispettare la normativa a tutela del patrimonio culturale e paesaggistico, esercitando in particolare tutti gli opportuni controlli e le attività idonee a salvaguardare il patrimonio stesso;
- contribuire all'adempimento di tutti gli obblighi normativi, anche in materia di acquisizione e circolazione dei beni culturali, o comunque necessari per tutelare i beni culturali e paesaggistici;
- monitorare le fasi di acquisizione dei beni culturali, ivi compresa la verifica della provenienza del bene culturale (ad es., acquisire dal venditore/fornitore le certificazioni e le autorizzazioni utili e necessarie).