

GLOBAL COMPLIANCE PROGRAM

(adottato dal Consiglio di Amministrazione di TERNA S.p.A. con delibera in data 10 novembre 2017 e successivamente aggiornato)

Storia delle revisioni

Rev.	Data	Descrizione
03	14/12/2023	Quarta emissione che ha previsto l'adeguamento del Global Compliance Program alle novità introdotte dalla LG054 Whistleblowing in materia di segnalazioni e modifica della composizione del Compliance Officer Bureau (COB)
02	02/09/2022	Terza emissione che ha previsto la revisione della struttura del Global Compliance Program per adeguarlo alle principali e più recenti best practice e normative applicabili in materia di compliance program, individuate a titolo esemplificativo nel par. 3.2. del Global Compliance Program. Adeguamento del documento seguendo il c.d. "approccio per processi", individuando e regolando i macro-processi aziendali rilevanti a livello di Gruppo, emersi nei risk assessment in ambito di corporate liability (in precedenza il GCP era strutturato per categorie di reati astrattamente rilevanti per il Gruppo) ciò al fine di rendere il GCP più coerente con le predette best practice e con i modelli di compliance da ultimo adottati dal Gruppo (i.e. Modelli di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001) e per meglio riflettere l'organizzazione delle società del Gruppo, nonché agevolare la comprensione del GCP da parte dei Destinatari.
01	18/12/2019	Seconda emissione
00	10/11/2017	Prima emissione

Approvato AD

Giuseppina Di Foggia

Sistemi di gestione e/o modelli organizzativi di riferimento:

x	Sistema di Gestione per la Qualità
	Sistema di Gestione Ambientale
	Sistema di Gestione per la sicurezza e la tutela della salute sui luoghi di lavoro
	Sistema di Gestione degli Incidenti Rilevanti - Seveso
	Sistema di Gestione per la sicurezza delle informazioni
	Sistema di Gestione dell'energia consumata per usi propri
	Sistema di Gestione per il Laboratorio LST
	Sistema di Gestione per il Centro di Taratura
x	Sistema di Gestione Anticorruzione
	Sistema di Gestione degli Asset
	Sistema di Gestione della Prevenzione e Controllo delle Infezioni
x	Sistema di Gestione della Compliance
	Business Continuity Management
	Tax Control Model
	Modello Privacy
	Modello 262
x	Modello 231

(apporre una "X" nella colonna di sinistra in riferimento alla riga interessata)

Indice

GLOSSARIO	4
1. PREMESSA	9
2. TOP LEVEL COMMITMENT	9
3. SCOPO, AMBITO DI APPLICAZIONE, QUADRO DI RIFERIMENTO, STRUTTURA DEL GCP E ADOZIONE, IMPLEMENTAZIONE E MODIFICHE DEL GCP	10
3.1. Scopo e Ambito di Applicazione.....	10
3.2. Il quadro di riferimento	11
3.3. Struttura del GCP	12
3.4. Adozione del GCP, implementazione e successive modifiche.....	13
4. RISK ASSESSMENT.....	15
5. IL GCP E GLI STANDARD GENERALI DI CONTROLLO	17
5.1. Il GCP e i riferimenti di controllo TERNA	17
5.2. Standard Generali di Controllo.....	18
5.3. Standard di gestione delle relazioni con i Terzi e Due Diligence	19

6. IL COMPLIANCE OFFICER	22
6.1. Nomina del Compliance Officer	22
6.2. Funzioni, poteri e flussi informativi	22
7. RELAZIONI CON ENTI PUBBLICI E FUNZIONARI PUBBLICI.....	25
8. RELAZIONI ISTITUZIONALI E GESTIONE DELLE ATTIVITÀ DI CORPORATE GIVING, INCLUSE LIBERALITÀ E SPONSORIZZAZIONI.....	29
9. ATTIVITÀ COMMERCIALI E RELAZIONI CON I CLIENTI.....	31
10. OPERAZIONI STRAORDINARIE (M&A, CESSIONI, ECC.) E GESTIONE DEI FLUSSI FINANZIARI	34
11. PROCUREMENT	37
12. HUMAN RESOURCES.....	39
13. AMMINISTRAZIONE, BILANCIO E FISCALE	41
14. GESTIONE DELLE INFORMAZIONI RISERVATE E PRIVILEGIATE.....	43
15. HEALTH, SAFETY AND ENVIRONMENT (“HSE”)	45
16. INFORMATION & COMMUNICATIONS TECHNOLOGY (“ICT”)	48
17. FORMAZIONE PER GLI ESPONENTI AZIENDALI E INFORMAZIONE DEI DESTINATARI .	51
18. SISTEMA DI WHISTLEBLOWING	53
18.1. Sistema di reporting (whistleblowing).....	53
18.2. Investigation.....	55
19. MONITORAGGIO E MIGLIORAMENTO CONTINUO	56
20. PROVVEDIMENTI DISCIPLINARI E RIMEDI CONTRATTUALI	57

GLOSSARIO

Action Plan: piano di interventi finalizzati al miglioramento del sistema di controllo individuato tenendo in considerazione gli esiti del Risk Assessment e la strategia di Risk Management individuata per il Rischio (tra evitare, ridurre, accettare e monitorare e trasferire).

Allegato Paese: il documento che costituisce la parte integrante del GCP predisposto in ciascuna Società Estera e che descrive i Compliance Program Locali e le procedure dalla stessa adottate a livello locale in attuazione al GCP.

Aree a Rischio: le aree di attività della Società Estera nel cui ambito può considerarsi in termini più concreti, il Rischio di commissione dei Reati.

Bribery Act: Bribery Act del Regno Unito del 2010.

COB: Compliance Officer Bureau, istituito nell'ambito delle Società Estere, che comprende il Compliance Officer e un Local Assistant, o il Compliance Officer e un Technical Assistant.

Codice Etico: il codice etico adottato nell'ambito del Gruppo Terna e approvato dal Consiglio di Amministrazione di TERNA il 21 maggio 2002 e relativi aggiornamenti, volto a definire i principi etico-comportamentali ai quali gli Amministratori, i Dipendenti e tutti coloro che operano in nome e per conto di TERNA o delle società del Gruppo Terna devono attenersi.

Compliance Officer o CO: soggetto individuato in ciascuna Società Estera con delibera dell'Organo Amministrativo avente il compito di favorire, nell'ambito della stessa, la diffusione della conoscenza del GCP e/o dei Compliance Program Locali previsti nell'Allegato Paese di riferimento e degli indirizzi della Capogruppo, nonchè agevolarne il funzionamento attraverso attività di formazione, informazione e attraverso l'implementazione di appositi flussi informativi.

Compliance Program Locali: programmi di compliance volti a prevenire la *corporate liability* adottati dalle Società Estere ai sensi della normativa locale applicabile nel Paese di riferimento e in linea con gli Standard Generali di Controllo e i Principi di Comportamento previsti dal Global Compliance Program.

Decreto 231: il D.Lgs. 8 giugno 2001 n. 231, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" e successive modifiche e integrazioni.

Destinatari: gli Esponenti Aziendali e gli Altri Destinatari.

DOJ: il U.S. Department of Justice.

Due Diligence: processo di verifica dei Terzi relativo all'instaurazione di rapporti contrattuali/commerciali con gli stessi o una specifica operazione.

Esponenti Aziendali: i dipendenti, gli amministratori e gli altri membri degli organi di gestione e di controllo delle Società Estere.

Facilitating Payments: indica i pagamenti fatti allo scopo di accelerare o garantire l'effettuazione di un'attività nell'esercizio di una funzione pubblica considerata di routine (per esempio, concessione di un permesso di soggiorno, concessione di un servizio di protezione da parte delle forze di polizia, organizzazione di un'attività ispettiva, concessione di una licenza commerciale, formalità connesse a operazioni di carico e scarico di merce).

FATF-GAFI o GAFI: Financial Action Task Force – Gruppo di Azione Finanziaria Internazionale¹ (organismo che coordina la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo).

FCPA: Foreign Corruption Practice Act degli Stati Uniti d'America del 1977 e successivi aggiornamenti.

Funzionario Pubblico: (a) qualunque funzionario, eletto o nominato, che esercita una pubblica funzione legislativa, amministrativa o giudiziaria; (b) qualunque persona che svolge funzioni pubbliche in qualsiasi ramo del governo nazionale, regionale o comunale o che esercita una funzione pubblica per qualsiasi agenzia o impresa pubblica, come i funzionari che esercitano funzioni pubbliche in imprese statali.

GCP o Global Compliance Program: il presente Global Compliance Program, documento adottato da TERNA in data 10 novembre 2017 e dalle Società Estere e sue successive modifiche.

Gestore: i soggetti, individuati dalla società, competenti per la gestione delle segnalazioni Whistleblowing.

Gruppo Terna: TERNA S.p.A. e le altre società dalla medesima controllate ai sensi dell'art. 93 del Decreto Legislativo 24 febbraio 1998, n. 58 (c.d. Testo Unico della Finanza).

Informazioni Privilegiate: le informazioni privilegiate e/o potenzialmente privilegiate relative a società quotate e, in particolare, a società quotate appartenenti al Gruppo Terna e ai relativi strumenti finanziari individuate dalla procedura per la tenuta e l'aggiornamento dei registri delle persone che hanno accesso a informazioni privilegiate e potenzialmente privilegiate (LG008).

Informazioni Riservate: le informazioni aziendali riguardanti la SE o altre società del Gruppo Terna, comprese le Informazioni Privilegiate, che non siano di pubblico dominio e che per oggetto o per altre caratteristiche,

¹ Il Gruppo d'azione finanziaria internazionale (GAFI) è un organismo internazionale il cui obiettivo è elaborare e promuovere strategie di lotta contro il riciclaggio di denaro e il finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa. (v. http://www.dt.mef.gov.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/organismi_internazionali/gafi/ <https://uif.bancaditalia.it/sistema-antiriciclaggio/organizzazione-internazionale/index.html?com.dotmarketing.htmlpage.language=102> [https://www.aif.va/ita/pdf/Regolamenti/IT-Istruzione_n.1-Aggiornamento_\(09.03.2021\).pdf](https://www.aif.va/ita/pdf/Regolamenti/IT-Istruzione_n.1-Aggiornamento_(09.03.2021).pdf))

abbiano comunque carattere riservato verso soggetti non tenuti a obblighi di riservatezza in base alla normativa vigente o per accordi contrattuali individuate dalla procedura per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate (LG005).

Linee Guida Anticorruzione o LG059: le linee guida Anticorruzione adottate dal Consiglio di Amministrazione di TERNA elaborate tenendo conto delle principali convenzioni internazionali, della normativa comunitaria, del FCPA e del Bribery Act in tema di prevenzione e lotta alla corruzione. Tali linee guida contengono principi e regole di comportamento per tutti gli Esponenti Aziendali (di tutte le società del Gruppo così come per qualsiasi terzo che agisca in nome e/o per conto di TERNA o del Gruppo Terna, quali fornitori, agenti, consulenti, partner commerciali o qualsiasi altra controparte.

Linea Guida Whistleblowing o LG054: la linea guida adottata da TERNA in materia di Whistleblowing.

Liste: per Liste si intendono

- i. le liste Paesi a rischio corruzione (ad es. indice di percezione della corruzione di Transparency International);
- ii. elenchi di soggetti (persone fisiche e/o giuridiche) predisposti dall'Unione Europea, da ogni singolo Stato membro dell'Unione Europea, dal Regno Unito, dagli Stati Uniti d'America, dalle Nazioni Unite e da ogni altra giurisdizione, e rilevanti – ai sensi della normativa applicabile o per effetto di disposizioni contrattuali, come di volta in volta aggiornate, integrate, modificate ed efficaci – per TERNA e le società del Gruppo Terna, che contengono gli elementi di identificazione dei soggetti (persone fisiche e/o giuridiche) ed attività con i quali, o in relazione alle quali, è vietato effettuare, direttamente o indirettamente, operazioni, in quanto soggetti a Misure Restrittive;
- iii. lista Paesi a rischio riciclaggio e finanziamento al terrorismo elaborate dall'UE, liste «black list»/«grey list» (indicate da GAFI², UE, ecc.), liste ONU relative alle sanzioni finanziarie applicate a soggetti ed entità collegati alle organizzazioni terroristiche.

Local Assistant: soggetto individuato all'interno di una funzione aziendale della Società Estera o comunque nell'ambito del Paese o dell'area geografica della Società Estera con delibera dell'Organo Amministrativo della stessa e con parere positivo del CO della Società Estera, deputato, quale presidio locale, ad assistere il CO nell'esecuzione dei propri compiti nel caso in cui il CO sia individuato in un soggetto non appartenente alla Società Estera o all'area geografica della stessa o nel caso in cui il CO ne abbia richiesto la nomina.

Management Locale: l'amministratore delegato o l'executive director o il componente dell'Organo Amministrativo con deleghe operative o funzione corrispondente.

²<https://uif.bancaditalia.it/sistema-antiriciclaggio/organizzazione-internazionale/index.html?com.dotmarketing.htmlpage.language=102>
[https://www.aif.va/ita/pdf/Regolamenti/IT-Istruzione_n.1-Aggiornamento_\(09.03.2021\).pdf](https://www.aif.va/ita/pdf/Regolamenti/IT-Istruzione_n.1-Aggiornamento_(09.03.2021).pdf)

Misure Restrittive: restrizioni commerciali e finanziarie adottate dall'Unione Europea, da ogni singolo Stato membro dell'Unione Europea, dal Regno Unito, dagli Stati Uniti d'America, dalle Nazioni Unite e da ogni altra giurisdizione, e rilevanti – ai sensi della normativa applicabile o per effetto di disposizioni contrattuali, come di volta in volta aggiornate, integrate, modificate ed efficaci – per TERNA e le società del Gruppo Terna nei confronti di Paesi terzi e/o di soggetti (persone fisiche e/o giuridiche) e/o di beni e servizi (inclusi software, tecnologie, engineering e assistenza tecnica) e attività.

Organo Amministrativo: Consiglio di Amministrazione o organismo o funzione corrispondente delle Società Estere.

Pubblica Amministrazione o P.A. o ente pubblico: ciascuno degli enti o apparati che concorrono all'esercizio delle funzioni legislativa, amministrativa o giudiziaria di un singolo stato, ivi compresi gli enti governativi.

PCR: la struttura Presidio Corporate Liability e e Compliance Risk nell'ambito di Compliance.

POC: la Direzione People Organization and Change.

Principi di Comportamento: gli standard minimi di comportamento connessi alle Aree a Rischio.

Processi: i macro-processi rilevanti, individuati dal GCP, nell'ambito dei quali vengono individuate le Aree a Rischio.

Reati: determinati tipi di comportamenti illeciti qualificabili come reati in diverse giurisdizioni e che potrebbero essere potenzialmente commessi da un Esponente Aziendale o da un Terzo e la cui prevenzione nel Gruppo deve essere considerata una priorità al fine di gestire il proprio business con onestà e integrità.

Red Flag: uno o più indicatori di anomalia/fattori di Rischio Potenziale (sotto il profilo della corruzione, riciclaggio o ulteriori fattispecie di reato rilevanti) che devono essere verificati nell'ambito della Due Diligence.

Rischio: qualsiasi evento futuro che nell'ambito dell'azienda, da solo o in correlazione con altri eventi interni o esterni, può influenzare negativamente il raggiungimento degli obiettivi indicati nelle normative di riferimento del singolo Paese.

Rischio Potenziale: la possibilità che un evento futuro e incerto in una specifica area/processo aziendale realizzi un Rischio.

Rischio Residuo: il Rischio di Reati connesso a una specifica area/processo aziendale mitigato dall'esistenza ed effettività dei controlli interni adottati.

Risk Assessment: l'analisi dei processi aziendali volta a identificare e valutare i potenziali rischi di commissione delle fattispecie di Reati rilevanti ed i relativi presidi esistenti.

Sistema di Controllo Interno e di Gestione dei Rischi o SCIGR: insieme della cultura, delle capacità, delle regole, procedure e delle pratiche aziendali, nonché delle strutture organizzative, volte a definire un sistema di accountability per l'identificazione, misurazione, gestione, mitigazione e controllo dei principali rischi a livello di Gruppo, mantenendo di conseguenza alta la fiducia degli stakeholders con riguardo al governo e al controllo del Gruppo medesimo.

Società Estera/e o SE: società non italiana/e del Gruppo Terna.

Standard Generali di Controllo: standard generali di controllo individuati e disciplinati dal GCP che ciascuna Società Estera deve adottare in coerenza con il SCIGR adottato dal Gruppo Terna volti a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati.

Technical Assistant: soggetto individuato nell'ambito della struttura PCR con delibera dell'Organo Amministrativo e parere positivo del CO della Società Estera, deputato ad assistere il CO nell'esecuzione dei propri compiti, nel caso in cui il CO non sia stato identificato nell'ambito della struttura PCR.

TERNA: la Capogruppo TERNA - Rete Elettrica Nazionale Società per Azioni (in forma abbreviata TERNA S.p.A.).

Terzi o Altri Destinatari: qualsiasi terzo che agisca in nome e/o per conto di una SE, quali fornitori, agenti, consulenti, partner commerciali o qualsiasi altra controparte.

1. PREMESSA

La Capogruppo TERNA - Rete Elettrica Nazionale Società per Azioni (“**TERNA**”) è la società responsabile in Italia della trasmissione e del dispacciamento dell’energia elettrica sulla rete ad alta e altissima tensione. Le sue azioni sono quotate sul Mercato italiano della Borsa Telematica organizzato e gestito da Borsa Italiana S.p.A., segmento Mercato Telematico Azionario (“MTA”), comprendente le imprese di media e grande capitalizzazione e allineato alle *best practice* internazionali e appartenenti all’indice Financial Times Stock Exchange - Milano Indice di Borsa (FTSE MIB). TERNA inoltre è tra i grandi emittenti italiani quotati presenti nell’indice MIB 40 ESG, il primo indice blue-chip per l’Italia dedicato alle best practice ambientali, sociali e di governance (ESG) che combina la misurazione della performance economica con valutazioni ESG in linea con i principi del Global Compact delle Nazioni Unite.

TERNA è la *holding* di un gruppo multinazionale che opera in un settore commerciale complesso e ampiamente regolamentato e in ambienti economici, politici, sociali e culturali estremamente variegati (il “**Gruppo Terna**”).

2. TOP LEVEL COMMITMENT

Il Gruppo Terna conduce il proprio business secondo i criteri di lealtà, legalità, correttezza, integrità e trasparenza, nel rispetto delle normative applicabili in Italia e all’estero in materia di *criminal corporate liability*.

Il Gruppo Terna promuove e diffonde una cultura dell’etica e di *compliance*. L’impegno è assunto, principalmente, da tutti i vertici del Gruppo Terna (*Top-level commitment*) che si adoperano per diffondere tale messaggio a tutti i livelli.

A tale scopo, i vertici delle singole società del Gruppo Terna definiscono e diffondono linee guida, procedure e politiche interne volte a regolare e formalizzare detto impegno al fine di prevenire la commissione di attività illecite.

In particolare, anche gli organi amministrativi delle società non italiane del Gruppo (le “**Società Estere**” o “**SE**”) esprimono e sono chiamati a diffondere, in modo chiaro, il messaggio di assoluta osservanza dei principi di etica, integrità e legalità del Gruppo Terna.

3. SCOPO, AMBITO DI APPLICAZIONE, QUADRO DI RIFERIMENTO, STRUTTURA DEL GCP E ADOZIONE, IMPLEMENTAZIONE E MODIFICHE DEL GCP

3.1. Scopo e Ambito di Applicazione

In molti Paesi esteri in cui opera il Gruppo Terna esiste un regime di responsabilità penale o assimilabile, suscettibile di applicazione alle persone giuridiche in relazione a comportamenti illeciti commessi da rappresentanti, dipendenti o soggetti terzi che agiscono nel loro interesse.

La maggior parte di tali normative estere incoraggia le aziende a dotarsi di strumenti di governo societario e sistemi di mitigazione dei rischi volti a prevenire la commissione di reati da parte di tali soggetti, prevedendo in alcuni casi un'esenzione o una mitigazione delle sanzioni applicabili qualora vengano adottate ed efficacemente attuate adeguate misure di prevenzione.

Al fine di armonizzare gli sforzi delle Società Estere nel prevenire la responsabilità penale aziendale e al fine di fornire alle stesse un approccio condiviso, coerente e uniforme contro possibili comportamenti illeciti, TERNA ha adottato, sin dal 10 novembre 2017 e con successivi aggiornamenti, il *global compliance program* (“**Global Compliance Program**” o “**GCP**”).

Il GCP mira a definire gli standard generali di controllo e i principi di comportamento applicabili ai dipendenti, agli amministratori e agli altri membri degli organi di gestione e di controllo delle SE (“**Esponenti Aziendali**”) nonché, ove applicabili, agli Altri Destinatari al fine di prevenire la commissione di fattispecie di reato rilevanti.

Il GCP costituisce, al pari delle procedure di cui al par. 5.1, un atto di indirizzo di TERNA la cui applicazione è rivolta alle Società Estere chiamate a recepirlo.

Ciascuna Società Estera, laddove opportuno o richiesto dalla normativa locale applicabile, definisce e adotta altresì dei propri Compliance Program Locali, in conformità con la suddetta normativa e in linea con quanto previsto dal presente GCP, riportati nell'ambito dell'Allegato Paese di riferimento da ciascuna approvato.

In tali contesti, il GCP è dunque integrato, come meglio descritto al par. 5.1, con le regole eventualmente previste nello specifico Allegato Paese, che include i Compliance Program Locali.

3.2. Il quadro di riferimento

Il GCP si ispira alle più importanti normative e *best practice* anche internazionali tra cui, a titolo esemplificativo e non esaustivo, si annoverano le seguenti:

- (i) il Decreto Legislativo dell'8/06/2001, n. 231 ("**Decreto 231**") e successivi aggiornamenti, che disciplina il regime di responsabilità amministrativa (simile a una responsabilità penale) delle persone giuridiche risultante dalla commissione di determinati reati per conto o nell'interesse delle stesse;
- (ii) "Codice di Corporate Governance" delle società quotate promosso da Borsa Italiana S.p.A.
- (iii) le 2010 *Federal Sentencing Guidelines Manual & Supplement*, adottate dalla United States Sentencing Commission il 1° novembre 2010;
- (iv) Foreign Corruption Practice Act ("**FCPA**") del 1977 e successivi aggiornamenti;
- (v) UK Bribery Act del 2010 e successivi aggiornamenti;
- (vi) la *Good Practise Guidance on Internal Controls, Ethics, and Compliance* adottata dal Consiglio dell'OCSE il 18 febbraio 2010;
- (vii) la "*Resource Guide to the U.S. Foreign Corrupt Practices Act*" emanata dal Criminal Division of the U.S. Department of Justice ("**DOJ**") e dall'Enforcement Division of the U.S. Securities and Exchange Commission del 2012 e successivi aggiornamenti;
- (viii) "*Evaluation of Corporate Compliance Programs*" del DOJ del 2017 e successivi aggiornamenti;
- (ix) l'*Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide* adottato dall'United Nations Office on Drugs and Crime (UNODC) nel settembre del 2013;
- (x) le raccomandazioni adottate dalla 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;
- (xi) 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);
- (xii) D.Lgs. 10 marzo 2023 n. 24, in 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;

(xiii) 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.

3.3. Struttura del GCP

Il presente documento, oltre a esplicitare l'impegno del *top management* nella promozione e definizione della cultura in materia di etica e compliance (cd. *top level commitment*), nonché le modalità di adozione del GCP, implementazione e successive modifiche da attuare anche in ciascuna Società Estera, individua e disciplina³:

- le modalità di Risk Assessment, descritte al par. 4, vevoli anche per l'individuazione delle Aree a Rischio nell'ambito del Gruppo Terna per la predisposizione dei Compliance Program Locali riportati negli Allegati Paese;
- gli standard generali di controllo ("**Standard Generali di Controllo**"), descritti al par. 5.2, che ciascuna Società Estera deve adottare in coerenza con il Sistema di Controllo Interno e Gestione dei Rischi di cui al par. 5.1, volti a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati;
- il ruolo del Compliance Officer, descritto nel par. 6, individuato quale figura nominata in ciascuna Società Estera e preposta a garantire la diffusione della conoscenza ed agevolare il funzionamento del Global Compliance Program e dell'Allegato Paese di riferimento;
- i macro-processi rilevanti (i "**Processi**"), che devono essere sempre tenuti in conto per l'applicazione del GCP da ciascuna Società Estera nell'ambito dei quali vengono individuate, tramite l'attività di Risk Assessment, le aree di attività nel cui ambito può considerarsi in termini più concreti il Rischio di commissione dei Reati (le "**Aree a Rischio**") in relazione a determinati tipi di comportamenti illeciti qualificabili come reati in diverse giurisdizioni e che potrebbero essere potenzialmente commessi da un Esponente Aziendale o da un Terzo e la cui prevenzione nel Gruppo deve essere considerata una priorità al fine di gestire il proprio business con onestà e integrità (i "**Reati**", descritti nell'Appendice A allegata al GCP a01LG058). Per ogni macro-processo sono individuati gli standard di comportamento minimi connessi alle Aree a Rischio (i "**Principi di Comportamento**").

I Principi di Comportamento di cui ai par. 7 e 10 devono intendersi applicabili trasversalmente per tutti i Processi disciplinati nei paragrafi da 7 a 16.

- I Processi descritti costituiscono la base di riferimento per ciascuna Società Estera per l'elaborazione, attraverso specifica attività di Risk Assessment, del rispettivo Allegato Paese (si vedano par. 7 - 16);

³ La struttura del GCP è basata sulle principali *best practice* e normative applicabili in materia di compliance program, così come individuate a titolo esemplificativo e non esaustivo nel par. 3.2. Per quanto concerne l'individuazione dei Processi e delle Aree a Rischio, questa è stata effettuata tenendo in considerazione i macro-processi e le macro-aree di rischio rilevanti a livello del Gruppo Terna, allo stato emerse nei Risk Assessment in ambito di corporate liability.

- la formazione agli Esponenti Aziendali e l'informazione dei Destinatari in ordine al GCP per garantire l'effettiva applicazione dei presidi dallo stesso predisposti, come indicato al par. 17;
- il sistema di *whistleblowing* per la gestione delle segnalazioni di comportamenti illeciti o irregolarità e di reporting interno, riportati al par. 18;
- i presidi per il monitoraggio e il miglioramento continuo del GCP e dei Compliance Program Locali, disciplinati al par. 19;
- i provvedimenti disciplinari e rimedi contrattuali applicabili in caso di violazione delle disposizioni individuate nell'ambito del GCP e che devono essere tenuti in considerazione dalle Società Estere nell'ambito dei propri Compliance Program Locali, disciplinati al par. 20.

3.4. Adozione del GCP, implementazione e successive modifiche

Il GCP esprime principi che rientrano tra i valori fondamentali del Gruppo Terna e ne ispirano l'organizzazione e le attività anche in attuazione dei principi del Codice Etico comuni alle Società Estere ed è stato approvato dal Consiglio di Amministrazione di TERNA.

TERNA promuove pertanto l'adozione del GCP da parte di tutte le società del Gruppo Terna.

Ciascuna Società Estera è chiamata ad approvare il GCP con delibera del Consiglio di Amministrazione o dell'organismo o della funzione corrispondente ("**Organo Amministrativo**").

Le società italiane controllanti⁴ Società Estere adottano il GCP con lo scopo di fornire un indirizzo comune a dette controllate per contrastare più efficacemente fenomeni di criminalità di impresa.

Eventuali e successive modifiche al GCP sono approvate dall'Amministratore Delegato di TERNA in virtù della delega conferita dal Consiglio di Amministrazione in sede di approvazione del GCP⁵, nonché, dall'Organo Amministrativo di ciascuna Società Estera e rispettive controllanti o, laddove sia stata conferita apposita delega, dall'Amministratore Delegato di ciascuna.

L'Organo Amministrativo di ciascuna Società Estera, in conformità alla propria autonomia e indipendenza:

- è responsabile della corretta individuazione di qualsiasi Processo e Area a Rischio o Principio di Comportamento, oltre a quelli individuati ai paragrafi 7 e ss. del GCP da attuare attraverso Compliance Program Locali o linee guida, procedure, politiche interne locali;

⁴ In ogni caso, le società controllanti di diritto italiano sono dotate di un compliance program in linea con la normativa italiana, i.e. il Modello di Organizzazione, Gestione e Controllo ex Decreto Legislativo 231/2001 in linea con quanto previsto dalla LG032 del Gruppo Terna "Implementazione e gestione dei Modelli Organizzativi ex d.lgs. 231/2001 nel Gruppo Terna".

⁵ Le Appendici A e B potranno essere aggiornate dal Direttore Industrial Program Management Office di TERNA S.p.A. in virtù della facoltà di subdelega conferita all'AD di TERNA S.p.A.

- adotta le misure più appropriate per l'implementazione e il monitoraggio del GCP, tenendo conto dell'organizzazione, della complessità delle attività, del profilo di rischio specifico e del quadro normativo applicabile alla società;
- è responsabile dell'adozione, implementazione e monitoraggio, laddove richiesto dalle normative nazionali, di Compliance Program Locali, richiamati nell'Allegato Paese di riferimento.

4. RISK ASSESSMENT

Alla base di ogni compliance program vi è lo svolgimento di un'analisi dei processi aziendali volta ad identificare e valutare i potenziali rischi di commissione delle fattispecie di Reati rilevanti ed i relativi presidi esistenti (“**Risk Assessment**”).

Le fasi che compongono il Risk Assessment sono le seguenti:

- (i) mappatura Aree a Rischio, ossia individuare e mappare, nell'ambito dei singoli processi aziendali, le aree e le relative attività che sono potenzialmente esposte al rischio di commissione dei Reati;
- (ii) valutazione del grado di Rischio Potenziale, effettuata alla luce dei possibili fattori idonei a generare il Rischio. Per “**Rischio**” si intende qualsiasi evento futuro che nell'ambito dell'azienda, da solo o in correlazione con altri eventi interni o esterni, può influenzare negativamente il raggiungimento degli obiettivi indicati nelle normative di riferimento del singolo Paese. La possibilità che un evento futuro e incerto in una specifica area/processo aziendale realizzi un Rischio costituisce un “**Rischio Potenziale**”;
- (iii) valutazione dell'adeguatezza dei protocolli interni, al fine di individuare tutte le procedure e i controlli idonei a mitigare i rischi potenziali, nonché eventuali necessità di adeguare tali controlli. Il sistema di controlli preventivi deve essere tale da garantire che i Rischi di commissione dei Reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un “livello accettabile”;
- (iv) calcolo del rischio residuo (il “**Rischio Residuo**”), inteso come il Rischio di Reati connesso a una specifica area/processo aziendale mitigato dall'esistenza ed effettività dei controlli interni adottati.

Tenendo in considerazione gli esiti del Risk Assessment e la strategia di Risk Management individuata per il Rischio (tra evitare, ridurre, accettare e monitorare e trasferire), viene effettuato un piano di interventi finalizzati al miglioramento del sistema di controllo (l’“**Action plan**”).

Ogni Società Estera effettua un Risk Assessment, elabora un Action Plan e attua le eventuali azioni correttive e di adeguamento al fine di presidiare la *corporate liability*.

A tal fine deve tenere conto, preliminarmente, dell'elenco dei Processi e delle Aree di Rischio rilevanti a livello generale per TERNA e il Gruppo Terna indicati nei par. 7 e ss.

Tale elenco, dunque, non esime le Società Estere (a) dall'effettuare la propria valutazione del rischio sulla base della normativa locale applicabile nonché delle peculiarità della propria attività e struttura organizzativa e (b) a definire, laddove opportuno, propri principi di controllo integrativi rispetto a quelli contenuti nel presente GCP, par. 5.2, nonché (c) a definire eventuali specifici principi di comportamento rispetto a quelli contenuti nei par. 7 e ss. del presente GCP. A tal fine, le Società Estere identificheranno:

- i) i propri processi e le proprie Aree a Rischio che possono comportare un Rischio specifico di commissione di un Reato attraverso un'analisi dei propri processi aziendali e delle possibili modalità di commissione di Reati individuati come rilevanti sulla base delle normative locali applicabili;
- ii) gli ulteriori standard di controllo e principi di comportamento da attuare attraverso Compliance Program Locali e/o procedure interne locali a cui tutti gli Esponenti Aziendali e, ove applicabili, i Terzi devono attenersi al fine di prevenire la commissione di Reati.

Le singole Società Estere svolgono e aggiornano costantemente la propria valutazione dei Rischi.

5. IL GCP E GLI STANDARD GENERALI DI CONTROLLO

5.1. Il GCP e i riferimenti di controllo TERNA

I dettami del GCP sono in generale ispirati all'insieme della cultura, delle capacità, delle regole, delle procedure e delle pratiche aziendali, nonché delle strutture organizzative, volti a definire un sistema di *accountability* per l'identificazione, misurazione, gestione, mitigazione e controllo dei principali rischi a livello di Gruppo mantenendo di conseguenza alta la fiducia degli stakeholders con riguardo al governo e al controllo del Gruppo medesimo, nel complesso, definito come il “**Sistema di Controllo Interno e di Gestione dei Rischi**” o “**SCIGR**” e pertanto sono integrati dalle seguenti procedure vigenti e applicabili nel Gruppo Terna:

- (i) i principi del Codice Etico adottato nel Gruppo, applicabili anche a tutte le Società Estere e che tutti i Destinatari sono tenuti a rispettare;
- (ii) Linee Guida, politiche e procedure adottate da TERNA e applicabili nel Gruppo Terna; in particolare:
 - a. Linea Guida Sistema di Controllo Interno e di Gestione dei rischi del Gruppo Terna (LG004);
 - b. Linea Guida Gestione dei rischi in Terna (LG038);
 - c. Linea Guida in materia di whistleblowing (LG054);
 - d. Linea-guida Anticorruzione (LG059);
 - e. Politica di corporate giving (LG024);
 - f. Linea Guida Regolamento Comitato Etico (LG014);
 - g. Linea Guida Golden Rule (LG042);
 - h. Trade Compliance Policy (LG061);
 - i. Politica di Sostenibilità (LG077);
 - j. Diversity & Inclusion (LG069);
 - k. Il rispetto dei “Diritti Umani” nel Gruppo Terna (LG057);
 - l. Linea Guida Due Diligence sulle Terze Parti (LG070);
 - m. Linee Guida in materia di Conflitto di Interessi (LG079);
 - n. Approvazione delle operazioni significative e gestione delle situazioni di interesse (LG006);
 - o. Procedura Operazioni con Parti Correlate (LG026);
 - p. Procedura per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate (LG005);
 - q. Procedura per la tenuta e l'aggiornamento dei registri delle persone che hanno accesso a informazioni privilegiate e potenzialmente privilegiate (LG008);

- r. Gestione delle ispezioni svolte dalla P.A. (IO416CA).

Inoltre, le previsioni del GCP sono integrate per ciascuna Società Estera da:

- i. le regole previste nello specifico Allegato Paese adottato da ciascuna SE, che include i Compliance Program Locali;
- ii. le disposizioni di corporate governance adottate dalle stesse SE in conformità alla legislazione applicabile e alle best practice internazionali, tra cui quelle indicate nel par. 3.2.;
- iii. il sistema di controllo interno e di gestione dei rischi adottato in ciascuna Società Estera (e.g. procedure e policy locali, principi di comportamento, ecc.).

Qualora leggi o normative locali o politiche e procedure aziendali così adottate dalle singole Società Estere prevedano regole più stringenti rispetto a quelle contenute nel presente GCP, le prime prevarranno.

5.2. Standard Generali di Controllo

Ogni Società Estera nel valutare l'opportunità di dotarsi di procedure locali – tenendo in considerazione la peculiare attività svolta e i rischi specifici associati come individuati sulla base del *Risk Assessment* che dovrà svolgere secondo quanto indicato al paragrafo 4 – dovrà in ogni caso:

- prevedere gli Standard Generali di Controllo individuati nel presente GCP (es. tracciabilità, individuazione dei ruoli e delle responsabilità, archiviazione, ecc.);
- dettagliare i controlli interni;
- prevedere l'applicazione di sanzioni disciplinari in caso di violazione delle stesse.

Gli Standard Generali di Controllo sono i seguenti:

- **segregazione dei ruoli:** l'assegnazione di ruoli, compiti e responsabilità all'interno di ogni società deve essere effettuata in conformità al principio di segregazione dei ruoli secondo cui nessun individuo può svolgere autonomamente un intero processo (i.e. secondo questo principio, nessun individuo può, da solo e in autonomia, eseguire un'azione, autorizzarla e successivamente controllarne l'esecuzione). Un'adeguata segregazione dei ruoli può essere garantita anche utilizzando sistemi informatici che consentano solo alle persone identificate e autorizzate di svolgere determinate operazioni;
- **potere di firma e autorizzazione:** ciascuna società deve emanare disposizioni formali in relazione all'esercizio dei poteri autorizzativi e di firma che devono essere coerenti con le responsabilità organizzative e gestionali attribuite;
- **trasparenza e tracciabilità dei processi:** l'identificazione e la tracciabilità delle fonti, delle informazioni e dei controlli effettuati in relazione alla formazione e all'attuazione delle decisioni della Società Estera,

nonché in relazione alla gestione delle risorse finanziarie, deve sempre essere garantita; è altresì opportuno garantire la corretta registrazione dei relativi dati e delle informazioni, attraverso sistemi informatici e/o supporto cartaceo;

- **corretta gestione delle relazioni con i Terzi e Due Diligence** (si veda par. 5.3).

5.3. Standard di gestione delle relazioni con i Terzi e Due Diligence

TERNA e le società del Gruppo Terna prestano particolare attenzione alla selezione dei Terzi. A tal fine, ogni volta che una società è impegnata in attività di *business* attraverso una *joint venture* oppure intende rivolgersi a un Terzo in connessione a qualsiasi *business*, deve essere condotta un'indagine sul Terzo, volta a individuarne la catena di controllo, il possesso di requisiti di onorabilità, professionali e finanziari, la sua credibilità sul mercato, nonché la sua conformità alle Leggi Anti-Corruzione vigenti, o leggi simili previste dal Paese in cui opera o opererà per conto di qualsiasi società del Gruppo Terna.

La Due Diligence dovrà essere proporzionata al rischio reale o percepito in relazione al Terzo e/o all'operazione (*risk based*).

La Due Diligence è condotta, sulla base dei criteri individuati dalla Capogruppo, che potranno includere: (i) ricerche tramite fonti pubbliche e altre fonti disponibili (ad es. contatti di business, camere di commercio locali, associazioni di imprese; ricerche su web o società specializzate, iscrizioni in Liste) su società, soci ed esponenti, al fine di reperire eventuali informazioni negative potenzialmente rilevanti a carico degli stessi; (ii) o approfondimenti svolti da consulenti terzi.

La Due Diligence è disciplinata da linee guida di indirizzo per il Gruppo di cui al par. 5.1 (in particolare, le Linee Guida Anticorruzione LG059 e la Linea Guida Due Diligence su Terze Parti LG070), nonché dalle procedure locali adottate dalle SE, ove esistenti.

La Due Diligence sul Terzo potrà essere svolta con il supporto delle strutture competenti del Gruppo Terna (secondo quanto previsto dalla Linea Guida Due Diligence su Terze Parti LG070) in riferimento alle procedure aziendali che prevedono l'attivazione delle verifiche di controparti.

In ogni caso, la Due Diligence condotta dovrà evidenziare potenziali Red Flag.

Di seguito sono elencati alcuni esempi di Red Flag che possono essere presi in considerazione nell'esecuzione della Due Diligence, quali potenziali fattori di rischio o indicatori della possibile commissione di Reati:

- se il Terzo o, in caso di società, i suoi soci, sono residenti o hanno sede legale o svolgono la propria attività in un Paese presente nelle cd. “black list”/“grey list” internazionali antiriciclaggio (ad es. pubblicate dal GAFI e dall’Unione Europea) o in un Paese identificato come Paese che fornisce supporto ad attività terroristiche o nel cui territorio operano organizzazioni terroristiche ovvero in quei Paesi considerati quali “Paradisi Fiscali” così come individuati da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE) o in un Paese ad alto rischio corruzione (si veda ad es. ranking di Transparency International) o sottoposti a sanzioni internazionali;
- se sussistono elementi di insufficienti, false o inconsistenti informazioni fornite dal Terzo o apparenti tentativi di celare l’identità del soggetto posto al vertice della catena di controllo;
- se il Terzo svolge attività/business che non risultano coerenti o non conformi con la prestazione contrattuale richiesta o se il Terzo o uno dei suoi esponenti sia in conflitto di interessi;
- se vi siano comunque operazioni o richieste che non sono coerenti con l’attività svolta dal Terzo, quali richieste di pagamento presso un Paese ad alto rischio che non abbia alcuna connessione con il Terzo (per esempio, un Paese con leggi molto protettive in materia di segreto bancario, o con controlli deboli sul riciclaggio di denaro o dove la criminalità/la corruzione è diffusa). A tale scopo i Paesi ad alto rischio devono essere valutati tenendo conto di indici internazionali, come il Transparency International Corruption Perceptions Index;
- se vi sia la richiesta di strutturare un’operazione in maniera tale da eludere le normali regole di contabilità e reportistica o tale da non mostrare alcun legittimo scopo commerciale, per esempio aumentando i prezzi o effettuando una parte del pagamento “sotto traccia” attraverso la stesura di side letter;
- se occorra ricorrere a consulenti o ad altri Terzi che abbiano stretti legami con un governo o con un partito politico, o che siano stati specificamente segnalati da un Funzionario Pubblico o da un cliente;
- se vi siano richieste di pagamento di commissioni, provvigioni o altre forme di remunerazione inusuali o richieste di pagamenti in contanti;
- se il Terzo sia apparentemente privo delle competenze, esperienza o risorse richiesti per il tipo di attività oppure abbia una struttura organizzativa aziendale assente o mezzi patrimoniali non adeguati;
- se il Terzo ha una struttura proprietaria anomala o particolarmente complessa data la natura del suo business;
- se il Terzo, con riferimento all’operazione, rifiuti di sottoscrivere un contratto;
- se il Terzo rifiuti di impegnarsi a rispettare o di rispettare le presenti Linee Guida e/o ulteriori procedure interne di compliance adottate dalla SE e/o valevoli per il Gruppo e non abbia adottato alcun codice di condotta o strumento di compliance similare atto a prevenire la commissione di reati;
- se il Terzo è o è stato sospeso dalla partecipazione a gare o dalla sottoscrizione di contratti con società statali/enti pubblici/enti governativi a fronte di indagini ispettive svolte;
- se il Terzo o uno dei suoi esponenti abbiano una reputazione discutibile o siano/siano stati indagati, rinviati a giudizio o condannati nell’ambito di un procedimento penale specialmente per reati quali corruzione, riciclaggio o frode o siano stati sottoposti a indagini o sanzionati da parte di autorità pubbliche

di vigilanza della borsa e dei mercati (es., Securities and Exchange Commission statunitense (SEC)) o siano stati interdetti o sottoposti a misure cautelari;

- se la sede operativa del Terzo è un ufficio virtuale;
- se il Terzo ha un socio occulto.

La presenza di una o più Red Flag richiede un esame maggiormente approfondito che può includere controlli aggiuntivi e/o appropriati livelli autorizzativi.

In caso di transazioni ad alto rischio o per situazioni particolarmente complesse, le analisi possono essere integrate da pareri e approfondimenti su specifiche questioni affidati a provider o consulenti specializzati nelle materie di riferimento.

È necessario un monitoraggio nel corso del rapporto contrattuale per assicurare che il Terzo mantenga i requisiti individuati e approvati, se necessario aggiornando periodicamente la Due Diligence. Nel caso in cui un Terzo perda tali requisiti o emerga un Red Flag durante la vigenza del rapporto contrattuale, dovranno essere definite misure appropriate da applicare.

I Terzi dovranno essere adeguatamente informati sui contenuti del GCP e, laddove esistenti, dei Compliance Program Locali e dovranno impegnarsi a rispettare i Principi di Comportamento contenuti nei predetti documenti mediante la sottoscrizione di apposite clausole contrattuali, così come previsto al successivo par.

17.

6. IL COMPLIANCE OFFICER

6.1. Nomina del Compliance Officer

In ciascuna Società Estera è nominato un Compliance Officer (“**Compliance Officer**” o “**CO**”), soggetto individuato con delibera dell’Organo Amministrativo, avente il compito di favorire, nell’ambito della stessa, la diffusione della conoscenza del GCP e/o dei Compliance Program Locali previsti nell’Allegato Paese di riferimento e degli indirizzi della Capogruppo, nonché agevolarne il funzionamento attraverso le attività di formazione/informazione relative al GCP di cui al par. 17 e attraverso l’implementazione di appositi flussi informativi, come dettagliato al successivo par. 6.2.

Il CO deve essere in possesso di competenze adeguate in materia giuridica o di controllo e gestione dei rischi aziendali, da valutare alla luce del *curriculum vitae* e delle esperienze professionali pregresse.

Il CO deve, inoltre, essere in possesso di requisiti di onorabilità, da valutare tenendo conto della condotta pregressa e del rispetto dei principi etici che governano l’operato del Gruppo Terna.

Il CO, per l’esecuzione dei propri compiti, è eventualmente affiancato da soggetti nominati con delibera dell’Organo Amministrativo della Società Estera e previo parere positivo dello stesso CO che insieme costituiscono il Compliance Officer Bureau (“**COB**”),

Tali soggetti possono essere individuati:

- all’interno di una funzione aziendale della Società Estera o comunque nell’ambito del Paese o dell’area geografica della Società Estera nel caso in cui il CO sia individuato in un soggetto non appartenente alla Società Estera o all’area geografica della stessa o nel caso in cui il CO ne abbia richiesto la nomina (“**Local Assistant**”),
- nell’ambito della struttura Presidio Corporate Liability e Compliance Risk nell’ambito di Compliance (“**PCR**”), deputato ad assistere il CO nell’esecuzione dei propri compiti, nel caso in cui il CO non sia stato identificato nell’ambito della struttura PCR (“**Technical Assistant**”).

Il coordinamento nella gestione delle tematiche di compliance a livello di Gruppo Terna è garantito in occasione delle riunioni convocate ai sensi del Modello 231 della Capogruppo dal Presidente dell’OdV di Terna S.p.A.

Il COB, ove istituito, si riunisce periodicamente e comunque quando necessario: anche in tali occasioni può essere assicurato il coordinamento.

6.2. Funzioni, poteri e flussi informativi

In particolare, il CO deve:

- favorire la diffusione della conoscenza del Global Compliance Program e dei Compliance Program Locali adottati come previsti nell’Allegato Paese di riferimento e degli indirizzi della Capogruppo di cui al par.

5.1 nonché agevolarne il funzionamento attraverso le attività di formazione/informazione relative al GCP di cui al par. 17 e/o attraverso l'implementazione di appositi flussi informativi;

- monitorare i comportamenti posti in essere all'interno dei processi della SE e delle Aree a Rischio ed effettuare i controlli per l'accertamento di presunte violazioni delle prescrizioni del Global Compliance Program come integrato dal relativo Allegato Paese;
- coordinarsi con il Management Locale della SE per il migliore monitoraggio delle attività nelle Aree a Rischio;
- monitorare sulla effettiva attuazione di tutte le necessarie misure disciplinari al fine di punire qualsiasi colpevole discostamento dalle regole di comportamento prestabilite;
- informare periodicamente l'Organo Amministrativo della Società Estera, relativamente ad ogni rilevante iniziativa intrapresa riguardante il Global Compliance Program e i Compliance Program Locali adottati nelle specifiche società indicate nell'Allegato Paese;
- informare tempestivamente l'Organo Amministrativo della Società Estera relativamente ad ogni eventuale accertata violazione del Global Compliance Program e dell'Allegato Paese di riferimento, nonché dei Compliance Program Locali quali specifici presidi locali adottati al fine di evitare che attraverso la SE siano commessi i reati presupposto di cui al Decreto 231 nell'interesse e/o vantaggio della SE o del Gruppo Terna, nonché delle procedure e delle Linee Guida valevoli per il Gruppo Terna;
- qualora venga a conoscenza di eventi o informazioni che ritiene essere di interesse di una società del Gruppo Terna, provvedere a informarne l'organismo di vigilanza istituito ai sensi del Decreto 231 della società interessata di diritto italiano.

Ai fini del corretto svolgimento di tali attività, al CO viene garantita un'adeguata autonomia e indipendenza, anche rispetto al Management Locale. Il CO deve essere dotato di effettivi poteri di ispezione e controllo, nonché avere possibilità di accesso alle informazioni aziendali rilevanti.

In ogni caso, la Società Estera mette a disposizione del proprio CO ogni risorsa che dovesse rendersi necessaria o opportuna per l'efficace espletamento delle funzioni di vigilanza, compreso il supporto di professionisti esterni individuati dal CO medesimo per valutazioni tecniche di particolare complessità. A tal fine la Società Estera attribuisce al CO risorse finanziarie (budget) e personale sufficienti per lo svolgimento della propria attività e atti a garantire l'efficace implementazione del GCP.

Con riferimento ai flussi informativi nei confronti del CO previsti nel presente paragrafo, si rimanda all'individuazione effettuata nell'Appendice allegata al GCP sub "Appendice B – a02LG058". Tale individuazione potrà essere ulteriormente dettagliata nell'ambito di ciascun Allegato Paese, in ragione delle peculiarità organizzative e dell'attività della società stessa.

Il Local Assistant (quale eventuale presidio locale e per le specifiche competenze connesse all'area di appartenenza geografica) e il Technical Assistant hanno il compito di supportare il CO nelle attività di:

- organizzazione, gestione e verbalizzazione delle riunioni;
- gestione dei flussi informativi;
- erogazione dei corsi di formazione;
- gestione delle attività di informazione;
- elaborazione del piano di verifiche relativo alle aree a rischio;
- ogni altra attività che si dovesse rendere necessaria.

7. RELAZIONI CON ENTI PUBBLICI E FUNZIONARI PUBBLICI

I Principi di Comportamento di cui al presente paragrafo, relativi alle relazioni con gli enti pubblici e funzionari pubblici, costituiscono uno dei principali pilastri richiamati dal DOJ, data la rilevanza nel contesto internazionale della corruzione dei pubblici ufficiali, caposaldo delle principali normative (quali FCPA e UK Bribery Act).

Tali Principi di Comportamento devono intendersi applicabili in tutti i rapporti con detti soggetti e trasversalmente anche ai successivi Processi disciplinati nei paragrafi da 8 a 16.

Per ente pubblico o “**Pubblica Amministrazione**” (“**P.A.**” o “**ente pubblico**”) si intende ciascuno degli enti o apparati che concorrono all’esercizio delle funzioni legislativa, amministrativa o giudiziaria di un singolo stato, ivi compresi gli enti governativi.

Per funzionario pubblico (“**Funzionario Pubblico**”) si intende, ai fini del presente documento, (a) qualunque funzionario, eletto o nominato che esercita una pubblica funzione legislativa, amministrativa o giudiziaria; (b) qualunque persona che svolge funzioni pubbliche in qualsiasi ramo del governo nazionale, regionale o comunale o che esercita una funzione pubblica per qualsiasi agenzia o impresa pubblica, come i funzionari che esercitano funzioni pubbliche in imprese statali.

Per ciascuna Società Estera, le definizioni che precedono devono essere utilizzate tenendo conto della legislazione locale applicabile, così come i Reati astrattamente configurabili di seguito rappresentati.

POSSIBILI AREE A RISCHIO

- (i) negoziazione e gestione dei contratti conclusi con Pubbliche Amministrazioni;
- (ii) partecipazione a gare pubbliche;
- (iii) gestione delle relazioni - diverse dalle relazioni contrattuali - con enti pubblici (ad esempio con riferimento a quanto richiesto in materia di salute, sicurezza e ambiente, gestione del personale, pagamento delle imposte, pratiche doganali);
- (iv) gestione delle controversie (processi, arbitrati, procedimenti extragiudiziali);
- (v) selezione di partner, intermediari e consulenti nonché negoziazione e gestione dei relativi contratti;
- (vi) gestione dei flussi finanziari;
- (vii) l'erogazione di Facilitating Payments e contributi politici;
- (viii) l'esercizio della delega in materia di espropri;
- (ix) gestione delle iniziative no profit, corporate giving (incluse liberalità e sponsorizzazioni);
- (x) gestione degli omaggi e delle spese di intrattenimento e di ospitalità;

- (xi) selezione e assunzione del personale;
- (xii) partecipazioni a ispezioni, indagini, accessi e verifiche espletate da Funzionari Pubblici;
- (xiii) gestione di finanziamenti pubblici ricevuti e sovvenzioni o garanzie ottenute;
- (xiv) espletamento di procedure per l'ottenimento di provvedimenti autorizzativi da parte delle Pubbliche Amministrazioni;
- (xv) invio di flussi informatici verso le Pubbliche Amministrazioni.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Reati societari
- Reati informatici
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Criminalità organizzata anche a carattere transnazionale
- Reati tributari

PRINCIPI DI COMPORTAMENTO

Nella conduzione di attività con Pubbliche Amministrazioni e/o Funzionari Pubblici, i Destinatari devono agire con integrità e onestà e rispettando tutte le leggi e i regolamenti applicabili.

Per l'individuazione degli obblighi posti in capo ai Destinatari (in base a specifici accordi contrattuali) al fine di prevenire la commissione di reati di tipo corruttivo si fa rinvio alle Linee Guida Anticorruzione (LG059) richiamate al par. 5.1.

Le Società Estere dovranno garantire:

- la tracciabilità di qualsiasi relazione, comunicazione e rapporto rilevante con la Pubblica Amministrazione (ad esempio procedimenti amministrativi volti ad ottenere un'autorizzazione, una licenza o atto simile, *joint venture* con enti pubblici, ecc.);
- il coinvolgimento di almeno due soggetti autorizzati nella gestione delle relazioni con la Pubblica Amministrazione;
- l'effettuazione di **assunzioni di personale** esclusivamente in base a necessità aziendali reali e dimostrabili, avvalendosi di un processo di selezione che coinvolga almeno due funzioni e che si basi su criteri di oggettività, competenza e professionalità, evitando qualsiasi favoritismo o conflitto di interessi o qualsiasi azione che si concretizzi in favoritismi, nepotismi o forme clientelari idonee ad influenzare

l'indipendenza di un Funzionario Pubblico o ad indurlo ad assicurare un qualsiasi vantaggio per la Società Estera o per il Gruppo Terna;

- la formalizzazione di eventuali accordi con i Funzionari Pubblici e P.A. (in forma scritta o contratti digitali).

Inoltre, i Destinatari, nell'ambito della relazione con le Pubbliche Amministrazioni, non devono in alcun modo:

- a) inviare documenti falsi o artefatti, in tutto o in parte, durante la partecipazione a gare pubbliche;
- b) indurre in qualsiasi forma la Pubblica Amministrazione a effettuare una valutazione erronea durante l'esame di **richieste di autorizzazione**, licenze, nulla osta, concessioni, ecc.;
- c) omettere informazioni dovute al fine di permettere ad una delle società del Gruppo Terna di ottenere un vantaggio a proprio favore in una qualsiasi delle circostanze di cui alle lettere a) e b) sopra indicate;
- d) avere comportamenti finalizzati a ottenere da una Pubblica Amministrazione qualsiasi tipo di sovvenzione, **finanziamento pubblico**, prestito agevolato o altre erogazioni dello stesso tipo, mediante dichiarazioni e/o documenti artefatti o falsi o omissione di informazioni pertinenti o, più in generale, per mezzo di artificio o di inganno, volti a portare in errore l'istituzione;
- e) utilizzare i fondi ricevuti da Pubbliche Amministrazioni per fini diversi da quelli per i quali sono stati concessi.

Le Società Estere devono, inoltre, garantire:

- che tutte le dichiarazioni rilasciate alle Pubbliche Amministrazioni nazionali o internazionali (ad es. per ottenere fondi, sovvenzioni o prestiti) includano solo dati corretti e siano sottoscritte da soggetti autorizzati e che tali fondi, sovvenzioni o prestiti siano adeguatamente contabilizzati;
- una corretta separazione dei compiti, assicurando che le fasi di richiesta, di gestione e di segnalazione in relazione ai procedimenti pubblici ai fini dell'ottenimento di fondi, sovvenzioni o prestiti pubblici siano gestiti da Esponenti Aziendali diversi all'interno dell'organizzazione;
- il coinvolgimento delle funzioni competenti nelle attività di raccolta e di analisi delle informazioni necessarie ai fini dell'espletamento di attività di rendicontazione;
- l'approvazione da parte di adeguati livelli gerarchici della documentazione e della successiva attività di rendicontazione da presentare in relazione alla richiesta di sovvenzioni, prestiti e garanzie.

In relazione ai **facilitating payments**, cioè ai pagamenti fatti allo scopo di accelerare o garantire l'effettuazione di un'attività nell'esercizio di una funzione pubblica considerata di routine (per esempio, concessione di un permesso di soggiorno, concessione di un servizio di protezione da parte delle forze di polizia, organizzazione di un'attività ispettiva, concessione di una licenza commerciale, formalità connesse a operazioni di carico e scarico di merce) ("**Facilitating Payments**") e ai contributi politici, le SE garantiscono:

- che sia vietato ogni tipo di Facilitating Payments da parte degli Esponenti Aziendali e degli Altri Destinatari;

- che sia vietato ogni tipo di contributo politico a partiti o qualunque forma di sostegno a campagne politiche per conto della Società Estera o una qualunque società del Gruppo Terna. Tali contributi politici o sostegni possono includere, senza limitazioni:
 - a) danaro;
 - b) beni diversi dal danaro (come, ad esempio attrezzature prestate o donate, servizi di tecnologia gratuiti, la messa a disposizione di risorse umane); e/o
 - c) l'utilizzo di risorse societarie (come ad esempio: strutture, posta elettronica, uffici).

Tale regola non vieta all'Esponente Aziendale di esercitare il suo diritto di partecipare ad attività politiche a livello inequivocabilmente personale.

Con riferimento a eventuali altre Aree a Rischio non individuate nel presente paragrafo, si deve fare riferimento ai Principi di Comportamento individuati nei Processi indicati nel prosieguo e nelle Linee Guida Anticorruzione (LG059) richiamate al par 5.1.

8. RELAZIONI ISTITUZIONALI E GESTIONE DELLE ATTIVITÀ DI CORPORATE GIVING, INCLUSE LIBERALITÀ E SPONSORIZZAZIONI

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo di relazioni istituzionali, gestione del corporate giving, ivi incluse liberalità e sponsorizzazioni.

POSSIBILI AREE DI RISCHIO

- (i) Gestione dei rapporti che i Destinatari intrattengono con rappresentanti nazionali o internazionali nell'ambito di attività di monitoraggio e analisi dell'environment politico e istituzionale;
- (ii) Attività di corporate giving volte in favore di Funzionari Pubblici, Pubblica Amministrazione, società scientifiche, fondazioni e associazioni e, più in generale, anche di soggetti privati, quali sponsorizzazioni, liberalità in denaro, liberalità in natura (cessioni a titolo gratuito o messa a disposizione di terzi di asset, know how o servizi aziendali), nonché programmi di volontariato.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Reati societari
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Criminalità organizzata anche a carattere transnazionale
- Reati tributari

PRINCIPI DI COMPORAMENTO

Con riferimento all'area riguardante le **relazioni istituzionali**, in ogni SE è previsto per i Destinatari il divieto di:

- effettuare elargizioni in denaro di propria iniziativa o a seguito di sollecitazione nei confronti di Funzionari Pubblici al fine di far ottenere un vantaggio alla Società Estera o a una qualunque società del Gruppo Terna;
- presentare documentazione che contenga dati, informazioni non veritiere e/o ometta dati, informazioni, al fine di agevolare l'ottenimento di autorizzazioni/titoli in favore della Società.

Nell'ambito delle attività di **corporate giving**, in ogni SE ai Destinatari è fatto divieto di distribuire e/o ricevere omaggi e regali o altri vantaggi di qualsiasi natura al di fuori di quanto previsto dalle policy aziendali. In

particolare, è vietata qualsiasi liberalità - effettuata di propria iniziativa o a seguito di sollecitazione - a Funzionari Pubblici (anche in quei Paesi in cui l'elargizione di doni rappresenta una prassi diffusa) o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un vantaggio per qualsiasi Società Estera o di qualunque società del Gruppo Terna.

Le liberalità consentite dalle policy aziendali si devono caratterizzare sempre per l'esiguità del loro valore o perché volte a promuovere iniziative di carattere sociale, ambientale, umanitario e/o culturale ovvero la brand image del Gruppo Terna. Le regalie offerte e ricevute devono essere documentate in modo adeguato secondo quanto previsto dalle procedure aziendali.

Inoltre, le attività di corporate giving:

- (i) devono essere effettuate coerentemente con i principi del Codice Etico e le procedure aziendali applicabili in materia, tra cui la Politica di Corporate Giving (LG024) richiamata al par 5.1 e nei limiti del budget approvato;
- (ii) devono essere effettuate solo in favore di enti/soggetti affidabili e ben noti per integrità e correttezza professionale. A tal fine, gli Esponenti Aziendali devono svolgere verifiche preventive circa l'onorabilità dei soggetti beneficiari dell'attività di corporate giving;
- (iii) devono essere approvate secondo adeguati livelli autorizzativi e la relativa richiesta deve includere:
(a) un'adeguata descrizione circa la natura e la finalità del singolo contributo/sponsorizzazione, (b) una Due Diligence sul beneficiario e (c) la verifica sulla legittimità del contributo o sponsorizzazione, in base alle leggi applicabili;
- (iv) devono essere formalizzate in appositi accordi scritti/lettera che (i) definiscano chiaramente l'oggetto e le finalità per le quali il contributo può essere utilizzato, (ii) prevedano, ove applicabili, controlli sull'utilizzo del contributo erogato in conformità a quanto previsto dall'accordo e (iii) contengano apposite previsioni volte a garantire il rispetto delle leggi applicabili.

Gli Esponenti Aziendali sono tenuti a:

- mantenere la tracciabilità dei processi autorizzativi dell'attività di corporate giving, garantendo la collegialità delle decisioni in merito;
- effettuare i pagamenti al beneficiario esclusivamente su un conto a questo intestato;
- verificare che i fondi versati siano stati utilizzati per gli scopi previsti;
- verificare ex post l'effettività della controprestazione nell'ambito delle attività di sponsorizzazione;
- informare con periodicità almeno annuale il CO delle attività di corporate giving, liberalità, sponsorizzazioni svolte nel corso del periodo di riferimento.

9. ATTIVITÀ COMMERCIALI E RELAZIONI CON I CLIENTI

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo commerciale e alle relazioni con i clienti.

POSSIBILI AREE DI RISCHIO

- (i) Negoziazione e gestione dei contratti conclusi con qualsiasi soggetto (pubblico o privato)
- (ii) Partecipazione a procedure di gara o di negoziazione diretta indette da enti pubblici e privati per l'assegnazione di commesse (di appalto, di fornitura o di servizi), di concessioni, di partnership, di asset (complessi aziendali, partecipazioni, ecc.)
- (iii) Rapporti con business partner (inclusi partner di joint venture, agenti e intermediari) e gestione dei rapporti di partnership
- (iv) Operazioni finanziarie o commerciali che coinvolgano società del Gruppo Terna concluse con persone fisiche e giuridiche residenti (o con società controllate direttamente o indirettamente da queste) nei Paesi a rischio individuati in Liste di Paesi e/o in Liste di persone fisiche o giuridiche indicate, altresì, dal FATF-GAFI che coordina la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Reati societari
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Criminalità organizzata anche a carattere transnazionale
- Reati contro la personalità individuale
- Reati tributari

PRINCIPI DI COMPORTAMENTO

I rapporti con i clienti o i potenziali clienti nonché con i partner commerciali devono essere gestiti in modo corretto, trasparente, equo e cooperativo.

In ogni SE è previsto per i Destinatari il divieto di:

- effettuare elargizioni in denaro di propria iniziativa o a seguito di sollecitazione nei confronti di Funzionari Pubblici;

- presentare documentazione che contenga dati, informazioni rilevanti non veritiere e/o ometta dati, informazioni, al fine di far ottenere alla società l'aggiudicazione della gara/commissa;
- affidare lavori, servizi e forniture e disporre i relativi pagamenti senza rispettare i requisiti di forma e tracciabilità richiesti dalle normative vigenti in materia di contratti pubblici e di tracciabilità dei flussi finanziari, ove applicabili;
- effettuare pagamenti o riconoscere compensi in favore di soggetti terzi, senza adeguata giustificazione contrattuale o comunque non adeguatamente documentati, giustificati e autorizzati.

Le Società Estere dovranno garantire:

- il rispetto delle procedure adottate dal Gruppo Terna applicabili al processo commerciale (quali le linee guida e/o istruzioni di indirizzo emanate per il Gruppo Terna e le *policy* locali adottate individualmente da ciascuna Società Estera o dalla relativa controllante, ove applicabili, per la gestione delle attività di export controls (Trade Compliance Policy - LG061).

Inoltre, nell'ambito del processo commerciale, è fatto obbligo di:

- svolgere una Due Diligence nei confronti della controparte in linea con quanto previsto dal par. 5.3;
- improntare tutti i rapporti con le controparti ai principi della trasparenza e dell'integrità e prevedere prestazioni e compensi in linea con le prassi di mercato, accertando che non vi siano aspetti che possano favorire la commissione di Reati in Italia o all'estero;
- nel caso in cui risultino coinvolti nelle operazioni commerciali, in sede di Due Diligence o nella successiva fase di monitoraggio del rapporto commerciale, soggetti i cui nominativi siano contenuti nelle Liste, o i quali siano notoriamente controllati da soggetti contenuti nelle Liste medesime, garantire il rispetto di quanto disciplinato dalla Linea Guida Due Diligence su Terze Parti (LG070) e dalla Trade Compliance Policy (LG061);
- verificare che la documentazione e le comunicazioni formali prodotte nel corso di svolgimento della procedura di gara/o attribuzione della commessa siano gestiti e siglati solo dai soggetti preventivamente identificati ed autorizzati dalla SE;
- garantire la tracciabilità delle fasi di formazione delle decisioni e i livelli autorizzativi in modo da essere sempre ricostruibili attraverso gli atti e la documentazione interna;
- definire tutte le partnership e le attività di vendita attraverso rapporti contrattuali, firmati sulla base del sistema di poteri e deleghe in vigore in azienda e comprensivi di clausole in materia di compliance (corporate liability o GCP, Codice Etico, Trade Compliance e procedure in ambito export controls, anticorruzione);
- con particolare riferimento ai contratti con **agenti e intermediari**, prevedere che questi dovranno anche (i) descrivere chiaramente i servizi che verranno prestati; (ii) definire la natura delle commissioni/provvigioni (fisse, variabili, success fees, ecc.) e il loro ammontare in linea con gli standard di mercato (iii) stabilire i target da raggiungere;

- archiviare tutta la documentazione a supporto delle singole attività.

I principi del libero mercato rientrano tra i valori fondamentali del Gruppo Terna e ne ispirano l'organizzazione e le attività. Pertanto, i comportamenti sono adottati nel rispetto delle regole della leale competizione.

10. OPERAZIONI STRAORDINARIE (M&A, CESSIONI, ECC.) E GESTIONE DEI FLUSSI FINANZIARI

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo relativo alle operazioni straordinarie (M&A, cessioni, ecc.) e alla gestione dei flussi finanziari.

POSSIBILI AREE DI RISCHIO

- (i) Compimento di operazioni straordinarie (acquisizioni e cessioni di partecipazioni societarie, fusioni, scissioni, acquisizioni, cessioni e affitti di ramo d'azienda, ecc.)
- (ii) Gestione delle attività di integrazione post-acquisizione
- (iii) Gestione dei flussi finanziari, per tali intendendosi tutte quelle attività o rapporti che comportano un pagamento o un incasso da o verso la SE, inclusi i cd. rapporti infragruppo.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Reati societari
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Reati di criminalità organizzata anche a carattere transnazionale
- Reati tributari
- Reati di market abuse

PRINCIPI DI COMPORTAMENTO

(I) Operazioni straordinarie e fase post-acquisition

Nello svolgimento delle operazioni di M&A devono essere rispettati i seguenti standard:

- svolgimento di una Due Diligence sulla società target (compresi i rapporti contrattuali in essere della società target) e sulle potenziali controparti che tenga in particolare considerazione il suo profilo etico-reputazionale e, in caso di società, la storia d'impresa e il background della società;
- svolgimento di verifiche circa le implicazioni fiscali derivanti dalle operazioni che si intendono realizzare;
- formalizzazione delle operazioni in contratti scritti inserendo le clausole necessarie ad assicurare il rispetto delle leggi applicabili e delle procedure adottate (corporate liability o GCP, Codice Etico, Trade Compliance e procedure in ambito export controls, anticorruzione) dal Gruppo Terna;
- corretta valutazione, contabilizzazione delle acquisizioni e/o operazioni societarie;
- una volta acquisita una società, dovranno essere poste in essere azioni volte:

- all'adozione del GCP e pertanto anche al recepimento ed eventuale necessario adeguamento previsto delle procedure vigenti e applicabili nel Gruppo Terna quali quelle di cui al par. 5.1 lett. i) e ii) del presente GCP nelle nuove *legal entities* derivanti dall'acquisizione;
- all'adozione da parte di queste di presidi di controllo il più possibile in linea con quelli di cui ai par. 5.2 e 5.3 del presente GCP;
- alla formazione e/o informazione del relativo personale per l'integrazione.

(II) Gestione dei Flussi Finanziari

La gestione dei pagamenti e degli incassi deve avvenire nel rispetto dei seguenti standard minimi:

- i pagamenti devono essere effettuati/ricevuti solo in conformità alla normativa di volta in volta applicabile, alle previsioni contrattuali da cui originano, ai principi contabili in materia di flussi finanziari applicabili;
- tutti i pagamenti devono essere autorizzati nel rispetto delle deleghe e procure rilasciate;
- per quanto possibile, è necessario garantire la segregazione di ruoli e responsabilità dei soggetti coinvolti nel processo dei pagamenti (es. gestione anagrafiche fornitori, benestari, esecuzione materiale del pagamento, etc);
- in ogni caso, le SE non accetteranno e non effettueranno pagamenti:
 - (i) a/da un soggetto diverso dalla controparte contrattuale o (ii) da/a conti correnti diversi da quelli previsti contrattualmente o (iii) da/a un Paese diverso da quello delle parti o di esecuzione del contratto, senza adeguata giustificazione contrattuale o comunque non adeguatamente documentati, giustificati e autorizzati.
 - da/su conti cifrati o in contanti o strumenti assimilabili⁶;
 - nel caso in cui sia indicato/delegato/nominato un soggetto terzo come *payer*, dovrà essere richiesta la documentazione in merito alla formale individuazione come *payer* di quel soggetto e le motivazioni sottese a tale interposizione o triangolazione⁷;
- è fatto divieto di disporre pagamenti o incassare denaro verso/da Paesi inseriti nelle Liste internazionali senza adeguata documentazione comprovante la reale e specifica necessità;
- deve essere rivolta sempre particolare attenzione ed effettuati gli opportuni controlli relativamente (i) alla sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio riciclaggio e finanziamento del terrorismo, ecc.) ed eventuali schemi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie; (ii) alle transazioni su/da conti correnti accessi presso Paesi a rischio riciclaggio o a finanziamento del terrorismo (di cui alle Liste ad es. GAFI/FATF);

⁶ La gestione delle transazioni avviene nel rispetto del divieto di utilizzo del contante o altro strumento finanziario al portatore, per qualunque operazione di incasso, pagamento, trasferimento fondi, impiego o altro utilizzo di disponibilità finanziarie; nonché nel rispetto del divieto di utilizzo di conti correnti o libretti di risparmio in forma anonima o con intestazione fittizia. Eventuali eccezioni all'utilizzo di denaro contante o altro strumento finanziario al portatore devono essere espressamente previste dalle procedure della società o del Gruppo Terna applicabili e devono essere scrupolosamente rispettati i limiti all'utilizzo dei contanti previsti dalle normative di riferimento.

⁷ A titolo esemplificativo, potranno essere richiesti: (i) un certificato della camera di commercio relativo all'ente pagante; (ii) un documento d'identità del relativo rappresentante legale; (iii) una procura che attesti la delega di pagamento conferita a tale ente pagante; (iv) qualsiasi documento che fornisca il motivo di tale pagamento effettuato dall'ente pagante).

- i controlli sui pagamenti devono contemplare verifiche di coerenza e corrispondenza tra la titolarità del rapporto contrattuale (i.e. il soggetto creditore del pagamento) e l'intestazione del conto su cui effettuare la transazione;
- tutte le operazioni di pagamento/incassi devono essere effettuate con operatori finanziari abilitati che hanno adottato presidi volti a prevenire il fenomeno del riciclaggio;
- in ogni caso, non possono essere effettuati pagamenti in favore di soggetti che non siano chiaramente identificabili;
- in fase di esecuzione dei contratti dai quali derivino flussi finanziari, viene previsto un costante monitoraggio delle transazioni finanziarie effettuate/ricevute. Con particolare riferimento alle operazioni infragruppo, deve essere garantito che le prestazioni rese da/nei confronti delle società del Gruppo Terna siano a condizioni di mercato e regolate da appositi contratti.

Tali Principi di Comportamento devono intendersi applicabili a tutti gli incassi e pagamenti e trasversalmente anche nell'ambito di tutti i Processi disciplinati dal GCP nei paragrafi da 7 a 16.

11. PROCUREMENT

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo di procurement.

POSSIBILI AREE DI RISCHIO

- (i) Gestione delle procedure di gara/acquisto;
- (ii) Affidamento di incarichi professionali e di consulenze.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti dei Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Reati societari
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Reati di criminalità organizzata anche a carattere transnazionale
- Reati contro la personalità individuale
- Reati in violazione del diritto di autore
- Reati tributari

PRINCIPI DI COMPORAMENTO

Le SE devono garantire che:

- tutti i rapporti con i fornitori siano improntati ai principi della trasparenza e dell'integrità e dell'assenza di conflitti di interessi;
- tutti i rapporti con i fornitori prevedano prestazioni e corrispettivi in linea con le prassi di mercato, accertando l'assenza di termini e modalità che favoriscano la commissione di reati;
- sia assicurata una Due Diligence sui fornitori che tenga in considerazione la loro attendibilità commerciale, reputazionale e professionale;
- le relazioni con i fornitori siano formalizzate in contratti scritti che individuino, fra gli altri aspetti:
 - l'oggetto dell'incarico/prestazione e i soggetti che svolgeranno l'incarico o effettueranno la prestazione;
 - l'importo/corrispettivo pattuito e la relativa valuta;
 - il conto corrente presso il quale/dal quale verrà effettuato il pagamento oltre ai termini per la fatturazione (o le modalità di incasso/pagamento) e le condizioni di pagamento;
 - l'impegno del fornitore/consulente a rispettare le leggi nazionali della SE applicabili e le procedure della Società Estera;

- prevedere una clausola per cui i fornitori si impegnino nello svolgimento delle attività, al rispetto dei principi del Codice Etico, anche con riguardo all'impegno a non effettuare liberalità che superino il modico valore e che possano essere interpretate come eccedenti le normali pratiche commerciali o di cortesia, o comunque rivolte ad acquisire trattamenti di favore nella conduzione delle attività medesime;
- prevedere, nei contratti con i Terzi dai quali potrebbe sorgere responsabilità della Società ai sensi della normativa ambientale e della sicurezza sul lavoro, specifiche penali applicabili in caso di violazione, da parte di un fornitore o di un suo subappaltatore, di qualsiasi normativa, internazionale o locale, che tratti la tematica in parola;
- nel corso di esecuzione del contratto:
 - siano previste le seguenti misure di controllo: (i) aggiornamento periodico della Due Diligence con una frequenza da determinarsi in base al livello di rischio della controparte e/o in caso di revisione/modifica/rinegoziazione del contratto; (ii) attività di monitoraggio della corretta esecuzione del contratto;
 - siano rifiutate richieste di controparte relative ad aumenti ingiustificati del corrispettivo o sconti, per questioni non inerenti a modifiche delle condizioni contrattuali, anticipi non previsti a livello contrattuale;
 - siano riconosciuti corrispettivi solo previa verifica della corrispondenza tra prestazione ricevuta e previsioni contrattuali;
- i risultati delle attività di selezione, Due Diligence, la documentazione contabile e quella relativa agli accordi contrattuali con il fornitore devono essere registrati e archiviati;
- venga verificata la validità dei pagamenti, controllando che chi riceve o versa importi sia il soggetto indicato nella documentazione contrattuale.

12. HUMAN RESOURCES

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Human Resources.

POSSIBILI AREE DI RISCHIO

- (i) Selezione e assunzione del personale
- (ii) Incentivazione del personale e salary review
- (iii) Gestione della formazione del personale e gestione dei rapporti con la P.A. per l'ottenimento di contributi/finanziamenti in materia di formazione
- (iv) Amministrazione del personale
- (v) Gestione delle note spese
- (vi) Gestione dei rapporti con le Organizzazioni Sindacali

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione fra privati
- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Criminalità organizzata anche a carattere internazionale
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Reati di personalità individuale
- Reati tributari

PRINCIPI DI COMPORTAMENTO

Nell'ambito della SE deve essere assicurato il rispetto e l'osservanza di tutte le leggi e i regolamenti locali e le procedure della SE in materia di assunzione e gestione delle risorse umane.

In particolare, in ogni SE è previsto quanto segue:

- il divieto di assumere o effettuare promesse di **assunzione di personale** se non in base a necessità aziendali reali e dimostrabili, avvalendosi di un processo di **selezione del personale** che coinvolga almeno due funzioni e che si basi su criteri di oggettività, competenza e professionalità, evitando qualsiasi favoritismo o conflitto di interessi, o qualsiasi azione che si concretizzi in favoritismi, nepotismi o forme clientelari idonee a influenzare l'indipendenza di un Funzionario Pubblico o ad indurlo ad assicurare un qualsiasi vantaggio per la Società Estera o per il Gruppo Terna;
- il divieto di **incentivare** mediante promozioni, premi in denaro o altra forma taluni dipendenti, se non sulla base di criteri di oggettività, competenza e professionalità;

- l'adozione di piani di **incentivazione** del management in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino su un risultato ben determinato e misurabile;
- la chiara segregazione delle funzioni coinvolte nelle attività di selezione e assunzione del personale;
- la formalizzazione e la conservazione negli archivi aziendali della valutazione dei candidati;
- le decisioni riguardanti la **salary review del personale**, l'avanzamento di carriera e l'aumento della retribuzione, sulla base del merito, delle capacità, della professionalità e dell'esperienza;
- la pianificazione ed erogazione della **formazione** differenziata a seconda del livello e delle mansioni svolte dai singoli dipendenti;
- che la documentazione aziendale in materia di etica e compliance, incluso il GCP, sia resa disponibile agli Esponenti Aziendali mediante pubblicazione sulla rete intranet aziendale o portali della Capogruppo o mediante invio via mail o altre modalità di condivisione di documenti aziendali e che ad ogni neo-assunto sia consegnata (o indicata e messa a disposizione con le modalità sopra individuate) la documentazione in materia di compliance di riferimento per la SE;
- che al personale neo-assunto sia fatta firmare apposita dichiarazione di presa visione e di impegno al rispetto dei principi contenuti nella documentazione relativa all'etica e alla compliance.
- con riferimento all'**amministrazione del personale**, la corretta predisposizione, registrazione ed archiviazione di tutta la documentazione relativa alla gestione amministrativa del rapporto contrattuale nonché dei trattamenti previdenziali, assicurativi e fiscali del personale, al fine di consentire la ricostruzione delle diverse fasi del processo;
- con riferimento ai rimborsi delle **note spese**, la richiesta dalla funzione competente, prima della liquidazione di tali spese, di appropriata documentazione che includa anche l'originale delle ricevute comprovanti tali esborsi. Tali rimborsi dovranno poi essere accuratamente riportati nei registri contabili delle Società Estere;
- che i dipendenti siano tenuti a segnalare qualsiasi situazione che indichi o suggerisca un potenziale conflitto di interessi nell'ambito delle loro attività e qualsiasi potenziale violazione delle suddette politiche e procedure;
- che nella gestione dei **rapporti con le organizzazioni sindacali**, sia prevista la formalizzazione degli incontri e, almeno per i casi più significativi, delle riunioni e/o delle comunicazioni che intercorrono con tali soggetti, nonché l'adeguata archiviazione della documentazione rilevante.

13. AMMINISTRAZIONE, BILANCIO E FISCALE

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Amministrazione, Bilancio e Fiscale.

POSSIBILI AREE DI RISCHIO

- (i) Redazione di documenti da condividere con gli azionisti o con il pubblico (ad es. bilanci, relazioni finanziarie periodiche) che riguardino la situazione economico-patrimoniale o finanziaria di una Società Estera anche qualora questi documenti siano diversi da quelli predisposti nel contesto dell'informativa finanziaria periodica;
- (ii) Gestione delle relazioni con i revisori esterni;
- (iii) Gestione della contabilità (attiva e passiva);
- (iv) Gestione dei rapporti infragruppo, con specifico riferimento alla gestione dei contratti intercompany;
- (v) Gestione degli adempimenti fiscali.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione fra privati
- Corruzione nei confronti dei Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Reati societari
- Criminalità organizzata anche a carattere transnazionale
- Riciclaggio, reati connessi e finanziamento al terrorismo
- Reati tributari
- Reati di market abuse

PRINCIPI DI COMPORAMENTO

Le Società Estere sono tenute a gestire la contabilità in maniera veritiera e corretta.

Il personale operante nell'ambito della **gestione della contabilità** deve svolgere accuratamente le proprie mansioni al fine di assicurare che:

- a) i dati e le informazioni utilizzate per la preparazione delle relazioni finanziarie periodiche siano accurati e diligentemente verificati;
- b) tutte le voci di bilancio, la cui determinazione e quantificazione sia suscettibile di valutazioni discrezionali, siano quanto più possibile oggettive e supportate da adeguata documentazione;

- c) siano previste verifiche volte ad accertare il corretto svolgimento dell'attività di chiusura dei documenti economico/finanziari e, qualora si riscontrino anomalie nelle contabilizzazioni eseguite, prevedere l'obbligo di segnalazione delle stesse alle strutture competenti;
- d) tutte le operazioni siano eseguite nel rispetto del sistema autorizzativo adottato;
- e) le fatture e l'ulteriore documentazione rilevante in relazione alle operazioni compiute siano accuratamente verificate, registrate e archiviate;
- f) le operazioni siano registrate in modo da consentire la predisposizione del bilancio in conformità ai principi contabili applicabili o qualsiasi altro criterio applicabile;
- g) l'accesso al relativo archivio documentale sia permesso solo ai soggetti autorizzati in base al sistema autorizzativo in vigore.

Inoltre, alle Società Estere è vietato porre in essere qualsiasi comportamento che impedisca ovvero ostacoli le **attività di controllo, di vigilanza e di revisione legale** da parte dei revisori esterni attraverso l'occultamento della documentazione o l'uso di altri mezzi fraudolenti.

In ogni SE è previsto il divieto di:

- gestire la **fiscaltà** in maniera difforme rispetto alla normativa vigente;
- indicare o inviare per l'elaborazione o l'inserimento nelle **comunicazioni**, dati falsi, artefatti, incompleti o comunque non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria;
- rappresentare in **contabilità** - o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali - dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria;
- registrare in contabilità operazioni a valori non corretti rispetto alla documentazione di riferimento, oppure a fronte di transazioni inesistenti in tutto o in parte, o senza un'adeguata documentazione di supporto che ne consenta, in primis, una corretta rilevazione contabile e, successivamente, una ricostruzione accurata.

Infine, alle Società Estere è richiesto di effettuare in modo corretto, completo, appropriato e tempestivo tutte le **comunicazioni verso qualsiasi autorità finanziaria** (come previsto dalla legge applicabile locale), non impedendo alle stesse, in alcun modo, di svolgere i propri compiti anche in occasione di qualsiasi ispezione.

In relazione ai **rapporti infragruppo**, le attività devono essere disciplinate da appositi contratti di service formalizzati. Inoltre, le transazioni con le società del Gruppo Terna devono essere valutate per assicurare (a) la convenienza tecnica ed economica dell'operazione, (b) che la valutazione dell'ammontare economico delle prestazioni sia effettuata al valore di mercato effettivo e (c) che il rapporto contrattuale sia sostanzialmente conforme alle operazioni commerciali in effetti realizzate e alla loro rappresentazione contabile.

14. GESTIONE DELLE INFORMAZIONI RISERVATE E PRIVILEGIATE

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Gestione delle Informazioni Riservate e Privilegiate.

POSSIBILI AREE DI RISCHIO

- (i) Gestione dei rapporti ed incontri con gli investitori, con gli analisti finanziari, con i media ed in generale gestione dell'informativa pubblica;
- (ii) Gestione dei contenuti aziendali pubblicati sul sito internet aziendale e social media e organizzazione di eventi;
- (iii) Gestione delle informazioni aziendali riguardanti la SE o altre società del Gruppo Terna, comprese le Informazioni Privilegiate e/o potenzialmente privilegiate, che non siano di pubblico dominio e che per oggetto o per altre caratteristiche abbiano comunque carattere riservato verso soggetti non tenuti ad obblighi di riservatezza in base alla normativa vigente o per accordi contrattuali individuate dalla procedura per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate (LG005) di cui al par. 5.1 ("**Informazioni Riservate**");
- (iv) Gestione delle informazioni privilegiate e/o potenzialmente privilegiate relative a società quotate e, in particolare, a società quotate appartenenti al Gruppo Terna e ai relativi strumenti finanziari individuate dalla procedura per la gestione, il trattamento e la comunicazione delle informazioni aziendali relative a Terna S.p.A. e alle società controllate (LG005) per la tenuta e l'aggiornamento dei registri delle persone che hanno accesso a informazioni privilegiate e potenzialmente privilegiate (LG008) di cui al par. 5.1 ("**Informazioni Privilegiate**");
- (v) Ogni genere di transazione sugli strumenti finanziari in portfolio della SE.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Reati di market abuse
- Reati di Riciclaggio, reati connessi e finanziamento al terrorismo
- Reati societari
- Criminalità organizzata anche a carattere transnazionale
- Reati tributari

PRINCIPI DI COMPORTAMENTO

La gestione delle Informazioni Riservate e/o Informazioni Privilegiate è garantita nel rispetto delle procedure valedoli per il Gruppo Terna in materia di market abuse (LG005; LG008) nonché in conformità alle normative comunitarie e locali in materia.

Gli Esponenti Aziendali delle SE:

- si impegnano a non esprimere opinioni, rilasciare dichiarazioni o fornire informazioni ai media per conto della SE o di società del Gruppo Terna al di fuori dei canali e delle modalità stabilite in ambito aziendale, adottando ogni necessaria cautela affinché la relativa circolazione nel contesto aziendale possa svolgersi senza pregiudizio del carattere riservato/privilegiato/potenzialmente privilegiato delle informazioni stesse e secondo il principio del c.d. *need to know* e tenendo conto degli indirizzi di cui alle LG005 e LG008;
- si impegnano affinché l'organizzazione degli eventi aziendali dedicati agli organi di informazione sia regolata in modo tale da evitare l'offerta di doni o forme di intrattenimento che possano influenzare l'obiettività di giudizio e l'indipendenza degli organi di informazione partecipanti;
- si impegnano affinché i rapporti con agenzie di rating e società di certificazione siano limitati allo scambio di informazioni che si ritenga necessario – sulla base delle previsioni contrattuali pattuite – per l'adempimento dell'incarico, evitando qualsiasi condotta potenzialmente idonea a lederne l'indipendenza.

Per gli Esponenti Aziendali della SE è previsto il divieto di:

- servirsi di Informazioni Privilegiate per negoziare, direttamente o indirettamente, strumenti finanziari al fine di ottenere vantaggio personale o per favorire soggetti terzi o una società del Gruppo Terna;
- raccomandare o indurre qualcuno, sulla base di Informazioni Privilegiate, a porre in essere transazioni su strumenti finanziari;
- rivelare Informazioni Riservate, Informazioni Privilegiate a soggetti terzi, salvo che ciò sia richiesto da un'Autorità Pubblica o stabilito in specifici contratti in virtù dei quali la controparte sia vincolata ad utilizzare le informazioni solo per lo scopo previsto e a mantenerne la segretezza;
- diffondere informazioni false o fuorvianti (siano esse relative alla SE/società del Gruppo Terna) tramite i media, internet, o altro mezzo, al fine di alterare il prezzo di mercato di strumenti finanziari;
- compiere qualsiasi transazione su strumenti finanziari che sia contraria alla disciplina relativa ai reati di market abuse prevista dalla normativa applicabile;
- accedere abusivamente al sistema informatico o telematico aziendale al fine di alterare e/o cancellare dati o informazioni;
- inviare attraverso un sistema informatico aziendale informazioni o dati falsificati o, in qualunque modo, alterati.

15. HEALTH, SAFETY AND ENVIRONMENT (“HSE”)

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Health, Safety and Environment (“HSE”).

POSSIBILI AREE DI RISCHIO

- (i) Rispetto delle normative applicabili in tema di salute e sicurezza e ambiente e dei relativi adempimenti;
- (i) Formazione del personale in materia di salute e sicurezza e ambientale;
- (ii) Selezione dei Terzi che siano tenuti a svolgere specifiche attività che possono avere impatti sull’ambiente (ad esempio, la gestione e lo smaltimento dei rifiuti) nonché dei Terzi coinvolti nella gestione degli aspetti in materia di salute e sicurezza nei luoghi di lavoro.

REATI ASTRATTAMENTE CONFIGURABILI

- Corruzione nei confronti di Funzionari Pubblici
- Frodi contro la Pubblica Amministrazione
- Corruzione fra privati
- Criminalità organizzata anche a carattere transnazionale
- Reati ambientali
- Reati in materia di Salute e Sicurezza nei Luoghi di Lavoro
- Reati contro la personalità individuale

PRINCIPI DI COMPORTAMENTO

A) Salute e Sicurezza nei Luoghi di Lavoro

Indipendentemente dall’ampiezza della legislazione locale in materia di salute e sicurezza sul luogo di lavoro, la SE è tenuta a promuovere un’efficace cultura della protezione della sicurezza sul luogo di lavoro, favorendo la consapevolezza in merito ai rischi e alle responsabilità delle condotte dei singoli.

Le SE devono tenere in considerazione la sicurezza dei lavoratori attraverso ogni fase dell’attività e devono impegnarsi ad adottare tutte le misure considerate necessarie al fine di proteggere l’integrità fisica e morale dei suoi lavoratori.

In particolare, la SE deve:

- a. considerare il rispetto delle previsioni di legge in materia di salute e sicurezza dei lavoratori sul luogo di lavoro quale una priorità e attribuire a tal fine le risorse economiche necessarie;

- b. responsabilizzare l'organizzazione aziendale al fine di evitare che l'attività di prevenzione venga considerata di competenza esclusiva di alcuni soggetti;
- c. identificare correttamente i requisiti richiesti in materia di salute e sicurezza sui luoghi di lavoro da leggi e regolamenti locali;
- d. per quanto possibile e permesso dall'evoluzione delle migliori pratiche, valutare i rischi per i lavoratori allo scopo di proteggerli, anche adottando i materiali e l'attrezzatura più adeguati, al fine di ridurre il rischio alla radice;
- e. impegnarsi al miglioramento continuo e alla prevenzione, valutando correttamente quei rischi che non sono evitabili e mitigarli adeguatamente tramite l'implementazione di appropriate misure di sicurezza individuali e collettive (es.: fornire dispositivi di protezione individuali adeguati alle mansioni svolte; dotare l'area di lavoro di un kit di pronto soccorso);
- f. diffondere informazioni in merito alla salute e sicurezza sul luogo di lavoro, aggiornate e specifiche con riferimento alle attività esercitate, assicurando che i lavoratori siano correttamente istruiti e formati;
- g. assicurare che i lavoratori siano coinvolti periodicamente in merito ai temi relativi alla salute e sicurezza sul luogo di lavoro ed effettuare adeguate attività di monitoraggio per la gestione, rettifica, inibizione di comportamenti posti in violazione delle norme;
- h. assicurare che i piani di incentivazione del management siano adottati in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino su un risultato ben determinato e misurabile;
- i. prendere in considerazione e analizzare ogni episodio di mancato rispetto della normativa o area di miglioramento, emersa come tale a seguito dell'attività lavorativa o durante ispezioni;
- j. strutturare l'organizzazione dell'attività di lavoro al fine di proteggere l'integrità dei lavoratori, dei Terzi e della comunità nel cui ambito la SE opera.

Inoltre, con particolare riferimento alla [selezione di Terzi coinvolti nella gestione degli aspetti inerenti la salute e sicurezza nei luoghi di lavoro](#), la SE deve garantire:

- la verifica dell'idoneità tecnica-professionale del Terzo;
- la stipula di un contratto che preveda anche specifiche penali applicabili in caso di violazione, da parte di un fornitore o di un suo subappaltatore, di qualsiasi normativa, internazionale o locale, applicabile in materia di salute e sicurezza nei luoghi di lavoro;
- la gestione delle problematiche connesse a sicurezza e analisi dei rischi.

Al fine di mantenere un corretto monitoraggio delle Aree a Rischio, ciascuna SE alloca risorse organizzative, strumentali ed economiche per assicurare, da un lato, il pieno rispetto delle previsioni di legge sulla prevenzione degli incidenti sul luogo di lavoro e, dall'altro lato, il continuo miglioramento della situazione

relativa alla salute e alla sicurezza sul luogo di lavoro, anche tramite l'implementazione e l'aggiornamento delle relative misure precauzionali.

Gli Esponenti Aziendali devono cooperare al fine di garantire il pieno rispetto delle disposizioni di legge, delle procedure aziendali e di ogni altra normativa interna volta a proteggere la sicurezza e la salute dei lavoratori sul luogo di lavoro.

B) Ambiente

La SE considera il rispetto e la protezione dell'ambiente una priorità e, in particolare:

- a. diffonde nella società informazioni riguardo alla protezione dell'ambiente con riferimento alle attività esercitate, promuovendo la consapevolezza di tale tematica e assicurando che le attività vengano svolte nel rispetto della normativa applicabile;
- b. identifica correttamente i requisiti richiesti in materia ambientale da leggi e regolamenti locali e valuta i rischi ambientali connessi alle principali attività condotte;
- c. adotta strumenti adeguati al fine di impedire che le attività aziendali causino qualsivoglia forma di pregiudizio o danno all'ecosistema (es. dovuti ad una non corretta gestione dello smaltimento dei rifiuti o al mancato rispetto della fauna locale) ed effettua adeguate attività di monitoraggio per la gestione, rettifica, inibizione di comportamenti posti in violazione delle norme;
- d. assicura che i piani di incentivazione del management siano adottati in modo da garantire che gli obiettivi fissati siano tali da non determinare comportamenti abusivi e si concentrino, invece, su un risultato ben determinato e misurabile;
- e. si adopera per una gestione dei rifiuti orientata al recupero, al reimpiego e al riciclaggio dei materiali, al fine di garantire un maggior grado di protezione della salute dell'uomo e dell'ambiente.

Analogamente a quanto previsto sopra, nella selezione di Terzi coinvolti nella gestione degli aspetti ambientale, la SE deve garantire:

- la verifica dell'idoneità tecnica-professionale del Terzo;
- la stipula di un contratto che preveda anche specifiche penali applicabili in caso di violazione, da parte di un fornitore o di un suo subappaltatore, di qualsiasi normativa, internazionale o locale, applicabile in materia ambientale;
- la gestione delle problematiche connesse alle tematiche ambientali.

16. INFORMATION & COMMUNICATIONS TECHNOLOGY (“ICT”)

I Principi di Comportamento di cui al presente paragrafo si riferiscono al processo Information & Communications Technology (“ICT”).

POSSIBILI AREE DI RISCHIO

- (i) Gestione dei sistemi informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l’evoluzione della piattaforma tecnologica e applicativa IT nonché la sicurezza informatica, fisica e logica; ivi incluse:
- a. la gestione dell’attività di manutenzione dei sistemi esistenti e gestione dell’attività di elaborazione dei dati;
 - b. ogni attività aziendale compiuta utilizzando intranet, internet, il sistema di posta elettronica o ogni altro strumento informatico;
 - c. la gestione e la protezione delle postazioni di lavoro, dei computer portatili, dei telefoni cellulari e delle unità di archiviazione;
 - d. la programmazione delle misure da adottare sui sistemi telematici nonché della protezione, classificazione e trattamento delle informazioni e dei dati.

REATI ASTRATTAMENTE CONFIGURABILI

- Reati Informatici
- Corruzione nei confronti di Funzionari Pubblici
- Corruzione fra privati
- Frodi contro la Pubblica Amministrazione
- Reati societari
- Reati tributari
- Criminalità Organizzata anche a carattere transnazionale
- Reati in violazione del diritto d’autore
- Reati di market abuse

PRINCIPI DI COMPORTAMENTO

Ogni Esponente Aziendale si astiene dal commettere (e la SE assicura, tramite l’implementazione di adeguate misure organizzative, tecniche e fisiche, che siano evitate) le seguenti condotte:

- la manomissione o l’alterazione del sistema informatico e/o dei documenti informatici della SE;
- l’illegittimo accesso di soggetti terzi al sistema informatico;

- un uso improprio delle credenziali informatiche;
- l'intervenire illegalmente con qualsiasi modalità su dati, informazioni o programmi informatici;
- la condivisione non autorizzata di informazioni commerciali al di fuori dall'azienda e l'utilizzo di dispositivi personali o non autorizzati per trasmettere o archiviare informazioni o dati aziendali (es.: divulgare, cedere o condividere le proprie credenziali di accesso ai sistemi e alla rete aziendale della società o di Terzi; accedere abusivamente al sistema informatico di Terzi);
- lo sfruttamento di falle nelle misure di sicurezza del sistema informatico aziendale al fine di ottenere accesso a informazioni in assenza della dovuta autorizzazione;
- l'installazione o modificazione di software o banche dati o hardware in assenza di preventiva autorizzazione;
- l'utilizzo di software non autorizzati o di hardware che possano essere impiegati per compromettere la sicurezza di sistemi informatici (quali software per identificare le credenziali, decrittare file criptati, ecc.);
- il mascherare, oscurare o sostituire la propria identità e inviare e-mail riportanti false generalità o inviare intenzionalmente e-mail contenenti virus o altri programmi in grado di danneggiare o intercettare dati;
- l'acquistare e/o utilizzare prodotti tutelati da diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- l'accedere abusivamente al sito internet della SE al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettere dati o contenuti multimediali (immagini, infografica, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;
- il lasciare gli strumenti informatici in dotazione, come personal computer o Smartphone, incustoditi o sbloccati quando non in uso;
- l'apertura di e-mail o allegati sospetti ricevuti via posta elettronica o altro mezzo di comunicazione. In tal caso dovrà segnalare alla struttura di cybersecurity di riferimento qualsiasi comunicazione sospetta.

Le Società Estere dovranno garantire, inoltre, la predisposizione di copie di backup dei dati informatici presenti sui server aziendali nel rispetto dei criteri di riservatezza delle informazioni previsti dalla normativa anche aziendale di riferimento.

Le SE, al fine di individuare comportamenti insoliti e potenziali vulnerabilità e carenze nei sistemi aziendali, assicurano un monitoraggio periodico delle attività svolte dal personale sul sistema informatico aziendale, nel rispetto della legislazione locale applicabile.

Inoltre, le SE promuovono, anche tramite specifiche sessioni formative, laddove necessarie, la consapevolezza del personale circa l'importanza di un corretto e adeguato utilizzo degli strumenti informatici in loro possesso.

17. FORMAZIONE PER GLI ESPONENTI AZIENDALI E INFORMAZIONE DEI DESTINATARI

La struttura People Organization and Change di TERNA (“**POC**”) deve organizzare periodicamente sessioni di formazione obbligatorie per tutti gli Esponenti Aziendali (ivi incluso il personale di nuova assunzione) sui contenuti del Global Compliance Program.

La formazione dovrà basarsi sulle normative e best practice applicabili e sull’importanza del rispetto del GCP. In tal modo, gli Esponenti Aziendali saranno messi nelle condizioni di comprendere chiaramente ed essere consapevoli dei diversi Reati, dei rischi, delle relative responsabilità personali e aziendali e delle azioni da porre in essere per prevenire la commissione di attività illecite.

POC è responsabile di:

- (i) pianificare ed erogare la formazione con il supporto di PCR;
- (ii) assicurare che ogni Esponente Aziendale partecipi regolarmente agli incontri di formazione;
- (iii) raccogliere le registrazioni delle partecipazioni, le copie del materiale utilizzato e le date della formazione.

Ogni Società Estera è responsabile nel garantire adeguata formazione per gli Esponenti Aziendali e informazione per i Destinatari sui propri Compliance Program Locali e procedure locali.

Ciascuna Società Estera può valutare l’organizzazione di sessioni specifiche di formazione per gli Esponenti Aziendali che siano più direttamente coinvolti nei propri Processi e nelle relative Aree a Rischio. La Società Estera in tal caso potrà avvalersi del sostegno di POC ove sussistano specifici contratti di servizio intercompany al riguardo. Il supporto di POC potrà essere fornito anche nel caso in cui TERNA valuti la formazione da erogare come necessaria per ottemperare ad obblighi di legge.

La SE garantisce che la documentazione aziendale in materia di etica e compliance, incluso il GCP, sia resa disponibile agli Esponenti Aziendali mediante pubblicazione sulla rete intranet aziendale o portali della Capogruppo o mediante invio via mail o altre modalità di condivisione di documenti aziendali e che ad ogni neo-assunto sia consegnata (o indicata e messa a disposizione con le modalità sopra individuate) la documentazione in materia di compliance di riferimento per la SE.

Al personale neo-assunto verrà fatta firmare apposita dichiarazione di presa visione e di impegno al rispetto dei principi contenuti nella documentazione relativa all’etica e alla compliance.

I principi e i contenuti del GCP che siano applicabili ai Terzi sono resi conoscibili attraverso la documentazione contrattuale che dovrà prevedere clausole volte a garantire il rispetto da parte del Terzo dei Principi di Comportamento individuati dal GCP a loro direttamente applicabili. Laddove la SE abbia adottato

un proprio Compliance Program Locale, le clausole contrattuali dovranno altresì prevedere il rispetto dei predetti programmi e delle normative applicabili.

Le attività di informazione e di formazione sono documentate, monitorate e valutate in termini di adeguatezza ed efficacia.

18. SISTEMA DI WHISTLEBLOWING

18.1. Sistema di reporting (whistleblowing)

Chiunque può segnalare atti e/o comportamenti illeciti, commissivi o omissivi che costituiscono violazioni - anche sospette - dei Principi di Comportamento di cui al GCP e dei Compliance Program Locali dei principi sanciti nel Codice Etico, della normativa interna, rappresentata da tutte le disposizioni, procedure, linee guida o istruzioni operative della società destinataria della Segnalazione nonché violazioni di *policy*, regole aziendali che possano tradursi in fattispecie di reato o, in ogni caso, che possano comportare un danno per il Gruppo o per le singole società del Gruppo.

Gli Esponenti Aziendali hanno il dovere di segnalare ogni violazione o presunta violazione dei Principi di Comportamento di cui al GCP e ai Compliance Program Locali adottati nella specifica SE indicati nel relativo Allegato Paese.

Le segnalazioni attinenti a violazioni del GCP e dei Compliance Program Locali e dei loro atti attuativi adottati nella specifica SE riportati nell' Allegato Paese di riferimento, devono essere sempre portate a conoscenza del CO.

Le Società devono istituire un sistema di segnalazione delle violazioni e indicarne il gestore, spiegare il sistema di segnalazione delle violazioni, garantire la riservatezza dell'identità del segnalante e la confidenzialità sui contenuti della segnalazione, fatti salvi gli obblighi di Legge, tutelare chi effettua segnalazioni in buona fede e con uno spirito di lealtà nei confronti dell'azienda da ritorsioni o effetti negativi sulla sua posizione professionale; raccogliere le segnalazioni, valutarle secondo le procedure previste e definire le eventuali, in caso di accertata violazione, sanzioni commisurate alla gravità della violazione.

Al riguardo la modalità di segnalazione e la gestione delle segnalazioni Whistleblowing sono disciplinate nella LG054, applicabile anche alle Società estere nel rispetto della legislazione locale e adeguatamente regolata tramite accordi infragruppo.

a) Whistleblowing secondo LG054

Nel caso in cui la SE aderisca al sistema di segnalazione previsto nella LG054 si ricorda che i canali interni di segnalazione previsti si ricorda essere i seguenti ivi descritti:

1. **Portale informatico**, accessibile al seguente indirizzo <https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione>. (ITA/ENG)
2. **Posta ordinaria** all'indirizzo: Responsabile Audit c/o TERNA S.p.A., Viale Egidio Galbani, 70 – 00156 Roma, utilizzando la seguente dicitura **“segnalazione whistleblowing, riservata – non aprire”**.

3. **Incontro diretto:** il segnalante ha la possibilità di richiedere un incontro con il Responsabile Audit al fine di comunicargli direttamente l'oggetto della segnalazione. Suddetto incontro viene fissato tramite una richiesta effettuata dal segnalante tramite Portale (<https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione>) o apposita e-mail all'indirizzo whistleblowing@terna.it, specificando il nome della società del Gruppo Terna oggetto della segnalazione.

Le disposizioni della LG054 applicabili saranno quelle previste per le segnalazioni ordinarie, non essendo applicabile la specifica normativa italiana in materia.

Deve essere garantito il trattamento dei dati secondo la Disciplina Privacy applicabile, nonché il generale divieto di ritorsioni previsto dal Codice Etico, espressamente sanzionabile per le segnalazioni effettuate in buona fede e con uno spirito di lealtà nei confronti dell'azienda.

b) Whistleblowing Società Estere

In caso di impossibilità della SE di adottare la disciplina del whistleblowing con i canali di segnalazione interni così come descritti dalla LG054, le SE apprestano, in linea con la normativa locale, modalità di segnalazione delle informazioni sulle violazioni coerenti con le previsioni del Codice Etico sopra indicate nel presente paragrafo 18.1 in materia di tutele del segnalante e provvedono a:

- comunicare a Terna S.p.A., anche tramite il CO, i presidi istituiti o da istituire che possono prevedere il coinvolgimento del CO nominato ai sensi del Global Compliance Program, quale programma di Compliance indirizzato a tutte le SE;
- assicurare adeguata informazione circa il sistema di segnalazione delle informazioni sulle violazioni, le modalità di utilizzo e il sistema di tutele approntato.

La SE, inoltre, dovrà implementare un adeguato sistema di monitoraggio propedeutico alla definizione di una reportistica annuale verso Terna S.p.A., anche per il tramite del CO, relativa alle segnalazioni ricevute, con l'indicazione delle seguenti informazioni:

- numero di segnalazioni ricevute;
- breve descrizione dell'area normativa della segnalazione (ad es. Privacy; Cyber security; Corporate governance; Salute e sicurezza; Risorse Umane; Sostenibilità; Fiscale; Acquisti; Security), con specifica evidenza (anche ai fini dell'attività di rendicontazione di sostenibilità effettuata secondo i GRI standards) del numero di casi in cui sono state segnalate discriminazioni o molestie;
- numero di segnalazioni gestite;
- numero di segnalazioni infondate;

- numero di segnalazioni fondate; rispetto alle quali dovrà essere indicata distintamente la tipologia delle attività promosse (ad es. un'attività di informazione o di formazione oppure approfondimenti e attività informative omogenee sul territorio inerenti procedure in essere, correzione di processi interni, avvio di un procedimento disciplinare, trasferimento dei risultati delle attività di accertamento all'autorità giudiziaria, archiviazione per mancanza di evidenze).

In nessuno caso dovrà essere condiviso con Terna S.p.A. l'oggetto e/o contenuto delle segnalazioni ricevute.

Tale reportistica sarà rivolta, oltre che verso il proprio AD/AU/Executive Director e il proprio CO, anche verso il Chief Risk Officer, il Responsabile Internal Audit e il Comitato Etico nominati da Terna.

La SE dovrà inoltre individuare il gestore del canale di segnalazione apprestato nel rispetto della disciplina privacy applicabile e chi analizza e promuove le azioni più opportune in base alle risultanze istruttorie nonché declinare i presidi di gestione con propria disposizione/procedura aggiornando altresì i richiami nei Compliance Program locali e sul sito internet ove disponibile.

Per quanto attiene ai ruoli e alle responsabilità, nel trattamento delle segnalazioni che resta in capo al Gestore, può essere richiesto supporto al Compliance Officer nominato dalla società interessata e/o di consulenti esterni.

18.2. Investigation

Tutte le volte in cui viene ricevuta una segnalazione, è attuato un processo volto a gestire la segnalazione e a monitorare la sua tempestiva risoluzione. Tale processo è attuato e tracciato a cura dei soggetti formalmente individuati per la gestione delle segnalazioni.

A seguito della segnalazione, gli Esponenti Aziendali sono tenuti a cooperare con le relative indagini ove coinvolti nell'istruttoria.

La mancata cooperazione e la mancata trasmissione di informazioni oneste e veritiere potrebbero determinare l'adozione di azioni disciplinari

Sulla base delle risultanze verranno adottate le azioni più opportune nei confronti del segnalante, del soggetto segnalato, nonché le azioni correttive più adeguate con riferimento ai Processi interessati dalla segnalazione.

19. MONITORAGGIO E MIGLIORAMENTO CONTINUO

TERNA monitora sull'efficace attuazione del GCP a livello del Gruppo Terna. A tal fine, viene chiaramente individuata, a livello del Gruppo Terna, la struttura Presidio Corporate Liability e e Compliance Risk quale responsabile del monitoraggio e del miglioramento continuo del GCP.

In particolare, viene previsto lo svolgimento di periodiche attività di audit e di testing volte a:

- assicurare l'efficacia del GCP;
- intercettare eventuali violazioni;
- individuare eventuali azioni di miglioramento o correttive a livello strutturale o nell'ambito dei singoli Processi, in ottica di rafforzare il Sistema di Controllo Interno e Gestione dei Rischi.

Inoltre, il monitoraggio sull'effettiva attuazione del GCP come integrato dal relativo Allegato Paese da parte delle Società Estere viene effettuato dal CO nominato (*si veda par. 6*).

In caso di dubbi sull'interpretazione, sull'implementazione o sul rispetto di qualsiasi Area a Rischio, degli Standard Generali di Controllo o dei Principi di Comportamento, ciascun Esponente Aziendale dovrà consultarsi con il Presidio Corporate Liability e e Compliance Risk prima di agire, usando l'indirizzo e-mail pubblicato sul sito web di TERNA.

20. PROVVEDIMENTI DISCIPLINARI E RIMEDI CONTRATTUALI

Le violazioni delle leggi sulla responsabilità penale o assimilabile delle persone giuridiche possono avere conseguenze penali, civili e amministrative, tra cui l'irrogazione di sanzioni (pecuniarie e interdittive) e la reclusione, così come un grave danno alla reputazione del Gruppo Terna.

La piena effettività del GCP e/o di una politica, una procedura o un'istruzione locale a esso correlata o di qualsiasi altra procedura del Gruppo Terna applicabile, nonché dei Compliance Program Locali, viene garantita mediante l'applicazione di apposite sanzioni in caso di violazione dei principi contenuti nei predetti documenti.

In caso di violazioni commesse dagli Esponenti Aziendali, le relative sanzioni disciplinari saranno comminate dalla singola Società Estera, in conformità con il sistema disciplinare già in vigore e in linea con la contrattazione collettiva nazionale e la regolamentazione locale applicabile in materia, nonché sulla base dei Compliance Program Locali.

In aggiunta, le Società Estere adotteranno adeguate sanzioni in caso di (i) violazione delle normative locali in materia di *corporate liability* (laddove applicabili); (ii) atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di eventuali *whistleblower* per motivi collegati alla segnalazione nonché di violazione delle misure di tutela del *whistleblower* e di effettuazione con dolo o colpa grave di segnalazioni che si rivelino infondate.

Tra le misure disciplinari applicabili possono essere previste quella della cessazione del rapporto di lavoro e del risarcimento dei danni (*sul punto si vedano Allegati Paese di riferimento*).

Le misure disciplinari dovranno essere applicate a prescindere dagli esiti di eventuali procedimenti penali avviati dalle autorità giudiziarie competenti.

In caso di violazioni da parte dei Terzi, ciascuna Società Estera adotterà appropriate misure, compresa – a titolo esemplificativo ma non esaustivo – la risoluzione del contratto.