GLOBAL COMPLIANCE PROGRAM

a seguire il testo del documento in lingua italiana e inglese; in caso di dubbi interpretativi, prevale il testo in lingua italiana

(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

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 Internazionale[1] (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)

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 GAFI[2], 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)

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 disciplina[3]:

- le modalità di Risk Assessment, descritte al par. 4, valevoli 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 stuttura 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 controllanti[4] 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 GCP[5], 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 addizionali 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 COMPORTAMENTO

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/commessa;
- 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 assimilabili[6];
  - 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 triangolazione[7];
- 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 accesi 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 COMPORTAMENTO

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 COMPORTAMENTO

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 **fiscalità** 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 procedure 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 valevoli 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'acquisire 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 immettervi 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 la confidenzialità sui contenuti della segnalazione, fatti salvi gli obblighi di Legge, tutelare chi effettui 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.

GLOBAL COMPLIANCE PROGRAMME

the text of the document is attached hereto in both Italian and English; in the event of doubts regarding interpretation, the Italian text shall prevail

(adopted by the Board of Directors of TERNA S.p.A with its resolution of 10 November 2017 and subsequently updated)

Revision history

Revision	Date	Description
03	14/12/2023	Fourth issue that provided for the revision of the Global Compliance Programme to bring it in line with the changes introduced by LG054 Whistleblowing on reporting and changes in the composition of the Compliance Officer Bureau (COB)
02	02/09/2022	Third issue that provided for the revision of the structure of the Global Compliance Programme to bring it in line with the main and most recent best practices and regulations applicable to compliance programmes, identified by way of example in section 3.2. of the Global Compliance Programme. Adaptation of the document following the so-called "process approach", identifying and regulating the relevant corporate macro-processes at Group level, which emerged from the risk assessments in the area of corporate liability (previously, the GCP was structured by categories of crimes abstractly relevant to the Group), in order to make the GCP more consistent with the aforementioned best practices and with the compliance models recently adopted by the Group (i.e. Organizational, Management and Control Models pursuant to Italian Legislative Decree 231/2001) and to better reflect the organisation of the Group companies, as well as to facilitate the understanding of the GCP by the Recipients.
01	18/12/2019	Second issue
00	10/11/2017	First issue

Approved
Giuseppina Di Foggia

Reference management systems and/or organisational models:

X	Quality Management System
	Environmental Management System
	Occupational Health and Safety Management System
	Major Accident Management System - Seveso
	Information Security Management System
	Energy Consumed for Own Use Management System
	LLW Laboratory Management System
	Calibration Centre Management System
X	Anti-Bribery Management System
	Asset Management System
	Infection Prevention and Control Management System
	Business Continuity Management
	Privacy Model
	262 Model
X	Compliance Management System
X	231 Model

*(place an "**X**" in the left-hand column with reference to the line in question)*

Index

GLOSSARY

Action Plan: plan of actions aimed at improving the control system identified taking into account the outcomes of the Risk Assessment and the Risk Management strategy identified for the Risk (between avoid, reduce, accept and monitor and transfer).

Administrative Body: Board of Directors or corresponding body or function of Foreign Companies.

Anti-Bribery Guidelines or **LG059**: the Anti-Corruption guidelines adopted by the TERNA Board of Directors set out keeping into consideration the main international conventions, EU legislation, the FCPA and the Bribery Act regarding the prevention and fight against corruption. These guidelines contain principles and rules of conduct for all Company Representatives (of all Group companies as well as any third party acting in the name and/or on behalf of TERNA or the Terna Group, such as suppliers, agents, consultants, business partners or any other counterparty.

Areas at Risk: activity areas of the Non-Italian Company more at risk when it comes to the commission of Crimes.

Bribery Act: UK Bribery Act of 2010.

COB: Compliance Officer Bureau, established within Non-Italian Companies, comprising the Compliance Officer and a Local Assistant, or the Compliance Officer and a Technical Assistant.

Code of Ethics: the Code of Ethics adopted within the Terna Group and approved by TERNA's Board of Directors on May 21, 2002 and relative updates, aimed at defining the ethical-behavioural principles with which Directors, Employees and all those who work in the name and on behalf of TERNA or Terna Group companies must comply.

Company Representatives: employees, directors and other members of the management and control bodies of Foreign Companies.

Compliance Officer or CO: a person identified in each Non-Italian Company by resolution of the Administrative Body with the task of fostering, within the same Company, the dissemination of knowledge of the GCP and/or of the Local Compliance Programmes envisaged in the Country Annex and of the Parent Company's policies, as well as of facilitating their operation through training and information activities and through the implementation of specific information flows.

Confidential Information: company information concerning the NIC or other Terna Group companies, including Privileged Information, which is not in the public domain and which, due to its subject matter or other characteristics, is in of a confidential nature towards parties not bound by confidentiality obligations pursuant

to current law or contractual agreements identified by the procedure for managing, processing, and communicating corporate information of Terna S.p.A. and its subsidiaries (LG005).

Country Annex: the document constituting the integral part of the GCP prepared in each Non-Italian Company and describing the Local Compliance Programmes and procedures adopted locally in implementation of the GCP.

Crimes: certain types of unlawful conduct that qualify as crimes in different jurisdictions and that could potentially be committed by a corporate officer or a third party and whose prevention in the Group must be considered a priority in order to manage its business with honesty and integrity.

Decree 231: the Italian Legislative Decree no. 231 of 8 June 2001, containing "*Rules of corporate liability for legal persons, companies and associations, including those without legal personality, in accordance with art. 11 of Italian Law no. 300 of 29 September 2000*" as amended.

DOJ: the U.S. Department of Justice.

Due Diligence: the process of auditing Third parties relating to the establishment of contractual/commercial relations with them or a specific transaction.

Facilitating Payments: means payments made for the purpose of expediting or securing the performance of an activity in the exercise of a public function considered routine (e.g. granting of a residence permit, granting of a police protection service, organisation of an inspection activity, granting of a business licence, formalities connected with the loading and unloading of goods).

FATF-GAFI or **GAFI**: Financial Action Task Force - International Financial Action Group[8] (body coordinating the fight against money laundering and terrorist financing).

FCPA: Foreign Corruption Practice Act of the United States of 1977 and subsequent updates.

GCP or **Global Compliance Programme**: this Global Compliance Programme, a document adopted by TERNA on 10 November 2017 and by the Foreign Companies and its subsequent amendments.

General Control Standards: general control standards identified and regulated by the GCP that each Non-Italian Company must adopt in line with the SCIGR adopted by the Terna Group aimed at allowing, through an adequate process of identification, measurement, management and monitoring of the main risks, a healthy, correct and coherent management of the company in line with the set objectives.

[8] The Financial Action Task Force (FATF) is an international body whose objective is to develop and promote strategies to combat money laundering and the financing of terrorism and the proliferation of weapons of mass destruction. (see 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)

ICT: the Information & Communications Technology structure.

Internal Control and Risk Management System or **SCIGR**: the set of corporate culture, capabilities, rules, procedures and practices, as well as organisational structures, aimed at defining an accountability system for the identification, measurement, management, mitigation and control of the main risks at Group level, thus maintaining a high level of stakeholder confidence in the governance and control of the Group.

Lists: Lists are defined as

iv. list of countries at risk of money laundering and terrorist financing drawn up by the EU, 'black list'/'grey list' lists (indicated by FATF[9], EU, etc.), UN lists of financial sanctions applied to individuals and entities linked to terrorist organisations.

v. list of subjects (natural and/or legal persons) prepared by the European Union, by each individual member state of the European Union, by the United Kingdom, by the United States of America, by the United Nations and by any other jurisdiction, and relevant - under the terms of the Italian legislation or as a result of the contractual provisions, as from time to time updated, supplemented, amended and effective - for Terna S.p.A. and the Terna Group companies, that contain the elements of identification of the subjects (natural and/or legal persons) and activities with which, or in relation to which, it is prohibited to perform, directly or indirectly, Transactions, as they are subject to Restrictive Measures;

vi. lists of countries at risk of corruption (e.g. Transparency International's corruption perception index);

Local Assistant: a person identified within a corporate function of the Non-Italian Company or, in any case, within the country or geographic area of the Non-Italian Company by resolution of the Administrative Body of the same and with the positive opinion of the CO of the Non-Italian Company, appointed, as local assistant, to assist the CO in the execution of his/her duties in the event the CO is identified in a person not belonging to the Non-Italian Company or the geographic area of the same or in the event the CO has requested his/her appointment.

Local Compliance Programmes: compliance programmes aimed at preventing *corporate liability* adopted by Foreign Companies in accordance with the local regulations applicable in the country of reference and in line with the General Control Standards and Principles of Conduct provided by the Global Compliance Programme.

Local Management: the chief executive officer or executive director or member of the Administrative Body with operational powers or corresponding function.

Manager: the persons, identified by the company, competent for the management of Whistleblowing reports.

[9] 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)

Non-Italian Company(ies) or **NIC**: non-Italian company(ies) of the Terna Group.

PCR: the Corporate Liability and Compliance Risk structure dealing with Compliance.

POC: the People Organisation and Change department.

Potential Risk: the possibility that a future, uncertain event in a specific business area/process will constitute a Risk.

Principles of Conduct: the minimum standards of conduct related to the Risk Areas.

Privileged Information: privileged and/or potentially privileged information related to listed companies and, in particular, to listed companies belonging to the Terna Group and to the related financial instruments identified by the procedure for keeping and updating registers of persons who have access to privileged and potentially privileged information (LG008).

Processes: the relevant macro-processes, identified by GCP, within which the Risk Areas are identified.

Public Administration or **P.A.** or **public body**: each of the bodies or apparatuses concurring in the exercise of the legislative, administrative or judicial functions of an individual state, including governmental bodies.

Public Official: (a) any elected or appointed official exercising a legislative, administrative or judicial public function; (b) any person exercising public functions in any branch of national, regional or municipal government or exercising a public function for any public agency or public enterprise, such as officials exercising public functions in state enterprises.

Recipients: Corporate Representatives and Other Recipients.

Red Flag: one or more anomaly indicators/Potential Risk factors (in terms of corruption, money laundering or other relevant crimes) to be checked as part of Due Diligence.

Residual Risk: the Risk of Crimes related to a specific business area/process mitigated by the existence and effectiveness of the internal controls adopted.

Restrictive Measures: commercial and financial restrictions adopted by the European Union, by each individual Member State of the European Union, by the United Kingdom, by the United States of America, by the United Nations and by any other jurisdiction, and relevant — under the terms of the applicable regulations or as a result of the contractual provisions, as updated, supplemented, amended and effective from time to time — for TERNA and the Terna Group companies in relation to third countries and/or subjects (natural and/or legal persons) and/or goods and services (including software, technologies, engineering and technical assistance) and activities.

Risk Assessment: the analysis of corporate processes aimed at identifying and assessing the potential risks of commission of the relevant Crimes and the relevant existing safeguards.

Risk: any future event that within the company, alone or in conjunction with other internal or external events, may adversely affect the achievement of the objectives set out in the relevant regulations of the individual country.

Technical Assistant: a person identified within the PCR structure by resolution of the Administrative Body and positive opinion of the CO of the Non-Italian Company, appointed to assist the CO in the performance of his/her duties, in the event that the CO has not been identified within the PCR structure.

Terna Group: TERNA S.p.A. and its subsidiaries according to the terms established in Article 93 of the Italian Legislative Decree no. 58 of 24 June 1998, (the so called Consolidated Law on Finance).

TERNA: the Parent Company TERNA - Rete Elettrica Nazionale Società per Azioni (in abbreviated form Terna S.p.A.).

Third Parties or **Other Recipients**: any third party acting in the name and/or on behalf of an NIC, such as suppliers, agents, consultants, business partners or any other counterparty.

Whistleblowing Guidelines or LG054: TERNA's whistleblowing guidelines.

21. INTRODUCTION

Parent Company TERNA - Rete Elettrica Nazionale Società per Azioni ("**TERNA**") is the Italian company which conducts electricity transmission and dispatching over the high voltage and extra-high voltage grid throughout Italy. Its shares are listed on the Italian Stock Exchange organised and managed by Borsa Italiana S.p.A., Mercato Telematico Azionario (MTA) segment, which includes medium and large capitalisation companies and is aligned with international *best practices* and belongs to the Financial Times Stock Exchange - Milan Index (FTSE MIB). TERNA is also among the large Italian listed issuers present in the MIB 40 ESG index, the first blue-chip index for Italy dedicated to environmental, social and governance (ESG) best practices that combines economic performance measurement with ESG assessments in line with the principles of the UN Global Compact.

TERNA is the *holding* of a multinational group operating in a complex and highly regulated business sector and in different economic, political, social and cultural environments (the "**Terna Group**").

22. TOP-LEVEL COMMITMENT

The Terna Group conducts its business in accordance with the criteria of loyalty, legality, fairness, integrity and transparency, in compliance with the regulations applicable in Italy and abroad on the subject of *criminal corporate liability*.

The Terna Group promotes and disseminates a culture of ethics and *compliance*. The commitment is mainly made by all the Terna Group's top management (Top-level commitment) who work to spread this message at all levels.

To this end, the top management of individual Terna Group companies define and disseminate guidelines, procedures and internal policies aimed at regulating and formalising such commitment in order to prevent the commission of unlawful activities.

In particular, the administrative bodies of the Group's non-Italian companies (the '**Non-Italian Companies**' or '**NICs**') also express and are called upon to disseminate, in a clear manner, the message of absolute observance of the Terna Group's principles of ethics, integrity and legality.

23. PURPOSE, SCOPE, FRAMEWORK OF REFERENCE, STRUCTURE OF THE GCP AND ADOPTION, IMPLEMENTATION AND AMENDMENTS OF THE GCP

23.1. Scope and field of application

In many of the foreign countries in which Terna Group operates, a criminal or quasi-criminal corporate liability regime has been established which enables courts to sanction corporate entities for criminal behaviours by their representatives, employees or third parties acting on their behalf.

Most of these regulations encourage companies to adopt corporate governance structures and risk mitigation systems to make efforts to prevent these individuals from committing crimes, also providing for an exemption or mitigation of applicable penalties in the event of the adoption and effective implementation of adequate preventing measures.

In order to harmonize the efforts of the Non-Italian Companies in preventing criminal corporate liability and to deliver a shared, consistent and global approach against illicit behaviours, TERNA has adopted, since 10 November 2017 and as subsequently updated, the *global compliance programme* ("**Global Compliance Programme**" or "**GCP**").

The GCP aims to define the general control standards and rules of conduct that apply to employees, directors and other members of the managing and control bodies of NICs ("**Company Representatives**"), as well as Other Recipients, if applicable, to prevent the commission of relevant offences.

The GCP constitutes, like the procedures referred to in section 5.1, an act of TERNA whose application is addressed to the Non-Italian Companies called upon to implement it.

Each Non-Italian Company, where appropriate or required by applicable local regulations, shall also define and adopt its own Local Compliance Programmes, in accordance with the aforesaid regulations and in line with the provisions of this GCP, set out in the Country Annex approved by each.

In such contexts, the GCP is therefore integrated, as described in more detail in section 5.1, with any rules provided for in the specific Country Annex, which includes Local Compliance Programmes.

23.2. The framework of reference

The GCP has been inspired to the most relevant international regulations and best practices, including but not limited to:

(xiv) Italian Legislative Decree no. 231 of 8 June 2001 (**Decreto 231**) and subsequent updates, which disciplines a regime of administrative liability (akin to a criminal liability) of legal entities as a result of certain crimes committed on behalf or for the benefit of such entities;

(xv) the Corporate Governance Code of listed companies promoted by Borsa Italiana S.p.A.

(xvi) the 2010 Federal Sentencing Guidelines Manual & Supplement, adopted by the United States Sentencing Commission on November 1, 2010;

(xvii) Foreign Corruption Practice Act (**FCPA**) of 1977 and subsequent updates;

(xviii) UK Bribery Act of 2010 and subsequent updates;

(xix) the Good Practice Guidance on Internal Controls, Ethics, and Compliance adopted by the OECD Council on 18 February 2010;

(xx) the 'Resource Guide to the U.S. Foreign Corrupt Practices Act' issued by the Criminal Division of the U.S. Department of Justice (**DOJ**) and the Enforcement Division of the U.S. Securities and Exchange Commission of 2012 and subsequent updates;

(xxi) the DOJ 'Evaluation of Corporate Compliance Programs' of 2017 and subsequent updates;

(xxii) the Anti-Corruption Ethics and Compliance Programme for Business: A Practical Guide adopted by the United Nations Office on Drugs and Crime (UNODC) in September 2013;

(xxiii) the recommendations adopted by the Financial Action Task Force - Gruppo d'Azione Finanziaria Internazionale (**FATF-GAFI** or **GAFI**) on money laundering and terrorist financing of 2012 and subsequent updates;

(xxiv) European regulations on money laundering, search, seizure and confiscation of the proceeds of crime and on the financing of terrorism (including Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 and Delegated Regulation (EU) 2016/1675 and subsequent updates);

(xxv) Italian Legislative Decree No. 24 of 10 March 2023, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on provisions concerning the protection of persons who report breaches of national laws;

(xxvi) Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

23.3. Structure of the GCP

This document, in addition to making explicit the commitment of the top management in the promotion and definition of a culture of ethics and compliance (so-called top-level commitment), as well as the methods of adoption of the GCP, implementation and subsequent updates to be implemented also in each Non-Italian Company, identifies and regulates[10]:

- Risk Assessment methods, described in section 4, which are also valid for the identification of Risk Areas within the Terna Group for the preparation of the Local Compliance Programmes reported in the Country Annexes;
- **General Control Standards**, described in section 5.2, which each Non-Italian Company must adopt in line with the Internal Control and Risk Management System referred to in section 5.1, aimed at enabling, through an adequate process of identification, measurement, management and monitoring of the main risks, a sound, correct and consistent management of the company with its objectives;
- the role of the Compliance Officer, described in section 6, identified as the figure appointed in each Non-Italian Company and responsible for ensuring the dissemination of knowledge and facilitating the operation of the Global Compliance Programme and of the Country Annex of reference;
- the relevant macro-processes (the '**Processes'**), which must always be taken into account for the application of the GCP by each Non-Italian Company, within which to identify, through the Risk Assessment activity, the activity areas in the context of which the Risk of commission of Crimes may be considered in more concrete terms (the '**Risk Areas**') in relation to certain types of unlawful conduct qualifying as crimes in different jurisdictions and which could potentially be committed by a corporate officer or a Third Party and whose prevention in the Group must be considered a priority in order to manage its business with honesty and integrity (the '**Crimes**', described in Appendix A attached to GCP a01LG058). For each macro-process, minimum standards of conduct related to Risk Areas are identified (the '**Principles of Conduct**').

The Principles of Conduct set out in section 7 and 10 are to be understood as applying across the board to all Processes regulated in paragraphs 7 to 16.

- The Processes described constitute the reference basis for each Non-Italian Company for drafting, through specific Risk Assessment activities, the respective Country Annex (see section 7–16);

[10] The structure of the GCP is based on the main best practices and regulations applicable to compliance programmes, as identified by way of example and not exhaustively in section 3.2. With regard to the identification of Processes and Risk Areas, this was carried out taking into consideration the macro-processes and macro-risk areas relevant at the level of the Terna Group, as they emerged in the Risk Assessments in the area of corporate liability.

- training of Company Representatives and information to Recipients on the GCP to ensure the effective application of the safeguards set out therein, as indicated in section 17;
- the whistleblowing system for handling reports of unlawful conduct or irregularities and internal reporting, set out in section 18;
- the safeguards for the continuous monitoring and improvement of the GCP and Local Compliance Programmes, regulated in section 19;
- the disciplinary measures and contractual remedies applicable in the event of a breach of the provisions identified in the GCP and which must be taken into account by the Non-Italian Companies as part of their Local Compliance Programmes, governed by section 20.

23.4. Adoption of the GCP, implementation and subsequent updates

The GCP expresses principles that are part of the Terna Group's fundamental values and inspire its organisation and activities, also in implementation of the principles of the Code of Ethics common to Non-Italian Companies, and has been approved by TERNA's Board of Directors.

TERNA therefore promotes the adoption of the GCP by all Terna Group companies.

Each Non-Italian Company is required to approve the GCP by resolution of the Board of Directors or the corresponding body or function ("**Administrative Body**").

Italian parent companies to[11] Non-Italian Companies adopt the GCP with the aim of providing a common guideline to these subsidiaries to combat corporate crime more effectively.

Possible and subsequent updates to the GCP are approved by TERNA's CEO by virtue of the proxy conferred by the Board of Directors when approving the GCP[12], as well as by the Administrative Body of each Non-Italian Company and their respective parent companies or, where a specific proxy has been conferred, by the CEO of each.

The Administrative Body of each Non-Italian Company, in compliance with their own autonomy and independence:

- is responsible for the proper identification of any Process and Area at Risk or Principle of Conduct, in addition to those identified in Paragraphs 7 et seq. of the GCP to be implemented through Local Compliance Programmes or local internal guidelines, procedures and policies;

[11] In any case, the Italian parent companies are equipped with a compliance programme in line with Italian regulations, i.e. the Organisation, Management and Control Model pursuant to Italian Legislative Decree no. 231/2001 in line with the Terna Group's LG032 "Implementation and Management of Organisational Models Pursuant to Legislative Decree no. 231/2001 in the Terna Group'.
[12] Appendices A and B may be updated by TERNA S.p.A.'s Industrial Programme Management Office Director by virtue of the power of sub-delegation granted to TERNA S.p.A.'s CEO.

- adopts the most appropriate measures for the implementation and monitoring of the GCP, taking into account the company's organization, complexity of business, specific risk profile and regulatory framework;
- is responsible for the adoption, implementation and monitoring, where required by national regulations, of Local Compliance Programmes, referred to in the relevant Country Annex.

24. RISK ASSESSMENT

The basis of every compliance programme is the performance of an analysis of the corporate processes aimed at identifying and assessing the potential risks of commission of the relevant Crimes and the relevant existing safeguards (**Risk Assessment**).

The steps that make up the Risk Assessment are as follows:

(v) mapping of Risk Areas, i.e. identifying and mapping, within the framework of individual company processes, the areas and related activities that are potentially exposed to the risk of commission of Crimes;

(vi) assessment of the degree of Potential Risk, carried out in the light of possible factors likely to generate the Risk. "**Risk**" means any future event within the company that, alone or in conjunction with other internal or external events, may adversely affect the achievement of the objectives set out in the relevant regulations of the individual country. The possibility of a future, uncertain event in a specific business area/process creating a Risk constitutes a **Potential Risk**;

(vii) assessing the adequacy of internal protocols, in order to identify all procedures and controls suitable to mitigate potential risks, as well as any need to adapt these controls. The system of preventive controls must be such as to ensure that the Risks of commission of Crimes, according to the methods identified and documented in the previous phase, are reduced to an acceptable level;

(viii) calculation of residual risk (the **Residual Risk**), understood as the Risk of Crimes associated with a specific corporate area/process mitigated by the existence and effectiveness of the internal controls adopted.

Taking into consideration the outcomes of the Risk Assessment and the Risk Management strategy identified for the Risk (between avoid, reduce, accept and monitor and transfer), a plan of action is carried out to improve the control system (the **Action plan**).

Each Non-Italian Company performs a Risk Assessment, draws up an Action Plan and implements any corrective and adjustment actions in order to guard against corporate liability.

To this end, it must first take into account the list of Processes and Risk Areas of general relevance for TERNA and the Terna Group indicated in section 7 *et seq*.

This list, therefore, does not exempt Non-Italian Companies (a) from carrying out their own risk assessment on the basis of the applicable local regulations as well as the peculiarities of their business and organisational structure and (b) from defining, where appropriate, their own control principles in addition to those contained in this GCP, section 5.2, as well as (c) to define any specific principles of conduct with respect to those contained in section 7 *et seq*. of this GCP. To this end, the Non-Italian Companies will identify:

iii) their own processes and Risk Areas that may entail a specific Risk of commission of a Crime through an analysis of their own business processes and of the possible ways in which Crimes identified as relevant on the basis of applicable local regulations may be committed;

iv) additional control standards and principles of conduct to be implemented through Local Compliance Programmes and/or local internal procedures to which all corporate officers and, where applicable, Third Parties must adhere in order to prevent the commission of Crimes.

Individual Non-Italian Companies carry out and constantly update their own Risk assessments.

25. THE GCP AND GENERAL CONTROL STANDARDS

25.1. The GCP and TERNA control references

The dictates of the GCP are generally inspired by the set of corporate culture, capabilities, rules, procedures and practices, as well as organisational structures, aimed at defining an accountability system for the identification, measurement, management, mitigation and control of the main risks at Group level, thus maintaining a high level of stakeholder confidence in the governance and control of the Group as a whole, defined as the **Internal Control and Risk Management System** or **SCIGR**, and are therefore supplemented by the following procedures in force and applicable in the Terna Group:

(iii) the principles of the Code of Ethics adopted within the Group, also applicable to all the Non-Italian Companies and which all Recipients are required to respect;

(iv) Guidelines, policies and procedures adopted by TERNA and applicable in the Terna Group; in particular:

a. Internal Control and Risk Management System of the Terna Group Guidelines (LG004);
b. Risk Management Guidelines in Terna (LG038);
c. Whistleblowing Guidelines (LG054);
d. Anti-Corruption Guidelines (LG059);
e. Corporate Giving Policy (LG024);
f. Ethics Committee Regulation Guidelines (LG014);
g. Golden Rule Guidelines (LG042);
h. Trade Compliance Policy (LG061);
i. Sustainability Policy (LG077);
j. Diversity & Inclusion (LG069);
k. Respect for 'Human Rights' within the Terna Group (LG057);
l. Third Party Due Diligence Guidelines (LG070);
m. Conflict of Interest Guidelines (LG079);
n. Approval of significant transactions and management of situations of interest (LG006);
o. Procedure for Transactions with Related Parties (LG026);
p. Procedure for Managing, Processing and Communicating Corporate Information of Terna S.p.A. and its subsidiaries (LG005);
q. Procedure for the maintenance and upkeep of the Registers of Persons with access to Privileged Information and Potential Privileged Information (LG008);

r. Management of inspections carried out by the P.A. (IO416CA).

In addition, the provisions of the GCP are supplemented for each Non-Italian Company by:

iv. the rules laid down in the specific Country Annex adopted by each NIC, which includes the Local Compliance Programmes;

v. the corporate governance provisions adopted by the NICs themselves in accordance with applicable legislation and international best practices, including those set out in section 3.2.;

vi. the internal control and risk management system adopted in each Non-Italian Company (e.g. local procedures and policies, principles of conduct, etc.).

If local laws and regulations, or policies and corporate procedures adopted by the single Non-Italian Companies contain mandatory requirements that exceed the requirements of this GCP, such requirements will prevail.

25.2. General Standards of Control

Each Non-Italian Company, in assessing the advisability of adopting local procedures, taking into account the unique activity performed and the specific associated risks as identified on the basis of the Risk Assessment to be carried out in accordance with paragraph 4 - shall in any event:

- provide for the General Control Standards identified in this GCP (e.g. traceability, identification of roles and responsibilities, archiving, etc.);
- detail internal controls;
- provide for the application of disciplinary sanctions in the event of violations.

The General Control Standards are as follows:

- **segregation of duties**: the assignment of roles, tasks and responsibilities within each company shall be made in compliance with segregation of duties according to which no individual may autonomously perform an entire process (i.e. in accordance with this principle, no individual can be autonomously in charge of performing an action, authorizing it and subsequently check it).
  Adequate segregation of roles can also be ensured by using IT systems that allow only identified and authorised persons to carry out certain operations;
- **authorization and signatory powers**: every company must issue formal provisions in relation to the exercise of authorization and signatory powers, which must be consistent with the allocated organizational and managerial responsibilities;

- **transparency and traceability of processes:** the identification and traceability of sources, information and controls carried out in relation to the formation and implementation of the decisions of the Non-Italian Company and the management of financial resources must be guaranteed; it is also appropriate to ensure the correct recording of the relevant data and information, in electronic and/or paper format;
- **proper management of relations with Third Parties and Due Diligence** (see section *5.3).*

25.3. Third-Party Relationship Management Standards and Due Diligence

TERNA and Terna Group companies pay special attention to the selection of Third Parties. To this end, every time a company is engaged in business activities through a joint venture or intends to approach a Third Party in connection with any business, an investigation must be conducted on the Third Party, aimed at identifying its chain of control, its possession of honour, professional and financial requisites, its credibility in the market, as well as its compliance with the Anti-Corruption Laws in force, or similar laws established by the country in which it operates or will operate on behalf of any Terna Group company.

Due Diligence should be proportionate to the real or perceived risk in relation to the third party and/or the transaction (risk based).

Due Diligence is conducted, based on criteria identified by the Parent Company, which may include: (i) searches through public and other available sources (e.g. business contacts, local chambers of commerce, business associations; web searches or specialised companies, entries in Lists) on companies, shareholders and exponents, in order to find any potentially relevant negative information on them; (ii) or in-depth investigations carried out by third-party consultants.

Due Diligence is governed by guidelines for the Group set out in section 5.1 (in particular, Anti-Bribery Guidelines LG059 and Third-Party Due Diligence Guidelines LG070), as well as the local procedures adopted by the NICs, if any.

Due Diligence on Third Parties may be carried out with the support of the competent Terna Group structures (in accordance with the provisions of the Third-Party Due Diligence Guidelines LG070) with reference to the company procedures that provide for the activation of counterparty audits.

In any case, the Due Diligence conducted should highlight potential Red Flags.

Listed below are some examples of Red Flags that may be taken into account when performing Due Diligence, such as potential risk factors or indicators of the possible commission of Crimes:

- if the Third party or, in the case of a company, its shareholders, is resident or has its registered office or carries on its activities in a country listed in the so-called international anti-money laundering blacklist/greylist (e.g. published by the FATF and the European Union) or in a country identified as a country that provides support to terrorist activities or in whose territory terrorist organisations operate or in those countries considered as tax havens as identified by recognised national and/or international bodies (e.g. Revenue Agency, OECD) or in a country with a high risk of corruption (see e.g. Transparency International rankings) or subject to international sanctions;
- if the information provided by the Third Party is insufficient, false or inconsistent or in case of apparent attempts to conceal the identity of the person at the top of the control chain;
- if the third party engages in activities/business that are inconsistent or not in line with the contractual performance required or if the third party or one of its representatives has a conflict of interest;
- in case of transactions or requests which are inconsistent with the activities carried out by the Third Party, such as requests for payments in a high-risk country which has no connection to the Third Party (for example, a Country with very protectionist laws on bank secrecy, with weak money laundering controls or where criminality/corruption is widespread). To this end, high-risk countries must be assessed taking into consideration international indexes such as the Transparency International Corruption Perceptions Index;
- if there is a request to structure a transaction in a way such to evade normal accounting and reporting regulations or such to not demonstrate any legitimate commercial interest, such as increasing the prices or making part of the payment “below the radar” through the drafting of a side letter;
- in case of relations with consultants or other Third Parties who have close links with a government or political party, or which have been specifically chosen by a public official or a client;
- if there are requests for the payment of commissions, fees or other forms of irregular remuneration or requests for payments in cash;
- if the third party is apparently lacking the skills, experience or resources required for the type of activity or has no corporate organisational structure or inadequate assets;
- if the third party has an abnormal or particularly complex ownership structure given the nature of its business;
- if the Third Party, with respect to the transaction, refuses to enter into a contract;
- if the Third Party refuses to undertake to abide by or comply with these Guidelines and/or further internal compliance procedures adopted by the NIC and/or applicable to the Group and has not adopted any code of conduct or similar compliance instrument designed to prevent the commission of crimes;
- if the Third Party has or had been suspended to join tenders or enter into contract with state-owned companies/public bodies/governmental agencies due to compliance investigations carried out;
- if the third party or any of its representatives have a questionable reputation or are/were investigated, indicted or convicted in criminal proceedings especially for crimes such as bribery, money laundering or fraud, or have been investigated or sanctioned by public stock exchange and market supervisory

authorities (e.g., US Securities and Exchange Commission (SEC)) or have been disqualified or subject to precautionary measures;

- if the address of the Third Party business is a virtual office;
- if the Third Party has an undisclosed beneficial owner.

The presence of one or more Red Flags requires a more in-depth examination that may include additional controls and/or appropriate authorisation levels.

For high-risk transactions or particularly complex situations, the analyses may be supplemented with opinions and investigations on specific questions entrusted to providers or consultants specialised in the subjects of reference.

Monitoring throughout the contractual relationship is necessary to ensure that the third party maintains the identified and approved requirements, if necessary by periodically updating the Due Diligence. In the event that a Third Party loses these requirements or a Red Flag emerges during the term of the contractual relationship, appropriate measures to be applied shall be defined.

Third parties shall be adequately informed of the contents of the GCP and, where they exist, of the Local Compliance Programmes and shall undertake to comply with the Principles of Conduct contained in the aforesaid documents by signing appropriate contractual clauses, as provided for in the following paragraph. 17.

26. THE COMPLIANCE OFFICER

26.1. Appointment of the Compliance Officer

In each Non-Italian Company, a Compliance Officer (**Compliance Officer** or **CO**) is appointed, a person identified by resolution of the Administrative Body, whose task is to promote, within the same, the dissemination of knowledge of the GCP and/or of the Local Compliance Programmes established in the Country Annex and of the Parent Company's guidelines, as well as to facilitate its operation through the training/information activities relating to the GCP referred to in section 17 and through the implementation of appropriate information flows, as detailed in the following section 6.2.
The CO must possess appropriate legal or corporate risk control and management skills, to be assessed in the light of their CV and previous professional experience.
The CO must also meet the requirements of integrity, to be assessed taking into account past conduct and compliance with the ethical principles that govern the Terna Group's operations.

For the performance of his/her duties, the CO is possibly assisted by persons appointed by resolution of the Administrative Body of the Non-Italian Company and subject to the positive opinion of the CO himself/herself which, together, constitute the Compliance Officer Bureau ("COB").
Such persons can be identified:

- within a corporate function of the Non-Italian Company or in the country or geographical area of the Non-Italian Company in the event that the CO is identified in a person not belonging to the Non-Italian Company or the geographical area of the Non-Italian Company or in the event that the CO has requested the appointment (**Local Assistant**),
- within the Corporate Liability and Compliance Risk structure regarding Compliance ("**PCR**"), assigned to assist the CO in the performance of duties, if the CO has not been identified within the PCR structure ("**Technical Assistant**").

The coordination of the management compliance issued at Terna Group level is guaranteed on the occasion of the meetings convened pursuant to the 231 Model of the Parent Company by the President of the Terna S.p.A. SB.

Where established, the COP gathers periodically and anyway when necessary: the coordination can be ensured in such occasions as well.

26.2. Functions, powers and information flows

In particular, the CO must:

- promote spreading awareness of the Global Compliance Programme and of the Local Compliance Programmes adopted as provided for in the Country Annex of reference and of the Parent Company's guidelines set out in section 5.1 as well as facilitating its operation through the training/information activities related to the GCP mentioned in section 17 and/or through the implementation of appropriate information flows;
- monitor the conduct within NIC processes and Risk Areas and carry out checks for alleged violations of the requirements of the Global Compliance Programme as supplemented by the relevant Country Annex;
- coordinate with the NIC Local Management for a better monitoring of activities in Areas at Risk;
- monitor the effective implementation of all necessary disciplinary measures in order to punish any culpable deviation from the established rules of conduct;
- periodically inform the Administrative Body of the Non-Italian Company of any relevant initiative taken concerning the Global Compliance Programme and the Local Compliance Programmes adopted in the specific companies listed in the Country Annex;
- promptly inform the Administrative Body of the Non-Italian Company of any ascertained violation of the Global Compliance Programme and of the Country Annex of reference, as well as of the Local Compliance Programmes such as specific local safeguards adopted in order to avoid that the predicate crimes pursuant to Decree 231 are committed through the NIC in the interest and/or to the advantage of the NIC or of the Terna Group, as well as of the procedures and Guidelines valid for the Terna Group;
- if it becomes aware of events or information that it considers to be of interest to a Terna Group company, it must inform the supervisory body established pursuant to Decree no. 231 of the company concerned under Italian law.

For the proper performance of these activities, the CO is guaranteed adequate autonomy and independence, also with respect to the Local Management. The CO must have effective powers of inspection and control, as well as access to relevant company information.

In any case, the Non-Italian Company makes available to its CO any resource deemed necessary or appropriate for an effective performance of supervisory functions, including the support of external professionals identified by the CO himself/herself for particularly complex technical assessments. To this end, the Non-Italian Company allocates to the CO sufficient financial resources (budget) and personnel to carry out his/her activities and to ensure the effective implementation of the GCP.

With reference to the information flows to the CO provided for in this paragraph, please refer to the identification made in the Appendix attached to the GCP under "Appendix B - a02LG058". This identification may be further detailed within each Country Annex, due to the organisational peculiarities and activity of the company itself.

The Local Assistant (as a possible local assistant and for specific skills related to the geographical area) and the Technical Assistant have the task of supporting the CO in the activities of:

- organising, managing, and recording meetings;
- managing information flows;
- providing training courses;
- managing information activities;
- developing the audit plan for risk areas;
- any other activities that may be necessary.

26.3.

27. RELATIONS WITH PUBLIC BODIES AND PUBLIC OFFICIALS

The Principles of Conduct referred to in this paragraph, relating to relations with public bodies and public officials, are one of the main pillars referred to by the DOJ, given the relevance in the international context of bribery of public officials, the cornerstone of major legislation (such as the FCPA and the UK Bribery Act).

These Principles of Conduct are to be understood as applicable in all relations with such persons and also transversally to the subsequent Processes regulated in paragraphs 8 to 16.

Public body or **Public Administration** (**P.A.** or **public body**) means each of the bodies or apparatuses that contribute to the exercise of the legislative, administrative or judicial functions of an individual state, including governmental bodies.

For the purposes of this document, public official (**Public Official**) means (a) any elected or appointed official exercising a legislative, administrative or judicial public function; (b) any person performing public functions in any branch of the national, regional or municipal government or exercising a public function for any public agency or public enterprise, such as officials exercising public functions in state enterprises.

For each Non-Italian Company, the foregoing definitions must be used taking into account the applicable local legislation, as well as the Crimes that may be abstractly configured below.

POSSIBLE RISK AREAS

(xvi) negotiation and management of contracts concluded with the Public Administration;
(xvii) participation to public tenders;
(xviii) management of relationships, different from contractual relationships, with public bodies (e.g. with reference to health, safety and environment requirements, management of personnel, payment of taxes, customs practices);
(xix) management of disputes (lawsuits, arbitration, out-of-court proceedings);
(xx) selection of partners, intermediaries and consultants and negotiation and execution of the related contracts;
(xxi) management of cash flows;
(xxii) provision of Facilitating Payments and political contributions;
(xxiii) exercise of the power of attorney in matters of expropriation;
(xxiv) management of non-profit initiatives, corporate giving (including donations and sponsorships);
(xxv) management of gifts, entertainments and hospitality expenses;
(xxvi) recruitment;

(xxvii) participation in inspections, investigations, accesses and checks carried out by Public Officials;
(xxviii) management of the received public funding, grants or guarantees obtained;
(xxix) carrying out procedures for obtaining authorisation measures from the Public Administration;
(xxx) sending information flows to the Public Administration.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corporate crimes
- Cybercrimes
- Money laundering, related crimes and terrorist financing
- Organised crime, also of a transnational nature
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

When conducting business with Public Administrations and/or Public Officials, Recipients must act with integrity and honesty and comply with all applicable laws and regulations.

The obligations applicable to Recipients (pursuant to specific contractual terms) for prevention of bribery crimes are set out in the Anti-Bribery Guidelines (LG059) recalled in section 5.1.

Non-Italian Companies must guarantee:

- the traceability of any relation, communication and relevant relationship (e.g. administrative proceedings aiming at obtaining an authorization, a license or similar act, joint ventures with public entities) entered with the Public Administration;
- the involvement of at least two authorised persons in the management of relations with the Public Administration;
- the **hiring of personnel** exclusively on the basis of real and demonstrable corporate needs, using a selection process that involves at least two functions and is based on criteria of objectivity, competence and professionalism, avoiding any favouritism or conflict of interest or any action that takes the form of favouritism, nepotism or forms of patronage that could influence the independence of a Public Official or induce him/her to ensure any advantage for the Non-Italian Company or the Terna Group;
- the formalisation of any agreements with Public Officials and P.A. (in written form or digital contracts).

Moreover, the Recipients, in their relations with the Public Administration, must not in any way:

a) submit false or altered documents, either fully or in part, during the participation to public calls for tenders;
b) carry out cheating behaviours against the Public Administration which may induce the latter to make a wrongful assessment during the examination of **requests for authorizations**, licenses, clearances, concessions, etc.;
c) omit due information in order to direct in the favour of one of the Terna Group companies a Public Authorities' decisions in relation to any of the circumstances described at let. a) and b) above;
d) carry out behaviours aimed at obtaining from a Public Administration any type of grant, **public funding**, facilitated loan or other disbursements of the same type, by means of altered or falsified statements and/or documents, or the omission of necessary information or, more in general, by means of artifice or deception, aimed at leading the grantee institution into error;
e) use sums received from Public Administration as funds, contributions or loans for purposes other than those for which they were granted.

Non-Italian Companies must also ensure:

- all the statements rendered to national or international Public Administration (e.g. for the purpose of obtaining funds, grants or loans) contain only true information and be signed by authorized signatories and, where said funds, grants or loans are obtained, these are appropriately accounted for;
- request, management and reporting phases in relation to public proceedings for the purpose of obtaining public funds, grants or loans are managed by different Company Representatives within the organization;
- the involvement of the relevant functions in the activities of collecting and analysing the information needed for reporting purposes;
- the documentation and the subsequent reporting to be submitted in relation to the request of subsidies, grants, loans and guarantees are approved by adequate hierarchical levels.

In relation to **facilitating payments**, i.e. payments made for the purpose of expediting or securing the performance of an activity in the exercise of a public function that is considered routine (e.g. granting of a residence permit, granting of a police protection service, organisation of an inspection activity, granting of a business licence, formalities connected with the loading and unloading of goods) ('**Facilitating Payments**') and political contributions, the NICs guarantee:

- that any kind of Facilitating Payment by Company Representatives and Other Recipients is prohibited;
- that any type of political contribution to parties or any form of support for political campaigns on behalf of the Non-Italian Company or any Terna Group company is prohibited. Such political contributions or support may include, without limitation:
  a) money;

b) goods other than money (e.g. loaned or donated equipment, free technology services, provision of human resources); and/or
c) the use of corporate resources (e.g. facilities, e-mail, offices).

This rule does not prohibit the Company Representative from exercising his/her right to participate in political activities on an unequivocally personal level.

With reference to any other Risk Areas not identified in this section, reference should be made to the Principles of Conduct identified in the Processes indicated below and in the Anti-Bribery Guidelines (LG059) referred to in section 5.1.

28. INSTITUTIONAL RELATIONS AND MANAGEMENT OF CORPORATE GIVING ACTIVITIES, INCLUDING DONATIONS AND SPONSORSHIPS

The Principles of Conduct in this paragraph refer to the process of institutional relations, management of corporate giving, including donations and sponsorships.

POSSIBLE RISK AREAS

(iii) Management of relationships between the Recipients and national or international representatives concerning monitoring activities and the analysis of the political and institutional environment;

(iv) Corporate giving activities in favour of Public Officials, Public Administration, scientific societies, foundations and associations and, more generally, of private parties, such as sponsorships, donations in cash, donations in kind (free transfers or making available to third parties of company assets, know-how or services), as well as volunteer programmes.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Corporate crimes
- Money laundering, related crimes and terrorist financing
- Organised crime, also of a transnational nature
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

With reference to the area concerning **institutional relations**, in each NIC the Recipients are prohibited from:

- making cash donations on one's own initiative or as a result of solicitation towards Public Officials in order to obtain an advantage for the Non-Italian Company or any Terna Group company;
- submit documentation containing data, untrue information and/or omitting data, information, in order to facilitate the obtaining of authorisations/securities in favour of the Company.

When it comes to **corporate giving** activities, each NIC prohibits its Recipients from distributing and/or receiving gifts and presents or other advantages of a nature other than what envisaged by the corporate policy. In particular, any kind of donation is prohibited - on one's own initiative or as a result of solicitation - towards Public Officials (even in those Countries where making gifts is a widespread practice) or their families,

which may influence the independence of judgement or ensure an advantage for any Non-Italian Company or any Terna Group company.

The donations allowed by corporate policies must always be of a small value or aimed at promoting social, environmental, humanitarian and/or cultural initiatives or the brand image of the Terna Group. Gifts offered or received must be sufficiently documented as per the company procedures.

In addition, corporate giving activities:

(v) must be carried out consistently with the principles of the Code of Ethics and the applicable company procedures, including the Corporate Giving Policy (LG024) referred to in section 5.1, and within the limits of the approved budget;

(vi) must only be carried out in favour of trustworthy entities/subjects known for their integrity and professional correctness. To this end, corporate officers must carry out prior checks on the good repute of the persons benefiting from corporate giving;

(vii) must be approved according to appropriate authorisation levels and the application must include: (a) an adequate description of the nature and purpose of the individual contribution/sponsorship, (b) a Due Diligence on the beneficiary, and (c) verification of the legality of the contribution or sponsorship, according to applicable laws;

(viii) must be formalised in specific written agreements/letters that (i) clearly define the purpose and scope for which the contribution may be used, (ii) provide, where applicable, for controls on the use of the contribution granted in accordance with the terms of the agreement, and (iii) contain appropriate provisions to ensure compliance with applicable laws.

Company Representatives are required to:

- maintain the traceability of corporate giving authorisation processes, guaranteeing the collective character of related decisions;
- make payments to the beneficiary exclusively to an account in the beneficiary's name;
- verify that the funds paid have been used for the intended purposes;
- verify ex post the effectiveness of the consideration concerning sponsorship activities;
- inform the CO at least once a year about corporate giving activities, donations and sponsorships during the period of reference.

29. COMMERCIAL ACTIVITIES AND CUSTOMER RELATIONS

The Principles of Conduct referred to in this paragraph relate to the business process and customer relations.

POSSIBLE RISK AREAS

(v) Negotiation and management of contracts concluded with any entity (public or private)

(vi) Participation in tenders or direct negotiation procedures initiated by public and private entities for the assignment of orders (contracts, supply, services), concessions, partnerships, assets (company complexes, participations, etc.)

(vii) Relations with business partners (including joint venture partners, agents and intermediaries) and management of partnership relations

(viii) Financial or commercial transactions involving Terna Group companies concluded with natural and legal persons resident (or with companies directly or indirectly controlled by them) in risk countries identified in Lists of Countries and/or in Lists of natural or legal persons also indicated by the FATF-GAFI which coordinates the fight against money laundering and terrorist financing.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Corporate crimes
- Money laundering, related crimes and terrorist financing
- Organised crime, also of a transnational nature
- Crimes against Individuals
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

Relations with customers or potential customers as well as with business partners must be managed in a fair, transparent, equitable and cooperative manner.

In each NIC, the Recipients are prohibited from:

- making cash donations on their own initiative or as a result of solicitation towards Public Officials;
- presenting documentation containing false data or relevant information and/or omitting data or information aimed at making the company obtain tenders/orders;

- entrust works, services and supplies and arrange the related payments without complying with the form and traceability requirements of the current regulations on public contracts and the traceability of financial flows, where applicable;
- making payments or recognising compensation in favour of third parties, without adequate contractual justification or in any case not adequately documented, justified and authorised.

Non-Italian Companies must guarantee:

- compliance with the procedures adopted by the Terna Group applicable to the trade process (such as the guidelines and/or instructions issued for the Terna Group and the local policies adopted individually by each Non-Italian Company or its parent, where applicable, for the management of export controls (Trade Compliance Policy - LG061).

Furthermore, as part of the business process, it is obligatory to:

- conduct Due Diligence against the counterparty in line with the provisions of section 5.3;
- base all relations with the counterparties on the principles of transparency and integrity and envisage performances and compensations in line with market practices, making sure that there are no aspects that may favour the commission of Crimes in Italy or abroad;
- in the event that persons whose names are on the Lists, or who are known to be controlled by persons on the Lists, are involved in business transactions, during due diligence or subsequent monitoring of the business relationship, ensure compliance with the provisions of the Third Party Due Diligence Guidelines (LG070) and the Trade Compliance Policy (LG061);
- verify that the documentation and formal communications produced during the tender procedure/or allocation of the order are managed and signed only by subjects previously identified and authorised by the NIC;
- ensure the traceability of decision-making and levels of authorization so that they can always be reconstructed using the internal records and documentation;
- define all partnerships and sales activities through contractual relationships, signed on the basis of the system of powers and delegations in force in the company and including compliance clauses (corporate liability or GCP, Code of Ethics, Trade Compliance and export control procedures, anti-corruption);
- with particular reference to contracts with **agents and intermediaries**, provide that they must also (i) clearly describe the services to be provided; (ii) define the nature of the commissions/fees (fixed, variable, success fees, etc.) and their amount in line with market standards (iii) establish the targets to be achieved;
- archive all documentation supporting individual activities.

The principles of the free market are among Terna's fundamental values and inspire its organisation and activities. Therefore, conduct is adopted in accordance with the rules of fair competition.

30. EXTRAORDINARY TRANSACTIONS (M&A, TRANSFERS, ETC.) AND MANAGEMENT OF CASH FLOWS

The Principles of Conduct referred to in this paragraph relate to the process concerning extraordinary transactions (M&A, transfers, etc.) and the management of cash flows.

POSSIBLE RISK AREAS

(iv) Carrying out extraordinary transactions (acquisitions and transfers of company shareholdings, mergers, demergers, acquisitions, transfers and leases of business branches, etc.)

(v) Management of post-acquisition integration activities

(vi) Management of cash flows, by which is meant all those activities or relationships involving a payment or collection to or from the NIC, including so-called intra-group relationships.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Corporate crimes
- Money laundering, related crimes and terrorist financing
- Organised crime, also of a transnational nature
- Tax crimes
- Market Abuse

KEY STANDARDS OF BEHAVIOUR

(I) **Extraordinary transactions and post-acquisition phase**

The following standards must be observed when conducting M&A transactions:

- conduct a Due Diligence on the target company (including the target company's existing contractual relationships) and potential counterparties, taking into particular consideration its ethical and reputational profile and, in the case of companies, the company's business history and background;
- perform checks on the tax implications deriving from the operations to be carried out;
- formalise transactions in written contracts by including the necessary clauses to ensure compliance with applicable laws and the procedures adopted (corporate liability or GCP, Code of Ethics, Trade Compliance and export control procedures, anti-corruption) by the Terna Group;
- correct valuation, accounting of acquisitions and/or corporate transactions;

- once a company has been acquired, actions will have to be taken to:
  - adopt the GCP and, therefore, also carry out the transposition and any necessary adaptation of the procedures in force and applicable in the Terna Group such as those set forth in section 5.1 i) and ii) of this GCP in the new legal entities resulting from the acquisition;
  - adopt control measures as close as possible to those referred to in section 5.2 and 5.3 of this GCP;
  - train and/or inform the relevant personnel for integration.

(II) Cash Flow Management

The management of payments and collections must comply with the following minimum standards:

- payments are to be made/received only in accordance with the legislation applicable from time to time, the contractual provisions from which they originate, and the applicable cash flow accounting principles;
- all payments must be authorized in compliance with the proxies and powers of attorney issued;
- as far as possible, it is necessary to ensure the segregation of roles and responsibilities of the parties involved in the payment process (e.g. management of supplier master data, payment receipt, material execution of payment, etc.);
- in any case, the NICs will not accept or make payments:
  - (i) to/from a party other than the contractual counterparty or (ii) from/to a current account other than those contractually provided for or (iii) from/to a country other than that of the parties or of performance of the contract, without adequate contractual justification or otherwise not adequately documented, justified and authorised.
  - from/to numbered accounts or cash or similar instruments[13];
  - in the event that a third party is indicated/delegated/appointed as payer, documentation must be requested as to the formal identification of that party as payer and the underlying reasons for such interposition or triangulation[14];
- it is prohibited to make payments or collect money to/from countries included in International lists without suitable documentation proving a real and specific need;
- particular attention must always be paid to and appropriate checks must be carried out in relation to (i) the registered office of the counterparty company (e.g. tax havens, countries at risk of money laundering or terrorist financing, etc.) and any company and trust structures used for extraordinary transactions or operations; (ii) transactions to/from current accounts opened in countries at risk of money laundering or terrorist financing (as set out in the GAFI/FATF lists, for example);

[13] Transactions are managed in compliance with the prohibition to use cash or any other bearer financial instrument, for any operation of collection, payment, transfer of funds, use or other use of financial resources; as well as in compliance with the prohibition to use current accounts or passbooks in anonymous form or with a fictitious heading. Any exceptions to the use of cash or other bearer financial instruments must be expressly provided for in the applicable Company or Terna Group procedures, and the limits on the use of cash provided for by the relevant regulations must be scrupulously observed.

14 By way of example, the following may be requested: (i) a certificate from the chamber of commerce relating to the paying entity; (ii) an identity document of its legal representative; (iii) a power of attorney attesting to the power of payment conferred on that paying entity; (iv) any document giving the reason for such payment made by the paying entity).

- checks on payments must also include consistency checks and the correspondence between the entitlement of the contractual relationship (i.e. the creditor of the payment) and the heading of the account on which the transaction is to be carried out;
- all payment/collection transactions must be carried out with licensed financial operators that have adopted safeguards to prevent money laundering;
- in any case, no payments may be made to persons who are not clearly identifiable;
- during the execution of contracts from which cash flows are derived, constant monitoring of financial transactions made/received is envisaged. With particular reference to intra-group transactions, it must be ensured that services rendered from/to Terna Group companies are at market conditions and regulated by specific contracts.

These Principles of Conduct are to be understood as applying to all receipts and payments and also across all Processes regulated by the GCP in paragraphs 7 to 16.

31. PROCUREMENT

The Principles of Conduct referred to in this paragraph relate to the procurement process.

POSSIBLE RISK AREAS

(iii) Management of tender/purchasing procedures;

(iv) Appointment of professional and consultancy roles.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Corporate crimes
- Money laundering, related crimes and terrorist financing
- Organised crime, also of a transnational nature
- Crimes against Individuals
- Crimes related to Copyright infringement
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

NICs must ensure:

- that all relations with suppliers are characterised by the principles of transparency and integrity and the absence of conflicts of interest;
- that all relations with suppliers provide for services and fees in line with market practices, ensuring the absence of terms and conditions conducive to the commission of crimes;
- Due Diligence on suppliers, taking into account their commercial, reputational and professional reliability;
- that relations with suppliers are formalised in written contracts that identify, among other aspects:
  - the object of the assignment/performance and the persons who will perform the assignment/performance;
  - the agreed amount/compensation and its currency;
  - the current account to which/from which payment will be made as well as the terms for invoicing (or the method of collection/payment) and the terms of payment;
  - an undertaking by the supplier/consultant to comply with the applicable NIC national laws and procedures of the Non-Italian Company;

- a clause according to which suppliers commit to the performance of activities, to respecting the principles of the Code of Ethics also when it comes to the commitment not to make donations that exceed a modest value and that could be interpreted as exceeding the normal commercial or courtesy practices, or anyway aimed at acquiring preferential treatment in conducting activities;
- in the agreements with the Third Parties where Company's liability under environmental law may arise, specific and enforceable contractual penalties in case of breach, by a contractor or any of its subcontractors, of any applicable international or local legislation addressing the issue in question;

- during the execution of the contract:
  - the following control measures are envisaged: (i) periodic updates of the Due Diligence at a frequency to be determined according to the counterparty's level of risk and/or in the event of revision/amendment/renegotiation of the contract; (ii) monitoring of the proper performance of the contract;
  - refusal of requests by the counterparty for unjustified fee increases or discounts, for matters not related to changes in contractual conditions, advances not provided for in the contract;
  - consideration shall be paid only upon verification of the correspondence between the service received and the contractual provisions;
- the results of selection activities, due diligence, accounting documentation and documentation relating to contractual agreements with the supplier must be recorded and archived;
- the validity of the payments is verified by checking that the person receiving or paying amounts is the person named in the contractual documentation.

32. HUMAN RESOURCES

The Principles of Conduct referred to in this paragraph relate to the Human Resources process.

POSSIBLE RISK AREAS

(vii) Staff selection and recruitment
(viii) Staff incentive and salary review
(ix) Management of staff training and of relations with the P.A. for the purpose of obtaining training grants/funding
(x) Staff administration
(xi) Expense report management
(xii) Management of relations with Trade Unions

ABSTRACTLY CONFIGURED CRIMES

- Corruption between individuals
- Bribery of Public Officials
- Fraud against the Public Administration
- Organised crime, also of an international nature
- Money laundering, related crimes and terrorist financing
- Crimes against individuals
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

Within the NIC, the respect for and observance of all local laws and regulations and the procedures of the NIC concerning the recruitment and management of human resources must be ensured.

In particular, the following is provided for in each NIC:

- the prohibition to recruit or make promises to **recruit personnel** unless based on real and demonstrable business needs, using a process of **personnel selection** which involves at least two functions and is based on criteria of objectivity, competence and professionalism, avoiding any favouritism or conflict of interest, or any action that takes the form of favouritism, nepotism or forms of patronage suitable to influence the independence of a Public Official or induce him/her to ensure any advantage for the Non-Italian Company or for the Terna Group;
- the prohibition to **encourage** certain employees through promotions, money or other prizes not based on criteria of objectivity, competence and professionalism;

- grant that management **incentive** plans are adopted in a way to ensure that the objectives set thereto are such as not to lead to abusive behaviour and are focused on a well determined and measurable outcome;
- the clear segregation of the functions involved in personnel selection and recruitment activities;
- the formalisation and preservation in the company files of the candidates' evaluations;
- decisions regarding **staff salary review**, career advancement and salary increase, based on merit, skills, professionalism and experience;
- planning and provision of **training**, differentiated according to the levels and tasks carried out by individual employees;
- the company's ethics and compliance documentation, including the GCP, is made available to corporate officers by means of publication on the company intranet or parent company portals or by email or other means of sharing company documents, and each new employee is given (or indicated and made available in the manner identified above) the compliance documentation relevant to the NIC;
- new employees are made to sign a declaration of acknowledgement and commitment to the principles contained in the ethics and compliance documentation.
- with reference to **staff administration**, the proper preparation, recording and archiving of all documentation relating to the administrative management of the contractual relationship as well as the social security, insurance and tax treatment of personnel, in order to allow the reconstruction of the different stages of the process;
- in relation to reimbursement of **expenses**, proper documentation, including original receipts supporting the payment of the expenses or incurring the cost, needs to be submitted to the appropriate accounting department before payment. These reimbursements must then be accurately reported in the accounting records of the NIC;
- employees are required to report any situation that indicates or suggests a potential conflict of interest in their activities and any potential breach of the above policies and procedures;
- in the management of **relations with trade unions**, provision is made for the formalisation of meetings and, at least for the most significant cases, meetings and/or communications with such persons, as well as the adequate archiving of relevant documentation.

33. ADMINISTRATION, BUDGET AND TAXATION

The Principles of Conduct referred to in this paragraph relate to the Administration, Budget and Taxation process.

POSSIBLE RISK AREAS

(vi) Drafting of documents to be released to shareholders or to the public (e.g. financial statements, periodic financial reporting) regarding the assets and liabilities, revenues and expenses or cash flows of the Non-Italian Company, even if such documents are other than the periodical accounting ones;
(vii) Management of relationships with the external auditors;
(viii) Management of keep books, records and accounts (assets and liabilities);
(ix) Management of inter-company relations, with specific reference to the management of inter-company contracts;
(x) Management of tax requirements.

ABSTRACTLY CONFIGURED CRIMES

- Corruption between individuals
- Bribery of Public Officials
- Fraud against the Public Administration
- Corporate crimes
- Organised crime, also of a transnational nature
- Money laundering, related crimes and terrorist financing
- Tax crimes
- Market Abuse

KEY STANDARDS OF BEHAVIOUR

Non-Italian Companies are required to properly keep books, records and accounts, in a duly and accurate manner.

Personnel which have been assigned to **keep books, records and accounts** are required to properly act to ensure that:

a) the data and information used for the preparation of periodic financial reporting are accurate and diligently verified;

b) all balance items, whose determination and quantification entail discretional valuations, are objective and supported by appropriate documentation;
c) checks are envisaged, aimed at ascertaining the correct closure of economic/financial documents and, if anomalies are found in the accounting activities performed, provide for the obligation to report them to the competent units;
d) transactions are executed in accordance with the management's general or specific authorizations;
e) invoices and other relevant documentation related to the transactions are properly vetted, recorded and stored;
f) transactions are recorded as necessary to permit the preparation of financial statements in conformity with the applicable accounting principles or any other criteria applicable;
g) access to such transactions records is allowed only in accordance with management's general or specific authorizations.

Furthermore, the Non-Italian Companies are prevented to perform any conduct which impedes and, in any case, obstructs the **checking, supervisory and auditing activities** by the external auditors through the concealment of documentation or the use of other fraudulent means.

In each NIC, it is forbidden to:

- manage **taxation** in breach of the legislation in force;
- state, send for processing or include in **communications** false, artificial or incomplete data, or in any case data which does not correspond to the truth, regarding assets or the economic or financial position;
- enter into the **accounts** - or transmit for the processing and entering into financial statements, reports and prospectuses or other social communications - false or incomplete data or anyway data that do not correspond to the truth concerning assets or the economic and financial position;
- record in the accounts transactions at values that are incorrect with respect to the reference documentation, or with respect to transactions that do not exist in whole or in part, or without adequate supporting documentation to allow, firstly, a correct accounting entry and, subsequently, an accurate reconstruction.

Finally, Non-Italian Companies are required to make all **communications towards any public financial authority** (as provided for by the local applicable law) in a correct, complete, proper and expeditious manner, not preventing them, in any way, from performing their duties, even in the context of any inspection.

In relation to **intra-group relations**, activities must be governed by formalised service contracts. In addition, transactions with Terna Group companies must be assessed to ensure (a) the technical and economic convenience of the transaction, (b) that the economic amount of the services is measured at actual market

value, and (c) that the contractual relationship is substantially consistent with the business transactions actually carried out and their accounting representation.

34. MANAGEMENT OF CONFIDENTIAL AND PRIVILEGED INFORMATION

The Principles of Conduct referred to in this paragraph relate to the Confidential and Privileged Information Management process.

POSSIBLE RISK AREAS

(vi) Management of relations with investors, with financial analysts, the media and public information management in general;

(vii) Management of corporate content published on the company website and social media and organising events;

(viii) Management of corporate information concerning the NIC or other Terna Group companies, including Privileged Information and/or potentially privileged information, which is not in the public domain and which, due to its subject matter or other characteristics, is confidential to parties not bound by confidentiality obligations under current laws or contractual agreements identified by the procedure for managing, processing and communicating corporate information of Terna S.p.A. and its subsidiaries (LG005) as per section 5.1 (**Confidential Information**);

(ix) Management of privileged and/or potentially privileged information related to listed companies and, in particular, to listed companies belonging to the Terna Group and to the related financial instruments identified by the procedures for managing, processing and communicating corporate information of Terna S.p.A. and its subsidiaries (LG005) for keeping and updating registers of persons who have access to privileged and potentially privileged information (LG008) as per section 5.1 (**Privileged information**);

(x) Any kind of transactions relating to financial instruments in the NIC portfolio.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Market Abuse
- Crimes of Money Laundering, Related Crimes and Terrorist Financing
- Corporate crimes
- Organised crime, also of a transnational nature
- Tax crimes

KEY STANDARDS OF BEHAVIOUR

Management of Confidential Information and/or Privileged Information is guaranteed in compliance with the procedures applicable to the Terna Group regarding market abuse (LG005; LG008) as well as in compliance with relevant EU and local regulations.

The Corporate Representatives of the NIC:

- undertake not to express opinions, make statements or provide information to the media on behalf of the NIC or Terna Group companies outside the channels and methods established within the company, adopting all necessary caution so that the relative circulation within the company context can take place without prejudice to the confidential/privileged/potentially privileged nature of the information itself and according to the principle of the need to know and taking into account the guidelines as per LG005 and LG008;
- undertake to make sure that the organisation of corporate events dedicated to the media is regulated in such a way so as to avoid the offer of gifts or forms of entertainment that may affect the objectivity and independence of the media taking part;
- undertake to make sure the relationships between rating agencies and certification companies are limited to the exchange of information deemed necessary, based on the contractual provisions agreed, to perform the assignment, avoiding any conduct that could potentially affect their independence.

Corporate officers of the NIC are prohibited from:

- using privileged Information to carry out, either directly or indirectly, negotiation of financial instruments in order to obtain personal advantage or favour Third Parties or a Terna Group company;
- recommending or inducing anybody, on the basis of Inside Information, to perform transactions on financial instruments;
- disclosing Privileged Information to Third Parties, except when this is requested by a Public Authority or is set out in specific contracts according to which the counter-parts are obliged to use the information just for the originally intended purpose and to maintain its confidentiality;
- spreading false or misleading information (whether about the NIC/Terna Group company) through the media, the Internet, or else, in order to alter the market price of financial instruments;
- performing any transactions on financial instruments against the market abuse regulations envisaged by applicable laws;
- abusively accessing the company's computer or telematic system in order to alter and/or delete data or information;
- sending through a company computer system falsified or, in any way, altered information or data.

35. HEALTH, SAFETY AND ENVIRONMENT (HSE)

The Principles of Conduct in this paragraph refer to the Health, Safety and Environment ('HSE') process.

POSSIBLE RISK AREAS

(ii) Compliance with applicable health and safety and environmental laws and with the relative obligations;
(iii) Training of personnel on health and safety and environment;
(iv) Selection of Third Parties that are required to carry out specific activities that may have an impact on the environment (e.g. waste management and disposal) as well as Third Parties involved in the management of health and safety aspects in the workplace.

ABSTRACTLY CONFIGURED CRIMES

- Bribery of Public Officials
- Fraud against the Public Administration
- Corruption between individuals
- Organised crime, also of a transnational nature
- Environmental crimes
- Crimes concerning Health and Safety in the Workplace
- Crimes against Individuals

KEY STANDARDS OF BEHAVIOUR

A) Health and Safety in the Workplace

Regardless of the wideness of local legislation addressing health and safety in the workplace, NIC shall promote a strong culture of workplace safety protection, increasing awareness regarding risks and responsibilities of individual behaviours.

NICs shall always take into account the safety of workers, throughout any phase of the activity and shall commit to adopting all the measures which are deemed to be necessary to protect their workers' physical and moral integrity.

In particular, an NIC must:

k. consider the compliance to the provisions of law governing the health and safety of workers in the workplace as a priority and allocate the necessary economic resources to this purpose;
l. make the company organisation responsible in order to avoid prevention activities being considered the exclusive responsibility of certain individuals;

m. correctly identify health and safety requirements in the workplace from local laws and regulations;
n. as far as possible and allowed by the best techniques' evolution, evaluate the risks for workers with the aim of protection, also by adopting the most adequate and safe materials and equipment, in order to reduce the risk at the source;
o. commit to continuous improvement and prevention, correctly assessing those risks that cannot be avoided and mitigating them adequately through the implementation of appropriate individual and collective safety measures (e.g.: provide personal protective equipment appropriate to the tasks performed; equip the work area with a first aid kit);
p. disseminate information regarding health and safety in the workplace, up to date and specific with reference to the activity performed, ensuring that workers are properly instructed and trained;
q. ensure that workers are regularly involved in occupational health and safety issues and carry out appropriate monitoring activities to manage, rectify, inhibit behaviour in breach of the rules;
r. grant that management incentive plans are adopted in a way to ensure that the objectives set thereto are such as not to lead to abusive behaviour and are focused on a well determined and measurable outcome;
s. timely consider and analyse any non-compliance or improvement area emerged during the working activity or during inspections;
t. set the organization of the working activity in order to protect the integrity of workers, Third Parties and the community within which the NIC operates.

Furthermore, with particular reference to the **selection of Third Parties involved in managing workplace health and safety**, the NIC must ensure:

- the verification of the technical-professional suitability of the Third party;
- the stipulation of a contract that also provides for specific penalties applicable in the event of violation by a supplier or its subcontractor of any applicable international or local regulations on health and safety in the workplace;
- the management of security and risk analysis issues.

In order to keep a proper monitoring of the Areas at Risk, each Non-Italian Company assigns organizational, instrumental and economic resources to ensure, on the one hand, full compliance with the current provisions of law on accident prevention in the workplace and, on the other hand, the continuous improvement of health and safety in the workplace, also by means of implementing and updating the relevant preventive measures.

Company Representatives must cooperate in order to grant the full respect of the provisions of law, corporate procedures and of any other internal regulation aimed at protecting the safety and health of workers in the workplace.

B) Environment

The NIC shall consider the respect and protection of the environment as a priority and, in particular, it shall:

f. disseminate within the company information regarding environmental protection with reference to the activities performed, promoting awareness to such issue and ensuring that the activities are performed in compliance with relevant applicable legislation;

g. correctly identify the environmental requirements of local laws and regulations and assess the environmental risks associated with the main activities carried out;

h. adopt appropriate instruments to prevent corporate activities from causing any form of harm or damage to the ecosystem (e.g. due to incorrect waste disposal management or failure to respect local fauna) and carry out appropriate monitoring activities for the management, rectification, inhibition of conduct in breach of the rules;

i. grant that management incentive plans are adopted in a way to ensure that the objectives set thereto are such as not to lead to abusive behaviour and are focused on a well determined and measurable outcome;

j. work towards managing waste so as to recover, re-use and recycle the materials and guarantee a higher level of protection for human health and the environment.

Similarly to the above, when selecting Third parties involved in the management of environmental aspects, the NIC must ensure:

- the verification of the technical-professional suitability of the Third party;
- the stipulation of a contract that also provides for specific penalties applicable in the event of violation by a supplier or its subcontractor of any applicable international or local environmental regulations;
- the management of problems related to environmental issues.

36. INFORMATION & COMMUNICATIONS TECHNOLOGY ("ICT")

The Principles of Conduct in this paragraph refer to the Information & Communications Technology ("ICT") process.

POSSIBLE RISK AREAS

(ii) Management of company computer systems to ensure their operation and maintenance, the evolution of the technological and applicative IT platform, as well as information, physical and logical security; including:

a. management of the maintenance of the existing systems and management of data processing activities;
b. any company activity performed by using Intranet, Internet, the mail system or any other IT instruments;
c. management and protection of workstations, laptops, mobiles and storage devices;
d. planning of the measures to be adopted on transmission systems as well as security, classification and processing of information and data.

ABSTRACTLY CONFIGURED CRIMES

- Cybercrimes
- Bribery of Public Officials
- Corruption between individuals
- Fraud against the Public Administration
- Corporate crimes
- Tax crimes
- Organised crime, also of a transnational nature
- Copyright Crimes
- Market Abuse

KEY STANDARDS OF BEHAVIOUR

Each Company Representative shall refrain from incurring into (and the NIC shall ensure, through the implementation of proper organizational, technical and physical measures, the avoidance of) the following misconducts:

- the tampering or alteration of the NIC's computer system and/or IT documents;
- the illicit access of Third Parties to the computer systems;

- an improper use of IT credentials;
- the unlawful interference in any way with data, information or computer programmes;
- the unauthorised sharing of business information outside the company and the use of personal or unauthorised devices to transmit or store company information or data (e.g.: disclosing, handing over or sharing one's own access credentials to the company's or third parties' systems and corporate network; unauthorised access to third parties' computer systems);
- the exploitation of any flaws in the security measures of corporate IT system to gain access to the information without proper authorization;
- the installation of or changes to the software or databases or hardware without prior authorization;
- the use of unauthorized software or hardware that could be used to compromise the security of IT systems (such as software to identify the credentials, decrypt encrypted files, etc.);
- hide, render anonymous, or substitute one's own identity and send of e-mails reporting false information or intentionally send e-mails containing viruses or other programs that can damage or wiretap data;
- acquire and/or use products that are protected by copyright in violation of contract guarantees provided for the intellectual property rights of others;
- illegally access the NIC's website in order to illegally tamper with or alter any data contained therein or enter multimedia data or content (images, infographics, videos, etc.) in violation of copyright laws and applicable company procedures;
- leave computer equipment such as personal computers or smartphones unattended or unlocked when not in use;
- open suspicious e-mails or attachments received by e-mail or other means of communication. In that case, any suspicious communications should be reported to the relevant cybersecurity structure.

Non-Italian Companies must also ensure that backup copies are made of the computer data on the company servers in compliance with the information confidentiality criteria provided for by the relevant legislation, including company regulations.

NICs shall ensure a periodical monitoring, in compliance with local applicable law, on the activities performed on the corporate IT system by the personnel, in order to detect unusual behaviour and potential vulnerabilities in corporate systems.

Furthermore, the Non-Italian Companies shall increase, also through specific training sessions where needed, the personnel's awareness about the importance of a correct and proper use of the IT tools in their possession.

37. TRAINING FOR CORPORATE OFFICERS AND INFORMATION OF RECIPIENTS

TERNA's People Organization and Change ('**POC**') structure shall periodically organise mandatory training sessions for all Company Representatives (including newly-hired personnel) on the contents of the Global Compliance Program.

Training should be based on applicable regulations and best practices and the importance of GCP compliance. In this way, Company Representatives will be put in a position to clearly understand and be aware of the different crimes, the risks, the related personal and corporate responsibilities and the actions to be taken to prevent the commission of unlawful activities.

POC is responsible for:

(iv) planning and delivering training with the support of the PCR;

(v) ensuring that each Company Representative regularly attends training sessions; and

(vi) collecting attendance registration and copies of training materials and training dates.

Each Non-Italian Company is responsible for ensuring adequate training for Company Representatives and inform Recipients on their local Compliance Programmes and procedures.

Each Non-Italian Company may evaluate the organisation of specific training sessions for Company Representatives who are more directly involved in its Processes and related Risk Areas. The Non-Italian Company may in this case avail itself of the support of POC if specific intercompany service contracts exist in this regard. POC support may also be provided if TERNA assesses the training to be provided as necessary to comply with legal obligations.

The NIC shall ensure that the corporate ethics and compliance documentation, including the GCP, is made available to Company Representatives by means of publication on the corporate intranet or portals of the parent company or by e-mail or other means of sharing corporate documents, and that each new employee is given (or indicated and made available in the manner identified above) the compliance documentation relevant for the NIC.

Newly recruited staff will be made to sign a declaration of acknowledgement and commitment to the principles contained in the ethics and compliance documentation.

The principles and contents of the GCP that are applicable to Third Parties shall be made known through contractual documentation, which shall include clauses aimed at ensuring compliance by the Third Party with the Principles of Conduct identified by the GCP that are directly applicable to them. Where the NIC has adopted its own Local Compliance Programme, the contractual clauses shall also provide for compliance with the aforementioned programmes and applicable regulations.

Information and training activities are documented, monitored and evaluated in terms of adequacy and effectiveness.

38. WHISTLEBLOWING SYSTEM

38.1. Reporting system (whistleblowing)

Anyone can report unlawful acts and/or conduct, whether committed or omitted, that constitute breaches - or even suspected breaches - of the Rules of Conduct referred to in the GCP and in the Local Compliance Programmes of the principles sanctioned in the Code of Ethics,
of internal regulations represented by all the provisions, procedures, guidelines or operating instructions of the company receiving the Report, as well as violations of policies, company rules that could result in criminal crimes or, in any case, that could result in damage to the Group or individual Group companies.

Company Representatives have a duty to report any violation or alleged violation of the Principles of Conduct set out in the GCP and the Local Compliance Programmes adopted in the specific NIC set out in the relevant Country Annex.

Reports of violations of the GCP and the Local Compliance Programmes and their implementing acts adopted in the specific NIC reported in the relevant Country Annex must always be brought to the attention of the CO.

The Companies must set up a system for reporting violations and indicate its manager, explain the system, guarantee the confidentiality of the whistleblower's identity and of the contents of the report, unless when otherwise prescribed by Law, safeguard those making reports in good faith and in spirit of loyalty towards the company against retaliation or negative effects in relation to their professional positions; collect the reports, assess them according to the procedures provided and, in case of an ascertained violation, define any penalties proportionate to the severity of the violation.

The reporting procedure and the management of Whistleblowing reports are disciplined by LG054, which is also applicable to Non-Italian companies in compliance with local legislation and regulated by infra-group agreements.

b) Whistleblowing according to LG054

Should the NIC adhere to the reporting system set out by LG054, please bear in mind that the internal reporting channels are the following:

4. **IT portal**, accessible at https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione. (ITA/ENG)
5. **Ordinary Mail** to: Audit Manager c/o TERNA S.p.A., Viale Egidio Galbani, 70 – 00156 Rome, using the following wording "**whistleblowing report, confidential – do not open**".
6. **Face-to-face meeting**: the Whistleblower has the option of requesting a meeting with the Audit Manager to inform him/her directly of the subject of the report. This meeting is arranged by means of a request sent by the whistleblower via the Portal (https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione)

or by e-mail to whistleblowing@terna.it, specifying the name of the Terna Group company that is the subject of the report.

The applicable provisions of LG054 are those envisaged for ordinary reports, as the specific Italian provisions on the matter are not applicable.

The processing of data in accordance with the applicable Privacy Policy must be guaranteed, as well as the general prohibition on retaliation contemplated in the Code of Ethics, which expressly protects Reports made in good faith and in a spirit of loyalty to the company.

c) Non-Italian Company Whistleblowing

Should it be impossible for the NIC to adopt the whistleblowing regulation using internal reporting channels as per LG054, the NIC shall put in place - in line with local regulations - reporting procedures for Information on breaches that are consistent with the provisions of the Code of Ethics mentioned in paragraph 18-1 above referring to the protection of the Whistleblower and shall:

- notify Terna S.p.A., also via the CO, of the controls introduced or that will be introduced, which could involve the CO appointed in terms of the Global Compliance Program, as the Compliance program addressed to all NICs;
- ensure that adequate information is available regarding the reporting system for Information on breaches, the user procedures and protection system put in place.

In addition, the NIC must implement a suitable monitoring system for the preparation of an annual report to Terna S.p.A., also via the CO, concerning the reports received, featuring the following information:

- number of reports received;
- brief description of the area of reference of the report (e.g. Privacy; Cyber security; Corporate Governance; Health and safety; Human Resources; Sustainability; Tax; Procurement; Security), with specific evidence of the number of cases when discrimination or harassment has taken place (also for sustainability accounting purposes in accordance with GRI standards);
- number of reports managed;
- number of unfounded reports;
- number of founded reports; for which the type of activities promoted (e.g. information or training activities or in-depth or information activities on the territory concerning existing procedures, correction of internal processes, start of a disciplinary procedure, transfer of the results of assessment activities to the judicial authority, archiving due to lack of evidence) must be indicated separately.

In no case must the object and/or content of the reports received be shared with Terna S.p.A.

The report shall be addressed, in addition to the CEO/AU/Executive Director and CO, also to the Chief Risk Officer, the Internal Audit Manager and the Ethics Committee appointed by Terna.

The NIC must also identify the manager of the reporting channel in compliance of the applicable privacy rules and the person analysing and promoting the most appropriate measures based on the investigative findings as well as identify the management controls with its own provision/procedure, also updating the reminders in the local Compliance Programme and on the website where available.

****

With regard to roles and responsibilities, support may be requested in handling reports which fall under the responsibility of the Manager from the Compliance Officer appointed by the company concerned and/or external consultants.

38.2. Investigation

All the times a report is received, a procedure is activated to handle the report and monitor its prompt resolution. Such procedure is implemented and tracked by the subjects formally identified to manage the reports.

Following the report, Company Representatives are required to cooperate with the relevant investigation where involved. Failure to cooperate and provide honest, truthful information could result in disciplinary action.

On the basis of the findings, the most appropriate actions will be taken against the reporter, the reported person, as well as the most appropriate corrective actions with reference to the Processes concerned by the report.

39. MONITORING AND CONTINUOUS IMPROVEMENT

TERNA monitors the effective implementation of the GCP at the Terna Group level. To this end, the Corporate Liability and International Compliance structure is clearly identified at Terna Group level as being responsible for monitoring and continuously improving the GCP.

In particular, periodic auditing and testing activities are envisaged aimed at:

- ensuring the effectiveness of the GCP;
- intercepting possible violations;
- identifying any improvement or corrective actions at a structural level or within individual Processes, with a view to strengthening the Internal Control and Risk Management System.

Furthermore, the monitoring of the actual implementation of the GCP as supplemented by the relevant Country Annex by Non-Italian Companies is carried out by the appointed CO (see section *6*).

When in doubt about the interpretation, implementation, or compliance with any Area at Risk, General Standards of Control or Key Standard of Behaviour respectively, each Company Representative shall consult with the Corporate Liability and International Compliance structure in advance, using the dedicated e-mail address published on the TERNA website.

40. DISCIPLINARY SYSTEM AND CONTRACTUAL REMEDIES

Violations of laws on criminal or quasi-criminal liabilities of corporate entities can cause criminal, civil and regulatory penalties, including sanctions (fines and disqualification measures) and jail, as well as a damage to the Terna Group reputation.

The full effectiveness of the GCP and/or a related local policy, procedure or instruction or any other applicable Terna Group procedure, as well as of the Local Compliance Programmes, is guaranteed through the application of appropriate sanctions in the event of violation of the principles contained in the aforementioned documents.

In the event of violations committed by Company Representatives, the relevant disciplinary sanctions will be imposed by the individual Non-Italian Company, in accordance with the disciplinary system already in force and in line with the national collective bargaining agreement and the applicable local regulations on the matter, as well as on the basis of the Local Compliance Programmes.

In addition, Non-Italian Companies shall adopt appropriate sanctions in the event of (i) violation of local corporate liability regulations (where applicable); (ii) direct or indirect retaliatory or discriminatory acts against whistleblowers for reasons related to whistleblowing, as well as violation of whistleblower protection measures and malicious or grossly negligent reporting that proves to be unfounded.

Applicable disciplinary measures may include termination of employment and compensation for damages (see relevant Country Annexes).

The disciplinary measures shall be applied despite the results of any possible criminal procedure carried out by the relevant judicial authority.

In the event of violations by Third Parties, each Non-Italian Company shall take appropriate measures, including but not limited to termination of the contract.