Terna

LG054

Whistleblowing

24/03/2026

LINEE GUIDA

Approvato

F. Salerni (**SDS**)

Storia delle revisioni

Rev. 05 del 24/03/2026	*Sesta emissione, adeguamento normativo.*
Rev. 04 del 14/12/2023	*Quinta emissione.*
Rev. 03 del 12/07/2023	*Quarta emissione.*
Rev. 02 del 21/12/2018	*Terza emissione.*
Rev. 01 del 27/01/2017	*Seconda emissione.*
Rev. 00 del 30/09/2016	*Prima emissione.*

Sistemi di Gestione e/o Modelli Organizzativi di riferimento

	Sistemi di Gestione certificati/accreditati
☑	***SGQ*** *(Qualità)*
☑	***SGA*** *(Ambiente)*
☑	***SGSL*** *(Sicurezza e Salute sui luoghi di Lavoro)*
☑	***SGPIR*** *(Prev. Incidenti Rilevanti – Direttiva Seveso)*
☑	***SGSI*** *(Sicurezza delle Informazioni)*
☑	***SGE*** *(Energia consumata per usi propri)*
☑	***SGQ LST*** *(Laboratorio LST)*
☑	***SGQ TAR*** *(Centro di Taratura)*
☑	***SGAC*** *(Anticorruzione)*
☑	***SGAM*** *(Gestione Asset)*
☑	***SGPCI*** *(Prev. e Controllo Infezioni – Biosafety)*
☑	***SGC*** *(Compliance)*
☐	***SGPG*** *(Parità di Genere)*
☐	***SGPAC*** *(Processi Amministrativi e Contabili)*

	Modelli Organizzativi
☑	***BCM*** *(Business Continuity Model)*
☑	***TCM*** *(Tax Compliance Model)*
☑	***PRV*** *(Modello Privacy)*
☑	***M262*** *(Modello 262)*
☑	***M231*** *(Modello 231)*
☐	***MIMP*** *(Modello Imparzialità)*
☐	***SCIIS*** *(Sist. Controllo Informativa di Sostenibilità)*

(Per approfondimenti sui Sistemi di Gestione certificati/accreditati, clicca qui)

Indice

1. Generalità

Terna è da sempre particolarmente attenta alla prevenzione dei rischi che potrebbero compromettere la gestione responsabile e sostenibile del proprio *business* e, coerentemente con la propria missione e al proprio sistema di controllo interno, anche alla possibilità di conoscere le situazioni critiche e di correggerle consolidando il rapporto di fiducia con gli *stakeholder*.

Il Gruppo Terna, al fine di garantire una gestione responsabile ed in linea con le prescrizioni legislative, già dal settembre 2016 ha implementato e aggiornato un sistema per la ricezione e gestione delle segnalazioni di Violazioni di normative interne o esterne, a garanzia della correttezza e trasparenza nella conduzione degli affari e delle attività svolte e a tutela della posizione e immagine aziendale, che possano arrecare danno o pregiudizio all'azienda, come una frode, un rischio generico o una situazione potenzialmente pericolosa. Ciò ha garantito il mantenimento del sistema anche in *compliance* alle disposizioni normative intervenute nel 2017 prima, recanti "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*", e nel 2023 poi, con il D.Lgs. n. 24/2023 in materia di *whistleblowing*[1] recante "*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*" (di seguito anche il "**Decreto WB"** o "**D.Lgs. 24/2023**") e le Linee Guida emanate dall'Autorità Nazionale Anticorruzione ("**ANAC**") ai sensi dell'art. 10 del Decreto WB[2].

Tale sistema costituisce parte integrante dei presidi etici del Gruppo (Codice Etico) e di *corporate liability*, quali i Modelli di Organizzazione e Gestione ex D.lgs. 231/01 ("**Modelli 231**") e, per quanto applicabile alle società estere del Gruppo, del Global Compliance Program (LG058).

Il "whistleblowing" trova, quindi, una sua collocazione nell'ambito degli strumenti di controllo interno attraverso i quali Terna traccia le linee di condotta da tenere nello svolgimento del proprio *business*. Segnalare eventuali comportamenti disonesti che possano tradursi in frodi o che rappresentino un rischio di danno nei confronti di colleghi e di azionisti o che costituiscano atti di natura lesiva o illecita degli interessi e della reputazione stessa dell'azienda, può essere un'efficace forma di contrasto alla corruzione, se opportunamente regolamentata.

Con la presente Linea Guida, si intendono definire per il Gruppo Terna le modalità di gestione delle Segnalazioni di atti e/o comportamenti illeciti, commissivi o omissivi di cui si venga a conoscenza nell'ambito delle società del Gruppo, anche in conformità alla normativa vigente in materia e che costituiscono Violazioni, anche sospette:

(i) dei principi sanciti nel Codice Etico,

(ii) della normativa interna, rappresentata da tutte le disposizioni, procedure, linee guida o istruzioni operative della società destinataria della Segnalazione, tra cui anche il Modello di Organizzazione e

[1] *Whistleblowing* è il termine inglese che deriva dall'espressione metaforica "*to blow the whistle*" che veniva usata col significato di interrompere qualcosa bruscamente) è lo strumento che consente a chiunque di segnalare comportamenti illeciti, anche presunti.

[2] L'art. 10 del Decreto WB dispone che ANAC, sentito il Garante per la protezione dei dati personali, adotta, entro tre mesi dalla data di entrata in vigore del Decreto WB, le linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni esterne. L''ANAC ha pubblicato sul proprio sito internet la Delibera n. 311 del 12 luglio 2023 depositata presso la segreteria del Consiglio in data 13 luglio 2023 e pubblicata, tramite avviso in Gazzetta Ufficiale n. 172 del 25 luglio 2023 contenente le "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne*".
ANAC ha altresì pubblicato sul sito istituzionale la Delibera 301 del 12 luglio 2023, depositata presso la segreteria del Consiglio in data 13 luglio 2023 e in vigore dal 15 luglio 2023 come da comunicato pubblicato in Gazzetta Ufficiale in pari data e recante il "*Regolamento per la gestione delle segnalazioni esterne e per l'esercizio del potere sanzionatorio dell'ANAC in attuazione del Decreto Legislativo 10 marzo 2023, n. 24*".
ANAC, successivamente, ha pubblicato sul proprio sito internet le Delibere n. 478 e 479 del 26 novembre 2025, pubblicata nella Gazzetta Ufficiale n. 300 del 29 dicembre 2025, avente ad oggetto rispettivamente Linee guida in materia di whistleblowing sui canali interni ed esterni di segnalazione

Gestione ex D.lgs. 231/01 (il "**Modello 231**"), le linea-guida anticorruzione, il Global Compliance Program, nonché violazioni di policy, regole aziendali che possano tradursi in frodi o in un danno anche potenziale, nei confronti di colleghi, azionisti e *stakeholder* in generale o che costituiscano atti di natura lesiva o illecita degli interessi e della reputazione stessa dell'azienda e
(iii) le violazioni, previste dal D.Lgs. 24/2023, "*di disposizioni normative nazionali o della UE che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato*".
Nello specifico, si dà atto che il presente documento è stato redatto anche in conformità a quanto previsto dal Decreto WB che costituisce lo strumento legislativo in materia per contrastare e prevenire la corruzione, i comportamenti non conformi ai principi di buon andamento e imparzialità della Pubblica Amministrazione e la prevenzione di violazioni di legge nel settore pubblico e privato. Il Decreto WB, in particolare, ha introdotto un sistema integrato di regole destinato al settore pubblico e privato che coordina il diritto europeo e nazionale con l'obiettivo di incentivare le segnalazioni di illeciti che pregiudichino l'interesse pubblico o l'integrità dell'ente. Il nuovo regime innalza il livello di protezione di cui beneficiano i Segnalanti.

2. Scopo del documento

La presente Linea Guida ha lo scopo di disciplinare la gestione delle Segnalazioni di Violazioni (whistleblowing), di individuare e regolamentare i canali interni delle società del Gruppo attivati per le Segnalazioni e il relativo funzionamento, definire l'oggetto delle Segnalazioni e i soggetti che possono effettuarle, la competenza e le modalità di gestione delle attività di analisi e indagine conseguenti al ricevimento delle Segnalazioni (ruoli e responsabilità) e i relativi termini, le misure di tutela del Segnalante, le condizioni per l'effettuazione di Segnalazioni esterne e della Divulgazione pubblica, nonché le modalità e i termini di conservazione dei dati ai fini delle attività di gestione in ambito whistleblowing, anche nel rispetto della normativa privacy[3].
Sono inoltre disciplinate le modalità di divulgazione delle informazioni sull'utilizzo dei canali di segnalazione e dei presupposti per effettuare le Segnalazioni attraverso tali canali, sui soggetti competenti alla gestione delle Segnalazioni e le procedure di riferimento, le iniziative di sensibilizzazione e formazione del personale, nonché le modalità di aggiornamento delle linee guida stesse.

Si osserva, altresì, che la presente Linea Guida è stata redatta in conformità con le previsioni normative applicabili ad uno specifico perimetro di società italiane e di cui al Decreto WB e alle Linee Guida ANAC conseguenti[4], ove sono disciplinate specifiche condizioni e modalità in materia di whistleblowing, afferenti: all'ambito di applicazione; all'ambito oggettivo della protezione; ai canali di presentazione delle Segnalazioni e alle modalità di presentazione; alla tutela della riservatezza e da

[3] Il perimetro normativo privacy è composto dai seguenti provvedimenti nazionali e sovranazionali: Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*"; Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR); Decreto legislativo 30 giugno 2003, n. 196, "*Testo Unico sulla Privacy*" e successive modifiche e integrazioni e Provvedimenti collegati al Codice emessi dall'Autorità Garante in materia di Protezione dei Dati Personali.

[4] Si tratta delle Linee Guida ANAC come anche da ultimo aggiornate con Delibera n. 478 del 26 novembre 2025

eventuali Ritorsioni; alle limitazioni di responsabilità per chi segnala, denuncia o effettua Divulgazioni pubbliche ("**Segnalazioni rilevanti"**).
Pertanto, per le Segnalazioni che non rientrano nel suddetto perimetro normativo ("**Segnalazioni ordinarie"**), le seguenti previsioni trovano applicazione limitatamente: al contenuto minimo della Segnalazione (par. 6.2.1); ai canali interni di Segnalazione (par. 6.4); alla gestione delle Segnalazioni (par. 6.5), fatta eccezione per i riscontri e le tempistiche previste dal Decreto WB; alla gestione dei potenziali conflitti d'interesse (par. 6.6).
È in ogni caso garantito anche per le Segnalazioni ordinarie 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.

3. Ambito di applicazione

La presente Linea Guida si applica a Terna e a tutte le società del Gruppo Terna, comprese le società controllate estere, fermo quanto previsto al successivo par. 7[5].

4. Riferimenti

4.1 Riferimenti esterni

- 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 e ss. mm. ii.;
- Legge 30 novembre 2017, n. 179 e s.m.i., "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"[6];
- Legge 6 novembre 2012, n. 190 e s.m.i, "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- Decreto Legislativo 8 giugno 2001, n. 231 e s.m.i. (o **D.Lgs. 231/01**), "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";

[5] Le disposizioni del D.Lgs. n. 24/2023 richiamate nell'ambito delle presenti Linee Guida si applicano, ai sensi dell'art. 24, comma 2 del Decreto WB, solo dal 17 dicembre 2023 alle società del Gruppo Terna che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove. Ai sensi del verbale del CdA della Fondazione Terna del 17 dicembre 2025, le disposizioni della presente Linea Guida trovano applicazione, in quanto applicabili, a Fondazione Terna.

[6] L'applicazione di tale legge è limitata alle sole società del Gruppo che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove, in quanto l'obbligo di istituzione del canale interno di cui al D.Lgs. n. 24/2023 ha effetto a decorrere dal 17 dicembre 2023, ai sensi dell'art. 24, comma 2 del Decreto WB.

- Decreto legislativo 30 giugno 2003, n. 196, “Testo Unico sulla Privacy” e s.m.i. e Provvedimenti collegati emessi dall’Autorità Garante in materia di Protezione dei Dati Personali;
- Regolamento Europeo 2016/679 (o “**GDPR**”): relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) e ai Provvedimenti dell’Autorità Garante in materia di protezione dei dati personali;
- Decreto Legislativo 10 agosto 2018, n. 101 e s.m.i., recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Decreto Legislativo 18 maggio 2018, n. 51, recante attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio e s.m.i.;
- Linee guida in materia di valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment o “**DPIA**”) e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento 2016/679/UE (Working Party 248 rev. 01);
- Linee Guida emanate dall’ANAC ai sensi dell’art. 10 del Decreto WB in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne pubblicate sul sito istituzionale dell’ANAC;
- Regolamento ANAC per la gestione delle segnalazioni esterne e per l’esercizio del potere sanzionatorio dell’ANAC in attuazione del D.Lgs 24/2023 pubblicato sul sito istituzionale dell’ANAC;
- 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.

4.2 Normativa interna

- Codice Etico;
- Modello di organizzazione e gestione ex D.lgs. 8 giugno 2001 n. 231 di TERNA S.p.A. e delle società controllate;
- LG014 - Regolamento del Comitato Etico;
- LG050 - L’adozione del Codice Etico nelle società del Gruppo Terna
- LG018 - Information Security Policy Indirizzi strategici;
- LG039 - La disciplina della Privacy in Terna;
- LG058 - Global Compliance Program;
- LG059 - Linee Guida Anticorruzione;
- IO009SER - Gestione del servizio di Protocollo Informatico;

- PL02 - Politica del Sistema di Gestione Integrato del Gruppo Terna;
- IO202SG - Gestione delle attività di compliance ai sensi della norma UNI ISO 37301:2021

5. Definizioni e abbreviazioni

In aggiunta ai termini ed alle espressioni definiti in altri paragrafi della presente Linea Guida (o nei documenti ad essa allegati), ai fini della stessa, i termini e le espressioni qui di seguito elencati hanno il significato indicato a fianco di ciascuno di essi.

- **Amministratore del sistema**: soggetto che ha tutte le funzionalità del Whistle Editor e che, a differenza di quest'ultimo, gestisce anche le abilitazioni degli utenti interni.
- **Altri soggetti**: i soggetti di cui al par. 6.1.2 della presente Linea Guida e individuati dall'art. 3, comma 5, del D.Lgs. n. 24/2023.
- **Audit** (o **AU**)**:** la Direzione Audit di Terna nell'ambito della quale è svolta l'istruttoria che segue alla Segnalazione e ne comunica l'esito al Comitato Etico tramite Portale.
- **CISO:** il Chief Information Security Officer.
- **Codice Etico:** documento contenente principi positivi e di regole di comportamento volontariamente adottati nell'ambito del Gruppo Terna e resi pubblici come concreta espressione dei propositi esposti verso i soggetti con cui il Gruppo entra in contatto.
- **Comitato Etico:** l'organo aziendale competente per la gestione delle Segnalazioni ricevute al fine di darvi seguito. I componenti, nominati dall'Amministratore Delegato di Terna S.p.A., vengono scelti per rappresentare un punto di vista eterogeneo e un equilibrio tra le diverse società del Gruppo, funzioni e ruoli aziendali.
- **Compliance Officer** (o **CO**): soggetto individuato, ai sensi della LG058, in ciascuna società estera del Gruppo avente il compito di favorire, nell'ambito della stessa, la diffusione della conoscenza del Global Compliance Program e/o dei Compliance Program Locali previsti nell'Allegato Paese di riferimento e degli indirizzi della Capogruppo, nonché agevolarne il funzionamento attraverso attività di formazione, informazione e attraverso l'implementazione di appositi flussi informativi.
- **Contesto lavorativo**: si intendono le attività lavorative o professionali, presenti o passate svolte dal Segnalante per Terna o per la diversa società del Gruppo destinataria della Segnalazione, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce Informazioni sulle Violazioni e nel cui ambito potrebbe rischiare di subire Ritorsioni in caso di Segnalazione;
- **Disciplina Privacy**: si fa riferimento con tale definizione alla vigente normativa privacy in materia di protezione dei dati personali, per tale intendendosi il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, il D.Lgs. n. 196/2003, il D.Lgs. n. 101 del 2018 nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile, ivi compresi i provvedimenti del Garante per la protezione dei dati personali.
- **Divulgazione pubblica** o **divulgare pubblicamente**: rendere di pubblico dominio Informazioni sulle Violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone nei casi previsti dal D.Lgs. n. 24/2023.
- **ITD-ESP:** struttura Enterprise Services and Platforms nell'ambito di IT & Digitale.

- **Facilitatore**: persona fisica che fornisce assistenza al Segnalante per l'effettuazione della Segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata ai sensi del D.Lgs. n. 24/2023.
- **Gestore della segnalazione** o **Gestore**: i soggetti, individuati dalla società, competenti per la gestione delle Segnalazioni come disciplinata al par. 6.5 della presente Linea Guida, nel rispetto dei principi di autonomia, imparzialità e indipendenza.
- **Informazioni sulle violazioni**: informazioni, compresi i fondati sospetti, riguardanti Violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico nell'ambito del contesto lavorativo, nonché gli elementi riguardanti condotte volte ad occultare tali Violazioni. Non sono ricomprese tra le Informazioni sulle violazioni segnalabili o denunciabili le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla sola base di indiscrezioni o vociferazioni scarsamente attendibili (cd. voci di corridoio).
- **Organismo di Vigilanza** o **OdV**: l'organismo, dotato di autonomi poteri di iniziativa e di controllo, istituito dalla società ai sensi del D.lgs. 231/01 e preposto alla vigilanza sul funzionamento e sull'osservanza del Modello 231 nonché al relativo aggiornamento. **Owner:** dipendente della Direzione Audit debitamente autorizzato e formato cui è assegnato il processo di verifica della Segnalazione come indicato al par. 6.5.
- **PCE:** il Presidente del Comitato Etico.
- **Persona coinvolta**: la persona fisica o giuridica menzionata nella Segnalazione interna o esterna ovvero nella Divulgazione pubblica come persona alla quale la Violazione è attribuita o come persona comunque implicata nella Violazione segnalata o Divulgata pubblicamente.
- **RU**: la Direzione Risorse Umane di Terna.
- **Portale informatico** o **Portale:** è lo strumento informatico *web-based* specificatamente predisposto per le Segnalazioni, in forma scritta e in forma orale, delle Violazioni per le società del Gruppo accessibile all'indirizzo https://whistleblowing.terna.it/ e nell'ambito del quale sono istituiti gli appositi canali dedicati alle società del Gruppo anche ai sensi del Decreto WB.
- **Referente per la segnalazione** o **Referente:** il soggetto designato dalla Società controllata rilevante che viene coinvolto dal Gestore nel caso in cui la Segnalazione sia attinente a detta società come previsto al par. 6.5 della presente Linea Guida.
- **Repository:** rappresenta il *data base* predisposto per ciascun canale interno istituito sul Portale informatico e preposto all'archiviazione di tutte le Segnalazioni pervenute, a prescindere dalle modalità adottate per la Segnalazione.
- **Responsabile Audit** o **RIA:** il Direttore Audit di Terna.
- **Ritorsione**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione, della denuncia all'autorità giudiziaria o contabile o della Divulgazione pubblica e che provoca o può provocare al Segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto da intendersi come danno ingiustificato. In particolare, secondo quanto disposto dall'art. 17 comma 4 del

D.Lgs. 24/2023 e dalle Linee Guida ANAC, costituiscono ritorsioni a titolo meramente esemplificativo:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di demerito o referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.
- possono costituire ritorsioni, ad esempio, anche la pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati; una valutazione della performance artatamente negativa; una revoca ingiustificata di incarichi; un ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto; il reiterato rigetto di richieste (ad es. ferie, congedi); la sospensione ingiustificata di brevetti, licenze, etc..
- Rientrano inoltre nella nozione di "ritorsione", ai fini delle presenti Linee Guida, anche ogni ostacolo o tentativo di ostacolo alla Segnalazione.

- **Riscontro**: comunicazione al Segnalante di informazioni relative al Seguito che viene dato o che si intende dare alla Segnalazione anche ai sensi del D.Lgs. n. 24/2023.
- **SE** o **società estera**: società non italiana/e del Gruppo Terna.
- **Segnalante**: la persona fisica che effettua la Segnalazione di Informazioni sulle Violazioni acquisite nell'ambito del contesto lavorativo di Terna o della diversa società del Gruppo destinataria della Segnalazione.
- **Segnalato**: la persona fisica o giuridica menzionata nella Segnalazione come persona alla quale la Violazione è attribuita o come persona comunque coinvolta nella Violazione segnalata.
- **Segnalazione**: la comunicazione scritta od orale di Informazioni sulle Violazioni.

- **Segnalazione esterna**: la comunicazione, scritta od orale, delle Informazioni sulle Violazioni nei casi previsti dal D.Lgs. n. 24/2023, presentata tramite il canale di segnalazione esterna istituito da ANAC.
- **Segnalazione interna**: la comunicazione, scritta od orale, delle Informazioni sulle Violazioni, presentata tramite i canali interni per le Segnalazioni istituiti per la società del Gruppo Terna destinataria della Segnalazione.
- **Seguito**: l'azione intrapresa dal Gestore per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.
- **Sistema Disciplinare**: il sistema disciplinare vigente in ambito aziendale, illustrato all'interno dei Modelli 231 o, per le SE, previsto nell'ambito del Global Compliance Program come adottato in ciascuna SE. Le misure disciplinari e le relative sanzioni, ove adottabili in relazione ai soggetti destinatari delle stesse, sono individuate dalla società sulla base dei principi di proporzionalità e adeguatezza, in relazione alla idoneità a svolgere una funzione deterrente e, successivamente, sanzionatoria, nonché tenendo conto delle diverse qualifiche dei soggetti cui esse si applicano.
- **Società controllate non rilevanti:** per tali società si intendono le società del Gruppo Terna con meno di duecentoquarantanove dipendenti ai sensi dell'art. 4, comma 4, D.Lgs. n. 24/2023 aventi sede in Italia e, ai fini delle presenti Linee Guida, anche le società estere.
- **Società controllate rilevanti:** per tali società si intendono le società del Gruppo Terna con più di duecentoquarantanove dipendenti ai sensi dell'art. 4, comma 4, D.Lgs. n. 24/2023 e aventi sede in Italia.
- **Violazioni**: atti e/o comportamenti illeciti, commissivi o omissivi che costituiscono violazioni, anche sospette, 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 tra cui anche il Modello 231, le linea-guida anticorruzione, il Global Compliance Program, nonché violazioni di policy, regole aziendali che possano tradursi in frodi o in un danno anche potenziale, nei confronti di colleghi, azionisti e stakeholder in generale o che costituiscano atti di natura lesiva o illecita degli interessi e della reputazione stessa dell'azienda e le violazioni, previste dal Decreto WB, "*di disposizioni normative nazionali o della UE che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato*";
- **Whistle Editor:** soggetto individuato dal RIA nell'ambito Audit e tra quelli inseriti tra gli utenti del portale, per l'inserimento al Portale delle Segnalazioni pervenute fuori portale. Aggiorna le informazioni riportate nelle varie sezioni del Portale per le utilità diverse: disclaimer, Frequently Asked Questions (FAQ), liste valori, gestione tipologiche, …).

6. Condizioni, modalità di effettuazione delle Segnalazioni e tutele connesse

6.1 Ambito soggettivo

Secondo quanto previsto dal Codice Etico, ciascuna società del Gruppo Terna offre ai Segnalanti la massima riservatezza e tutela, per chi effettua Segnalazioni in buona fede e con uno spirito di lealtà nei confronti dell'azienda, da Ritorsioni o effetti negativi sulla sua posizione professionale, sanzionando chi commette atti ritorsivi.

Con riferimento invece al sistema di tutele previsto dalla presente Linee Guida ai sensi del Decreto WB è opportuno distinguere due categorie di soggetti:

- il "***Segnalante**;*
- gli "***Altri soggetti**"*.

6.1.1 Segnalanti

La Segnalazione di una Violazione può essere trasmessa da "chiunque".
Con specifico riferimento invece alle previsioni del Decreto WB e alle tutele connesse, possono effettuare una Segnalazione tutti coloro che operano nel "*contesto lavorativo*" di Terna o della diversa società del Gruppo destinataria della Segnalazione in qualità di:

- lavoratori subordinati di una delle società appartenenti al Gruppo;
- lavoratori autonomi che svolgono la propria attività lavorativa presso una delle società del Gruppo;
- coloro che hanno un rapporto di collaborazione professionale con l'ente (es. fornitori), liberi professionisti (es. avvocati, commercialisti, notai etc.) e i consulenti che prestano la propria attività presso una delle società del Gruppo;
- volontari e i tirocinanti, retribuiti e non retribuiti che svolgono la propria attività presso una delle società del Gruppo;
- azionisti, da intendersi come le persone fisiche che detengono azioni in uno dei soggetti del settore pubblico, ove questi ultimi assumano veste societaria, es. società in controllo pubblico, società in house, società cooperativa etc. Si tratta di coloro che siano venuti a conoscenza di violazioni oggetto di segnalazione nell'esercizio dei diritti di cui sono titolari in ragione del loro ruolo di azionisti rivestito nella società;persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso una delle società del Gruppo.

Possono altresì effettuare Segnalazioni coloro che:

- segnalino informazioni acquisite nell'ambito di un rapporto di lavoro con il Gruppo Terna nel frattempo terminato purché le Informazioni sulle Violazioni siano state acquisite prima dello scioglimento del rapporto stesso;
- segnalino informazioni acquisite nel caso in cui il rapporto di lavoro non è ancora iniziato laddove le informazioni riguardanti una Violazione siano state acquisite durante il processo di selezione o altre fasi delle trattative precontrattuali;
- segnalino informazioni acquisite durante lo svolgimento del periodo di prova presso una delle società del Gruppo.

6.1.2 Altri soggetti

Nella categoria degli "Altri soggetti" meritevoli di protezione nel caso di Segnalazioni ai sensi del Decreto WB, rientrano, invece:

- i Facilitatori;
- le persone del medesimo contesto lavorativo del Segnalante e che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado;

- i colleghi di lavoro del Segnalante e che lavorano nel medesimo contesto lavorativo dello stesso e che hanno con detto soggetto un rapporto abituale e corrente[7];
- gli enti di proprietà del Segnalante o per i quali lo stesso lavora, nonché gli enti che operano nel medesimo contesto lavorativo.

6.2 Oggetto della Segnalazione

Possono essere segnalate tutte le Violazioni. Con specifico riferimento invece alle previsioni del Decreto WB, sono considerate Segnalazioni rilevanti (che consentono cioè, l'applicazione delle misure di tutela indicate nel successivo paragrafo 6.3) le Segnalazioni di Violazioni relative a tutti quei comportamenti, atti od omissioni che siano idonei a ledere l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato.

In particolare, è possibile distinguere tre categorie[8]:

1. ***Violazioni di disposizioni nazionali ed europee che consistono in illeciti riguardanti i seguenti settori***: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità del prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
2. ***Violazioni di disposizioni europee*** che consistono in: i) atti od omissioni che ledono gli interessi finanziari dell'Unione; ii) atti ed omissioni riguardanti il mercato interno[9]; iii) atti e comportamenti che vanificano l'oggetto o la finalità delle disposizioni degli atti dell'Unione nei settori sopra richiamati, iv) Violazioni delle misure restrittive dell'Unione Europea di cui al capo I-bis, del titolo I, del libro II del codice penale, nonché dell'articolo 12, comma 1-bis, del d.lgs. n. 25 luglio 1998, n. 286 in «*Attuazione della direttiva (UE) 2024/1226 del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673*»; (v) violazioni del Regolamento (UE) n. 2024/1689 (c.d. AI Act)[10].
3. ***Violazioni di disposizioni nazionali*** che consistono in: i) illeciti amministrativi, contabili, civili o penali; ii) condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o violazioni dei Modelli 231. Tali illeciti e condotte non devono rientrare nelle categorie dei precedenti punti 1. e 2.

6.2.1 Contenuto minimo della Segnalazione

La Segnalazione deve avere i seguenti elementi essenziali di seguito riportati.

---

[7] "*Nel caso di colleghi di lavoro, il legislatore ha previsto che si tratti di coloro che, al momento della segnalazione, lavorano con il segnalante (esclusi quindi gli ex colleghi) e che abbiano con quest'ultimo un rapporto abituale e corrente. La norma si riferisce, quindi, a rapporti che non siano meramente sporadici, occasionali, episodici ed eccezionali ma attuali, protratti nel tempo, connotati da una certa continuità tali da determinare un rapporto di "comunanza", di amicizia*.", così le Linee Guida ANAC approvate con Delibera ANAC 311 del 12/7/2023 pag. 22.

[8] Ai sensi del Decreto WB, rispetto alle suddette categorie di Violazioni, occorre distinguere a seconda che: (i) l'ente sia concessionario di pubblico di servizio (o comunque l'ente che opera in tale ambito), nel qual caso trovano applicazione tutte le categorie di Violazioni; (ii) abbia più di 50 dipendenti e abbia adottato un Modello 231, nel qual caso trovano applicazione la categoria di Violazioni di disposizioni europee e condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o Violazioni del Modello 231; (iii) abbia meno di 50 dipendenti ma abbia adottato un Modello 231, nel qual caso potranno essere segnalate le Violazioni condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o Violazioni del Modello 231.

[9] Rientrano in tale ambito tutte le Violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le Violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società.

[10] Ai sensi dell'art. 113 Regolamento (UE) 2024/1689, l'art. 87 – che prevede l'applicazione della Direttiva (UE) 2019/1937 alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni – si applica a decorrere dal 2 agosto 2026.

- **Segnalante**: la Segnalazione deve contenere i riferimenti identificativi del soggetto autore della Segnalazione[11]. Le Segnalazioni devono essere rese in buona fede e non in forma anonima.
- **Oggetto**: una chiara descrizione dei fatti oggetto di Segnalazione, con indicazione delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti nonché delle modalità attraverso cui il Segnalante è venuto a conoscenza dei fatti.
- **Segnalato e Persone coinvolte**: le generalità o qualsiasi elemento (come la funzione/ruolo aziendale) che consenta un'agevole identificazione del/i presunto/i autore/i del comportamento illecito e delle Persone coinvolte.
- **Società del Gruppo**: la Segnalazione dovrà riportare l'indicazione relativa a quale società del Gruppo è riferita la Segnalazione nel caso in cui la Segnalazione sia effettuata in un canale condiviso tra più società del Gruppo.

Le Segnalazioni verranno esaminate laddove ammissibili, non manifestamente infondate, circostanziate e contenenti elementi utili per la ricostruzione e l'accertamento delle Violazioni. Resta salva la facoltà del Comitato Etico di valutare la Segnalazione alla luce del caso concreto e della sussistenza di elementi idonei a consentire la successiva attività istruttoria.

Inoltre, il Segnalante potrà fornire i seguenti ulteriori elementi:

- l'indicazione di **eventuali altre persone** che possono riferire sui fatti oggetto della Segnalazione;
- **l'invio di eventuali documenti** che possono confermare la fondatezza di tali fatti;
- **ogni altra informazione** che possa agevolare la raccolta di evidenze su quanto segnalato.

Il Segnalante potrà, inoltre, fornire eventuale documentazione utile a meglio circostanziare la Segnalazione.
Infine, per agevolare la corretta individuazione delle altre persone coinvolte di cui al par. 6.1.2 della presente Linea Guida e individuate dall'art. 3 del D.Lgs. n. 24/2023 alle quali garantire la riservatezza e le tutele agli stessi accordate e indicate al successivo par. 6.3, è opportuno che il Segnalante indichi esplicitamente l'esistenza di tali soggetti, specificando la sussistenza dei relativi presupposti.

6.2.2 Limitazioni dell'oggetto della Segnalazione

Esulano dal perimetro di applicazione del Decreto WB (e non consentono, pertanto, l'applicazione delle misure di tutela indicate nel successivo paragrafo 6.3) le:

- rivendicazioni, contestazioni, richieste di carattere personale del Segnalante o della persona che abbia sporto una denuncia all'autorità giudiziaria o contabile, relative esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate[12];
- Segnalazioni di Violazioni che sono già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali riguardanti servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente o

[11] Da intendersi come i dati personali idonei a consentire, in via dedicata e riservata, l'interlocuzione tra la Società e il Segnalante e l'invio dei feedback in merito al Seguito della Segnalazione.
[12] "*Sono quindi, escluse, ad esempio, le segnalazioni riguardanti vertenze di lavoro e fasi precontenziose, discriminazioni tra colleghi, conflitti interpersonali tra la persona segnalante e un altro lavoratore o con i superiori gerarchici, segnalazioni relative a trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di lesioni dell'interesse pubblico o dell'integrità dell'amministrazione pubblica o dell'ente privato*", così le Linee Guida ANAC approvate con Delibera ANAC 311 del 12/7/2023 pag. 28.

da quelli nazionali che costituiscono attuazione degli atti dell'Unione[13], e alle Segnalazioni di Violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea;

- Segnalazioni anonime, essendo la presente Linea Guida preordinata a tutelare il Segnalante da rischi di Ritorsioni.

Quanto alle Segnalazioni anonime si ricorda che le tutele di cui al paragrafo 6.3 possono trovare applicazione qualora a seguito di una Segnalazione anonima venga svelato il nome del Segnalante. La massima tutela di riservatezza offerta ai Segnalanti anche nel caso delle Segnalazioni ordinarie richiede che anche le stesse non siano effettuate in forma anonima.

Si ricorda inoltre che, ai sensi dell'art. 1, comma 3, del Decreto WB, esulano dall'ambito di applicazione delle tutele previste dallo stesso Decreto WB e della presente Linea Guida, le Segnalazioni aventi ad oggetto le seguenti materie: a) informazioni classificate; b) segreto professionale forense e medico; c) segretezza delle deliberazioni degli organi giurisdizionali.

Le Segnalazioni non devono assumere toni ingiuriosi o contenere offese personali o giudizi volti a offendere o ledere l'onore e/o il decoro personale e/o professionale della persona a cui i fatti segnalati sono riferiti.
È vietato in tutti i casi:

- l'invio di Segnalazioni con finalità puramente diffamatorie e calunniose;
- l'invio di Segnalazioni che attengano esclusivamente ad aspetti della vita privata, senza alcun collegamento diretto o indiretto con l'attività aziendale/professionale del Segnalato;
- l'invio di Segnalazioni aventi ad oggetto contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale del Segnalante;
- l'invio di Segnalazioni di natura discriminatoria, in quanto riferite a orientamenti sessuali, religiosi e politici o all'origine etnica del Segnalato;
- l'invio di Segnalazioni effettuate con l'unico scopo di danneggiare il Segnalato.

Potranno essere comminate azioni disciplinari a tutti i dipendenti del Gruppo che presentino Segnalazioni di questo tipo. Inoltre, potrà essere sanzionato il Segnalante che ha effettuato la Segnalazione con dolo o colpa grave, qualora la Segnalazione si rilevi infondata.

6.3 Tutele del Segnalante

L'istituto del whistleblowing può riscontrare una certa diffidenza nell'applicazione, a causa del timore del potenziale Segnalante di non essere adeguatamente protetto dal rischio di Ritorsioni o discriminazioni sul lavoro proprio a causa delle Segnalazioni. Terna e le società del Gruppo tutelano la riservatezza e proteggono il Segnalante dalle misure ritorsive secondo quanto riportato al precedente par. 2.

[13] Indicati nella parte II dell'allegato alla direttiva (UE) 2019/193725.
"Si pensi ad esempio, alle procedure di segnalazione in materia di abusi di mercato di cui al Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio alla direttiva di esecuzione (UE) 2015/2392 della Commissione adottata sulla base del suddetto regolamento, che contengono già disposizioni dettagliate sulla protezione degli informatori", così le Linee Guida ANAC approvate con Delibera ANAC 311 del 12/7/2023 pag. 28.

Con particolare riferimento al Decreto WB, sono adottate misure a tutela della riservatezza dell'identità del Segnalante sia in fase di ricezione sia in quella della gestione della Segnalazione attraverso l'utilizzo dei canali interni di Segnalazione appositamente istituiti.
A tal proposito, occorre distinguere il concetto di "riservatezza" da quello di "anonimato", in quanto il primo presuppone la conoscenza dell'identità del Segnalante, necessaria al fine di poter assicurare una tutela adeguata. L'anonimato, infatti, potrebbe ostacolare l'accertamento sulla fondatezza della denuncia.
Sono inoltre adottate idonee misure in modo da garantire i Segnalanti contro qualsiasi forma di Ritorsione, discriminazione o penalizzazione connesse alla Segnalazione e, tenendo conto delle condizioni e dei requisiti previsti dal Decreto WB, tali misure sono adottate anche al fine di tutelare le altre persone coinvolte di cui al par. 6.1.2 della presente Linea Guida e individuate dall'art. 3 del D.Lgs. n. 24/2023, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle persone coinvolte.
Tali garanzie consistono da un lato, nel divieto di Ritorsioni per le Segnalazioni effettuate posto in capo alla società, e dall'altro, nel regime di nullità degli atti ritorsivi eventualmente subiti in violazione di tale divieto[14].
Per beneficiare del regime di protezione previsto dal Decreto WB, devono sussistere alcune condizioni:

- che il Segnalante sia un soggetto compreso nell'elenco di cui all'articolo 3 del D.Lgs. n. 24/2023 (come indicato al precedente par. 6.1.1);
- che le Informazioni sulle Violazioni segnalate rientrino nell'ambito oggettivo previsto dal D.Lgs. n. 24/2023 e riportato al precedente par. 6.2;
- che il Segnalante al momento della Segnalazione o della denuncia all'autorità giudiziaria o contabile o della Divulgazione pubblica avesse "fondato motivo" di ritenere veritiere le informazioni[15];
- che la Segnalazione sia effettuata secondo le procedure previste dai canali interni (istituiti ai sensi della presente Linea Guida come riportato al successivo par. 6.4) o esterni (gestiti da ANAC come riportato al successivo par. 6.9) o secondo quanto previsto per la Divulgazione pubblica ai sensi dell'art. 15 del Decreto WB (e riportato al successivo par. 6.10).

Costituisce motivo di applicazione dei provvedimenti sanzionatori previsti dal Sistema Disciplinare, la violazione delle misure di tutela rispettivamente apprestate in favore del Segnalante e degli Altri soggetti di cui al par. 6.1.2 della presente Linea Guida e individuate dall'art. 3, comma 5, del D.Lgs. n. 24/2023. In particolare, sono sanzionabili disciplinarmente, secondo quanto previsto dal D.Lgs. n. 24/2023:

- i comportamenti ritorsivi in violazione dell'art. 17 D.Lgs. n. 24/2023, ossia i comportamenti, atti od omissioni anche solo tentati o minacciati posti in essere in ragione della Segnalazione e che possono provocare al Segnalante in via diretta o indiretta un danno ingiusto;
- le condotte idonee ad ostacolare la Segnalazione;
- le violazioni delle misure di tutela del Segnalante con riferimento all'obbligo di riservatezza.

La riservatezza del Segnalante non è garantita quando:

[14] Le eventuali Ritorsioni, ai sensi dell'art. 19 del Decreto WB, possono essere comunicate ad ANAC per gli accertamenti di competenza sulle stesse.

[15] Sulla base di circostanze concrete allegabili e informazioni acquisibili e, quindi, non su semplici illazioni.

- vi è il consenso espresso del Segnalante alla rivelazione della sua identità;
- è stata accertata con sentenza di primo grado la responsabilità penale e/o civile del Segnalante per reati di calunnia o diffamazione o comunque per reati commessi con la Segnalazione;
- l'anonimato non è opponibile per legge se l'identità del Segnalante è richiesta dall'autorità giudiziaria in relazione a indagini (penali, tributarie o amministrative) o ispezioni di Organi di Controllo originatisi a seguito della Segnalazione stessa.

6.3.1 Limitazioni della tutela del Segnalante e tutela del Segnalato

Il Decreto WB ammette dei casi in cui il Segnalante non ha diritto di tutela:

- qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale del Segnalante per i reati di diffamazione o di calunnia o nel caso in cui tali reati siano commessi con la denuncia all'autorità giudiziaria o contabile;
- in caso di responsabilità civile per lo stesso titolo per dolo o colpa grave.

In entrambe le ipotesi al Segnalante o denunciante verrà irrogata una sanzione disciplinare.
Non è, peraltro, esclusa la responsabilità penale, civile o amministrativa per tutti quei comportamenti, atti od omissioni non collegati alla Segnalazione, alla denuncia all'autorità giudiziaria o contabile o alla Divulgazione pubblica o che non sono strettamente necessari a rivelare la Violazione (art. 20, comma 4, del D.Lgs. n. 24/2023).
Costituisce motivo di applicazione dei provvedimenti sanzionatori, previsti dal Sistema Disciplinare, la violazione di quanto previsto dal D.Lgs. n. 24/2023 in materia di Segnalazioni di condotte illecite.
In particolare, sono sanzionabili disciplinarmente i casi in cui è accertata, anche con sentenza di primo grado, la responsabilità civile del Segnalante per diffamazione o calunnia nei casi di dolo o colpa grave, salvo che il medesimo sia stato già condannato, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile, ferme restando le sanzioni amministrative ANAC ai sensi dell'art 21 del citato Decreto WB.

Quanto alla tutela del Segnalato, nella gestione dei canali di Segnalazione istituiti ai sensi delle presenti Linee Guida è assicurata anche la tutela della riservatezza dell'identità del Segnalato secondo quanto previsto dal Decreto WB al fine di evitare la indebita circolazione di informazioni personali, non solo verso l'esterno, ma anche all'interno della società in capo, eventualmente, a soggetti non autorizzati al trattamento di tali dati, fino alla conclusione dei procedimenti avviati in ragione della segnalazione.
Il Segnalato non ha il diritto di essere sempre informato della Segnalazione che lo riguarda. Il Segnalato sarà informato della Segnalazione che lo riguarda a seguito delle attività di verifica e di analisi della Segnalazione laddove: (i) vi sia un procedimento avviato nei suoi confronti a seguito dell'attività di verifica e di analisi della Segnalazione e (ii) tale procedimento sia fondato in tutto o in parte sulla Segnalazione. In tal caso, il Segnalato può essere sentito o viene sentito, dietro sua richiesta, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.
Infine, qualora la contestazione sia fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato, la Segnalazione sarà

utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del Segnalante alla rivelazione della propria identità (di cui al par. 6.4.1).

6.3.2 Divieto di Ritorsione

Sono vietate le Ritorsioni ed è sanzionata ogni misura ritorsiva nei confronti della persona del Segnalante o di chi denuncia all'autorità giudiziaria o contabile le Violazioni previste dal Decreto WB delle quali si è venuti a conoscenza.
La società tutela il Segnalante e gli Altri soggetti indicati dall'art. 3 del D.Lgs. n. 24/2023 (e riportati al precedente par. 6.1.2) da qualsiasi forma di Ritorsione, attraverso il riconoscimento di regole volte a impedire o sterilizzare gli effetti di atti o provvedimenti volti a punire il Segnalante per aver rivelato informazioni e/o ad ostacolarne la Segnalazione.
All'interno di questo divieto imposto dalla normativa vigente vi rientra non solo il comportamento, atto o omissione posto in essere in ragione della Segnalazione che cagioni un danno ingiusto al Segnalante, ma anche il tentativo attuato o la minaccia di Ritorsione. Il danno ingiusto provocato può essere anche indiretto.
Inoltre, l'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla Segnalazione, alla Divulgazione pubblica o alla denuncia, nel caso del Segnalante, è a carico della società che li ha posti in essere, che sarà, dunque, tenuta a dimostrare che le misure assunte sono fondate su ragioni estranee alla Segnalazione.
Per quanto riguarda invece gli Altri soggetti, ricade in capo a quest'ultimi l'onere di provare che il comportamento, l'atto o omissione è stato posto in essere a causa della Segnalazione, avente dunque carattere ritorsivo.
A presidio di questa forma di tutela, la normativa vigente prevede che il Segnalante possa comunicare all'ANAC le misure ritorsive che ritenga di aver subito.

6.4 Canali interni per effettuare la Segnalazione

Sono individuati i seguenti canali interni per effettuare le Segnalazioni ("**canali di segnalazione interni**") idonei a garantire la riservatezza dell'identità del Segnalante e la sicurezza delle informazioni, prevedendone l'accesso selettivo solo da parte del personale specificamente autorizzato. In particolare, sono disponibili:

- un **Portale informatico**, che assicura un efficace punto di accesso ai canali dedicati delle società del Gruppo Terna cui si intende indirizzare una segnalazione. Il Portale informatico garantisce la sicurezza e la protezione dei dati dell'identità del Segnalante attraverso un sistema avanzato di criptazione delle comunicazioni, la riservatezza della persona coinvolta e della persona comunque menzionata nella Segnalazione, nonché del contenuto della Segnalazione e della relativa documentazione, in linea con quanto previsto dal Decreto WB.
- **modalità di segnalazione diretta**, volta a consentire che le Segnalazioni siano effettuate attraverso incontri concordati da effettuarsi esclusivamente con i soggetti appositamente autorizzati per la ricezione delle Segnalazioni.
- **canale di posta ordinaria,** che permette di effettuare le Segnalazioni a mezzo posta ordinaria e garantisce, laddove possibile rispetto ai dati forniti dal Segnalante, nella fase di gestione della Segnalazione stessa il trattamento disposto dal Decreto WB ai fini delle comunicazioni con il Segnalante.

I canali interni istituiti devono essere intesi come canali privilegiati.

Tale principio, come previsto dalla normativa di riferimento, è volto, da un lato, "a favorire una cultura della buona comunicazione e della responsabilità sociale d'impresa all'interno delle organizzazioni", dall'altro a fare in modo che i Segnalanti, facendo emergere atti, omissioni o condotte illecite, contribuiscano significativamente al miglioramento della propria organizzazione[16].
I canali interni sono gestiti, come disciplinato al successivo par. 6.5 da soggetti formalmente individuati.
Qualora la Segnalazione sia presentata erroneamente ad un soggetto non competente (diverso da quello formalmente individuato) o ad un canale di altra società del Gruppo diversa da quella interessata, laddove il Segnalante dichiari espressamente di voler beneficiare delle tutele in materia di whistleblowing apprestate dal Decreto WB o tale volontà sia chiaramente deducibile da comportamenti concludenti che rinviino al Decreto WB, le Segnalazioni dovranno essere inoltrate al Gestore (per il tramite del Responsabile Audit) entro 7 giorni dal loro ricevimento, senza trattenerne copia, dando altresì contestuale notizia della trasmissione al Segnalante ove possibile.

6.4.1 Portale informatico

Per effettuare una Segnalazione, il Segnalante dovrà accedere al Portale in cui troverà il canale dedicato alla società del Gruppo cui intende rivolgere la Segnalazione. Il link di accesso al Portale è il seguente: https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione.

I canali delle Società

Nell'ambito del Portale sono presenti i distinti canali di Segnalazione propri delle società rilevanti del Gruppo ai sensi dell'art. 4, comma 4, del Decreto WB e un canale condiviso per le restanti società del Gruppo Terna In particolare, sono previsti all'interno del Portale i canali di:

- Terna S.p.A.;
- Terna Rete Italia S.p.A.;
- Tamini Trasformatori S.r.l.;
- Altenia S.r.l.
- Altre società del Gruppo Terna[17]/Enti.

Le modalità di Segnalazione

Il Segnalante, accedendo al canale della società del Gruppo selezionato (ad es. il canale di Terna S.p.A. oppure il canale di Terna Rete Italia S.p.A. o altro canale), ha la possibilità di effettuare la propria Segnalazione sia in forma scritta, elaborandone manualmente il contenuto, sia in forma orale, tramite l'invio di un messaggio vocale previo espresso consenso alla registrazione della propria voce. Sarà possibile il riascolto, salvataggio o rigetto della Segnalazione prima dell'invio della stessa: dopo l'invio, nel caso di Segnalazione orale, il sistema prevede la modifica dei parametri vocali in modo da rendere la registrazione non riconoscibile.
Le Segnalazioni devono essere rese in buona fede e non in forma anonima.
Per effettuare la Segnalazione, dopo aver ricevuto l'apposita informativa sul trattamento dei dati, il Segnalante dovrà registrare i suoi dati nei campi indicati. Tale registrazione prevede l'inserimento di un indirizzo e-mail e di un numero di telefono personali, al fine di ricevere il doppio codice di

[16] Ai sensi dell'art. 47 della Direttiva (UE) 1937/2019.

[17] Ai sensi dell'art. 4, comma 4 del D.lgs. n. 24/2023, tali società possono condividere il canale di segnalazione interna e la relativa gestione.

sicurezza per i successivi accessi e consentire, in via dedicata e riservata, l'interlocuzione tra la società e il Segnalante per eventuali ulteriori chiarimenti e per l'invio dei *feedback* in merito al Seguito della Segnalazione effettuata.
I dati relativi all'identità del Segnalante saranno custoditi all'interno del *tool informatico* e coperti da un sistema di criptazione (tale da rendere la Segnalazione anonimizzata ma non anonima). I dati potranno essere decriptati qualora strettamente necessario per esigenze istruttorie mantenendone la riservatezza mentre, solo nei casi previsti dal Decreto WB e previo consenso espresso del Segnalante, potranno essere disvelati a persone diverse da quelle competenti a ricevere o a dare seguito alla Segnalazione (cioè, quando ciò occorra al fine di consentire la difesa dell'incolpato in un procedimento disciplinare che si fonda solo sulla Segnalazione e in cui la conoscenza del Segnalante sia indispensabile per la difesa della persona coinvolta). In tale caso, prima della richiesta di decriptazione il RIA si adopererà per acquisire, tramite la stessa piattaforma, il consenso dal Segnalante fornendogli le motivazioni.
La richiesta motivata di decriptazione è rivolta, tramite Portale, dal Presidente del Comitato Etico ("**PCE**") al Chief Information Security Officer ("**CISO**") di Terna[18] il quale supporta le attività per la decriptazione dei dati dell'identità del Segnalante senza avere alcun accesso alla Segnalazione. Il CISO verrà, in tale occasione, informato dell'acquisizione del consenso del Segnalante ove occorra ai sensi del Decreto WB. In caso di impedimento del PCE, la richiesta di decriptazione è fatta dal RIA, con conoscenza PCE.

La gestione del Portale
Il RIA, nella gestione delle Segnalazioni e oltre ai compiti specificamente attribuiti alla Direzione Audit ai fini istruttori, presidia e gestisce sotto la sua responsabilità il Portale (salvo quanto espressamente escluso in caso di conflitto di interessi o in ragione di specifici compiti attribuiti ad altre categorie di utenti es. per la modifica del verbale del Comitato Etico che ha esaminato le evidenze istruttorie).
Nell'ambito della gestione del Portale, il RIA provvede al caricamento delle Segnalazioni pervenute fuori Portale e all'assegnazione tramite Portale delle Segnalazioni ricevute autorizzando, ove non vi provveda direttamente, il **Whistle Editor** a procedere in sua vece.
Per lo svolgimento di attività di aggiornamento e amministrazione del Portale, il RIA si può avvalere dell'**Editor del Portale**, quale soggetto individuato dal RIA, nell'ambito di Audit e tra quelli censiti quali utenti del Portale. Al ruolo di Editor del Portale non è associato alcun accesso alle Segnalazioni.
Tramite il Portale, il RIA (o il PCE nel caso di conflitto di interesse del RIA) individuerà, nell'ambito Audit e tra i soggetti censiti quali utenti del Portale e come indicato al successivo par. 6.5, l'Owner per lo svolgimento dell'istruttoria quale soggetto a ciò debitamente autorizzato e formato. Nell'ambito di dette attività, l'Owner è il soggetto che provvederà a riportare la documentazione istruttoria nell'ambito del Repository del canale interessato, nonché provvederà alle interlocuzioni con il Segnalante tramite Portale, restituendogli i *feedback*.
L'Owner, ove debitamente autorizzato dal RIA (o il PCE nel caso di conflitto di interesse del RIA), provvede alla cancellazione delle Segnalazioni ove ricorrano i presupposti del Decreto WB e/o sia

[18] Nel caso di Segnalazione relativa a Società controllata rilevante, la richiesta è comunicata per conoscenza anche al Referente individuato per la specifica Segnalazione come indicato al par. 6.5.

trascorso il termine di conservazione delle stesse[19], informandone preventivamente i Referenti della Società controllata rilevante ove del caso.
Gli accessi al Portale saranno tracciati così come le sostituzioni e cancellazioni di documenti e relazioni.
La gestione delle funzionalità tecniche e gli aggiornamenti della piattaforma sono rimessi all'Amministratore del sistema del Portale incaricato dalla struttura *Enterprise Services and Platforms* ("**ITD-ESP**") di Terna che vi provvederà in base agli input di Audit: tale Amministratore non potrà vedere e gestire alcuna Segnalazione mantenendo i privilegi massimi su tutte le funzionalità della piattaforma afferenti al ruolo di mero supporto tecnico.

6.4.2 Incontro diretto

In via alternativa al canale di segnalazione sopra citato, 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. Tale casella di posta elettronica può essere utilizzata esclusivamente al fine di trasmettere la richiesta di incontro e non può essere utilizzata per trasmettere segnalazioni scritte.

6.4.3 Posta ordinaria

L'uso del Portale costituisce la maggiore garanzia per la riservatezza. Eventuali Segnalazioni, che potranno essere altrimenti effettuate a mezzo posta ordinaria, saranno ammesse se indirizzate alla società del Gruppo interessata, all'attenzione del Responsabile Audit c/o TERNA S.p.A., Viale Egidio Galbani, 70 – 00156 Roma, utilizzando la seguente dicitura "*segnalazione whistleblowing, riservata – non aprire*" e se debitamente circostanziate, al fine di consentire la valutazione dei fatti e fondate su elementi di fatto precisi e concordanti secondo quanto previsto dal Decreto WB, potranno essere ammesse, sebbene non potranno essere considerate quali Segnalazioni ai sensi del Decreto WB ai fini della gestione delle comunicazioni con il Segnalante e dei *feedback*. In assenza della summenzionata espressa dicitura, la Segnalazione non potrà essere ricevuta e gestita in conformità a quanto disposto dal D.Lgs. 24/2023.
Saranno adottate tutte le più opportune misure per garantire, anche rispetto a questa modalità, la riservatezza delle informazioni e dei dati della Segnalazione.

6.5 Gestione delle Segnalazioni

6.5.1 Soggetti competenti

Sono individuati formalmente i soggetti competenti per la gestione della Segnalazione, ai sensi del D.Lgs. n. 24/2023, del Codice Etico e della normativa in materia di tutela dei dati personali.
Gli organi aziendali competenti per la gestione delle Segnalazioni sono:

[19] Ai sensi dell'art. 14 comma 1 del D.Lgs. 24/2023, le Segnalazioni e la relativa documentazione sono conservati e archiviati nel Repository per ciascun canale interno per il tempo necessario al trattamento della Segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di Segnalazione, salvo ulteriore conservazione in caso di procedimenti giudiziari o richieste delle Autorità o avvio di contenziosi, analogamente la documentazione cartacea relativa a Segnalazioni pervenute fuori Portale secondo quanto disciplinato sub par.6.8. Con riferimento, invece, alle Segnalazioni relative a fattispecie non contemplate dal D.Lgs. 24/2023, i dati verranno conservati sempre all'interno del Repository per tutto il tempo strettamente necessario al perseguimento delle finalità per cui sono stati raccolti e in conformità con quanto previsto dalle disposizioni a tutela dei diritti degli interessati e nel rispetto dei termini di prescrizione previsti per Legge.

- il Responsabile Audit, con riguardo al ricevimento e all'istruttoria delle Segnalazioni;
- il Comitato Etico, con riferimento all'analisi dell'ammissibilità e del contenuto e dell'istruttoria della Segnalazione e per dare diligente seguito alla Segnalazione stessa.

I componenti del Comitato Etico sono nominati dall'Amministratore Delegato di Terna.
Le Segnalazioni vengono gestite dal RIA, unitamente ai membri del Comitato Etico, in modo trasparente attraverso un iter predefinito.
Nella gestione delle Segnalazioni, i suddetti organi aziendali competenti, ciascuno nell'ambito dei propri compiti, assicurano:

- il rilascio al Segnalante di un avviso di ricevimento della Segnalazione entro sette giorni dalla data di ricezione per le Segnalazioni ai sensi del Decreto WB;
- il mantenimento, laddove possibile anche in base al canale scelto dal segnalante, di interazioni con quest'ultimo richiedendo, se necessario, ulteriori informazioni e integrazioni documentali;
- di dare diligente seguito alle Segnalazioni ricevute;
- di fornire Riscontro alla Segnalazione entro tre mesi dalla data di avviso di ricevimento della Segnalazione o, in mancanza di tale avviso entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione.

La gestione delle Segnalazioni per le società del Gruppo Terna avviene in base a idonei accordi infragruppo con Terna e prevede modalità volte ad assicurare il coinvolgimento delle Società controllate rilevanti. Al riguardo, anche in tali casi è previsto, in coerenza con quanto indicato nel presente paragrafo, il coinvolgimento del Responsabile Audit, incaricato di assicurare il rispetto delle prescrizioni normative in materia di ricezione, analisi e Riscontro alle Segnalazioni pervenute, fermo restando il ruolo centrale del Comitato Etico e la raccolta, trattazione e gestione separata delle Segnalazioni pervenute per ciascuna società. Tuttavia, nel caso in cui la Segnalazione sia stata indirizzata al canale della Società controllata rilevante e riguardi la stessa, il Responsabile Audit coinvolge nella fase istruttoria anche un Referente (tra almeno due nominati), incaricato dalla Società controllata rilevante destinataria della Segnalazione al fine di assicurare la prossimità dell'attività di gestione della Segnalazione con la società stessa. Il Referente coinvolto potrà visualizzare tutte le evidenze istruttorie e sarà invitato a partecipare al Comitato Etico: organo chiamato a valutare l'esito dell'istruttoria e a dare seguito alla Segnalazione tenendo conto del parere del Referente.
I soggetti incaricati della gestione della Segnalazione non possono rivelare l'identità del Segnalante o altre informazioni da cui è possibile evincerla a nessun'altro soggetto che non sia debitamente coinvolto nell'attività istruttoria senza consenso espresso del Segnalante.
I soggetti competenti alla gestione della Segnalazione sono informati della presenza di una Segnalazione attraverso il RIA[20]. Le Segnalazioni saranno mostrate ai soggetti necessariamente coinvolti nella gestione della specifica Segnalazione (Owner, componenti del Comitato Etico compreso il Segretario del Comitato), in base alla profilazione sul singolo canale e alle assegnazioni effettuate dal RIA.

[20] Ad eccezione dei casi di potenziale conflitto di interesse del RIA nel qual caso la Segnalazione sarà trasmessa direttamente al Presidente del Comitato Etico.

- Nel caso di Segnalazione tramite Portale, il Responsabile Audit[21] viene informato con un alert generato dal Portale stesso che arriva sotto forma di notifica mail alla sua casella di posta elettronica. Il medesimo alert viene inviato dal RIA ai Referenti della Società controllata rilevante non in conflitto nel caso di Segnalazione indirizzata a quest'ultima[22].
- Nel caso in cui la Segnalazione avvenga tramite incontro diretto è necessario ricevere le Segnalazioni in almeno due soggetti. Il Responsabile Audit, accompagnato da altra persona appartenente alla Direzione Audit, riceve la richiesta di incontro secondo quanto disciplinato sub par. 6.4.2 e, dopo aver concordato l'incontro stesso, supporta il Segnalante per l'inserimento della Segnalazione all'interno del Repository della società del Gruppo interessata e avvia il processo di verifica come descritto al presente paragrafo.
- Nel caso in cui invece la Segnalazione sia stata effettuata tramite posta ordinaria, questa verrà ricevuta dal Responsabile Audit in accordo con quanto disciplinato dalla normativa interna in merito e secondo quanto previsto al paragrafo 6.4.3 della presente Linea Guida. Il Responsabile Audit, dopo aver verificato il contenuto della busta, provvede a inserire (direttamente o tramite Whistler Editor) la Segnalazione all'interno del Repository della Società destinataria della Segnalazione e avvia il processo di verifica come descritto nel presente paragrafo.

6.5.2 Fasi della gestione e attività istruttoria

Alla ricezione della Segnalazione mediante uno dei canali interni indicati nel par. 6.4., è svolta una preliminare valutazione della Segnalazione per stabilire:

(i) se la stessa abbia ad oggetto una Violazione;
(ii) se presenti i requisiti oggettivi e soggettivi di una Segnalazione rilevante.

Il Responsabile Audit, sulla base del contenuto della Segnalazione, definisce le modalità di approfondimento della Segnalazione ed i relativi soggetti da coinvolgere valutando i più idonei. Nello specifico il RIA (direttamente o tramite l'Editor del Portale) assegna la gestione del processo di verifica ad un dipendente della sua struttura debitamente autorizzato e formato (cd. "**Owner**"). Valuta, inoltre, l'eventuale coinvolgimento di altre strutture rispetto all'oggetto della Segnalazione stessa (es. Fraud Management, Data Protection & Privacy, etc.) se necessario ai fini istruttori, mantenendo la riservatezza della Segnalazione tra gli stessi e fornendo loro solo i dati necessari alle attività[23]. Il coinvolgimento di ulteriori strutture aziendali avviene nel rispetto del principio di minimizzazione dei dati, limitando la comunicazione alle sole informazioni strettamente necessarie allo svolgimento delle attività istruttorie assegnate. Affinché il Comitato Etico abbia tempestivamente accesso a tutta la documentazione istruttoria necessaria all'espletamento dei propri compiti, il RIA provvede altresì ad abilitare l'accesso alla specifica Segnalazione i componenti del Comitato Etico (e il Segretario del Comitato), escludendo gli eventuali componenti coinvolti nella Segnalazione.

[21] Terna ha identificato nel Responsabile Audit il soggetto deputato a ricevere le Segnalazioni fermo restando il ruolo centrale del Comitato Etico. La ragione di tale scelta è dovuta al posizionamento organizzativo di tale figura che, non avendo deleghe operative e riportando direttamente al Presidente del Consiglio di Amministrazione, è il soggetto in grado di assicurare la maggiore indipendenza nell'ambito delle attività inerenti alla gestione delle Segnalazioni.

[22] Tale messaggio sarà privo di alcun elemento afferente all'identità del Segnalante e/o al contenuto della Segnalazione. L'alert è volto a presidiare la conoscenza da parte della Società controllata rilevante dell'esistenza della Segnalazione ricevuta e monitorare la corrispondenza tra le Segnalazioni ricevute e quelle esaminate.

[23] Se il Segnalante ha dichiarato che la Segnalazione coinvolge il RIA (apponendo l'apposito flag sul Portale), il sistema informatico invierà la Segnalazione al Presidente del Comitato Etico che svolgerà le funzioni del RIA ai fini delle presenti Linee Guida relativamente alla gestione della Segnalazione.

Il Referente coinvolto (nel caso in cui la Segnalazione riguardi una Società controllata rilevante) potrà visualizzare tutte le evidenze istruttorie relative alla specifica Segnalazione.
Il Responsabile Audit, con la nomina dell'Owner, avvia l'attività istruttoria al fine di individuare, analizzare e valutare gli elementi a conferma della fondatezza e significatività dei fatti segnalati[24].
Gli esiti sono riportati nelle relazioni istruttorie (Report) predisposte dall'Owner e approvate dal RIA.
Il Report (sia la relazione finale sia le eventuali relazioni integrative) è condiviso nel caso di Segnalazione di Società controllata rilevante con il Referente individuato.

6.5.3 Ruolo del Comitato Etico

Il RIA condivide il Report finale con il Comitato Etico, al fine di:

- deliberare il Seguito da dare alla Segnalazione, ivi inclusa, ove ritenuto necessaria, l'integrazione dell'istruttoria;
- confermare l'archiviazione della stessa eventualmente proposta dal RIA.

I componenti del Comitato Etico sono informati dal Responsabile Audit, ovvero dal Presidente del Comitato Etico nei casi di cui al par. 6.6, attraverso il Portale per ogni Segnalazione ricevuta.
Le modalità di funzionamento del Comitato Etico sono disciplinate con apposito Regolamento del Comitato Etico25.
Il RIA, in qualità di Responsabile della Direzione Audit di Terna, nell'ambito della quale è svolta l'istruttoria, partecipa alle riunioni del Comitato Etico (se non interessato dalla Segnalazione) anche tramite un suo delegato (preferibilmente individuato nell'Owner incaricato per la Segnalazione).
Solo all'esito delle attività di gestione, il Gestore informerà i vertici o le funzioni aziendali competenti delle Società non rilevanti e delle Società controllate rilevanti (attraverso il Referente) per i conseguenti provvedimenti. Al Gestore non compete infatti alcuna valutazione in ordine alle responsabilità individuali e agli eventuali successivi provvedimenti o procedimenti conseguenti.

6.5.4 Segnalazioni relative a violazioni del Modello 231 e Flussi all'OdV

Con riferimento alle Segnalazioni che afferiscono al settore privato, non inerenti alla Concessione di pubblico servizio, le Violazioni rilevanti ai sensi della normativa di cui al D.lgs. 231/2001, nonché le Violazioni dei Modelli 231, si possono segnalare per il tramite dei soli canali di segnalazione interni.
Nel rispetto dell'obbligo di riservatezza previsto dal Decreto WB e dalle procedure aziendali applicabili, il Gestore (per il tramite del Responsabile Audit) trasmette tempestivamente all'indirizzo di posta elettronica dell'OdV della Società interessata (e alla Segreteria tecnica dell'OdV individuata dalla società) l'apposita informativa di ricezione di eventuali Segnalazioni aventi ad oggetto Violazioni anche potenziali del Modello 231 e/o comportamenti illeciti integranti le fattispecie di reato presupposto del D.Lgs. 231/2001. All'esito dell'attività istruttoria e a seguito della valutazione del Comitato Etico, il RIA trasmette tempestivamente una comunicazione all'OdV in cui, nel rispetto del principio di riservatezza, si condividono i) le attività istruttorie poste in essere, ii) le relative risultanze e iii) la determinazione assunta dal Comitato Etico.

[24] I dati manifestamente non utili alla trattazione di una specifica Segnalazione non sono raccolti o, in caso di raccolta accidentale, sono prontamente cancellati, interpretando il principio di minimizzazione previsto dall'art. 13 comma 2 del D.Lgs. 24/2023 in modo restrittivo laddove sia palese la assoluta irrilevanza rispetto alla vicenda segnalata e restando salve le norme di settore in materia di conservazione degli atti.

[25] Cfr. LG014 Regolamento Comitato Etico.

Qualora l'OdV riceva erroneamente Segnalazioni, provvederà ad inoltrarle al Gestore (per il tramite del Responsabile Audit) entro 7 giorni dal loro ricevimento senza trattenerne copia, dando altresì contestuale notizia della trasmissione al Segnalante ove possibile.

6.6 Gestione dei potenziali conflitti d'interesse

In caso di coinvolgimento del RIA nella Segnalazione, la stessa verrà gestita dal Presidente del Comitato Etico, così come disciplinato nel precedente paragrafo 6.4.1.
Le Segnalazioni saranno mostrate ai Gestori in base alla profilazione sul singolo canale e alle assegnazioni effettuate dal RIA. In caso di coinvolgimento nella Segnalazione di uno dei componenti del Comitato Etico, lo stesso non riceverà alcun avviso relativo alla Segnalazione che lo coinvolge e non parteciperà alle relative attività del Comitato Etico (secondo quanto previsto nel Regolamento Comitato Etico[26]).
Inoltre, con riferimento alla gestione delle Segnalazioni relative alle Società controllate rilevanti, ciascuna di esse individuerà almeno due Referenti come previsto al precedente par. 6.5: suddetto incarico è predeterminato rispetto alla ricezione della Segnalazione da parte del Responsabile Audit al fine di assicurare la prossimità dell'attività con la società del Gruppo destinataria della Segnalazione. Il RIA dovrà, una volta raccolta la Segnalazione, individuare uno tra i Referenti nominati. Laddove emerga un potenziale conflitto di interessi di uno dei Referenti, il Responsabile Audit dovrà optare per un altro tra i nominati, tenuto conto che il Referente coinvolto potrà visualizzare tutte le evidenze istruttorie e sarà invitato a partecipare al Comitato Etico chiamato a valutare l'esito dell'istruttoria e a dare seguito alla Segnalazione.

6.7 Trattamento dei dati personali

Il trattamento dei dati personali raccolti nell'ambito del procedimento di segnalazione viene svolto nel pieno rispetto della Disciplina Privacy, coerentemente con quanto previsto dal D.Lgs. 24/2023, tenuto conto dell'equo bilanciamento tra i diritti del Segnalato ed il diritto alla riservatezza dell'identità del Segnalante mettendo in atto le misure tecniche e organizzative previste nella presente Linea Guida adeguate a garantire la sicurezza dei dati personali in conformità alla normativa vigente. Tali misure comprendono, a titolo esemplificativo e non esaustivo, la segregazione degli accessi, la cifratura dei dati identificativi, la tracciatura degli accessi e delle operazioni effettuate sul sistema, nonché specifiche procedure di autorizzazione e formazione del personale coinvolto. Il trattamento dei dati personali effettuato nell'ambito del sistema di whistleblowing trova la propria base giuridica nell'adempimento di un obbligo legale al quale è soggetto il Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. c) del Regolamento (UE) 2016/679, come previsto dal D.Lgs. 24/2023. Nell'ambito della gestione delle Segnalazioni possono essere trattati, in via meramente eventuale e non sistematica, dati personali appartenenti a categorie particolari ai sensi dell'art. 9 del GDPR nonché dati relativi a condanne penali e reati ai sensi dell'art. 10 del GDPR, esclusivamente nei limiti in cui ciò sia strettamente necessario ai fini dell'accertamento dei fatti segnalati e nel rispetto delle garanzie previste dalla normativa vigente. È fatto salvo che, l'esercizio dei diritti da parte del Segnalante o del Segnalato (soggetti "interessati" ai sensi della Disciplina Privacy), in relazione ai propri dati personali trattati nell'ambito del processo di Whistleblowing, può essere limitato[27] per

[26] Cfr. LG014 Regolamento Comitato Etico.

[27] Ai sensi dell'art. 23 del GDPR e dell'art. 2-undecies del D.lgs. 196/2003.

garantire la tutela dei diritti e delle libertà altrui, con la precisazione che in nessuna circostanza può essere permesso al Segnalato di avvalersi dei propri diritti per ottenere informazioni sull'identità del Segnalante[28]. Le modalità operative per l'esercizio dei diritti degli interessati sono disciplinate dalla normativa interna in materia di protezione dei dati personali e dalle informative privacy rese disponibili ai soggetti interessati.
Il sistema di gestione delle Segnalazioni è pertanto strutturato in modo da garantire i diritti e le libertà degli interessati con specifica attribuzione di ruoli/responsabilità connesse al trattamento dei dati e relativa documentazione di contesto.
In particolare, nell'ambito del Gruppo, ai sensi del D.Lgs. 24/2023, le Società controllate rilevanti[29], tratteranno i dati del proprio canale di segnalazione interno in qualità di autonomi Titolari del trattamento. Per le altre società del Gruppo Terna[30], potrà essere utilizzato un canale di segnalazione condiviso con relativa gestione da parte delle società stesse, in qualità contitolari del trattamento, ai sensi dell'art. 26 del GDPR, sulla base di uno specifico Accordo di contitolarità in cui sono previste le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni, ai sensi degli artt. 13 e 14 del GDPR. I fornitori che supportano la gestione del Portale informatico e delle relative infrastrutture tecnologiche sono designati Responsabili del trattamento ai sensi dell'art. 28 del GDPR, sulla base di specifici accordi contrattuali che disciplinano le istruzioni, le misure di sicurezza e i limiti del trattamento.
Pertanto, viene resa disponibile la dovuta informativa privacy da parte delle società in qualità di "autonomi titolari" e "contitolari", in cui sono indicati finalità, termini e modalità di trattamento dei dati connessi alla procedura di segnalazione.
Sono espressamente autorizzati a trattare tali dati ai sensi degli artt. 29 e 32 del GDPR e dell'art. 2-quaterdecies del D.lgs. 196/2003 e, per ciò stesso, destinatari di specifiche istruzioni, i soggetti deputati al ricevimento e alla relativa gestione delle Segnalazioni.
Inoltre, coerentemente con le prescrizioni normative del D.Lgs. 24/2023, il sistema di ricevimento e gestione delle Segnalazioni tramite i canali interni è definito sulla base di una valutazione d'impatto sulla protezione dei dati (DIPIA) in cui vengono sistematizzati gli ambiti di trattamento e i connessi profili di rischio, nonché le misure tecnico-organizzative atte a ridurre i rischi identificati.

6.8 Archiviazione e conservazione delle Segnalazioni

Nel caso in cui la Segnalazione sia stata effettuata tramite il canale informatico interno di cui al par. 6.4.1, lo stesso funge da *Repository* ufficiale, consentendo l'archiviazione della Segnalazione, nonché la conservazione di tutta l'eventuale documentazione ad essa associata.
Nel caso in cui la Segnalazione avvenga tramite posta ordinaria o, alternativamente, con incontro diretto, è responsabilità del RIA provvedere al caricamento della Segnalazione sul Portale, nell'ambito del canale della Società destinataria della Segnalazione di cui al par. 6.4.1, per

[28] Ai sensi dell'art. 2-undecies del D.lgs. 196/2003, l'interessato non potrà esercitare i diritti, qualora dall'esercizio degli stessi possa derivare un pregiudizio effettivo e concreto agli interessi tutelati (a titolo indicativo, svolgimento delle investigazioni difensive, esercizio di diritti in sede giudiziaria; riservatezza dell'identità del dipendente che segnala l'illecito ecc.). Pertanto, il Titolare potrà, in ogni caso, ritardare, limitare o escludere l'esercizio di tali diritti con comunicazione motivata e resa senza ritardo all'interessato stesso.

[29] Alla data della presente Linea Guida: Terna S.p.A., Terna Rete Italia S.p.A. e Tamini Trasformatori S.r.l.

[30] Per tali società si intendono le società del Gruppo Terna con meno di 249 dipendenti ai sensi dell'art. 4, comma 4 del Decreto WB.

permetterne l'adeguata archiviazione, conservando al contempo la documentazione originale secondo modalità idonee a garantire, per quanto possibile, la riservatezza della stessa.
Le Segnalazioni e la relativa documentazione devono, infine, essere conservate per il tempo necessario al trattamento della Segnalazione e comunque, ai sensi del Decreto WB, non oltre cinque anni a decorrere dalla data di comunicazione dell'esito finale della procedura di Segnalazione o per il diverso termine di conservazione di legge, come indicato al par. 6.4.1. La decorrenza dei termini di conservazione discende dall'esito finale della Segnalazione (i.e. archiviazione diretta, risultanze dell'istruttoria finale; trasmissione alle Autorità competenti, etc.); sarà pertanto il RIA ad autorizzare la cancellazione e/o la distruzione di eventuale documentazione cartacea conservata come descritto al par. 6.4.1, informandone preventivamente i Referenti della Società controllata rilevante ove del caso.

6.9 Canale esterno

Secondo quanto previsto dal Decreto WB, il Segnalante può ricorrere ai canali di segnalazione esterna istituiti dall'ANAC, disponibili sul sito internet di ANAC[31], solo per le Violazioni previste dal Decreto WB (ad eccezione di quelle che afferiscono al settore privato, non inerenti alla Concessione di pubblico servizio), e laddove sussistano i seguenti presupposti stabiliti dal Decreto WB, ossia:

- mancata attivazione dei canali di segnalazione interni;
- la Segnalazione, effettuata in conformità alle previsioni di cui al Decreto WB e della presente Linea Guida, non ha avuto Seguito;
- ha fondati motivi di ritenere che, se effettuasse la Segnalazione interna, questa non avrebbe seguito o che andrebbe incontro a Ritorsioni. In ordine ai fondati motivi, si specifica che il Segnalante deve poter ritenere ragionevolmente sulla base di circostanze concrete allegate ed informazioni effettivamente acquisibili e, quindi, non su semplici illazioni, che, se effettuasse una Segnalazione interna:
    - alla stessa non sarebbe dato efficace seguito. Ciò si verifica quando, ad esempio, il responsabile ultimo nel contesto lavorativo sia coinvolto nella Violazione, vi sia il rischio che la Violazione o le relative prove possano essere occultate o distrutte, l'efficacia delle indagini svolte dalle autorità competenti potrebbe essere altrimenti compromessa o anche perché si ritiene che ANAC sarebbe più indicata a affrontare la specifica Violazione, soprattutto nelle materie di propria competenza;
    - questa potrebbe determinare il rischio di Ritorsione (ad esempio anche come conseguenza della violazione dell'obbligo di riservatezza dell'identità del Segnalante).
- ha fondati motivi di ritenere che la Violazione possa costituire un pericolo imminente o palese per il pubblico interesse. Si pensi, ad esempio, al caso in cui la Violazione richieda un intervento urgente, per salvaguardare la salute e la sicurezza delle persone o per proteggere l'ambiente[32].

[31] Nell'apposita sezione sul sito Internet dell'ANAC sono reperibili maggiori dettagli sulle modalità di comunicazione, ricezione e gestione delle Segnalazioni a detta Autorità. Secondo quanto previsto dal Decreto WB, la possibilità di ricorrere al canale esterno e alle Divulgazioni pubbliche è prevista solo per le società con un numero di dipendenti superiore a cinquanta.
Come indicato al paragrafo 6.5.2, le Segnalazioni che afferiscono al settore privato, non inerenti alla Concessione di pubblico servizio, relative a Violazioni rilevanti ai sensi della normativa di cui al D.lgs. 231/2001, nonché le Violazioni dei Modelli 231, si possono segnalare per il tramite dei soli canali di segnalazione interni.

[32] Ai sensi dell'art. 62 della Direttiva (UE) 1937/2019.

Il Segnalante e gli Altri soggetti possono comunicare all'ANAC, ai sensi dell'art. 19, comma 1, del Decreto WB le Ritorsioni che gli stessi ritengono di aver subito nel proprio contesto lavorativo in ragione delle Segnalazioni, denunce o Divulgazioni pubbliche.
Qualora la comunicazione di misure ritorsive pervenga al Gestore, il medesimo avvisa il Segnalante della possibilità di inoltro della stessa ad ANAC. Ad ANAC dovranno essere forniti gli elementi oggettivi dai quali sia possibile dedurre la consequenzialità tra Segnalazione, denuncia, Divulgazione pubblica effettuata e la lamentata Ritorsione.

6.10 Divulgazione pubblica

Secondo quanto previsto dal Decreto WB, il Segnalante[33] può, altresì, effettuare una Divulgazione pubblica delle Informazioni sulle violazioni che siano previste dal Decreto WB (ad eccezione di quelle che afferiscono al settore privato, non inerenti alla Concessione di pubblico servizio), di cui sia venuto a conoscenza nel contesto lavorativo, solo al ricorrere delle seguenti condizioni stabilite dallo stesso decreto, ossia:

- il Segnalante ha previamente utilizzato il canale interno o esterno, ma non vi sia stato Riscontro o non vi sia stato dato Seguito nei termini previsti;
- il Segnalante ha fondato motivo di ritenere che la Violazione possa costituire un pericolo imminente e palese per il pubblico interesse[34];
- il Segnalante ha fondato motivo di ritenere che la Segnalazione esterna possa comportare il rischio di Ritorsioni, o che possa non avere efficace seguito in ragione di specifiche circostanze del caso concreto[35].

I fondati motivi che legittimano il ricorso alla Divulgazione pubblica devono essere fondati sulla base di circostanze concrete che devono essere allegate alla Segnalazione e su informazioni effettivamente acquisibili.
Nella Divulgazione pubblica, ove il soggetto riveli volontariamente la propria identità, non viene in rilievo la tutela della riservatezza, ferme restando tutte le altre forme di protezione previste dal Decreto WB per il Segnalante. Laddove, invece, divulghi Violazioni utilizzando, ad esempio, uno pseudonimo o un *nickname*, che comunque non ne consente l'identificazione, la Segnalazione potrà essere trattata, ai fini della riservatezza dei dati del Segnalante e nel caso di disvelamento successivo dell'identità dello stesso, alla stregua di una Segnalazione anonima (quindi non potranno essere garantite le tutele previste dal Decreto); al divulgatore, nel caso di disvelamento successivo, saranno comunque garantite le tutele previste in caso di Ritorsioni.
Al Segnalante è richiesto di trasmettere alla Società la Segnalazione oggetto di Divulgazione pubblica effettuata tramite l'apposita e-mail istituita all'indirizzo whistleblowing@terna.it, al fine di consentire al Segnalante di beneficiare delle tutele apprestate (si veda al riguardo il paragrafo 6.3 della presente Linea Guida).

---

[33] "*nel caso in cui sia soggetto distinto da chi costituisce fonte di informazione giornalistica*" (cfr. par. 3.3 della Delibera n. 311 del 12 luglio 2023 depositata presso la segreteria del Consiglio in data 13 luglio 2023 e pubblicata, tramite avviso in Gazzetta Ufficiale n. 172 del 25 luglio 2023 contenente le "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne*").
Come indicato al paragrafo 6.5.2, le Segnalazioni che afferiscono al settore privato, non inerenti alla Concessione di pubblico servizio, relative a Violazioni rilevanti ai sensi della normativa di cui al D.lgs. 231/2001, nonché le Violazioni dei Modelli 231, si possono segnalare per il tramite dei soli canali di segnalazione interni.

[34] Considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la Violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti.

[35] Perché, ad esempio, potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'autorità preposta a ricevere la Segnalazione e l'autore della Violazione. Dovrebbe in altri termini trattarsi di situazioni particolarmente gravi di negligenza o comportamenti dolosi all'interno della società.

7. Società estere

La disciplina di whistleblowing, nei canali di segnalazione interni e nelle tutele previste per il Segnalante ed il Segnalato così come sopra descritte, si applica anche alle Società estere nel rispetto della legislazione locale.

A tal proposito, si precisa che il trasferimento di dati personali provenienti da Paesi Terzi è ammesso ai sensi e nei limiti della legge applicabile nel singolo caso. A tal fine gli accordi infragruppo, che potranno regolare la gestione delle Segnalazioni per le società estere ai sensi del par. 6.5, saranno accompagnati da ulteriori specifici accordi per assicurare il trattamento dei dati in conformità alla legge applicabile. Per quanto attiene ai ruoli e alle responsabilità, nel trattamento delle Segnalazioni in capo al Gestore, può essere richiesto supporto al Compliance Officer nominato dalla società interessata e/o di consulenti esterni; il coinvolgimento del CO in tale fase è circoscritto all'acquisizione di informazioni funzionali all'istruttoria.

Invece, in caso di impossibilità della SE di adottare la disciplina del whistleblowing con i canali di segnalazione interni così come descritti nella presente Linea Guida, le SE appresteranno modalità di segnalazione delle Informazioni sulle violazioni coerenti con le previsioni del Codice Etico in materia di tutele del Segnalante e provvederanno 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.

8. Approvazione, revisione e divulgazione

I principi della presente Linea Guida rientrano tra i valori fondamentali del Gruppo Terna e ne ispirano l'organizzazione e le attività anche in attuazione delle disposizioni del Codice Etico. Per tale ragione, e rivolgendosi a tutti i dipendenti (inclusi i dipendenti assunti con contratto a tempo determinato), gli stagisti ed i lavoratori interinali, la presente Linea Guida è stata approvata dall'Amministratore Delegato e Direttore Generale di Terna S.p.A.

È promossa l'adozione della presente Linea Guida da parte di tutte le società del Gruppo, nonché la sua diffusione. A tal fine, sono promosse iniziative di sensibilizzazione e formazione del personale per divulgare le finalità dell'istituto del whistleblowing e la procedura per il suo utilizzo (quali ad esempio comunicazioni specifiche, eventi di formazione, newsletter, intranet, etc.).

Al riguardo, è svolta:

a) idonea formazione con riferimento al soggetto/soggetti preposti alla gestione dei canali interni anche mediante apposite sessioni formative e di induction;
b) idonea comunicazione, per il raggiungimento delle finalità informative, riguardo ai canali di segnalazione interni, alle procedure ed ai presupposti per effettuare le Segnalazioni interne, nonché al canale, alle procedure ed ai presupposti per effettuare Segnalazioni esterne ai sensi del Decreto WB. A tale ultimo riguardo, per le società italiane del Gruppo, si provvede alla pubblicazione delle suddette informazioni in una apposita sezione dedicata del sito internet, laddove esistente.

In merito al punto a), la formazione dovrà basarsi tenendo conto della normativa e *best practice* applicabili.

In merito al punto b), sono promosse iniziative di comunicazione anche per la divulgazione verso l'esterno delle finalità dell'istituto del whistleblowing e della procedura per il suo utilizzo. Ogni società del Gruppo garantisce che la presente Linea Guida in materia di whistleblowing sia resa disponibile all'interno mediante pubblicazione sulla rete intranet aziendale o mediante invio via e-mail o altre modalità di condivisione di documenti aziendali.
I principi e i contenuti dell'istituto del whistleblowing che siano applicabili ai Terzi sono resi conoscibili attraverso la documentazione contrattuale.
Le attività di informazione e di formazione sono documentate, monitorate e valutate in termini di adeguatezza ed efficacia.

Eventuali modifiche e/o integrazioni che si dovessero rendere necessarie od anche solo opportune in ragione di evoluzioni normative e/o giurisprudenziali o di allineamento con le *best practice* e con le linee guida ANAC o in relazione ad azioni di monitoraggio intraprese o sopravvenute esigenze operative od organizzative potranno essere apportate dal Direttore Strategia Digitale e Sostenibilità fornendo, ove necessario o anche solo opportuno, istruzioni operative per disciplinare specifici profili applicativi della presente linea guida ed eventuali indirizzi alle società controllate. Delle suddette modifiche e/o integrazioni, dovrà essere previamente informato il Comitato Etico e, ove assumano natura sostanziale, le organizzazioni sindacali.

9. Reporting

Con cadenza annuale e con riferimento all'anno solare, le Segnalazioni, ove pervenute nel periodo, saranno oggetto di specifica reportistica (con indicazione del numero di Segnalazioni ricevute, del numero di Segnalazioni archiviate e dello stato di avanzamento delle relative istruttorie) predisposta dal RIA, in cui i dati delle Segnalazioni saranno anonimizzati e raccolti in forma aggregata, verso il Comitato Etico con riguardo a Terna S.p.A., mentre per le altre società del Gruppo anche verso l'AD/Amministratore Unico, al fine di fornire una rappresentazione complessiva del funzionamento del sistema di whistleblowing e, per quanto di competenza, periodicamente e di norma ogni sei mesi, verso gli OdV/CO. Ove il RIA non avesse avuto visibilità delle segnalazioni nei casi di conflitto di interessi, l'integrazione della summenzionata reportistica verrà svolta dal Comitato Etico per il tramite del Segretario del Comitato Etico.

10. Misure di sostegno da parte degli Enti del Terzo Settore (ETS)

Il Segnalante può rivolgersi, in qualsiasi momento, agli enti del Terzo settore inseriti nell'elenco pubblicato da ANAC ai sensi dell'art. 18 del D.Lgs. 24/2023, che forniscono misure di sostegno quali:

a) informazioni, assistenza e consulenza sulla normativa whistleblowing;
b) assistenza legale;
c) supporto psicologico.

L'elenco degli enti convenzionati e che esercitano, secondo le previsioni dei rispettivi statuti, le attività di cui al decreto legislativo 3 luglio 2017, n. 117.è disponibile sul sito istituzionale di ANAC.
Questo paragrafo descrive il contesto nel quale si inserisce il macro-processo o la tematica di governance/risk/compliance di riferimento.

Terna

LG054

Whistleblowing

24/03/2026

GUIDELINES

Index

1. General information

Terna has always been particularly mindful of preventing risks which could compromise the responsible and sustainable management of its business, and in line with its mission and its internal control system, as well as knowing about critical situations and correcting them by consolidating its relationship of trust with stakeholders.

To ensure responsible management and in line with legislative requirements, in September 2016, the Terna Group implemented and updated a system for receiving and managing the reports of Violations of internal or external regulations which could cause damage or harm to the company, such as fraud, a generic risk or a potentially dangerous situation, to ensure fairness and transparency in conducting its business and activities and protect the company's position and image. This ensured that the system was also compliant with the regulatory provisions introduced in 2017, firstly referred to as the "Provisions to protect those reporting crimes or irregularities of which they become aware through a public or private employment relationship", and subsequently, in 2023, with Italian Legislative Decree no. 24/2023 on whistleblowing[36] on the "Implementation of 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 provisions concerning the protection of persons who report breaches of national laws" (hereinafter the "**WB Decree**" or "**Leg. Decree 24/2023**") and the Guidelines issued by the National Anti-Corruption Authority ("**ANAC**") pursuant to Article 10 of the WB Decree[37].

This system forms an integral part of the Group's ethical safeguards (Code of Ethics) and corporate liability, such as the Organizational and Management Models pursuant to Italian Legislative Decree 231/01 ("**231 Models**"), and the Global Compliance Program (LG058) insofar as applicable to the Group's foreign companies.

Whistleblowing therefore represents one of the internal control tools that Terna employs to outline the Code of Conduct to be upheld in the course of its business.

If duly regulated, reporting any dishonest conduct that may lead to fraud, or which may present a risk of damage to colleagues or shareholders, or which constitutes harmful or unlawful action that

[36] "Whistleblowing" is the English term derived from the metaphorical expression 'to blow the whistle', which was used with the meaning of stopping something abruptly. It is the tool that allows anyone to report wrongdoing, even suspected wrongdoing.

[37] Article 10 of the WB Decree stipulates that ANAC, after consultation with the Personal Data Protection Authority ["*Garante per la protezione dei dati personali*"], shall adopt guidelines on procedures for the submission and management of external reports, within three months of the WB Decree coming into force. ANAC published on its website Resolution no. 311 of 12 July 2023, submitted to the Secretary of the Board on 13 July 2023 and published, through an announcement in Official Gazette no. 172 of 25 July 2023, containing "Draft Guidelines on the Protection of Persons Reporting Breaches of Union Law and the Protection of Persons Reporting Breaches of National Law. Procedures for the Submission and Management of External Reports".
ANAC also published on its institutional website Resolution 301 of 12 July 2023, submitted to the Secretary of the Board on 13 July 2023 and applicable from 15 July 2023 as per the announcement published in the Official Gazette on said date and containing the "Regulation for the management of external reports and exercise of the power of sanction of ANAC in implementation of Italian Legislative Decree no. 24 of 10 March 2023".
ANAC later published Resolutions No. 478 and 479 of 26 November 2025 on its website, concerning Guidelines in relation to whistleblowing through internal and external channels respectively, which were subsequently published in Official Journal No. 300 of 29 December 2025.

could damage the interests and reputation of the company, can be an effective method of combating corruption.

The purpose of these Guidelines is to define the methods for managing Reports of unlawful acts and/or conduct for the Terna Group, whether these were committed or omitted, and which the Group companies become aware of, also in compliance with the relevant applicable legislation and which constitute breaches, all be they suspected breaches of:

(i) the principles sanctioned in the Code of Ethics, internal regulations, represented by all the provisions, procedures, guidelines or operating instructions of the company receiving the report, including the Organizational and Management Model pursuant to Italian Legislative Decree no. 231/01 (the "**231 Model**"), the anti-corruption guidelines, the Global Compliance Program, as well as breaches of policies and company rules which could translate into fraud or damages, albeit potential, relative to colleagues, shareholders and stakeholders in general, or which constitute actions of an unlawful or harmful nature relative to the interests or reputation of the company, and (Iii) the breaches contemplated by Italian Legislative Decree 24/2023, "of national or EU regulatory provisions that harm the public interest or the integrity of the public administration or private entity".

Specifically, this document has also been drawn up in accordance with the provisions of the WB Decree, which represents the legislative instrument for fighting and preventing corruption, conduct that does not comply with the principles of sound administration and impartiality by the Public Administration and preventing breaches of the law in the public and private sectors. The WB Decree specifically introduced an integrated system of rules intended for the public and private sector that coordinates European and national law with the aim of incentivizing the reporting of wrongdoing that prejudices the public interest or integrity of an entity. The new regime raises the level of protection provided to Whistleblowers.

2. Purpose of the document

The purpose of these Guidelines is to identify and regulate the management of Reporting Breaches (whistleblowing), the Group Companies' internal channels activated for Reports and their operation, to define the subject of Reports and the persons who are entitled to make them, the responsibilities and procedures for managing the analysis and investigation activities following receipt of Reports (roles and responsibilities) and the relevant deadlines, the measures for protecting the Whistleblower, the conditions for making external Reports and public Disclosure, as well as the

procedures and deadlines for retaining data for the purposes of whistleblowing management activities, also in compliance with privacy legislation[38].
It also governs the procedures for disseminating information on the use of reporting channels and the prerequisites for making Reports using said channels, the persons qualified to handle Reports and the reference procedures, initiatives to raise awareness and train staff, and the procedures for updating the guidelines.

It should also be noted that these Guidelines were drafted in compliance with the regulatory provisions applicable to a specific perimeter of Italian companies and contemplated in the WB Decree and the consequent ANAC Guidelines[39], containing specific conditions and procedures governing whistleblowing, relating to the scope of application; the objective scope of protection; the channels for submitting Whistleblowing Reports and the procedures for submitting them; the protection of confidentiality and possible Retaliation; the limitations of liability for whistleblowers, complainants or whoever makes Public Disclosures ("**Significant Reports**").
With regard to Reports that do not fall within the aforementioned regulatory scope ("**Ordinary Reports**"), the following provisions apply only with regard to the minimum content of the Report (para. 6.2.1); the internal reporting channels (para. 6.4); the management of Reports (para. 6.5), with the exception of the feedback and timing specified in the WB Decree; the management of potential conflicts of interest (para. 6.6).
The processing of data is also guaranteed in the case of ordinary Reports in accordance with the applicable Privacy Policy, as well as the general prohibition on retaliation contemplated in the Code of Ethics, which is expressly protects Reports made in good faith and in a spirit of loyalty to the company.

3. Scope of application

These Guidelines apply to Terna and all Terna Group companies, including foreign subsidiaries, without prejudice to the provisions under para. 7 below. [40]

[38] The perimeter of privacy regulations includes the following national and supranational provisions: Italian Legislative Decree No. 101 of 10 August 2018 '*Provisions for the alignment of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC*'; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR); Italian Legislative Decree no. 196 of 30 June 2003, "Consolidated Law on Privacy" as amended, and Provisions related to the Code issued by the Italian Data Protection Authority.

[39] This refers to the ANAC Guidelines as also most recently updated through Resolution No. 478 of 26 November 2025.

[40] The provisions of Italian Legislative Decree no. 24/2023 referred to in these Guidelines apply, pursuant to Art. 24, para. 2 of the WB Decree, only with reference to the Terna Group companies that, over the last year, employed an average of 249 employees, with permanent or fixed-term employment contracts as from 17 December 2023. Pursuant to the minutes of the BoD of the Terna Foundation dated 17 December 2025, the provisions of these Guidelines apply to the Terna Foundation, to the extent that they are relevant.

4. References

4.1 External regulations

- 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, as amended;
- Italian Law no. 179 of 30 November 2017, as amended, "Provisions to protect those reporting crimes or irregularities which they become aware of through a public or private employment relationship"[41];Italian Law no. 190 of 6 November 2012, as amended, "Provisions for the prevention and suppression of corruption and wrongdoing in the public administration";
- Italian Legislative Decree no. 231 of 8 June 2001, as amended. (or **Legislative Decree 231/01**), "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";
- Italian Legislative Decree no. 196 of 30 June 2003, "Consolidated Law on Privacy", as amended, and provisions issued by the Personal Data Protection Authority;
- European Regulation 2016/679 (**GDPR**), relative to the protection of natural persons with regard to the processing of personal data and the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation) and the Provisions of the Personal Data Protection Authority regarding the protection of personal data;
- Italian Legislative Decree no. 101 of 10 August 2018, as amended, containing the provisions for the alignment of national regulations with provisions of Regulation (EU) 2016/679 of the European Parliament and Council, of 27 April 2016, relative to the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;
- Italian Legislative Decree no. 51 of 18 May 2018, implementing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by relevant authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offences or executing

[41] The application of this law is limited to Group companies that over the last year, have employed an average of up to two hundred and forty-nine employees, with permanent or fixed-term employment contracts, given that the obligation to set up the internal channel pursuant to Italian Legislative Decree No. 24/2023 takes effect from 17 December 2023, pursuant to Article 24, paragraph 2 of the WB Decree.

criminal penalties, and the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, as amended;

- Guidelines for the Data Protection Impact Assessment (**DPIA**) and determining whether processing "may present a high risk" relative to Regulation 2016/679/EU (Working Party 248 rev. 01);
- ISO-37001 2025 “Anti-Bribery Management Systems;
- ISO-37301:2021 “Management System for Compliance” standard;
- Guidelines issued by ANAC pursuant to Article 10 of the WB Decree on the protection of persons who report breaches of Union law and the protection of persons who report breaches of national laws — procedures for submitting and handling external reports — procedures for the submission and management of external reports published on the ANAC institutional website;
- ANAC Regulation for the management of external reports and exercise of the power of sanction of ANAC in implementation of Italian Legislative Decree no 24/2023, published on the ANAC institutional website;
- 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.

4.2 Internal Regulations

- Code of Ethics;
- Organizational and Management Model pursuant to Italian Legislative Decree no. 231 of 8 June 2001, of TERNA S.p.A. and subsidiaries;
- LG014 - Ethics Committee Regulations;
- LG050 TERNA Group companies’ adoption of the Code of Ethics;
- LG018 - Information Security Policy Strategic Guidelines;
- LG039 - Rules on Privacy in Terna;
- LG058 - Global Compliance Program;
- LG059 - Anti-Corruption Guidelines;
- IO009SER - Management of IT protocol services.

5. Glossary

In addition to the terms and expressions defined in other sections of these Guidelines (or in the annexed documents), for the purposes of these Guidelines, the terms and expressions listed below have the meaning specified alongside each of them.

- **System Administrator**: a party with all the functions of the Whistle Editor but who, unlike the latter, also manages internal user authorisations.
- **Other parties**: the parties referred to in para. 6.1.2 of these Guidelines and identified in Article 3, paragraph 5 of Italian Legislative Decree No. 24/2023.
- **Audit** (or **AU**)**:** Terna's Audit Department which conducts the preliminary investigations following the Report and communicates the outcome to the Ethics Committee via the Portal.
- **CISO:** the Chief Information Security Officer.
- **Code of Ethics:** document containing positive principles and rules of conduct voluntarily adopted within the Terna Group and made public as a tangible expression of the Group's intentions in relation to whoever it comes into contact with.
- **Ethics Committee:** the corporate body responsible for managing the Reports received and processing them. The members, appointed by Terna S.p.A.'s CEO, are chosen so as to represent a heterogeneous perspective and a balance between the various Group companies, corporate functions and roles.
- **Compliance Officer** (or **CO**): a person identified, pursuant to LG058, in each foreign Group company with the task of fostering the dissemination of knowledge of the Global Compliance Program and/or the Local Compliance Programs envisaged in the Country Annex and of the Parent Company's policies within the company itself, as well as facilitating their operation through training and information activities and through the implementation of specific information flows.
- **Work context**: this refers to the current or past work or professional activities carried out by the Whistleblower for Terna or for other Group companies that are recipients of the Report, whereby a person has acquired Information on Breaches, regardless of the nature of such activities, and regarding which he/she could risk suffering Retaliation in the event of a Report;
- **Privacy Regulations**: this definition refers to applicable Privacy legislation regarding personal data protection, meaning Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Italian Legislative Decree no. 196/2003, Italian Legislative Decree no. 101 of 2018 and any other applicable legislation on personal data protection, including the provisions of the Italian Data Protection Authority.
- **Public disclosure** or **public dissemination**: placing Information on Breaches in the public domain via the press or electronic media or, in any case, using means of dissemination that are capable of reaching a large number of people in the cases provided for by Italian Legislative Decree no. 24/2023.

- **ITD-ESP:** Enterprise Services and Platforms structure in the IT & Digital area.
- **Facilitator**: natural person who provides assistance to the Whistleblower in making the Report, operating within the same work context and whose assistance must be kept confidential pursuant to Italian Legislative Decree no. 24/2023.
- **Reporting Manager or Manager:** the parties identified by the company as being responsible for managing Reports as regulated in para. 6.5 of these Guidelines, in accordance with the principles of autonomy, impartiality and independence.
- **Information on breaches**: information, including well-founded suspicions, concerning Breaches committed or which, on the basis of concrete elements, could be committed in the organization with which the whistleblower or person filing the complaint to the judicial or accounting authorities has a legal relationship in the work context, as well as elements concerning conduct aimed at concealing said Breaches. Information on breaches does not include Information on reportable breaches that is clearly without substance, information that is fully in the public domain, or information acquired only on the basis of highly unreliable rumours or gossip (so-called office gossip).
- **Supervisory Body** or **SB**: the body with autonomous powers of initiative and control established by the company pursuant to Italian Legislative Decree 231/01 and appointed to monitor the functioning of and compliance with Model 231, as well as to update it.
- **Owner:** duly authorised and trained Audit Department employee assigned the Report verification process as per para. 6.5.
- **CEC:** the Chairperson of the Ethics Committee.
- **Person Involved**: the natural or legal person mentioned in the internal or external Report or in the Public Disclosure as the person to whom the Breach is attributed or as a person otherwise implicated in the reported or Publicly Disclosed Breach.
- **HR**: Terna's Human Resources Department.
- **IT Portal** or **Portal:** the web-based IT tool specifically set up for written and oral Reports of Breaches for Group Companies accessible at https://whistleblowing.terna.it/ and with specific channels dedicated to Group Companies set up pursuant to the WB Decree.
- **Contact Person for Whistleblowing** or **Contact Person:** the person designated by the relevant Subsidiary, who the Manager involves if the Report is relevant to that company as contemplated in para. 6.5 of these Guidelines.

- **Repository:** represents the database set up for each internal channel established on the IT Portal and used to file all the Reports received, regardless of the procedures used to make the Report.
- **Audit Manager** or **RIA:** Terna Audit Manager.
- **Retaliation**: any conduct, act or omission, albeit only attempted or threatened, carried out by reason of the Report, the report to the judicial or accounting authorities or the public Disclosure and that causes or may directly or indirectly cause unjustified prejudice to the Whistleblower or to the person making the Report. More specifically, pursuant to Art. 17 para. 4 of Italian Legislative Decree no. 24/2023 and the ANAC Guidelines, the following are examples of retaliation:
    - dismissal, suspension or equivalent measures;
    - relegation in grade or non-promotion;
    - change in functions, change in workplace, reduction in salary, change in working hours;
    - suspension of training or any restriction to accessing training;
    - demerit notes or negative references;
    - the adoption of disciplinary measures or other sanctions, including fines;
    - coercion, intimidation, harassment or ostracism;
    - discrimination or otherwise unfavourable treatment;
    - the failure to convert a fixed-term employment contract into an employment contract with an indefinite duration, where the employee had legitimate expectations of the contract being converted;
    - non-renewal or early termination of a fixed-term employment contract;
    - damage, including to a person's reputation, particularly on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
    - undue inclusion in lists on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
    - early termination or cancellation of the contract for the supply of goods or services;
    - cancellation of a licence or permit;
    - the request to undergo psychiatric or medical examinations.
    - retaliation may take the form, for example, of demanding results that are impossible to reach in the manner and time indicated, an artificially negative performance evaluation, unjustified withdrawal of duties, unjustified failure to assign duties with

corresponding assignment to another party, repeated rejection of requests (e.g. holidays or leave), or unjustified suspension of patents, licences, etc.

  - For the purposes of these Guidelines, preventing or attempting to prevent the Report also qualifies as a form of "retaliation".

- **Acknowledgement**: information provided to the Whistleblower on the Follow-up given or intended to be given to the Report, also pursuant to Italian Legislative Decree no. 24/2023.
- **SE or foreign company**: non-Italian company(ies) in the Terna Group.
- **Whistleblower**: the natural person reporting Information on Breaches acquired in the work context of Terna or of other Group companies that are recipients of the Report.
- **Reported Person**: the natural or legal person mentioned in the Report as the person to whom the Breach is attributed or as the person otherwise involved in the reported Breach.
- **Report**: the written or oral communication of Information on Breaches.
- **External reporting**: the written or oral communication of Information on Breaches in the cases contemplated by Italian Legislative Decree no. 24/2023, submitted via the external reporting channel set up by ANAC.
- **Internal Reporting**: the written or oral communication of Information on Breaches, submitted via the internal Reporting channels established for the Terna Group company that is the recipient of the Report.
- **Follow-up**: the action taken by the Manager to assess the existence of the reported facts, the outcome of the investigations and any measures taken.
- **Disciplinary system**: the disciplinary system applicable to the company, detailed in the 231 Models, or in the case of an FC, pursuant to the Global Compliance Program as adopted by each FC. Disciplinary measures and related sanctions, where applicable in relation to the recipients of the same, are identified by the company on the basis of the principles of proportionality and appropriateness, in relation to their suitability to act as a deterrent and, subsequently, as a sanction, as well as taking into account the different qualifications of the persons to whom they apply.
- **Non-significant subsidiaries**: companies in the Terna Group with less than two hundred and forty-nine employees pursuant to Art. 4, para. 4 of Italian Legislative Decree no. 24/2023 with their registered office in Italy as well as foreign companies, for the purposes of these Guidelines.

- **Significant subsidiaries**: companies in the Terna Group with more than two hundred and forty-nine employees pursuant to Art. 4, para. 4 of Italian Legislative Decree no. 24/2023 with their registered office in Italy.
- **Breaches**: unlawful acts and/or conduct, whether these were committed, omitted, and which constitute breaches, all be they suspected breaches of the principles in the Code of Ethics, internal regulations, represented by all the provisions, procedures, guidelines or operating instructions of the company receiving the report, including the 231 Model, the anti-corruption guidelines, the Global Compliance Program, as well as breaches of policies and company rules which could translate into fraud or damages, albeit potential, relative to colleagues, shareholders and stakeholders in general, or which constitute actions of an unlawful or harmful nature relative to the interests or reputation of the company, and the breaches contemplated by the WB Decree, "of national or EU regulatory provisions that harm the public interest or the integrity of the public administration or private entity".
- **Whistle Editor**: person identified by the RIA within the Audit framework and from portal users, for including Reports received outside the portal. It updates information in the various sections of the Portal according to different usages (disclaimers, Frequently Asked Questions (FAQs), value lists, type management, ...).

6. Conditions, procedures for making Reports and related protection

6.1 Subjective scope

Pursuant to the Code of Ethics, all Terna Group companies provide Whistleblowers with the utmost confidentiality, protecting those making Reports in good faith and in a spirit of loyalty towards the company from Retaliation or negative effects in relation to their professional positions, penalising those who commit retaliatory acts.

With reference to the system of protection provided in these Guidelines under the WB Decree, we note two distinct categories of parties:

- the "***Whistleblower";***
- the "***Other parties'"***.

6.1.1 Whistleblowers

The Report of a Breach can be sent by "anyone".

With specific reference to the provisions of the WB Decree and the related protections however, anyone operating in the "*working context*" of Terna or of the different recipient Group companies, may make a Report in their capacity as:

- employees of one of the companies belonging to the Group;
- self-employed persons who carry out their work for one of the Group companies;
- those who have a professional relationship with the entity (e.g. suppliers), freelancers (e.g. lawyers, accountants, notaries, etc.) and consultants who provide services to one of the Group companies;
- volunteers and paid and unpaid trainees carrying out their work at one of the Group companies;
- shareholders, understood as natural persons who hold shares in one of the parties of the public sector, where the latter assumes a corporate role, e.g. publicly controlled company, in-house company, co-operative, etc. These are persons who became aware of breaches subject to whistleblowing in the exercise of the rights held by them as a result of their role of shareholders in the company;
- shareholders and persons with administration, management, control, supervision or representative functions, even if these functions are exercised on a de facto basis, at one of the Group companies.

Reports may also be made by whoever:

- reports Information acquired in the scope of an employment relationship with the Terna Group that has since been terminated, provided that the information on the Breaches was acquired prior to the relationship being terminated;
- reports information acquired prior to the start of the employment relationship, where information concerning a Breach was acquired during the selection process or during other stages of the pre-contractual negotiations;
- reports information acquired during the probationary period at one of the Group companies.

6.1.2 Other subjects

The category of "Other parties" deserving protection in the case of Reports pursuant to the WB Decree includes:

- Facilitators;
- persons in the same work environment as the Whistleblower and who are connected to him/her by a permanent emotional or family relationship up to the fourth degree;
- the Whistleblower's work colleagues and those working in the same work environment as the Whistleblower and who have a habitual and current relationship with the latter[42];

[42] "In the case of work colleagues, lawmakers have stipulated that this refers to those working with the whistleblower at the time of the report (thus excluding former colleagues) and that had a current and habitual relationship with them. The law therefore refers to relationships that are not merely sporadic, occasional,

- entities owned by the Whistleblower or that they work for, as well as entities operating in the same work context.

6.2 Subject of the Report

All Breaches can be reported. With specific reference to the provisions of the WB Decree, significant Reports (in which case the protection measures stipulated in paragraph 6.3 are applicable) are considered the Reports on Breaches relating to all conduct, acts or omissions that are capable of damaging public interests or the integrity of the public administration or the private entity.

More specifically, there are three distinct categories[43]:

1. ***Breaches of national and European legislation referring to offences in the following areas***: public procurement; services, products and financial markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection and security of networks and information systems;
2. ***Breaches of European legislation*** referring to: i) acts or omissions that are damaging to the Union's financial interests; ii) acts and omissions relating to the internal market[44]; iii) acts and conduct that undermine the object or purpose of the provisions of Union legislation in the areas mentioned above; iv) violations of the restrictive measures of the European Union pursuant to chapter I-bis, title I, book II of the Italian Criminal Code, as well as of article 12, paragraph 1-bis, of Italian Legislative Decree No. 286 of 25 July 1998, in the context of the "*Implementation of Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673*"; v) violations of Regulation (EU) No. 2024/1689 (the so-called AI Act)[45].
3. ***Breaches of national legislation*** referring to: i) administrative, accounting, civil or criminal offences; ii) unlawful conduct that is relevant under Italian Legislative Decree no. 231/2001 or

episodic and exceptional, but rather those that extend over time, characterised by a certain continuity that could determine a relationship of "commonality", or friendship," as per the ANAC Guidelines approved with ANAC Resolution 311 of 12/7/2023, page 22.

[43] In terms of the WB Decree, with respect to the above categories of Breaches, a distinction must be made according to whether: (i) the entity is a public service concessionaire (or, in any case, an entity operating in that context), in which case all categories of Breaches apply; (ii) the entity has more than 50 employees and has adopted a 231 Model, in which case the category of Breaches of European law and unlawful conduct pertinent under Italian Legislative Decree no. 231/2001 or Breaches of the 231 Model shall apply; (iii) the entity has less than 50 employees but has adopted a 231 Model, in which case the Breaches of unlawful conduct pertinent under Italian Legislative Decree no. 231/2001 or Breaches of the 231 Model shall apply.

[44] This includes all breaches of EU competition and state aid rules, as well as breaches referring to the internal market related to acts that violate corporate tax rules or mechanisms with the purpose of obtaining a tax advantage that undermines the object or purpose of the applicable corporate tax laws.

[45] Pursuant to art. 113 of Regulation (EU) 2024/1689, art. 87 — which stipulates that Directive (EU) 2019/1937 shall apply to the reporting of breaches of this regulation and to the protection of persons who report such breaches — shall apply from 2 August 2026.

violations of 231 Models. These offences and conduct must not fall under the categories of points 1. and 2. above.

6.2.1 Minimum content of the Report

The Report must include the following essential elements.

- **Whistleblower**: the Report must contain the identifying references for the person making the Report[46]. Reports much be made in good faith and may not be made anonymously.
- **Subject matter**: a clear description of the facts that form the subject of the Report, indicating the circumstances of the time and place when the facts were committed/omitted as well as how the Whistleblower became aware of the facts.
- **Reported Person and Persons Involved**: the details or any element (such as the function/role in the company) making it easier to identify the alleged perpetrator(s) of the unlawful conduct and the Persons involved.
- **Group companies**: the Report must specify which Group company the Report refers to if the Report is made using a channel shared between several Group Companies.

Reports shall be examined where they are admissible, not obviously unfounded, substantiated and contain sufficient information for the Breaches to be reconstructed and confirmed. The Ethics Committee reserves the right to assess the Report in the light of the specific case and the existence of elements sufficient to allow the subsequent investigation.

In addition, the Whistleblower may provide the following additional details:

- **any other persons** who may be able to provide information about the facts in the Report;
- **any documents may be sent** that can confirm said facts;
- **any other information** that could facilitate the gathering of evidence on what has been reported.

The Whistleblower may also provide additional documentation that may be useful in substantiating the Report.

Finally, to facilitate the correct identification of the other persons involved pursuant to para. 6.1.2 of these Guidelines and identified under Art. 3 of Italian Legislative Decree no. 24/2023, to guarantee their confidentiality and protection as agreed and indicated in the following para. 6.3, it is recommended that the Whistleblower explicitly indicates these parties, specifying the existence of the corresponding conditions.

[46] To be understood as sufficient personal data to allow for dedicated and confidential dialogue between the Company and the Whistleblower, and for feedback to be sent following the Report.

6.2.2 Limitations to the subject of the Report

The following fall outside the scope of application of the WB Decree (and the protective measures set out in paragraph 6.3 below shall therefore not apply):

- claims, objections, requests of a personal nature of the Whistleblower or the person lodging a complaint with the judicial or accounting authorities, relating exclusively to his/her individual employment relationship, or inherent to his/her employment relationship with persons holding higher ranking positions[47];
- Reports of Breaches that on a mandatory basis are already regulated by European Union or national legislation referring to services, products and financial markets and the prevention of money laundering and terrorist financing, transport safety and environmental protection or by national legislation implementing Union laws[48], and Reports of Breaches relating to national security, and to procurements relating to defence or national security aspects, unless these aspects fall under the relevant secondary European Union legislation;
- Anonymous reporting, this Guideline is designed to protect the Whistleblower from the risk of Retaliation.

With regard to anonymous Reporting, it should be remembered that protection in terms of paragraph 6.3 may nonetheless apply if the name of the Whistleblower is revealed as a result of an anonymous Report.

The ultimate protection of confidentiality provided to Whistleblowers even in the case of ordinary Reports requires that these are not made anonymously.

It should also be remembered that, pursuant to Article 1, paragraph 3 of the WB Decree, Reports referring to the following issues fall outside the scope of application of the protection provided for by the Decree and these Guidelines on the subject of whistleblowing: a) classified information, b) forensic and medical professional secrecy, c) secrecy of the deliberations of judicial bodies.

Reports should not be made in an insulting way or contain personal insults or judgements intended to offend or harm the honour and/or personal and/or professional decorum of the person to whom the reported facts refer.

In any case, it is forbidden to:

[47] "This consequently excludes, for example, reports referring to work disputes and pre-dispute stages, discrimination among colleagues, interpersonal conflict between the whistleblower and another worker or with their superiors, reports relating to the processing of data carried out in the context of an individual work relationship without any damage to the public interest or integrity of the public administration or private entity", as per the ANAC Guidelines approved with ANAC Resolution 311 of 12/7/2023, page 28.

[48] Referred to in Part II of the Annex to Directive (EU) 2019/193725.
"For example, the reporting procedures referring to market abuses pursuant to Regulation (EU) no. 596/2014 of the European Parliament and Council, Implementation Directive (EU) 2015/2392 of the Commission adopted on the basis of the aforementioned regulation, which already contain detailed provisions on the protection of whistleblowers", as per the ANAC Guidelines approved with ANAC Resolution 311 of 12/7/2023, page 28.

- send Reports purely for defamatory and slanderous purposes;
- send Reports relating exclusively to aspects of a person's private life, without any direct or indirect connection to the business/professional activity of the Reported Person;
- send Reports concerning disputes, claims or requests related to the Whistleblower's personal interests;
- send Reports of a discriminatory nature, insofar as they refer to the sexual, religious or political orientation or ethnic origin of the Reported Person;
- send Reports made for the sole purpose of damaging the Reported Person.

Disciplinary action may be taken against any Group employee who files a report of this kind. In addition, a Whistleblower who has made a Report with malice or gross negligence may be sanctioned if the Report proves to be unfounded.

6.3 Protection for the Whistleblower

The whistleblowing procedure can be subject to a certain degree of mistrust in its application due to the fear that the potential Whistleblower may not be appropriately protected from the risk of Retaliation or discrimination in the workplace as a result of the Report. Terna and Group companies safeguard confidentiality and protect the Whistleblower from retaliatory measures as referred to in para. 2.

With specific reference to the WB Decree, measures are taken to protect the confidentiality of the Whistleblower's identity both during the receipt phase and when managing the Report using the internal Reporting channels set up for this purpose.

In this regard, it is necessary to distinguish between the concepts of "confidentiality" and "anonymity", in that the first one presupposes awareness of the Whistleblower's identity, which is necessary to ensure adequate protection. In fact, anonymity could prevent ascertaining the validity of the report.

Appropriate measures shall also be taken to ensure that Whistleblowers are protected against any form of Retaliation, discrimination or penalisation relating to the Report, and, taking into account the conditions and requirements pursuant to the WB Decree, said measures shall also be adopted to protect the other persons involved in accordance with para. 6.1.2 of these Guidelines and identified in Article 3 of Italian Legislative Decree No. 24/2023, without prejudice to the legal obligations and protection of the rights of the company or the persons involved.

On the one hand, these guarantees prohibit Retaliation for Reports made against the company and, on the other, invalidate any retaliatory acts suffered in violation of this prohibition[49].

[49] Any Retaliation, pursuant to Article 19 of the WB Decree, may be communicated to ANAC for the assessments falling within their remit.

Certain conditions must apply to benefit from the protection regime under the WB Decree:

- the Whistleblower is a person included in the list referred to in Article 3 of Italian Legislative Decree No. 24/2023 (as specified in para. 6.1.1) above;
- the Information on reported Breaches falls within the objective scope of Italian Legislative Decree No. 24/2023 and specified in para. 6.2;
- at the time of the Report or the report to the judicial or accounting authorities or the public disclosure, the whistleblower had "good reason" to believe the information was true[50];
- the Report was made in accordance with the procedures provided for by the internal channels (set up pursuant to these Guidelines as specified in para. 6.4) or external channels (managed by ANAC as referred to in para. 6.9 below) or as contemplated for Public Disclosure pursuant to Art. 15 of the WB Decree (and referred to in para. 6.10).

Grounds for applying the sanctions included in the Disciplinary System include a breach of the measures in place to protect the Whistleblower and the Other Parties referred to in para. 6.1.2 of these Guidelines and identified in Article 3, paragraph 5 of Italian Legislative Decree No. 24/2023. More specifically, the following is subject to disciplinary sanctions, in accordance with Italian Legislative Decree no. 24/2023:

- retaliatory conduct in breach of Article 17 of Italian Legislative Decree no. 24/2023, i.e. any conduct, act or omission, albeit only attempted or threatened, in respect of the Whistleblower and which may directly or indirectly cause wrongful damage to the Whistleblower;
- conduct that could obstruct the Report;
- breaches of the measures protecting the Whistleblower with regard to the duty of confidentiality.

The confidentiality of the Whistleblower is not guaranteed when:

- the Whistleblower gives his/her express consent to the disclosure of his/her identity;
- a first instance judgment has established the criminal and/or civil liability of the Whistleblower for the offences of slander or defamation or in any case for crimes committed in connection with the Report;
- anonymity is not enforceable by law if the Whistleblower's identity is required by the judicial authorities in connection to the investigations (criminal, tax or administrative) or inspections by Control Bodies arising from the Report itself.

6.3.1 Limitations on protection for the Whistleblower and protection of the Reported Person

The WB Decree contemplates cases where the whistleblower is not entitled to protection:

[50] On the basis of alleged concrete circumstances and acquired information and, therefore, not on mere inferences.

- if the Whistleblower's criminal liability for the crimes of defamation or slander is established, albeit by a first instance judgment, or if said crimes are committed by reporting to the judicial or accounting authorities;
- in case of civil liability for the same reason due to wilful misconduct or gross negligence.

In both cases, a disciplinary sanction will be imposed on the Whistleblower or complainant.

Criminal, civil or administrative liability is not, however, ruled out for conduct, acts or omissions that are not related to the Report, the report to the judicial or accounting authorities or the Public Disclosure or not strictly necessary to disclose the Breach (Art. 20, para. 4 of Italian Legislative Decree No. 24/2023).

The breach of the provisions of Italian Legislative Decree No. 24/2023 on the subject of reports of illicit conduct constitutes grounds for application of the penalties provided for by the Disciplinary System. More specifically, the following qualify for disciplinary sanctions: cases where the Whistleblower is found liable for defamation or slander in cases of wilful misconduct or gross negligence, unless the Whistleblower has already been convicted, albeit in the first instance, for the crimes of defamation or slander or in any case, the same crimes committed with the report to the judicial or accounting authorities, without prejudice to the administrative sanctions imposed by ANAC pursuant to Article 21 of the aforementioned WB Decree.

With regard to protection for the Reported Party, the management of the Reporting channels established in terms of these Guidelines also ensures protecting the confidentiality of the Reported party's identity in accordance with the WB Decree, so as to avoid the improper circulation of personal information, not only externally, but also within the company itself, to persons that are possibly not authorised to process said data, right up until the completion of the proceedings initiated due to the report.

The Reported Party is not entitled to always be informed about a Report that may refer to them. The Reported Party shall be informed about the Report that refers to them after the verification and analysis of the Report, in which case: (i) proceedings have been initiated against him/her following the verification and analysis of the Report and (ii) said proceedings are based entirely or partially on the Report. In this case, the Reported Party can be or will be heard, on the basis of his/her request, including by way of acquiring written remarks or documents in a hard-copy format.

Finally, if the complaint in the Report is substantiated, in its entirety or in part, and knowledge of the identity of the Whistleblower is indispensable for the accused's defence, the Report can used for the purposes of the disciplinary proceedings only if the Whistleblower expressly consents to the disclosure of his/her identity (as per para. 6.4.1).

6.3.2 Prohibition of Retaliation

Retaliation is forbidden and sanctions are applicable in the case of any retaliatory measures against the person of the Whistleblower or the person who reports the Breaches contemplated in the WB Decree to the judicial or accounting authorities, which they may become aware of.

The company protects the Whistleblower and the Other parties specified in Article 3 of Italian Legislative Decree no. 24/2023 (and referred to in the previous para. 6.1.2) from any form of Retaliation, by setting rules aimed at preventing or negating the effects of acts or measures aimed at punishing the Whistleblower for disclosing information and/or at preventing the Report.

This prohibition imposed by applicable legislation not only includes conduct, acts or omissions by reason of the Whistleblowing that causes unjust damage to the Whistleblower, but also attempted or threatened Retaliation. The unjustified harm caused may also be indirect.

The burden of proof that said conduct or acts were motivated by reasons extraneous to the Reporting, Public Disclosure or Complaint, in the case of the Whistleblower, falls to the company that implemented them, and will therefore be required to prove that the measures taken were based on reasons extraneous to the Reporting.

As far as Other persons are concerned, the onus is on them to prove that the conduct, act or omission was caused by the Report, and was therefore retaliatory in nature.

To safeguard this protection, current legislation specifies that the Whistleblower may inform the ANAC of the retaliatory measures he/she believes to have suffered.

6.4 Internal channels for making Reports

The following internal reporting channels are in place to make reports ("**internal reporting channels**"), which ensure the confidentiality of the Whistleblower's identity and the security of information, providing selective access only for specifically authorised personnel. In particular, the following are available:

- an **IT portal** ensures an effective access point to the channels dedicated to Terna Group companies, to which a report can be addressed. The IT Portal guarantees confidentiality and protection to the whistleblower's identity on the basis of an advanced communications encryption system, the confidentiality of the person involved and of the person in any case mentioned in the Report, as well as the content of the report and the relevant documentation are also guaranteed, in accordance with the provisions of the WB Decree.
- **direct reporting procedure**, aimed at enabling Reports to be made through agreed meetings to be held exclusively with the persons specifically authorised to receive Reports.
- **ordinary mail channel**, which allows Reports to be made by ordinary mail and where possible, with regard to the data provided by the Whistleblower, guarantees the treatment provided for in

the WB Decree for the purposes of communicating with the Whistleblower during the stages managing the Report itself.

The internal channels established should be understood as privileged channels.

This principle, as set out in the reference legislation, is aimed, on the one hand, at "fostering a culture of good communication and corporate social responsibility within organizations" and, on the other hand, at ensuring that by bringing to light acts, omissions or illegal conduct, Whistleblowers contribute significantly to improving their organization[51].

Internal channels are managed, as per para. 6.5 below, by persons that have been formally identified.

If the Report is erroneously submitted to a person that is not responsible for this (other than the person formally identified) or to a channel of another Group Company that is not the one involved, where the Whistleblower has specified that they wish to benefit from the whistleblowing protection provided by the WB Decree or that this intention is clearly evident from references made to the WB Decree, the Reports must be forwarded to the Manager (via the Audit Manager) within 7 days of their receipt, without retaining a copy thereof, also giving notice of the transmission to the Whistleblower, where possible.

6.4.1 IT portal

To make a Report, the Whistleblower must access the Portal, where he/she will find the channel dedicated to the Group company to whom the Report will be addressed. The access link to the Portal is as follows: https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione.

Company channels

The Portal has separate Reporting channels for the relevant Group companies pursuant to Article 4, paragraph 4 of the WB Decree and a shared channel for the remaining Terna Group Companies. More specifically, there are channels within the Portal for:

- Terna S.p.A.;
- Terna Rete Italia S.p.A.;
- Tamini Trasformatori S.r.l.;
- Altenia S.r.l.;
- Other Terna Group companies[52]/Bodies.

[51] Pursuant to Article 47 of Directive (EU) 1937/2019.

[52] Pursuant to Art. 4, paragraph 4 of Italian Legislative Decree No. 24/2023, these companies may share the internal reporting channel and its management.

Reporting procedures

By accessing the channel of the selected Group company (e.g. the Terna S.p.A. channel or the Terna Rete Italia S.p.A. channel or another channel), the Whistleblower has the option of making the Report either in writing by manually processing the content, or verbally by sending a voice message subject to express consent of the voice recording. It is possible to play back, save or reject the Report before sending it: after it has been sent, in the case of an oral Report, the system changes the voice parameters in the case of an Oral Report, so that the recording is not recognisable.

Reports much be made in good faith and may not be made anonymously.

To make a Report, after having received the appropriate data processing notice, the Whistleblower must register its data in the specified fields. This registration requires that a personal e-mail address and telephone number are provided, in order to receive the double security code for subsequent access and allow for the dialogue between the company and Whistleblower to be conducted in a dedicated and confidential manner regarding any further clarifications and the Feedback on the Report made.

Data on the whistleblower's identity will be stored in the IT tool and covered by an encryption system (to the extent that the report is anonymised but not anonymous). The data may be decrypted when strictly necessary for investigation purposes, while maintaining its confidentiality, and only in the cases provided for by the WB Decree and with the express consent of the Whistleblower, may they be disclosed to persons other than those qualified to receive or follow up the Report (i.e. when this is necessary to allow the accused to defend himself in disciplinary proceedings based solely on the Report, and where the knowledge of the Whistleblower is indispensable for the defence of the person involved). In this case, prior to requesting decryption, the RIA will endeavour to obtain the Whistleblower's consent via the same platform and provide him/her with the reasons.

The motivated request for decryption is sent via the Portal, by the Chairman of the Ethics Committee ("**ECP**") to Terna's Chief Information Security Officer ("**CISO**")[53] who supports the activities for decrypting the Whistleblower's identity data without having any access to the Report itself. In this case, the CISO will be informed that the Whistleblower's consent has been obtained, where required under the WB Decree. In case the ECP's impediment, the request for decryption is made by the RIA, with the ECP's knowledge.

[53] In the case of a Report concerning a significant Subsidiary, the request is also communicated for information to the Contact Person identified for the specific Report as specified in para. 6.5.

Portal Management

When managing Reports and in addition to the tasks specifically attributed to the Audit Department for investigation purposes, the RIA oversees and manages the Portal under its responsibility (except as expressly excluded in the event of a conflict of interests or due to specific tasks attributed to other categories of users, e.g. for the amendment of the minutes of the Ethics Committee that examined the evidence of the investigation).

In the scope of managing the Portal, the RIA is responsible for uploading the Reports received outside the Portal and for allocating the Reports received via the Portal, authorising the **Whistle Editor** to do so on its behalf if this is not done directly.

To carry out updating and administration activities on the Portal, the RIA may avail itself of the **Portal Editor**, as the entity identified by the RIA, within the scope of audits and from those registered as users of the Portal. No access to Reports is associated with the role of Portal Editor.

Through the Portal, the RIA (or the ECP in the case of a conflict of interests for the RIA) will identify, within the Audit framework and from the subjects registered as users of the Portal and as indicated in the para. 6.5 below, the Owner that will carry out the investigation as a duly authorised and qualified person. In the scope of these activities, the Owner is the person who will enter the documentation on the investigation into the Repository of the relevant channel, and liaise with the Whistleblower via the Portal, providing him/her with feedback.

Where duly authorised by the RIA (or the ECP in the case of a conflict of interests for the RIA), the owner shall delete the Reports where the requirements of the WB Decree have been met and/or the retention period of the Reports has expired[54], informing the significant Subsidiary's Contact Persons in advance, where applicable.

Access to the Portal will be tracked as well as the replacement and deletion of documents and reports.

The management of the technical functionalities and platform updates are entrusted to the Portal's System Administrator in charge of Terna's Enterprise Services and Platforms ("**ITD-ESP**") structure, who will do so on the basis of Audit's inputs: this Administrator will not be able to see and manage any Report while maintaining maximum privileges on all the platform functionalities pertaining to the role merely providing technical support.

[54] Under the terms of Art. 14, paragraph 1 of Italian Legislative Decree 24/2023, Reports and the relative documentation are retained and filed in the Repository for each internal channel for as long as necessary to process the Report, and in any case no longer than five years from the date when the final outcome of the Reporting procedure is communicated, unless further retention is required in the event of legal proceedings or requests by the Authorities or the commencement of litigation, or required by the Authorities or the start of the dispute. The same applies to the hard-copy documentation relating to the Report received outside the Portal pursuant to para. 6.8. Regarding Reports of crimes not contemplated by Italian Legislative Decree No. 24/2023, data will again be stored in the Repository for the time strictly necessary to pursue the purposes for which it was collected and in compliance with the provisions protecting the rights of data subjects and in accordance with the statute of limitations established by Law.

6.4.2 Direct meeting

As an alternative to the aforementioned reporting channel, 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. This email address may be used exclusively in order to send a request for a meeting and may not be used to send written reports

6.4.3 Ordinary Mail

The use of the Portal constitutes the greatest guarantee for confidentiality. Any Reports, which may otherwise be made by ordinary mail, will be accepted if addressed to the Group Company concerned, to the attention of the Audit Manager c/o TERNA S.p.A, Viale Egidio Galbani, 70 - 00156 Rome, using the following wording "*whistleblowing report, confidential - do not open*" and if duly substantiated, so that the facts can be assessed and based on precise and concordant elements of fact, although they may not be considered as reports under the WB Decree for the purposes of the management of communications with the whistleblower and feedback. In the absence of the specific wording shown above, the Report cannot be received and managed in accordance with the provisions of Italian Legislative Decree no. 24/2023.

All appropriate measures will be taken to ensure, also with respect to this method, the confidentiality of the information and data in the Report.

6.5 Management of Reports

6.5.1 Responsible persons

Individuals responsible for managing the Report are formally identified, pursuant to Italian Legislative Decree no. 24/2023, the Code of Ethics and personal data protection legislation.

The corporate bodies responsible for handling Reports are:

- the Audit Manager, in regard to receiving and investigating Reports;
- the Ethics Committee, in regard to analysing the admissibility, content and investigation into the Report and for the necessary follow-up to the Report.

The members of the Ethics Committee are appointed by Terna's CEO.

Reports are handled by the RIA, together with the members of the Ethics Committee, in a transparent manner through a pre-defined process.

In the handling of Reports, the aforementioned corporate bodies, each within the scope of its own remit, ensure:

- that an acknowledgement of receipt for the Report is issued to the Whistleblower within seven days of the date of receipt for Reports in terms of the WB Decree;
- where possible, also depending on the channel chosen by the whistleblower, maintaining contact with the latter, and if necessary, requesting additional information and documents;
- that there is a diligent follow-up to the Reports received;
- a Reply is provided to the Report within three months from the date that receipt of the Report was acknowledged or, in the absence of such an acknowledgement, within three months from the expiry of the period of seven days from the submission of the Report.

The management of Reports for Terna Group companies takes place on the basis of appropriate intra-group agreements with Terna and provides for procedures to ensure the involvement of the significant subsidiaries. In this respect, also in such cases, the involvement of the Audit Manager is required, consistently with what is indicated in this paragraph, to ensure compliance with the regulatory requirements concerning the receipt, analysis and Reply to the Reports received, without prejudice to the central role of the Ethics Committee and the separate collection, processing and management of the Reports received for each company. However, if the report has been addressed to the channel of a significant Subsidiary and concerns the same, the Audit Manager also involves a Contact Person (from among at least two nominated) in the preliminary investigation phase, appointed by the same significant subsidiary receiving the Report in order to ensure the proximity of the report management activity with the said company. The Contact person involved will be able to view all the investigative evidence and will be invited to attend the Ethics Committee: the body called on to assess the outcome of the investigation and to follow up on the Report, taking into account the Contact Person's opinion.

The persons in charge of handling the Report may not reveal the identity of the Whistleblower or other information from which it can be deduced to any other person who is not duly involved in the investigation without the Whistleblower's express consent.

The persons responsible for handling the Report are informed if there a Report is received via the RIA[55]. Reports will be shown to the persons necessarily involved in the management of the specific Report (Owner, Ethics Committee members including the Committee Secretary), according to the profiling on the individual channel and the assignments made by the RIA.

- In the case of a Report via the Portal, the Audit Manager[56] is informed by an alert generated by the Portal, which arrives in the form of an e-mail notification to his/her e-mail inbox. The

[55] Except in cases of potential conflicts of interest of the RIA, in which case the Report will be forwarded directly to the Chairperson of the Ethics Committee.

[56] Terna has identified the Audit Manager as the person appointed to receive Reports, without prejudice to the central role of the Ethics Committee. The reason for this choice is due to the manager's organizational positioning. Given that he/she has no operational powers and reports directly to the Chairperson

same alert is sent by the Audit Manager to the Contact Persons of the relevant Subsidiary without a conflict in the event of a Report addressed to the latter[57].

- In the event that Reporting is done on the basis of face-to-face meetings, two people need to receive the Reports. The Audit Manager, accompanied by another person from the Audit Department, receives the request for a meeting in accordance with para. 6.4.2 and, after agreeing to the meeting itself, supports the Whistleblower in entering the Report into the Repository of the Group company concerned and initiates the verification process as described in this paragraph.
- If, on the other hand, the Report is done via ordinary mail, it shall be received by the Audit Manager in accordance with the relevant internal rules and regulations and as provided for in paragraph 6.4.3 of these Guidelines. After verifying the contents of the envelope, the Audit Manager shall enter (directly or by means of a Whistler Editor) the Report into the Repository of the Company receiving the Report and start the verification process as described in this paragraph.

6.5.2 Stages of management and investigative activities

Upon receipt of a Report through one of the internal channels indicated in para. 6.4., a preliminary assessment is carried out on the Report to ascertain:

(iii) whether it concerns a Violation;

(iv) whether the objective and subjective requirements of a relevant Report are present.

Based on the content of the Report, the Audit Manager defines the procedures for investigating the Report and the persons to involve, assessing who will be most appropriate. Specifically, the RIA (directly or through the Portal Editor) shall assign the management of the verification process to a duly authorised and trained employee in its structure (the so-called "**Owner**"). They shall also assess any involvement of other structures in relation to the subject of the Report itself (e.g. Fraud Management, Data Protection & Privacy, etc.) if necessary for investigative purposes, maintaining the confidentiality of the Report in their regard and providing them only with the data needed for their activities[58]. The involvement of any additional corporate structures shall comply with the principle of

of the Board of Directors, they are the person that can provide the greatest level of independence in the context of the activities relating to managing the Reports.

[57] This message will not include any element relating to the Whistleblower's identity and/or the content of the Report. The purpose of the alert is to ensure that the relevant Subsidiary is aware of the existence of the Report received, and to monitor that the Reports received correspond with those that are examined.

[58] If the Whistleblower has declared that the Report involves the RIA (by ticking the appropriate flag on the Portal), the IT system will send the Report to the Chairperson of the Ethics Committee, who will perform the functions of the RIA for the purposes of these Guidelines with regard to handling the Report.

data minimisation, with communication limited solely to the information strictly necessary for the performance of the investigative activities assigned. In order to ensure that the Ethics Committee has timely access to all the investigative documentation necessary to perform its duties, the RIA shall also grant access to the specific Report to members of the Ethics Committee (and the Secretary of the Committee), excluding any members involved in the Report.

The Contact Person involved (in the event that the Report concerns a significant Subsidiary) will be able to view all the investigative evidence relating to the specific Report.

The Audit Manager, with the appointment of the Owner, initiates the investigative activities in order to identify, analyse and assess the elements confirming the validity and significance of the facts reported[59]. The results are included in the investigation reports (Reports) prepared by the Owner and approved by the Audit Manager. The Report (both the final report and any supplementary reports) is shared in the case of Significant Subsidiary Reports with the identified Contact Person.

6.5.3 Role of the Ethics Committee

The Audit Manager shares the final Report with the Ethics Committee, in order to:

- decide on the follow-up to be taken on the Report, including any additions to the investigation, where deemed necessary;
- confirm the closure of the Report, if this has been proposed by the Audit Manager.

Members of the Ethics Committee are informed by the Audit Manager, or by the Chairperson of the Ethics Committee in the cases referred to in para. 6.6, via the Portal for each Report received.

The operating procedures of the Ethics Committee are governed by specific Ethics Committee regulations[60].

The RIA, as the Manager of Terna's Audit Department, within which the investigation is carried out, also participates in meetings of the Ethics Committee (if not involved in the Report) through its delegate (preferably in the person of the Owner in charge of the Report).

Only upon completion of the management activities, the Manager shall inform top management or the relevant corporate functions of Companies that are not relevant and the relevant subsidiaries (via the Contact Person) for the consequent follow up measures. The Manager is not responsible for making any assessment regarding personal responsibility and any subsequent measures or proceedings.

[59] Information that is clearly not useful for managing a specific Report is not collected or, if accidentally collected, is promptly deleted, thus interpreting the principle of minimisation pursuant to Art. 13, para. 2 of Italian Legislative Decree no. 24/2023 on a restricted basis, where the absolute non-relevance is clear in relation to the reported event, and without prejudice to the sector regulations referring to the retention of documents.

[60] See LG014 Ethics Committee Regulation.

6.5.4 Reports of breaches of the 231 Model and Flows to the SB

With reference to Reports pertaining to the private sector, not related to the Concession of a public service, Breaches relevant to Italian Legislative Decree No. 231/2001, as well as Breaches of 231 Models, may only be reported via internal reporting channels.

In compliance with the confidentiality obligation stipulated in the WB Decree and in the applicable corporate procedures, the Manager (through the Audit Manager) promptly sends an e-mail to the Supervisory Body of the Company concerned (and to the Technical Secretariat of the Supervisory Board identified by the company) with the appropriate information on the receipt of any Reports concerning actual or potential breaches of the 231 Model and/or unlawful conduct constituting the types of offences covered by Italian Legislative Decree 231/2001. Following the outcome of the investigation and the assessment of the Ethics Committee, the RIA shall promptly send a notification to the SB in which it shares, in accordance with the principle of confidentiality: i) the investigative activities carried out; ii) the results thereof; iii) the decision taken by the Ethics Committee.

If the Supervisory Body erroneously receives Reports, it shall forward them to the Manager (via the Audit Manager) within 7 days of their receipt, without retaining a copy thereof, also giving notice of the transmission to the Whistleblower, where possible.

6.6 Managing potential conflicts of interest

If the RIA is involved in the Report, the Report will be handled by the Chairperson of the Ethics Committee, as regulated in paragraph 6.4.1 above.

Reports will be shown to Managers based on individual channel profiling and the assignments made by the RIA. If one of the members of the Ethics Committee is involved in the Report, he/she will not receive any notice concerning the Report involving him/her and will not participate in the relevant Ethics Committee activities (as stipulated in the Ethics Committee Regulation[61]).

Furthermore, with reference to the management of Reports concerning significant Subsidiaries, each of them will identify at least two Contact Persons as required in para. 6.5 above: this assignment is predetermined in relation to the receipt of the Report by the Audit Manager, to ensure proximity of the activity with the Group company to whom the Report is addressed. Once the Report has been received, the RIA identifies one of the appointed Contact Persons. Where a potential conflict of interests in relation to one of the Contact Persons emerges, the Audit Manager shall opt for another one from those appointed, bearing in mind that the Contact Person involved will be able to view all the investigative evidence and will be invited to participate in the Ethics Committee called to assess the outcome of the investigation and to follow up on the Report.

[61] See LG014 Ethics Committee Regulation.

6.7 Processing of personal data

Processing of personal data collected in the context of the reporting procedure occurs in full compliance of the Privacy Regulation, in keeping with the provisions under Italian Legislative Decree no. 24/2023, ensuring a fair balance between the Whistleblower's rights and their right to maintain their identity confidential, by implementing the technical and organizational measures in these Guidelines, which are appropriate to ensure the security of personal data in accordance with the legislation in force. These measures include, merely by way of non-exhaustive example, access segregation, the encryption of identifying data, the tracking of access and operations carried out on the system, as well as specific procedures for the authorisation and training of the personnel involved. The processing of personal data carried out as part of the whistleblowing system has its legal basis in the fulfilment of a legal obligation to which the Controller is subject, pursuant to art. 6, para. 1, letter c) of Regulation (EU) 2016/679, as provided for by Italian Legislative Decree 24/2023.
As part of the management of Reports, it may be necessary to process personal data belonging to special categories pursuant to art. 9 of the GDPR as well as data relating to criminal convictions and offences pursuant to art. 10 of the GDPR — merely on a case-by-case basis, not systematically — exclusively to the extent strictly necessary in order to ascertain the facts reported and in accordance with the guarantees provided for by the applicable legislation. This is without prejudice to the fact that, the exercising of rights by the Whistleblower or the Reported Person (the "data subjects" under the Privacy Policy), in relation to their personal data processed within the Whistleblowing process, may be limited[62] to ensure the protection of the rights and freedoms of others, with the specification that under no circumstances may the Reported Person be allowed to use their rights to obtain information on the Whistleblower's identity[63]. The operating procedures for exercising the rights of data subjects are regulated by internal rules on the protection of personal data and the privacy disclosures made available to the data subjects.
The Report management system is therefore structured in such a way as to guarantee the rights and freedoms of data subjects, with the specific allocation of roles/responsibilities related to data processing and the related background documentation.
More specifically, within the Group, pursuant to Italian Legislative Decree no. 24/2023, the significant subsidiaries[64], will process the data of their internal reporting channel as autonomous Data

[62] Pursuant to art. 23 of the GDPR and art. 2-undecies of Italian Legislative Decree 196/2003.

[63] Pursuant to Art. 2-undecies of Italian Legislative Decree no. 196/2003, the data subject will not be able to exercise their rights if exercising those rights could cause actual and material prejudice to the protected interests (by way of example, carrying out defence investigations, exercising rights in court; confidentiality of the identity of the employee reporting the offence, etc.). The Data Controller may therefore in any event, delay, limit or exclude the exercising of these rights by providing a prompt motivated notice to the data subject in this regard.

[64] As at the date of these Guidelines: Terna S.p.A., Terna Rete Italia S.p.A. and Tamini Trasformatori S.r.l.

Controllers. For the Terna Group Companies[65], a shared reporting channel may be used with the relative management by the companies themselves, as joint data controllers, pursuant to Art. 26 of the GDPR, on the basis of a specific Joint Ownership Agreement in which the respective responsibilities regarding compliance with the obligations deriving from the GDPR are stipulated, with particular regard to the exercising of the data subject's rights and the respective functions of disclosure of information, pursuant to Art. 13 and 14 of the GDPR. The suppliers who support the management of the IT Portal and the related technological infrastructure are designated as Data Processors pursuant to art. 28 of the GDPR, on the basis of specific contractual agreements which regulate the instructions, security measures and limits on processing.

Therefore, the mandatory privacy information is made available by the companies in their capacity as 'autonomous data controllers' and 'joint data controllers', specifying the purposes, terms and methods of data processing related to the reporting procedure.

They are expressly authorised to process said data pursuant to Articles 29 and 32 of the GDPR and Art. 2-quaterdecies of Italian Legislative Decree no. 196/2003 and, for this reason, the persons entrusted with the receipt and management of Reports are recipients of specific instructions.

In addition, in line with the regulatory requirements of Italian Legislative Decree no. 24/2023, the system for receiving and handling Reports through internal channels is defined on the basis of a data protection impact assessment (DPIA), where the areas of processing and associated risk profiles are systematised, including the technical-organizational measures to reduce the identified risks.

6.8 Filing and storing of Reports

If the Report was made through the internal IT channel pursuant to para. 6.4.1, the channel acts as an official Repository, allowing for the Report to be filed, and any associated documentation to be retained.

If the Report is made by ordinary mail or, alternatively, on the basis of a face-to-face meeting, it is the RIA's responsibility to upload the Report onto the Portal, in the channel of the company to whom the Report is addressed as per para. 6.4.1., so that it can be properly filed, whilst retaining the original documentation in such a way that ensures its confidentiality, as far as possible.

Finally, the Reports and related documentation must be kept for as long as necessary to process them, and in any case, pursuant to the WB Decree, for no longer than five years from the date when the final outcome of the Reporting procedure was communicated, or for the different retention

[65] These are Terna Group companies with fewer than 249 employees pursuant to Article 4, paragraph 4 of the WB Decree.

periods contemplated by law, as specified in para. 6.4.1. The starting date of the retention periods depends on the final outcome of the Report (i.e. direct filing, results of the final investigation; transmission to the relevant Authorities, etc.); the RIA will therefore be responsible for authorising the deletion and/or destruction of any hard-copy documentation retained as referred to in para. 6.4.1, informing the Contact Persons of the relevant Subsidiary in advance, where applicable.

6.9 External channel

Pursuant to the provisions of the WB Decree, the Whistleblower may use the external reporting channels set up by ANAC, available on the ANAC website[66], only for the Breaches referred to the WB Decree (except for those pertaining to the private sector, not inherent to the Concession of Public Services), and where the following prerequisites stipulated in the WB Decree apply, namely:

- failure to activate internal reporting channels;
- there was no Follow-up on the Report made in accordance with the provisions of the WB Decree and these Guidelines;
- the whistleblower has reasonable grounds to believe that, if he/she were to report internally, it would not be followed up on or that he/she would face Retaliation. With regard to reasonable grounds, it is specified that the Whistleblower must be able to reasonably believe, on the basis of the concrete circumstances attached and information actually acquirable and, therefore, not on mere inferences, that, if he/she made an internal Report:
  - it would not be effectively followed up. This is the case when, for instance, the person ultimately responsible in the work context is involved in the Breach, there is a risk that the Breach or related evidence might be concealed or destroyed, the effectiveness of investigations by the competent authorities might otherwise be compromised, or also because it is felt that ANAC would be better placed to deal with the specific Breach, especially in matters within its remit;
  - this could lead to the risk of Retaliation (e.g. also as a consequence of breaching the obligation to keep the identity of the Whistleblower confidential).
- he/she has reasonable grounds to believe that the Breach may constitute an imminent or obvious danger to the public interest. This is the case, for instance, when the Breach requires urgent action to safeguard the health and safety of persons or to protect the environment[67].

[66] More details are available in the specific section on the ANAC website, on how to communicate, receive and manage Reports to this Authority. According to the provisions of the WB Decree, the possibility of recourse to the external channel and Public Disclosure is exclusively reserved for companies with more than fifty employees.
As specified in paragraph 6.5.2., Reports pertaining to the private sector, not related to the Concession of a public service, Breaches relevant to Italian Legislative Decree No. 231/2001, as well as Breaches of 231 Models, may only be reported via internal reporting channels.

[67] Pursuant to Article 62 of Directive (EU) 1937/2019.

The Whistleblower and Other parties may communicate with ANAC, pursuant to Art. 19, para. 1 of the WB Decree, regarding the Retaliation that the former have suffered in their workplace following Reports, complaints or Public Disclosures.

If the Manager should receive the notification of retaliation, the Manager shall advise the Whistleblower that this could be forwarded to ANAC. The objective details shall be supplied to ANAC, which make clear the consequential link between the Report, complaint or Public Disclosure made and the Retaliation complained of.

6.10 Public Disclosure

In accordance with the provisions of the WB Decree, the Whistleblower[68] may also make a public Disclosure of Information on Breaches provided for in the WB Decree (with the exception of those pertaining to the private sector, not pertaining to the Public Service Concession), of which he/she has become aware in the context of his/her work, only if the following conditions set out in the same decree are met, namely:

- the Whistleblower had previously used the internal or external channel, but there was no Response or no Follow-up within the deadline;
- the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest[69];
- the Whistleblower has reasonable grounds to believe that an external Report may lead to the risk of Retaliation, or may be ineffective due to particular circumstances applicable to the specific case[70].

Reasonable grounds for recourse to Public Disclosure must be based on concrete circumstances, which must be attached to the Report, and on information actually acquirable.

In public disclosure, where the person voluntarily discloses his/her identity, the protection of confidentiality is not relevant, without prejudice to all other forms of protection provided by the WB Decree for the Whistleblower. Where, on the other hand, a person discloses Breaches using, for instance, a pseudonym or nickname, which in any case does not allow for them to be identified, the Report may be treated, for the purposes of the confidentiality of the Whistleblower's data and in the

[68] "*If they are a person that differs from the party providing the source of journalistic information*" (see para. 3.3 of Resolution No. 311 of 12 July 2023 were submitted to the Secretary of the Board on 13 July 2023 and published, through an announcement in Official Gazette No. 172 of 25 July 2023, containing "*Guidelines on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national law.* Procedures for the submission and management of external reports").
As specified in paragraph 6.5.2., Reports pertaining to the private sector, not related to the Concession of a public service, Breaches relevant to Italian Legislative Decree No. 231/2001, as well as Breaches of 231 Models, may only be reported via internal reporting channels.

[69] Considered as an emergency situation or risk of irreversible damage, including personal injury to one or more people, which requires that the Breach is promptly revealed on a broader scale to prevent its effects.

[70] Because, for example, there could be a risk that evidence is destroyed or there could be collusion between the authority responsible for receiving the Report and the person perpetrating the Breach. These should therefore be considered as especially serious cases of negligence or fraudulent conduct within the company.

event of subsequent disclosure of his/her identity, in the same way as an anonymous Report (therefore, the protection provided by the Decree cannot be guaranteed); in the event of subsequent disclosure, the Whistleblower will still be guaranteed the protection provided in the event of Retaliation.

The Whistleblower is required to send the Report subject to public disclosure to the Company using the specific e-mail set up at whistleblowing@terna.it,so as to allow the Whistleblower to benefit from the protection available (in this respect, see paragraph 6.3 of these Guidelines).

7. Foreign companies

Whistleblowing regulations, internal reporting channels and protection for the Whistleblower and Reported Person as described above, also apply to foreign Companies, in compliance with local legislation.

To that end, it should be noted that the transfer of personal data coming from third countries is allowed pursuant to and within the limits of the laws applying to the individual case. In this regard, infra-group agreements that could govern the management of Reports for foreign companies pursuant to para. 6.5, shall be supported by additional specific agreements to ensure that data is processed in accordance with applicable legislation.

With regard to roles and responsibilities, in handling reports which fall under the responsibility of the Manager, support may be requested from the Compliance Officer appointed by the company concerned and/or external consultants; the involvement of the CO at this stage is limited to the acquisition of information in furtherance of the investigation.

If on the other hand, it is impossible for the FC to adopt the whistleblowing regulation using internal reporting channels as per these Guidelines, the FC shall put in place reporting procedures for Information on breaches that are consistent with the Code of Ethics 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 FC.
- ensure that adequate information is available regarding the reporting system for Information on breaches, the user procedures and protection system put in place.

8. Approval, review and dissemination

The principles of these Guidelines are among the Terna Group's core values and inspire its organization and business, also in the implementation of the provisions of the Code of Ethics. For

this reason, these Guidelines are intended for all employees (including employees hired with fixed-term contracts), trainees and temporary workers, and are approved by the CEO and General Manager of Terna S.p.A.

The adoption and dissemination of these Guidelines by all Group companies is encouraged. To this end, staff awareness-raising and training initiatives are promoted to make the purpose of whistleblowing and the procedure for its use known (such as specific communications, training events, newsletters, intranet, etc.).

In this regard:

a) appropriate training is conducted with reference to the person(s) in charge of managing the internal channels, also by means of special training and induction sessions;
b) appropriate communication provided to achieve the information purposes, concerning the internal reporting channels, procedures and prerequisites for making internal Reports, as well as the channel, procedures and prerequisites for making external Reports under the WB Decree. With regard to the latter, the aforementioned information is published in a dedicated section of the website for the Group's Italian companies, where applicable.

With regard to point a), training must be based on the applicable legislation and best practices.

With regard to point b), communication initiatives to external parties are also promoted for disseminating the purposes of the institution of whistleblowing and the procedure for its use. All Group companies ensure that these Whistleblowing Guidelines are made available internally by posting them on the company intranet or by sending them via e-mail or other means for sharing company documents.

The whistleblowing principles and content that are applicable to third parties are made known through contract documentation.

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

Any amendments and/or additions that may become necessary or even simply appropriate due to regulatory and/or legal developments or to align with best practices and the ANAC guidelines, or in relation to monitoring actions undertaken or to supervening operational or organisational requirements shall be made by the Executive Vice President for Strategy, Digital and Sustainability; providing, where necessary or even simply appropriate, operating instructions to regulate specific profiles for the application of these guidelines and any guidance for subsidiaries. The Ethics Committee must be informed in advance of any such amendments and/or additions, as must the trade unions if they are significant in nature.

9. Reporting

On an annual basis and with reference to the calendar year, if Whistleblowing Reports are received during the period, these will be the subject of a specific report (indicating the number of Reports received, the number of Reports filed and the progress of the relative investigations) prepared by the RIA, in which the Report data will be anonymised and collected in an aggregate format, and sent to the Ethics Committee with regard to Terna S.p.A, and for the other Group companies, also to the CEO/Managing Director, in order to provide an overall representation of the functioning of the whistleblowing system and, within its remit also on a periodic basis, generally every six months, to the SB/CO. Where the RIA has not seen the reports, in cases of conflicts of interest, the Ethics Committee shall complete the reporting described above via the Secretary of the Ethics Committee.

10. Support from Bodies in the Third Sector

The Whistleblower may, at any time, avail of support from the third-sector bodies included on the list published by ANAC pursuant to art. 18 of Italian Legislative Decree 24/2023, which assist with such matters as:

a) information, assistance and consultancy on whistleblowing legislation;

b) legal assistance;

c) psychological support.

The list of partnered bodies which carry out the activities pursuant to Italian Legislative Decree No. 117 of July 3, 2017, in accordance with the provisions of their respective statutes, is available on the ANAC website.