Terna

LG054

Whistleblowing

24.03.2026

LEITLINIEN

Genehmigt

F. Salerni (SDS)

Historie der Revisionen

Rev. 05 vom 24.03.2026	*Sechste Ausgabe, gesetzliche Anpassung.*
Rev. 04 vom 14.12.2023	*Fünfte Ausgabe.*
Rev. 03 vom 12.07.2023	*Vierte Ausgabe.*
Rev. 02 vom 21.12.2018	*Dritte Ausgabe.*
Rev. 01 vom 27.01.2017	*Zweite Ausgabe.*
Rev. 00 vom 30.09.2016	*Erstausgabe.*

Relevante Managementsysteme und/oder Organisationsmodelle

	Zertifizierte/akkreditierte Managementsysteme
☑	***SGQ*** *(Qualität)*
☑	***SGA*** *(Umwelt)*
☑	***SGSL*** *(Sicherheit und Gesundheitsschutz am Arbeitsplatz)*
☑	***SGPIR*** *(Vorbeugung von schweren Unfälle – Seveso-Richtlinie)*
☑	***SGSI*** *(Informationssicherheit)*
☑	***SGE*** *(Eigenverbrauchte Energie)*
☑	***SGQ LST*** *(LST-Labor)*
☑	***SGQ TAR*** *(Kalibrierzentrum)*
☑	***SGAC*** *(Antikorruptionssystem)*
☑	***SGAM*** *(Asset-Management-System)*
☑	***SGPCI*** *(Infektionsprävention und -kontrolle – Biosafety)*
☑	***SGC*** *(Compliance)*
☐	***SGPG*** *(Geschlechtergleichstellung)*
☐	***SGPAC*** *(Administrative und buchhalterische Prozesse)*

	Organisationsmodelle
☑	***BCM*** *(Business Continuity Model)*
☑	***TCM*** *(Tax Compliance Model)*
☑	***PRV*** *(Datenschutzerklärung)*
☑	***M262*** *(Modell 262)*
☑	***M231*** *(Modell 231)*
☐	***MIMP*** *(Unparteilichkeitsmodell)*
☐	***SCIIS*** *(System zur Kontrolle der Nachhaltigkeitsberichterstattung)*

(Weitere Informationen zu zertifizierten/akkreditierten Managementsystemen finden Sie hier)

Inhalt

1. Allgemeines

Terna legt seit jeher besonderen Wert auf die Prävention von Risiken, die eine verantwortungsvolle und nachhaltige Führung des Unternehmens gefährden könnten, und ist im Einklang mit ihrer Mission und ihrem internen Kontrollsystem bestrebt, kritische Situationen zu erkennen und zu korrigieren, um das Vertrauensverhältnis zu den *Stakeholdern* zu festigen.

Die Terna-Gruppe hat bereits im September 2016 ein System zur Entgegennahme und Bearbeitung von Meldungen über Verstöße gegen interne oder externe Vorschriften eingeführt und fortlaufend aktualisiert, um eine verantwortungsvolle Unternehmensführung im Einklang mit den gesetzlichen Vorgaben zu gewährleisten. Das System dient der Sicherstellung von Korrektheit und Transparenz bei der Führung der Geschäfte und der durchgeführten Tätigkeiten sowie dem Schutz der Unternehmensposition und -reputation. Über das System können Situationen gemeldet werden, die dem Unternehmen Schaden oder Nachteile zufügen könnten, wie beispielsweise Betrug, generische Risiken oder potenziell gefährliche Umstände. Dies hat die Aufrechterhaltung des Systems auch im Einklang mit den im Jahr 2017 eingeführten gesetzlichen Bestimmungen gewährleistet, welche „*Vorschriften zum Schutz der Personen, die im Rahmen eines öffentlichen oder privaten Arbeitsverhältnisses Kenntnis von Straftaten oder Unregelmäßigkeiten erlangen und diese melden*“ enthalten. Ebenso wurde das System an die im Jahr 2023 erlassenen Vorgaben angepasst, insbesondere an das GvD Nr. 24/2023 zum *Whistleblowing*[1], das die „*Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 über den Schutz von Personen, die Verstöße gegen das Unionsrecht melden, sowie Bestimmungen zum Schutz von Personen, die Verstöße gegen nationale Vorschriften melden*“ vorsieht (nachfolgend auch „**WB-Dekret**“ oder „**GvD 24/2023**“). Zudem wurden die von der Nationalen Antikorruptionsbehörde (**ANAC**) gemäß Art. 10 des WB-Dekrets erlassenen Leitlinien berücksichtigt[2].

Dieses System bildet einen integralen Bestandteil der ethischen Grundsätze der Gruppe (Ethikkodex) sowie der *Corporate-Liability*-Instrumente, wie den Organisations- und Verwaltungsmodellen gemäß GvD 231/01 („**Modelle 231**“) und – soweit für die ausländischen Gesellschaften der Gruppe anwendbar – des Global Compliance Program (LG058).

Das „Whistleblowing-System“ ist somit Teil der internen Kontrollsysteme, mit denen Terna die Verhaltensregeln für die Ausübung der eigenen Geschäftstätigkeit festlegt. Das Melden von unehrlichem Verhalten, das zu Betrug führen kann, ein Schadensrisiko für Kolleginnen und Kollegen oder Anteilseigner darstellt oder Handlungen umfasst, die die Interessen oder den Ruf des Unternehmens verletzen oder rechtswidrig beeinträchtigen, kann – sofern angemessen geregelt – eine wirksame Form der Korruptionsbekämpfung darstellen.

Mit dieser Leitlinie werden für die Terna-Gruppe die Modalitäten für die Behandlung von Meldungen über rechtswidrige Handlungen und/oder Verhaltensweisen festgelegt, von denen im Rahmen der

[1] *Whistleblowing* ist ein aus dem Englischen entlehnter Begriff, der von der metaphorischen Redewendung „*to blow the whistle*“ (etw. abrupt unterbrechen) stammt. Er bezeichnet ein Instrument, das es jeder Person ermöglicht, rechtswidriges Verhalten – auch nur vermutete Verstöße – zu melden.

[2] Art. 10 des WB-Dekrets sieht vor, dass ANAC – nach Anhörung der Behörde für den Schutz personenbezogener Daten (*Garante per la protezione dei dati personali*) – innerhalb von drei Monaten ab Inkrafttreten des WB-Dekrets die Leitlinien zu den Verfahren für die Einreichung und Bearbeitung externer Meldungen erlässt. ANAC hat auf ihrer Internetseite den Beschluss Nr. 311 vom 12. Juli 2023 veröffentlicht, der am 13. Juli 2023 bei der Geschäftsstelle des Rates hinterlegt und mittels Bekanntmachung im Amtsblatt Nr. 172 vom 25. Juli 2023 publiziert wurde. Der Beschluss enthält die „*Leitlinien zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, sowie zum Schutz von Personen, die Verstöße gegen nationale Vorschriften melden. Verfahren zur Einreichung und Bearbeitung externer Meldungen*“.
ANAC hat zudem den Beschluss Nr. 301 vom 12. Juli 2023 auf ihrer institutionellen Website veröffentlicht, der am 13. Juli 2023 bei der Geschäftsstelle des Rates hinterlegt wurde und gemäß der am 15. Juli 2023 im Amtsblatt publizierten Mitteilung am selben Tag in Kraft getreten ist. Der Beschluss beinhaltet die „*Verordnung über die Bearbeitung externer Meldungen und die Ausübung der Sanktionsbefugnisse von ANAC zur Umsetzung des GvD vom 10. März 2023, Nr. 24*“.
ANAC hat anschließend die Beschlüsse Nr. 478 und Nr. 479 vom 26. November 2025 auf ihrer offiziellen Website veröffentlicht, die im Amtsblatt Nr. 300 vom 29. Dezember 2025 publiziert wurden. Diese betreffen die Leitlinien zum Whistleblowing in Bezug auf interne und externe Meldekanäle.

Gesellschaften der Gruppe Kenntnis erlangt wird – sei es durch Tun oder Unterlassen. Dies erfolgt auch in Übereinstimmung mit der in diesem Bereich geltenden Gesetzgebung. Die Leitlinie betrifft Meldungen über Verstöße, einschließlich bloß vermuteter Verstöße,
(i) gegen die im Ethikkodex verankerten Grundsätze,
(ii) gegen interne Vorschriften, bestehend aus allen Bestimmungen, Verfahren, Leitlinien oder operativen Anweisungen der von der Meldung betroffenen Gesellschaft, einschließlich des Organisations- und Verwaltungsmodells gemäß GvD 231/01 („**Modell 231**"), der Antikorruptionsleitlinien, des Global Compliance Program sowie Verstöße gegen Unternehmensrichtlinien oder -regeln, die zu Betrug oder auch nur potenziellem Schaden gegenüber Mitarbeitenden, Anteilseigner oder *Stakeholdern* im Allgemeinen führen können oder Handlungen darstellen, welche die Interessen oder den Ruf des Unternehmens beeinträchtigen oder rechtswidrig verletzen,
(iii) sowie Verstöße gemäß GvD 24/2023 „*gegen nationale oder EU-Rechtsvorschriften, die das öffentliche Interesse oder die Integrität der öffentlichen Verwaltung oder des privaten Rechtsträgers beeinträchtigen*".
Es wird insbesondere darauf hingewiesen, dass das vorliegende Dokument auch in Übereinstimmung mit den Bestimmungen des WB-Dekrets erstellt wurde, welches das gesetzliche Instrument zur Bekämpfung und Verhinderung von Korruption, von Verhaltensweisen, die nicht den Grundsätzen der ordnungsgemäßen Verwaltung und der Unparteilichkeit der öffentlichen Verwaltung entsprechen, sowie zur Prävention von Gesetzesverstößen im öffentlichen und privaten Sektor darstellt. Das WB-Dekret hat insbesondere ein integriertes Regelwerk eingeführt, das sowohl für den öffentlichen als auch für den privaten Sektor bestimmt ist und das europäische und nationale Recht koordiniert, mit dem Ziel, Meldungen über rechtswidrige Handlungen zu fördern, die das öffentliche Interesse oder die Integrität des Rechtsträgers beeinträchtigen könnten. Das neue Regelwerk erhöht das Schutzniveau, von dem Hinweisgebende profitieren.

2. Zweck des Dokuments

Die vorliegende Leitlinie hat zum Ziel, die Behandlung von Meldungen über Verstöße (Whistleblowing) zu regeln, die internen Meldekanäle der Gesellschaften der Gruppe festzulegen und deren Funktionsweise zu definieren, den Gegenstand der Meldungen sowie die Personen zu bestimmen, die Meldungen erstatten können, die Zuständigkeiten und die Modalitäten für die Durchführung der Analyse- und Untersuchungstätigkeiten nach Eingang der Meldungen (Rollen und Verantwortlichkeiten) sowie die entsprechenden Fristen festzulegen, die Schutzmaßnahmen zugunsten der hinweisgebenden Personen zu bestimmen, die Voraussetzungen für die Abgabe externer Meldungen und für die öffentliche Bekanntmachung zu regeln sowie die Modalitäten und Fristen für die Aufbewahrung der Daten im Rahmen der Whistleblowing-Verfahren festzulegen, auch unter Beachtung der Datenschutzvorschriften[3].
Es werden zudem die Modalitäten für die Bekanntmachung der Informationen über die Nutzung der Meldekanäle und über die Voraussetzungen für die Abgabe von Meldungen über diese Kanäle geregelt, ebenso wie die zuständigen Stellen für die Bearbeitung der Meldungen und die

[3] Der datenschutzrechtliche Rahmen besteht aus den folgenden nationalen und supranationalen Rechtsvorschriften: dem gesetzvertretenden Dekret vom 10. August 2018, Nr. 101, „*Bestimmungen zur Anpassung der nationalen Gesetzgebung an die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie über den freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*"; der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie über den freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO); dem gesetzvertretenden Dekret vom 30. Juni 2003, Nr. 196, „*Datenschutzkodex*", in der jeweils geltenden Fassung, sowie den mit dem Kodex verbundenen Maßnahmen der Datenschutzbehörde zum Schutz personenbezogener Daten.

entsprechenden Verfahren, die Sensibilisierungs- und Schulungsmaßnahmen für das Personal sowie die Modalitäten und Fristen für die Aktualisierung der Leitlinien selbst.

Ferner wird darauf hingewiesen, dass die vorliegende Leitlinie in Übereinstimmung mit den einschlägigen gesetzlichen Bestimmungen erstellt wurde, die für einen spezifischen Kreis italienischer Gesellschaften gelten, sowie mit dem WB-Dekret und den daraus folgenden ANAC-Leitlinien[4], in denen spezifische Bedingungen und Modalitäten im Bereich des Whistleblowings geregelt sind. Diese betreffen insbesondere: den Anwendungsbereich; den sachlichen Schutzbereich; die Meldekanäle und die Modalitäten der Meldungsabgabe; den Schutz der Vertraulichkeit und vor möglichen Repressalien; die Haftungsbeschränkungen für Personen, die Meldungen erstatten, Anzeigen machen oder öffentliche Offenlegungen vornehmen („**relevante Meldungen**“).
Für Meldungen, die nicht in den vorgenannten normativen Anwendungsbereich fallen („**ordentliche Meldungen**“), finden die nachstehenden Bestimmungen lediglich eingeschränkt Anwendung, und zwar hinsichtlich: des Mindestinhalts der Meldung (Abschnitt 6.2.1); der internen Meldekanäle (Abschnitt 6.4); der Bearbeitung der Meldungen (Abschnitt 6.5), mit Ausnahme der im WB-Dekret vorgesehenen Rückmeldungen und Fristen; sowie der Behandlung potenzieller Interessenkonflikte (Abschnitt 6.6).
Auch für die ordentlichen Meldungen wird in jedem Fall die Verarbeitung der Daten gemäß der jeweils anwendbaren Datenschutzregelung gewährleistet, ebenso wie das allgemeine Verbot von Repressalien, das im Ethikkodex vorgesehen ist und ausdrücklich sanktioniert wird, sofern Meldungen in gutem Glauben und im Sinne der Loyalität gegenüber dem Unternehmen erstattet werden.

3. Geltungsbereich

Die vorliegende Leitlinie findet Anwendung auf Terna und auf alle Gesellschaften der Terna-Gruppe, einschließlich der ausländischen Tochtergesellschaften, unbeschadet dessen, was im folgenden Abschnitt 7[5] vorgesehen ist.

4. Bezugsnormen

4.1 Externe Verweise

- GvD vom 10. März 2023, Nr. 24, zur Umsetzung der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 über den Schutz von Personen, die Verstöße gegen das Unionsrecht melden, sowie mit Bestimmungen über den Schutz von Personen, die Verstöße gegen nationale Rechtsvorschriften melden, in der jeweils geltenden Fassung;
- Gesetz Nr. 179 vom 30. November 2017 in geltender Fassung: „Bestimmungen zum Schutz der Hinweisgeber, die Vergehen oder Missstände melden, von denen sie im Rahmen eines

[4]Es handelt sich um die ANAC-Leitlinien, zuletzt aktualisiert durch den Beschluss Nr. 478 vom 26. November 2025

[5] Die in den vorliegenden Leitlinien genannten Bestimmungen des GvD Nr. 24/2023 finden gemäß Art. 24, Absatz 2 des WB-Dekrets erst ab dem 17. Dezember 2023 Anwendung auf jene Gesellschaften der Terna-Gruppe, die im letzten Jahr durchschnittlich bis zu zweihundertneunundvierzig Arbeitsnehmende mit unbefristeten oder befristeten Arbeitsverträgen beschäftigt haben. Gemäß dem Protokoll des Verwaltungsrats der Fondazione Terna vom 17. Dezember 2025 finden die Bestimmungen der vorliegenden Leitlinie, soweit anwendbar, auch auf die Fondazione Terna Anwendung.

privaten oder öffentlichen Arbeitsverhältnisses Kenntnis erhalten haben“[6];

- Gesetz Nr. 190 vom 6. November 2012 in geltender Fassung: „Bestimmungen zur Vorbeugung und Unterdrückung von Korruption und der Illegalität in der öffentlichen Verwaltung“;
- Gesetzvertretendes Dekret vom 8. Juni 2001, Nr. 231, in der jeweils geltenden Fassung (oder **GvD 231/01**), „Regelung der verwaltungsrechtlichen Haftung juristischer Personen, Unternehmen und Vereinigungen, auch ohne Rechtspersönlichkeit, gemäß Artikel 11 des Gesetzes vom 29. September 2000, Nr. 300“.
- Gesetzvertretendes Dekret vom 30. Juni 2003, Nr. 196, „Datenschutzkodex“, in der jeweils geltenden Fassung, sowie die damit verbundenen Maßnahmen der Datenschutzbehörde zum Schutz personenbezogener Daten;
- Europäische Verordnung 2016/679 (oder „**DSGVO**“): über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie über den freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), sowie die Maßnahmen der Datenschutzbehörde zum Schutz personenbezogener Daten;
- Gesetzvertretendes Dekret vom 10. August 2018, Nr. 101, in der jeweils geltenden Fassung, mit Bestimmungen zur Anpassung der nationalen Gesetzgebung an die Vorschriften der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie über den freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG;
- Gesetzvertretendes Dekret vom 18. Mai 2018, Nr. 51, in der jeweils geltenden Fassung, zur Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie über den freien Verkehr solcher Daten und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates;
- Leitlinien über die Datenschutz-Folgeabschätzungen (Data Protection Impact Assessment **„DPIA“**) und Prüfung der Möglichkeit, ob die Datenverarbeitung im Sinne der EU-Verordnung 2016/679 (Working Party 248 Rev. 01) „ein hohes Risiko darstellen könnte“;
- die von ANAC gemäß Art. 10 des WB-Dekrets erlassenen Leitlinien zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, sowie zum Schutz von Personen, die Verstöße gegen nationale Rechtsvorschriften melden – Verfahren für die Einreichung und Bearbeitung externer Meldungen, veröffentlicht auf der institutionellen Website von ANAC;
- ANAC-Regelung für die Bearbeitung externer Meldungen und für die Ausübung der Sanktionsbefugnis von ANAC in Umsetzung des GvD 24/2023, veröffentlicht auf der institutionellen Website von ANAC;
- Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 über den Schutz von Personen, die Verstöße gegen das Unionsrecht melden.

4.2 Interne Vorschriften

- Ethikkodex;

[6] Die Anwendung dieses Gesetzes ist auf jene Gesellschaften der Gruppe beschränkt, die im letzten Jahr durchschnittlich bis zu zweihundertneunundvierzig Arbeitnehmende mit unbefristeten oder befristeten Arbeitsverträgen beschäftigt haben, da die Verpflichtung zur Einrichtung des internen Meldekanals gemäß GvD Nr. 24/2023 gemäß Art. 24, Absatz 2 des WB-Dekrets ab dem 17. Dezember 2023 wirksam wird.

- Organisations- und Verwaltungsmodell gemäß GvD vom 8. Juni 2001, Nr. 231, von TERNA S.p.A. und den kontrollierten Gesellschaften;
- LG014 Regelwerk des Ethikausschusses (Regolamento del Comitato Etico);
- LG050 – Einführung des Ethikkodex in den Gesellschaften der Terna-Gruppe (L'adozione del Codice Etico nelle società del Gruppo Terna);
- LG018 – Leitlinie über die Informationssicherheit strategischer Adressaten („Information Security Policy Indirizzi strategici");
- LG039 – Datenschutzregelung bei Terna („La disciplina della Privacy in Terna");
- LG058 – „Global Compliance Program";
- LG059 – „Leitlinien zur Korruptionsbekämpfung";
- IO009SER – Verwaltung des Dienstes für Netzwerksicherheit („Gestione del servizio di Protocollo Informatico");
- PL02 – Integriertes Managementsystem der Terna-Gruppe;
- IO202SG – Management der Compliance-Tätigkeiten gemäß der Norm UNI ISO 37301:2021 (Gestione delle attività di compliance ai sensi della norma UNI ISO 37301:2021).

5. Definitionen und Abkürzungen

In Ergänzung zu den in anderen Abschnitten der vorliegenden Leitlinie (oder in den ihr beigefügten Dokumenten) definierten Begriffen und Ausdrücken haben die nachstehend aufgeführten Begriffe und Ausdrücke für die Zwecke dieser Leitlinie die jeweils daneben angegebene Bedeutung.

- **Systemadministrator**: Person, die über sämtliche Funktionalitäten des Whistle Editor verfügt und – im Unterschied zu diesem – auch die Berechtigungen der internen Nutzer verwaltet.
- **Sonstige Personen**: die in Abschnitt 6.1.2 der vorliegenden Leitlinie genannten Personen, die gemäß Art. 3, Absatz 5, des GvD Nr. 24/2023 bestimmt sind.
- **Audit** (oder **AU**)**:** die Audit-Direktion von Terna, innerhalb der die Prüfung durchgeführt wird, die auf eine Meldung folgt, und die das Ergebnis über das Portal an den Ethikausschuss übermittelt.
- **CISO:** der Chief Information Security Officer.
- **Ethikkodex:** Dokument, das positive Grundsätze und Verhaltensregeln enthält, die innerhalb der Terna-Gruppe freiwillig angenommen und veröffentlicht wurden, als konkrete Ausdrucksform der gegenüber den Stakeholdern erklärten Absichten.
- **Ethikausschuss:** das Unternehmensorgan, das für die Bearbeitung der eingegangenen Meldungen zuständig ist, um deren Weiterverfolgung sicherzustellen. Die Mitglieder werden vom Geschäftsführer von Terna S.p.A. ernannt und so ausgewählt, dass sie unterschiedliche Perspektiven sowie ein Gleichgewicht zwischen den verschiedenen Gesellschaften der Gruppe, Unternehmensfunktionen und Rollen repräsentieren.
- **Compliance Officer** (oder **CO**): die gemäß LG058 in jeder ausländischen Gesellschaft der Gruppe benannte Person, die innerhalb derselben die Verbreitung der Kenntnisse über das Global Compliance Program und/oder die im jeweiligen Länderanhang vorgesehenen lokalen Compliance-Programme sowie die Leitlinien der Muttergesellschaft fördert und deren Funktionsfähigkeit durch Schulungs- und Informationsmaßnahmen sowie durch die Implementierung entsprechender Informationsflüsse unterstützt.
- **Arbeitskontext**: die gegenwärtigen oder früheren beruflichen oder dienstlichen Tätigkeiten, die die hinweisgebende Person für Terna oder für die andere Gesellschaft der Gruppe, an die sich die Meldung richtet, ausgeübt hat und durch die sie – unabhängig von der Art dieser

Tätigkeiten – Informationen über Verstöße erlangt hat; in diesem Kontext könnte sie im Falle einer Meldung dem Risiko von Repressalien ausgesetzt sein.

- **Datenschutzvorschriften**: unter diesem Begriff versteht man die geltenden Datenschutzbestimmungen zum Schutz personenbezogener Daten, womit die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr, das GvD Nr. 196/2003, das GvD Nr. 101/2018 sowie jede sonstige anwendbare Datenschutzvorschrift – einschließlich der Maßnahmen der italienischen Datenschutzbehörde (Garante per la protezione dei dati personali) – gemeint sind.
- **Öffentliche Bekanntgabe** oder **öffentlich bekanntgeben**: unter diesem Begriff versteht man die Weitergabe von Informationen über Verstöße an die Öffentlichkeit durch die Presse, elektronische Medien oder andere Verbreitungsmittel, die geeignet sind, eine große Anzahl von Personen zu erreichen, in den in GvD Nr. 24/2023 vorgesehenen Fällen.
- **ITD-ESP:** Bereich Enterprise Services and Platforms im Rahmen von IT & Digital.
- **Unterstützer (Facilitator)**: natürliche Person, die der hinweisgebenden Person bei der Abgabe der Meldung Unterstützung leistet, im selben Arbeitskontext tätig ist und deren Unterstützung gemäß GvD Nr. 24/2023 vertraulich zu behandeln ist.
- **Meldungsbearbeiter** oder **Bearbeiter**: die von der Gesellschaft benannten Personen, die für die Bearbeitung von Meldungen gemäß Abschnitt 6.5 dieser Richtlinie zuständig sind und dabei die Grundsätze der Autonomie, Unparteilichkeit und Unabhängigkeit wahren.
- **Informationen über Verstößen**: Hierunter fallen Informationen – einschließlich begründeter Verdachtsmomente – über Verstöße, die begangen wurden oder die auf der Grundlage konkreter Anhaltspunkte innerhalb der Organisation begangen werden könnten, zu der die hinweisgebende Person oder die Person, die eine Anzeige bei der Justiz- oder Rechnungskontrollbehörde erstattet, im Rahmen des Arbeitskontexts in einem Rechtsverhältnis steht. Hierzu gehören auch Informationen über Handlungen oder Unterlassungen, die darauf abzielen, solche Verstöße zu verbergen. Nicht zu den melde- oder anzeigefähigen Informationen über Verstöße zählen offenkundig unbegründete Meldungen, Informationen, die bereits vollständig öffentlich bekannt sind, sowie Informationen, die ausschließlich auf unzuverlässigen Gerüchten oder schwer überprüfbaren Indiskretionen beruhen (sog. „Flurfunk“).
- **Überwachungsorgan** oder **OdV**: das Organ mit autonomen Initiativ- und Kontrollbefugnissen, das vom Unternehmen gemäß dem GvD 231/01 eingesetzt wurde und mit der Überwachung der Funktionsweise und der Einhaltung des Modells 231 sowie mit dessen Aktualisierung betraut ist.
- **Owner:** ein ordnungsgemäß befugter und geschulter Mitarbeiter der Audit-Direktion, dem der Prozess der Überprüfung der Meldung gemäß Abschnitt 6.5 zugewiesen ist.
- **PCE:** der Präsident des Ethikausschusses.
- **Betroffene Person**: die natürliche oder juristische Person, die in der internen oder externen Meldung bzw. in der öffentlichen Offenlegung als Person genannt wird, der der Verstoß zugerechnet wird, oder die in den gemeldeten oder öffentlich bekanntgemachten Verstoß anderweitig verwickelt ist.
- **RU (Direzione Risorse Umane)**: die Direktion Personalwesen von Terna.
- **IT-Portal** oder **Portal:** das *webbasiertes* IT-Tool, das speziell für Meldungen von Verstößen in schriftlicher und mündlicher Form für die Konzerngesellschaften eingerichtet ist,

zugänglich unter https://whistleblowing.terna.it/, und in dessen Rahmen die für die Konzerngesellschaften vorgesehenen Kanäle auch im Sinne des WB-Dekrets eingerichtet sind.

- **Ansprechpartner für die Meldung** oder **Ansprechpartner:** die von der betreffenden relevanten Tochtergesellschaft benannte natürliche oder juristische Person, die vom Bearbeiter hinzugezogen wird, sofern die Meldung diese Gesellschaft betrifft, wie in Ziff. 6.5 dieser Leitlinie vorgesehen.
- **Repository *(Datenbank):*** die für jeden im IT-Portal eingerichteten internen Kanal vorgesehene Datenbank, die der Archivierung aller eingegangenen Meldungen dient, unabhängig von der gewählten Übermittlungsform.
- **Leiter Audit** oder **RIA:** der Leiter der Audit-Direktion von Terna.
- **Repressalien**: jedes Verhalten, jede Handlung oder Unterlassung, auch nur versucht oder angedroht, das aufgrund einer Meldung, einer Anzeige bei der Justiz- oder Rechnungsprüfungsbehörde oder einer öffentlichen Bekanntmachung vorgenommen wird und der hinweisgebenden Person oder der anzeigenden Person unmittelbar oder mittelbar einen ungerechtfertigten Schaden zufügt oder zufügen kann. Insbesondere stellen gemäß Art. 17 Abs. 4 des GvD 24/2023 und den ANAC-Leitlinien nachstehende Handlungen lediglich beispielhaft Repressalien dar:
  - Entlassung, Suspendierung oder gleichwertige Maßnahmen;
  - Herabstufung oder Nicht-Beförderung;
  - Änderung der Aufgaben, des Arbeitsortes, der Vergütung oder der Arbeitszeiten;
  - Aussetzung von Schulungen oder jegliche Einschränkung des Zugangs zu Schulungen;
  - Abmahnungen oder negative Referenzen;
  - Verhängung disziplinarischer Sanktionen oder sonstiger Strafen, auch finanzieller Art;
  - Nötigung, Einschüchterung, Belästigung oder Ausgrenzung;
  - Diskriminierung oder eine sonstige Benachteiligung;
  - Nichtumwandlung eines befristeten Arbeitsvertrags in einen unbefristeten Arbeitsvertrag bei berechtigter Erwartung des Arbeitnehmers;
  - Nichtverlängerung oder vorzeitige Beendigung eines befristeten Arbeitsvertrags;
  - Schäden, auch am Ruf der Person, insbesondere in sozialen Medien, oder wirtschaftliche/finanzielle Nachteile, einschließlich Verlust wirtschaftlicher Chancen und Einkünfte;
  - Aufnahme in unzulässige Listen aufgrund einer formellen oder informellen Branchenvereinbarung, die dazu führen kann, dass die Person künftig keine Beschäftigung im betreffenden Sektor/der Branche findet;
  - vorzeitige Beendigung oder Kündigung eines Vertrags über die Lieferung von Waren oder Dienstleistungen
  - Entzug von Lizenzen oder Genehmigungen;
  - Anordnung psychiatrischer oder medizinischer Untersuchungen.
  - Auch folgende Handlungen können Repressalien darstellen: etwa die Forderung nach objektiv unerreichbaren Ergebnissen in den vorgegebenen Modalitäten und Fristen; eine künstlich negativ ausgestaltete Leistungsbeurteilung; ein nicht gerechtfertigter Entzug von Aufgaben; die ungerechtfertigte Nichtübertragung von Aufgaben bei gleichzeitiger Zuweisung derselben an eine andere Person; die wiederholte Ablehnung von Anträgen (z. B. Urlaub,

Freistellungen); die ungerechtfertigte Aussetzung von Befugnissen, Lizenzen, Berechtigungen usw.
    - In die Begriffsbestimmung der „Repressalie“ fallen im Rahmen der vorliegenden Leitlinien zudem auch jegliche Behinderung oder jeder Versuch einer Behinderung der Meldung.
- **Rückmeldung**: Mitteilung an die hinweisgebende Person über Informationen zur Weiterverfolgung der Meldung bzw. zu den Maßnahmen, die aufgrund der Meldung ergriffen werden oder ergriffen werden sollen, auch im Sinne des GvD Nr. 24/2023.
- **SE** oder **ausländische Gesellschaft**: nicht-italienische Gesellschaft/en der Terna-Gruppe.
- **Hinweisgebende Person**: die natürliche Person, die eine Meldung von Informationen über Verstöße erstattet, welche im Rahmen des Arbeitskontextes von Terna oder der anderen Gesellschaft der Terna-Gruppe, an die die Meldung gerichtet ist, erlangt wurden.
- **Gemeldete Person**: die natürliche oder juristische Person, die in der Meldung als Person genannt wird, der der Verstoß zugeschrieben wird, oder als Person, die in den gemeldeten Verstoß in irgendeiner Weise beteiligt ist.
- **Meldung**: die schriftliche oder mündliche Mitteilung von Informationen über Verstöße.
- **Externe Meldung**: die schriftliche oder mündliche Mitteilung von Informationen über Verstöße in den vom GvD Nr. 24/2023 vorgesehenen Fällen, eingereicht über den von der ANAC eingerichteten externen Meldekanal.
- **Interne Meldung**: die schriftliche oder mündliche Mitteilung von Informationen über Verstöße, eingereicht über die internen Meldekanäle derjenigen Gesellschaft der Terna-Gruppe, an die die Meldung gerichtet ist.
- **Weiterverfolgung**: die vom Bearbeiter unternommene Handlung zur Bewertung des Vorliegens der gemeldeten Tatsachen, des Ergebnisses der Ermittlungen und der gegebenenfalls ergriffenen Maßnahmen.
- **Disziplinarsystem**: das im Unternehmen geltende Disziplinarsystem, das in den Modellen 231 dargestellt ist oder – für die SE – im Rahmen des Global Compliance Program vorgesehen ist, wie es in jeder SE angewandt wird. Die Disziplinarmaßnahmen und die entsprechenden Sanktionen, sofern sie in Bezug auf die betroffenen Personen anwendbar sind, werden von der Gesellschaft auf der Grundlage der Grundsätze der Verhältnismäßigkeit und Angemessenheit festgelegt, in Bezug auf ihre Eignung, zunächst eine abschreckende und anschließend eine sanktionierende Funktion zu erfüllen, sowie unter Berücksichtigung der unterschiedlichen Qualifikationen der Personen, auf die sie Anwendung finden.
- **Nicht relevante Tochtergesellschaften:** darunter sind jene Gesellschaften der Terna-Gruppe zu verstehen, die gemäß Art. 4, Absatz 4, GvD Nr. 24/2023 weniger als zweihundertneunundvierzig Beschäftigte haben und ihren Sitz in Italien haben; für die Zwecke dieser Leitlinien gelten auch ausländische Gesellschaften als nicht relevant.
- **Relevante Tochtergesellschaften:** darunter sind jene Gesellschaften der Terna-Gruppe zu verstehen, die gemäß Art. 4, Absatz 4, GvD Nr. 24/2023 mehr als zweihundertneunundvierzig Beschäftigte haben und ihren Sitz in Italien haben.
- **Verstöße**: rechtswidrige Handlungen und/oder Verhaltensweisen, sei es durch Tun oder Unterlassen, die Verstöße – auch vermutete – gegen die im Ethikkodex verankerten Grundsätze, gegen die internen Vorschriften (bestehend aus allen Bestimmungen, Verfahren, Leitlinien oder operativen Anweisungen derjenigen Gesellschaft, an die die

Meldung gerichtet ist, einschließlich des Modells 231, der Antikorruptionsleitlinien und des Global Compliance Program) darstellen, sowie Verstöße gegen Unternehmensrichtlinien oder -regeln, die zu Betrug oder zu einem – auch potenziellen – Schaden gegenüber Kolleginnen und Kollegen, Anteilseigner oder Stakeholdern im Allgemeinen führen können oder Handlungen darstellen, die die Interessen oder die Reputation des Unternehmens beeinträchtigen oder rechtswidrig verletzen; ebenso die im WB-Dekret vorgesehenen Verstöße „*gegen nationale oder EU-Rechtsvorschriften, die das öffentliche Interesse oder die Integrität der öffentlichen Verwaltung oder des privaten Rechtsträgers beeinträchtigen*".

- **Whistle-Editor:** eine vom RIA (Leiter Internal Audit) im Bereich Audit benannte Person, die zu den Nutzern des Portals gehört und für das Einstellen in das Portal der Meldungen zuständig ist, die außerhalb des Portals eingegangen sind. Sie aktualisiert die in den verschiedenen Bereichen des Portals angegebenen Informationen für unterschiedliche Zwecke (Disclaimer, Frequently Asked Questions (FAQ), Wertelisten, Verwaltung der Kategorien usw.).

6. Bedingungen, Modalitäten für die Abgabe von Meldungen und damit verbundene Schutzmaßnahmen

6.1 Subjektiver Bereich

Gemäß den Bestimmungen des Ethikkodex bietet jede Gesellschaft der Terna-Gruppe den hinweisgebenden Personen größtmögliche Vertraulichkeit und Schutz. Dieser Schutz gilt für Personen, die Meldungen in gutem Glauben und mit Loyalität gegenüber dem Unternehmen erstatten, und umfasst den Schutz vor Repressalien oder sonstigen negativen Auswirkungen auf ihre berufliche Stellung. Zugleich werden Personen sanktioniert, die rücksichtsvolle oder rachsüchtige Handlungen begehen.
Im Hinblick auf das in diesen Leitlinien gemäß dem WB-Dekret vorgesehene Schutzsystem ist es angebracht, zwei Kategorien von Personen zu unterscheiden:

- die „***hinweisgebende Person***";
- die „***sonstigen Personen***"

6.1.1 Hinweisgebende Personen

Jede beliebige Person kann die Meldung eines Verstoßes einreichen.
Mit spezifischem Bezug auf die Bestimmungen des WB-Dekrets und die damit verbundenen Schutzmaßnahmen können Meldungen von allen Personen erstattet werden, die im „*Arbeitskontext*" von Terna oder derjenigen Gesellschaft der Terna-Gruppe tätig sind, an die die Meldung gerichtet ist, und zwar in ihrer Eigenschaft als:

- Beschäftigte einer der zur Terna-Gruppe gehörenden Gesellschaften;
- Selbstständige, die ihre berufliche Tätigkeit für eine Gesellschaft der Terna-Gruppe ausüben;
- Personen, die mit dem Unternehmen in einem beruflichen Kooperationsverhältnis stehen (z. B. Lieferanten), Freiberufler (z. B. Rechtsanwälte, Steuerberater, Notare usw.) sowie Berater, die ihre Tätigkeit bei einer der Gesellschaften der Gruppe erbringen;
- Freiwillige und Praktikantinnen/Praktikanten, sowohl vergütet als auch unvergütet, die ihre Tätigkeit bei einer der Gesellschaften der Gruppe ausüben;
- Anteilseigner, d. h. natürliche Personen, die Beteiligungen an einer Einrichtung des öffentlichen Sektors halten, sofern diese in der Form einer Gesellschaft organisiert ist (z. B. öffentlich kontrollierte Gesellschaften, In-house-Gesellschaften, Genossenschaften usw.).

Es handelt sich um Personen, die im Rahmen der Ausübung der ihnen als Anteilseigner zustehenden Rechte von Verstößen Kenntnis erlangt haben, die Gegenstand einer Meldung sind; sowie um Personen mit Verwaltungs-, Leitungs-, Kontroll-, Aufsichts- oder Vertretungsfunktionen, auch wenn diese Funktionen lediglich faktisch ausgeübt werden, bei einer der Gesellschaften der Gruppe.

Es können außerdem Meldungen von folgenden Personen erstattet werden:

- Personen, die Informationen im Rahmen eines inzwischen beendeten Arbeitsverhältnisses mit der Terna-Gruppe erlangt haben, sofern die Informationen über die Verstöße vor der Beendigung des Arbeitsverhältnisses erworben wurden;
- Personen, die Informationen erlangt haben, bevor ein Arbeitsverhältnis begonnen hat, sofern die Informationen über einen Verstoß während des Auswahlverfahrens oder anderer Phasen der vorvertraglichen Verhandlungen erlangt wurden;
- Personen, die Informationen während der Ableistung der Probezeit bei einer der Gesellschaften der Terna-Gruppe erlangt haben.

6.1.2 Sonstige Personen

Zur Kategorie der „sonstigen Personen“, die im Falle von Meldungen gemäß dem WB-Dekret schutzwürdig sind, gehören:

- die Unterstützer (Facilitators);
- Personen aus demselben Arbeitskontext wie die hinweisgebende Person, die zu dieser durch eine stabile affektive Bindung oder eine Verwandtschaft bis zum vierten Grad verbunden sind;
- Arbeitskolleginnen und -kollegen der hinweisgebenden Person, die im selben Arbeitskontext tätig sind und zu dieser Person eine regelmäßige und laufende berufliche Beziehung unterhalten[7];
- ebenso gehören dazu die Einrichtungen, die im Eigentum der hinweisgebenden Person stehen oder für die diese tätig ist, sowie die Einrichtungen, die im selben Arbeitskontext tätig sind.

6.2 Gegenstand der Meldung

Es können alle Verstöße gemeldet werden. Mit spezifischem Bezug auf die Bestimmungen des WB-Dekrets gelten hingegen jene Meldungen als relevante Meldungen (die also die Anwendung der im folgenden Abschnitt 6.3 genannten Schutzmaßnahmen ermöglichen), die Verstöße betreffen, welche durch Verhalten, Handlungen oder Unterlassungen geeignet sind, das öffentliche Interesse oder die Integrität der öffentlichen Verwaltung oder des privaten Rechtsträgers zu beeinträchtigen.

Insbesondere können drei Kategorien unterschieden werden:[8]:

1. ***Verstöße gegen nationale und europäische Vorschriften, die rechtswidrige Handlungen in folgenden Bereichen darstellen***: öffentliche Aufträge, Finanzdienstleistungen, Finanzprodukte

[7] *„Im Fall der Arbeitskollegen hat der Gesetzgeber vorgesehen, dass es sich um Personen handeln muss, die zum Zeitpunkt der Meldung mit der hinweisgebenden Person zusammenarbeiten (ehemalige Kolleginnen und Kollegen sind daher ausgeschlossen) und die mit dieser eine regelmäßige und laufende Beziehung unterhalten. Die Vorschrift bezieht sich daher auf Beziehungen, die nicht lediglich sporadisch, gelegentlich, episodisch oder außergewöhnlich sind, sondern auf aktuelle, über einen gewissen Zeitraum andauernde Beziehungen, die durch eine gewisse Kontinuität gekennzeichnet sind und eine Form von „Gemeinsamkeit“ oder Freundschaft begründen.* So heißt es in den von der ANAC mit Beschluss Nr. 311 vom 12.07.2023 genehmigten Leitlinien, S. 22.

[8] Nach Maßgabe des WB-Dekrets ist hinsichtlich der oben genannten Kategorien von Verstößen zu unterscheiden, je nachdem ob: (i) der Rechtsträger Konzessionär eines öffentlichen Dienstes ist (oder jedenfalls in diesem Bereich tätig ist); in diesem Fall finden alle Kategorien von Verstößen Anwendung; (ii) mehr als 50 Beschäftigte hat und ein Modell 231 eingeführt hat; in diesem Fall finden die Kategorie der Verstöße gegen europäische Vorschriften sowie die nach dem GvD 231/2001 relevanten rechtswidrigen Handlungen oder Verstöße gegen das 231-Modell Anwendung; (iii) weniger als 50 Beschäftigte hat, aber ein Modell 231 eingeführt hat; in diesem Fall können die nach dem GvD 231/2001 relevanten rechtswidrigen Handlungen oder Verstöße gegen das Modell 231 gemeldet werden.

und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung, Produktsicherheit und -konformität, Verkehrssicherheit, Umweltschutz, Strahlenschutz und nukleare Sicherheit, Sicherheit von Lebensmitteln und Futtermitteln sowie Gesundheit und Wohlbefinden der Tiere, öffentliche Gesundheit, Verbraucherschutz, Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netzen und Informationssystemen.

2. ***Verstöße gegen europäische Vorschriften***, die bestehen in: i) Handlungen oder Unterlassungen, welche die finanziellen Interessen der Union beeinträchtigen; ii) Handlungen oder Unterlassungen in Bezug auf den Binnenmarkt[9]; iii) Handlungen und Verhaltensweisen, die den Zweck oder das Ziel der Bestimmungen der Rechtsakte der Union in den oben genannten Bereichen vereiteln; iv) Verstößen gegen die restriktiven Maßnahmen der Europäischen Union gemäß Titel I-bis, Kapitel I, Buch II des Strafgesetzbuches sowie gemäß Artikel 12, Absatz 1-bis des GvD vom 25. Juli 1998, Nr. 286, in «*Umsetzung der Richtlinie (EU) 2024/1226 des Europäischen Parlaments und des Rates vom 24. April 2024 über die Festlegung von Straftatbeständen und Sanktionen bei Verstößen gegen restriktive Maßnahmen der Union und zur Änderung der Richtlinie (EU) 2018/1673*»; v) Verstößen gegen die Verordnung (EU) Nr. 2024/1689 (sog. AI Act).[10]
3. ***Verstöße gegen nationale Vorschriften***, die bestehen in: i) verwaltungsrechtlichen, buchhalterischen, zivilrechtlichen oder strafrechtlichen rechtswidrigen Handlungen; ii) rechtswidrigen Verhaltensweisen, die im Sinne des GvD 231/2001 relevant sind, oder Verstößen gegen die Modelle 231. Diese rechtswidrigen Handlungen und Verhaltensweisen dürfen nicht in die Kategorien der vorstehenden Punkte 1 und 2 fallen.

6.2.1 Mindestinhalt der Meldung

Die Meldung muss die nachstehend aufgeführten wesentlichen Elemente enthalten.

- **Hinweisgebende Person:** die Meldung muss die Identifikationsdaten der Person enthalten, die Meldung erstattet[11]. Die Meldungen müssen in gutem Glauben erfolgen und dürfen nicht anonym abgegeben werden.
- **Gegenstand**: eine klare Darstellung der der Meldung zugrunde liegenden Tatsachen, mit Angabe der zeitlichen und örtlichen Umstände, unter denen die Handlungen oder Unterlassungen begangen wurden, sowie der Art und Weise, wie die hinweisgebende Person von den Tatsachen Kenntnis erlangt hat.
- **Gemeldete Person und beteiligte Personen**: die Personalien oder jedes andere Element (wie etwa Funktion bzw. Rolle im Unternehmen), das eine einfache Identifizierung des/der mutmaßlichen Verursacher/s des rechtswidrigen Verhaltens sowie der beteiligten Personen ermöglicht.
- **Konzerngesellschaft:** die Meldung muss die Angabe enthalten, auf welche Gesellschaft der Gruppe sie sich bezieht, falls die Meldung über einen von mehreren Gesellschaften der Gruppe gemeinsam genutzten Meldekanal erfolgt.

Die Meldungen werden geprüft, sofern sie zulässig, nicht offensichtlich unbegründet, ausreichend

[9] In diesen Bereich fallen alle Verstöße gegen die Vorschriften der Europäischen Union im Bereich des Wettbewerbs und der staatlichen Beihilfen sowie jene Verstöße, die den Binnenmarkt betreffen und mit Handlungen verbunden sind, welche die Vorschriften über die Körperschaftsteuer verletzen oder Mechanismen darstellen, deren Zweck es ist, einen steuerlichen Vorteil zu erlangen, der den Gegenstand oder den Zweck der anwendbaren Vorschriften über die Körperschaftsteuer vereitelt.

[10] Gemäß Art. 113 der Verordnung (EU) 2024/1689 findet Art. 87 – der die Anwendung der Richtlinie (EU) 2019/1937 auf die Meldung von Verstößen gegen die vorliegende Verordnung sowie auf den Schutz der Personen, die solche Verstöße melden, vorsieht – ab dem 2. August 2026 Anwendung

[11] Darunter sind jene personenbezogenen Daten zu verstehen, die es ermöglichen, gesondert und vertraulich die Kommunikation zwischen dem Unternehmen und der hinweisgebenden Person sicherzustellen sowie die Übermittlung von Rückmeldungen über die Weiterverfolgung der Meldung zu gewährleisten.

konkretisiert und mit Elementen versehen sind, die für die Rekonstruktion und Feststellung der Verstöße hilfreich sind. Unberührt bleibt die Befugnis des Ethikausschusses, die Meldung im Lichte des konkreten Falls und der vorhandenen Elemente zu beurteilen, die eine anschließende Ermittlungs- bzw. Prüfungstätigkeit ermöglichen.

Die hinweisgebende Person kann zudem folgende weitere Elemente bereitstellen:

- die Angabe **etwaiger anderer Personen**, die zu den in der Meldung dargestellten Tatsachen Auskunft geben können;
- **Übermittlung von Unterlagen**, die diese Sachverhalte bestätigen können;
- **Alle sonstigen Informationen**, die Erhebung von Beweisen zu den gemeldeten Sachverhalten erleichtern können.

Die hinweisgebende Person kann außerdem etwaige Unterlagen vorlegen, die dazu dienen, die Meldung weiter zu konkretisieren.
Schließlich ist es – zur Erleichterung der korrekten Identifizierung der weiteren beteiligten Personen gemäß Abschnitt 6.1.2 dieser Leitlinie und gemäß Art. 3 des GvD Nr. 24/2023, denen Vertraulichkeit und die in Abschnitt 6.3 vorgesehenen Schutzmaßnahmen zu gewährleisten sind – zweckmäßig, dass die hinweisgebende Person das Vorhandensein solcher Personen ausdrücklich angibt und das Vorliegen der entsprechenden Voraussetzungen präzisiert.

6.2.2 Einschränkungen des Meldungsgegenstands

Vom Anwendungsbereich des WB-Dekrets ausgenommen (und daher nicht geeignet, die im folgenden Abschnitt 6.3 vorgesehenen Schutzmaßnahmen auszulösen) sind:

- Ansprüche, Beanstandungen oder Anliegen persönlicher Natur der hinweisgebenden Person oder der Person, die eine Anzeige bei der Justiz- oder Rechnungskontrollbehörde erstattet hat, welche sich ausschließlich auf das eigene individuelle Arbeitsverhältnis oder auf das Arbeitsverhältnis mit hierarchisch übergeordneten Personen beziehen[12];
- Meldungen über Verstöße, die bereits zwingend durch Rechtsakte der Europäischen Union oder durch nationale Vorschriften geregelt sind und Dienstleistungen, Finanzprodukte und Finanzmärkte, die Verhinderung von Geldwäsche und Terrorismusfinanzierung, die Verkehrssicherheit sowie den Umweltschutz betreffen, oder durch nationale Vorschriften, die der Umsetzung von Unionsakten dienen[13], sowie Meldungen über Verstöße im Bereich der nationalen Sicherheit und über Vergaben, die Aspekte der Verteidigung oder der nationalen Sicherheit betreffen, fallen nicht in den Anwendungsbereich, es sei denn, diese Aspekte sind im einschlägigen abgeleiteten Unionsrecht geregelt;
- Anonyme Meldungen, da die vorliegende Leitlinie darauf ausgerichtet ist, die hinweisgebende Person vor dem Risiko von Repressalien zu schützen.

Was anonyme Meldungen betrifft, wird daran erinnert, dass die in Abschnitt 6.3 vorgesehenen Schutzmaßnahmen Anwendung finden können, sofern im Anschluss an eine anonyme Meldung der Name der hinweisgebenden Person bekannt wird. Der umfassende Vertraulichkeitsschutz, der den

[12] *„Ausgeschlossen sind daher beispielsweise Meldungen, die Arbeitsstreitigkeiten und vorgerichtliche Phasen, Diskriminierungen zwischen Kolleginnen und Kollegen, zwischenmenschliche Konflikte zwischen der hinweisgebenden Person und einer anderen Arbeitskraft oder mit Vorgesetzten betreffen, sowie Meldungen über Datenverarbeitungen im Rahmen des individuellen Arbeitsverhältnisses, sofern keine Beeinträchtigung des öffentlichen Interesses oder der Integrität der öffentlichen Verwaltung oder des privaten Rechtsträgers vorliegt“*, so die von der ANAC mit Beschluss Nr. 311 vom 12.07.2023 genehmigten Leitlinien, S. 28.

[13] In Teil II des Anhangs der Richtlinie (EU) 2019/193725 angeführt.
„Man denke beispielsweise an die Meldeverfahren im Bereich des Marktmissbrauchs gemäß der Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates sowie der Durchführungsrichtlinie (EU) 2015/2392 der Kommission, die auf Grundlage der genannten Verordnung erlassen wurden und bereits detaillierte Bestimmungen zum Schutz von Hinweisgebern enthalten“, so die von der ANAC mit Beschluss Nr. 311 vom 12.07.2023 genehmigten Leitlinien, S. 28.

hinweisgebenden Personen auch im Fall von ordentlichen Meldungen gewährt wird, setzt voraus, dass auch diese nicht anonym erstattet werden.

Es wird zudem daran erinnert, dass gemäß Art. 1 Absatz 3 des WB-Dekrets Meldungen, die folgende Bereiche betreffen, vom Anwendungsbereich der in demselben WB-Dekret und in der vorliegenden Leitlinie vorgesehenen Schutzmaßnahmen ausgeschlossen sind: a) klassifizierte Informationen; b) anwaltliches und ärztliches Berufsgeheimnis; c) Geheimhaltung der Beratungen gerichtlicher Organe.

Die Meldungen dürfen keine beleidigenden Äußerungen oder persönliche Angriffe oder Urteile enthalten, die darauf abzielen, die Ehre und/oder die persönliche und/oder berufliche Würde der Person, auf die sich die gemeldeten Tatsachen beziehen, zu verletzen.
In allen Fällen ist Folgendes untersagt:

- die Übermittlung von Meldungen zu rein diffamierenden und verleumderischen Zwecken;
- die Übermittlung von Meldungen, die sich ausschließlich auf Aspekte des Privatlebens beziehen und keinerlei direkten oder indirekten Bezug zur unternehmerischen bzw. beruflichen Tätigkeit der gemeldeten Person aufweisen;
- die Übermittlung von Meldungen, die Beanstandungen, Ansprüche oder Anliegen betreffen, die mit einem persönlichen Interesse der hinweisgebenden Person verbunden sind;
- die Übermittlung von Meldungen diskriminierender Natur, die sich auf die sexuelle, religiöse oder politische Orientierung oder auf die ethnische Herkunft der gemeldeten Person beziehen;
- die Übermittlung von Meldungen mit dem alleinigen Ziel, die gemeldete Person zu schädigen.

Gegen alle Mitarbeitenden der Gruppe, die Meldungen dieser Art einreichen, können disziplinarische Maßnahmen ergriffen werden. Darüber hinaus kann eine hinweisgebende Person, die eine Meldung in böser Absicht oder grob fahrlässig gemacht hat, sanktioniert werden, wenn sich die Meldung als unbegründet erweist.

6.3 Schutzmaßnahmen für die hinweisgebende Person

Die Anwendung des Whistleblowing-Systems kann auf Misstrauen stoßen, da die potenzielle hinweisgebende Person möglicherweise befürchtet, aufgrund der Meldung nicht ausreichend vor dem Risiko von Repressalien und Diskriminierung am Arbeitsplatz geschützt zu sein. Terna und die Gesellschaften der Gruppe wahren die Vertraulichkeit und schützen die hinweisgebende Person vor Repressalien gemäß Abschnitt 2.
In Bezug auf das WB-Dekret werden Maßnahmen zum Schutz der Vertraulichkeit der Identität der hinweisgebenden Person sowohl in der Phase des Eingangs als auch in der Phase der Bearbeitung der Meldung ergriffen, und zwar durch die Nutzung der eigens eingerichteten internen Meldekanäle. Diesbezüglich sollte zwischen den Begriffen „Vertraulichkeit“ und „Anonymität“ unterschieden werden, da ersterer die bekannte Identität der hinweisgebenden Person voraussetzt, um einen angemessenen Schutz garantieren zu können. Hingegen könnte die Anonymität die Feststellung, ob die Anzeige begründet ist, behindern.
Es werden zudem geeignete Maßnahmen ergriffen, um die hinweisgebenden Personen vor jeder Form von Repressalien, Diskriminierung oder Benachteiligung im Zusammenhang mit der Meldung zu schützen; unter Berücksichtigung der im WB-Dekret vorgesehenen Bedingungen und Anforderungen werden solche Maßnahmen auch zum Schutz der weiteren beteiligten Personen

gemäß Abschnitt 6.1.2 der vorliegenden Leitlinie und gemäß Art. 3 des GvD Nr. 24/2023 ergriffen, unbeschadet gesetzlicher Verpflichtungen und des Schutzes der Rechte des Unternehmens oder der beteiligten Personen.
Diese Garantien bestehen einerseits im Verbot von Repressalien für die erstatteten Meldungen, das dem Unternehmen auferlegt ist, und andererseits in der Nichtigkeit der etwaigen repressiven Handlungen, die unter Verstoß gegen dieses Verbot erlitten wurden[14].
Um den im WB-Dekret vorgesehenen Schutz zu erhalten, müssen bestimmte Voraussetzungen erfüllt sein:

- dass die hinweisgebende Person zu den in Art. 3 des GvD Nr. 24/2023 aufgeführten Kategorien gehört (wie im vorhergehenden Abschnitt 6.1.1 angegeben);
- dass die gemeldeten Informationen über Verstöße in den sachlichen Anwendungsbereich des GvD Nr. 24/2023 fallen und im vorhergehenden Abschnitt 6.2 dargestellt sind;
- dass die hinweisgebende Person zum Zeitpunkt der Meldung oder der Anzeige bei der Justiz- oder Rechnungskontrollbehörde oder der öffentlichen Offenlegung einen begründeten Anlass hatte, die Informationen für wahr zu halten[15];
- dass die Meldung gemäß den für die internen Kanäle vorgesehenen Verfahren (eingerichtet gemäß der vorliegenden Leitlinie, wie in Abschnitt 6.4 dargestellt) oder den externen Kanälen (verwaltet von der ANAC, wie in Abschnitt 6.9 dargestellt) oder gemäß den Bestimmungen über die öffentliche Offenlegung nach Art. 15 des WB-Dekrets (wie in Abschnitt 6.10 dargestellt) erstattet wird.

Ein Verstoß gegen die zugunsten der hinweisgebenden Person bzw. der in Abschnitt 6.1.2 dieser Leitlinie genannten sonstigen Personen und gemäß Art. 3 Abs. 5 des Gesetzesdekrets Nr. 24/2023 vorgesehenen Schutzmaßnahmen stellt einen Grund für die Anwendung der im Disziplinarsystem vorgesehenen Sanktionen dar. Insbesondere sind nach Maßgabe des GvD Nr. 24/2023 disziplinarisch sanktionierbar:

- die repressiven Verhaltensweisen im Sinne von Art. 17 GvD Nr. 24/2023, das heißt Verhaltensweisen, Handlungen oder Unterlassungen, auch nur versuchte oder angedrohte, die aufgrund der Meldung gesetzt werden und der hinweisgebenden Person unmittelbar oder mittelbar einen ungerechtfertigten Schaden zufügen können;
- Verhaltensweisen, die geeignet sind, die Meldung zu behindern;
- Verstöße gegen die Schutzmaßnahmen zugunsten der hinweisgebenden Person in Bezug auf die Verpflichtung zur Wahrung der Vertraulichkeit.

Die Vertraulichkeit der hinweisgebenden Person ist nicht gewährleistet, wenn:

- die hinweisgebende Person ausdrücklich in die Offenlegung ihrer Identität eingewilligt hat;
- die straf- und/oder zivilrechtliche Verantwortlichkeit der hinweisgebenden Person für Verleumdung, üble Nachrede oder sonstige im Zusammenhang mit der Meldung begangene Straftaten durch ein Urteil erster Instanz festgestellt wurde;
- die Anonymität gesetzlich nicht geltend gemacht werden kann, wenn die Identität der hinweisgebenden Person von der Justizbehörde im Zusammenhang mit Ermittlungen (strafrechtlichen, steuerrechtlichen oder verwaltungsrechtlichen) oder von Aufsichtsbehörden im Rahmen von aufgrund der Meldung eingeleiteten Prüfungen verlangt wird.

[14] Etwaige Repressalien können gemäß Art. 19 des WB-Dekrets der ANAC mitgeteilt werden, damit diese die hierfür vorgesehenen Prüfungen vornimmt.

[15] Auf der Grundlage vorlegbarer konkreter Umstände und erlangbarer Informationen und somit nicht auf bloßen Mutmaßungen.

6.3.1 Beschränkungen des Schutzes der hinweisgebenden Person und Schutz der gemeldeten Person

Das WB-Dekret sieht Fälle vor, in denen die hinweisgebende Person keinen Anspruch auf Schutz hat:

- wenn die strafrechtliche Verantwortlichkeit der hinweisgebenden Person wegen Verleumdung oder falscher Anschuldigung, auch durch ein Urteil erster Instanz, festgestellt wird oder wenn solche Straftaten durch die Anzeige bei der Justiz- oder Rechnungskontrollbehörde begangen werden;
- im Falle einer zivilrechtlichen Haftung aus demselben Grund aufgrund von Vorsatz oder grober Fahrlässigkeit.

In beiden Fällen wird gegenüber der hinweisgebenden Person bzw. der anzeigenden Person eine disziplinarische Sanktion verhängt.

Unberührt bleibt zudem die straf-, zivil- oder verwaltungsrechtliche Verantwortlichkeit für alle Verhaltensweisen, Handlungen oder Unterlassungen, die nicht mit der Meldung, der Anzeige bei der Justiz- oder Rechnungskontrollbehörde oder der öffentlichen Offenlegung zusammenhängen oder die nicht unbedingt erforderlich sind, um den Verstoß offenzulegen (Art. 20 Abs. 4 GvD Nr. 24/2023).

Ein Verstoß gegen die Bestimmungen des GvD Nr. 24/2023 über die Meldung rechtswidrigen Verhaltens stellt einen Grund für die Anwendung der im Disziplinarverfahren vorgesehenen Sanktionen dar. Disziplinarisch sanktionierbar sind insbesondere die Fälle, in denen die zivilrechtliche Verantwortlichkeit der hinweisgebenden Person wegen Verleumdung oder falscher Anschuldigung bei Vorsatz oder grober Fahrlässigkeit festgestellt wird, auch durch ein Urteil erster Instanz. Dies gilt jedoch nicht, wenn die betreffende Person bereits – ebenfalls durch ein Urteil erster Instanz – wegen Verleumdung, falscher Anschuldigung oder einer ähnlichen, im Zusammenhang mit der Anzeige bei der Justiz- oder Rechnungskontrollbehörde begangenen Straftat verurteilt wurde. Unbeschadet hiervon können gemäß Art. 21 des genannten WB-Dekrets Verwaltungsstrafen von der ANAC verhängt werden.

Was den Schutz der gemeldeten Person betrifft, so wird bei der Verwaltung der gemäß den vorliegenden Leitlinien eingerichteten Meldekanäle auch die Vertraulichkeit der Identität der gemeldeten Person gewahrt, wie im WB-Dekret vorgesehen. Dies dient dazu, eine unzulässige Weitergabe personenbezogener Informationen zu verhindern – sowohl nach außen als auch innerhalb des Unternehmens gegenüber Personen, die zur Verarbeitung solcher Daten nicht befugt sind –, und zwar bis zum Abschluss der aufgrund der Meldung eingeleiteten Verfahren.

Der gemeldeten Person steht kein automatisches Recht zu, stets über die sie betreffende Meldung informiert zu werden. Die gemeldete Person wird über die sie betreffende Meldung erst nach Abschluss der Prüf- und Analysehandlungen informiert, und zwar nur dann, wenn: (i) ein Verfahren aufgrund der Prüf- und Analysehandlungen gegen sie eingeleitet wurde und (ii) dieses Verfahren ganz oder teilweise auf der Meldung beruht. In diesem Fall kann die gemeldete Person angehört werden. Alternativ ist auch eine Anhörung im schriftlichen Verfahren möglich, bei der die Person schriftliche Stellungnahmen und Unterlagen vorlegt.

Schließlich gilt: Wenn der Vorwurf ganz oder teilweise auf der Meldung basiert und die Kenntnis der Identität der hinweisgebenden Person für die Verteidigung der beschuldigten Person unerlässlich ist, darf die Meldung im Disziplinarverfahren nur verwendet werden, wenn die hinweisgebende Person der Offenlegung ihrer Identität ausdrücklich zugestimmt hat (vgl. Abschnitt 6.4.1).

6.3.2 Verbot von Repressalien

Repressalien sind verboten, und jede gegen die hinweisgebende Person oder gegen Personen, die Verstöße im Sinne des WB-Dekrets der Justiz- oder Rechnungskontrollbehörde melden, gerichtete

rachsüchtige Maßnahme wird sanktioniert.
Das Unternehmen schützt die hinweisgebende Person sowie die sonstigen in Art. 3 des GvD Nr. 24/2023 genannten Personen (vgl. Abschnitt 6.1.2) vor jeder Form von Repressalie. Dies erfolgt durch die Einführung von Regeln, die darauf abzielen, Handlungen oder Maßnahmen zu verhindern oder deren Auswirkungen zu neutralisieren, die darauf gerichtet sind, die hinweisgebende Person für die Offenlegung von Informationen zu bestrafen und/oder die Meldung zu behindern.
In den Anwendungsbereich dieses gesetzlich vorgesehenen Verbots fallen nicht nur Verhaltensweisen, Handlungen oder Unterlassungen, die aufgrund der Meldung gesetzt werden und der hinweisgebenden Person einen ungerechtfertigten Schaden zufügen, sondern auch der bloße Versuch oder die Androhung einer Repressalie. Der verursachte ungerechtfertigte Schaden kann auch mittelbar eintreten.
Zudem liegt die Beweislast, dass solche Verhaltensweisen oder Maßnahmen aus Gründen erfolgen, die mit der Meldung, der öffentlichen Offenlegung oder der Anzeige nicht in Zusammenhang stehen, im Fall der hinweisgebenden Person bei der Gesellschaft, die sie gesetzt hat, welche daher verpflichtet ist nachzuweisen, dass die ergriffenen Maßnahmen auf Gründen beruhen, die mit der Meldung nicht in Zusammenhang stehen.
Was hingegen die sonstigen betroffenen Personen betrifft, so obliegt ihnen die Beweislast dafür, dass das betreffende Verhalten, die Handlung oder Unterlassung aufgrund der Meldung gesetzt wurde und somit einen rachsüchtigen Charakter aufweist.
Zum Schutz dieser Rechtsposition sieht die geltende Gesetzgebung vor, dass die hinweisgebende Person der ANAC etwaige Repressalien, die sie für erlitten hält, mitteilen kann.

6.4 Interne Meldekanäle für die Abgabe von Meldungen

Es stehen die folgenden internen Kanäle zur Verfügung, über die Meldungen („**interne Meldekanäle**“) abgegeben werden können. Sie sind so ausgestaltet, dass die Vertraulichkeit der Identität der hinweisgebenden Person sowie die Sicherheit der Informationen gewährleistet sind und ein selektiver Zugriff ausschließlich durch hierzu ausdrücklich befugtes Personal vorgesehen ist. Insbesondere stehen zur Verfügung:

- ein **elektronisches Portal**, das einen effizienten Zugang zu den für die einzelnen Gesellschaften der Terna-Gruppe vorgesehenen Meldekanälen bietet, an die eine Meldung gerichtet werden soll. Das elektronische Portal gewährleistet die Sicherheit und den Schutz der Daten zur Identität der hinweisgebenden Person durch ein fortschrittliches Verschlüsselungssystem für die Kommunikation sowie die Vertraulichkeit der betroffenen Person und jeder in der Meldung genannten Person, ebenso wie des Inhalts der Meldung und der zugehörigen Unterlagen, in Übereinstimmung mit den Vorgaben des WB-Dekrets.
- **ein direktes Meldeverfahren**, das es ermöglicht, Meldungen im Rahmen vereinbarter Treffen ausschließlich mit den für den Empfang der Meldungen ausdrücklich befugten Personen abzugeben.
- **ein Postweg-Kanal,** der die Abgabe von Meldungen per gewöhnlicher Post ermöglicht und – soweit dies anhand von der hinweisgebenden Person bereitgestellten Daten möglich ist – im Rahmen der Bearbeitung der Meldung die nach dem WB-Dekret vorgesehenen Modalitäten für die Kommunikation mit der hinweisgebenden Person sicherstellt.

Die eingerichteten internen Kanäle sind als bevorzugte Kanäle zu betrachten.

Dieses Prinzip dient – wie in der einschlägigen Gesetzgebung vorgesehen – einerseits dazu, „eine Kultur guter Kommunikation und der sozialen Unternehmensverantwortung innerhalb der Organisationen zu fördern“, und andererseits sicherzustellen, dass die hinweisgebenden Personen durch das Aufdecken von rechtswidrigen Handlungen, Unterlassungen oder Verhaltensweisen wesentlich zur Verbesserung der eigenen Organisation beitragen[16].
Die internen Meldekanäle werden – wie im folgenden Abschnitt 6.5 geregelt – von hierfür formal benannten Personen verwaltet.
Wird eine Meldung irrtümlich an eine unzuständige Person (also eine nicht formal benannte Stelle) oder an einen Meldekanal einer anderen Gesellschaft der Gruppe übermittelt, so ist – sofern die hinweisgebende Person ausdrücklich erklärt, die Schutzmechanismen des WB-Dekrets in Anspruch nehmen zu wollen, oder dieser Wille eindeutig aus ihrem Verhalten hervorgeht – die Meldung innerhalb von 7 Tagen nach Eingang an den Bearbeiter (über den Leiter Audit) weiterzuleiten, ohne eine Kopie zurückzubehalten. Gleichzeitig ist – soweit möglich – die hinweisgebende Person über die erfolgte Weiterleitung zu informieren.

6.4.1 Elektronisches Portal

Um eine Meldung abzugeben, muss die hinweisgebende Person auf das Portal zugreifen, in dem der jeweils für die betreffende Gesellschaft der Gruppe vorgesehene Meldekanal verfügbar ist. Der Zugangslink zum Portal lautet wie folgt: https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione.

Meldekanäle der Gesellschaften

Innerhalb des Portals sind die jeweils eigenen Meldekanäle der gemäß Art. 4 Abs. 4 des WB-Dekrets relevanten Gesellschaften der Gruppe sowie ein gemeinsamer Meldekanal für die übrigen Gesellschaften der Terna-Gruppe verfügbar. Insbesondere sind im Portal die folgenden Meldekanäle vorgesehen:

- Terna S.p.A.;
- Terna Rete Italia S.p.A.;
- Tamini Trasformatori S.r.l.;
- Altenia S.r.l.
- Weitere Gesellschaften der Terna-Gruppe[17]/Einrichtungen.

Modalitäten der Meldung

Die hinweisgebende Person hat, nachdem sie den Meldekanal der ausgewählten Gesellschaft der Gruppe aufgerufen hat (z. B. den Meldekanal von Terna S.p.A., Terna Rete Italia S.p.A. oder einen anderen Kanal), die Möglichkeit, ihre Meldung entweder schriftlich, indem sie den Inhalt manuell ausarbeitet, oder mündlich, durch Übermittlung einer Sprachnachricht nach ausdrücklicher Zustimmung zur Aufzeichnung ihrer Stimme, abzugeben. Vor dem Absenden der Meldung besteht die Möglichkeit, diese erneut anzuhören, zu speichern oder zu verwerfen. Nach dem Absenden wird bei mündlichen Meldungen das System die Stimmparameter verändern, sodass die Aufnahme nicht mehr identifizierbar ist.
Die Meldungen müssen in gutem Glauben erfolgen und dürfen nicht anonym abgegeben werden.

[16] Gemäß Art. 47 der Richtlinie (EU) 2019/1937.

[17] Gemäß Art. 4 Abs. 4 des GvD Nr. 24/2023 können diese Gesellschaften den internen Meldekanal sowie dessen Verwaltung gemeinsam nutzen.

Um die Meldung abzugeben, muss die hinweisgebende Person – nach Erhalt der entsprechenden Datenschutzinformation – ihre Daten in die vorgesehenen Felder eintragen. Diese Registrierung umfasst die Angabe einer persönlichen E-Mail-Adresse und einer persönlichen Telefonnummer, um den zweifachen Sicherheitscode für die folgenden Zugriffe zu erhalten und eine dedizierte und vertrauliche Kommunikation zwischen der Gesellschaft und der hinweisgebenden Person zu ermöglichen. Dies dient sowohl der Einholung etwaiger weiterer Klarstellungen als auch der Übermittlung des *Feedbacks* zur Weiterverfolgung der eingereichten Meldung.
Die Daten zur Identität der hinweisgebenden Person werden innerhalb des *IT-Tools* aufbewahrt und durch ein Verschlüsselungssystem geschützt, sodass die Meldung anonymisiert, jedoch nicht anonym ist. Die Daten können nur dann entschlüsselt werden, wenn dies für die Durchführung der erforderlichen Ermittlungen unbedingt notwendig ist. Dabei bleibt ihre Vertraulichkeit weiterhin gewährleistet. Eine Offenlegung der Daten gegenüber anderen Personen als jenen, die für den Empfang oder die Bearbeitung der Meldung zuständig sind, ist ausschließlich in den im WB-Dekret vorgesehenen Fällen und nur nach ausdrücklicher Zustimmung der hinweisgebenden Person zulässig (d. h. wenn dies erforderlich ist, um dem Beschuldigten die Verteidigung in einem Disziplinarverfahren zu ermöglichen, das ausschließlich auf der Meldung beruht und in dem die Kenntnis der Identität der hinweisgebenden Person für die Verteidigung der betroffenen Person unerlässlich ist). In diesem Fall wird sich der RIA vor der Beantragung der Entschlüsselung bemühen, über dieselbe Plattform die Einwilligung der hinweisgebenden Person einzuholen und ihr dabei die entsprechenden Gründe mitzuteilen.
Der begründete Antrag auf Entschlüsselung wird über das Portal vom Vorsitzenden des Ethikausschusses („**PCE**“) an den Chief Information Security Officer („**CISO**“) von Terna[18] gerichtet, der die Maßnahmen zur Entschlüsselung der Identitätsdaten der hinweisgebenden Person unterstützt, ohne jedoch irgendeinen Zugriff auf die Meldung selbst zu haben. Der CISO wird bei dieser Gelegenheit darüber informiert, dass – sofern dies gemäß dem WB-Dekret erforderlich ist – die Einwilligung der hinweisgebenden Person eingeholt wurde. Im Falle einer Verhinderung des PCE wird der Antrag auf Entschlüsselung vom RIA gestellt, wobei der PCE hiervon in Kenntnis gesetzt wird.

Verwaltung des Portals

Der RIA überwacht und verwaltet das Portal unter seiner Verantwortung im Rahmen der Bearbeitung der Meldungen und zusätzlich zu den Aufgaben, die der Audit-Direktion ausdrücklich zu Ermittlungszwecken zugewiesen sind. Dies gilt vorbehaltlich der ausdrücklich vorgesehenen Ausnahmen im Falle eines Interessenkonflikts oder aufgrund spezifischer Aufgaben, die anderen Benutzerkategorien übertragen sind (z. B. für die Änderung des Protokolls des Ethikausschusses, das die Ermittlungsergebnisse geprüft hat).
Im Rahmen der Portalverwaltung sorgt der RIA für das Hochladen der außerhalb des Portals eingegangenen Meldungen sowie für die Zuweisung der über das Portal eingegangenen Meldungen. Falls er dies nicht selbst vornimmt, erteilt er dem **Whistle Editor** die entsprechende Berechtigung, in seinem Namen tätig zu werden.
Für die Durchführung von Aktualisierungs- und Administrations-tätigkeiten am Portal kann sich der RIA des **Portal-Editors** bedienen, der vom RIA innerhalb des Audit-Bereichs und unter den als Portalbenutzer erfassten Personen bestimmt wird. Der Rolle des Portal-Editors ist kein Zugriff auf die Meldungen zugeordnet.

[18] Handelt es sich um eine Meldung, die eine relevante kontrollierte Gesellschaft betrifft, wird der Antrag zudem dem für die betreffende Meldung benannten Referenten, wie in Abschnitt 6.5 vorgesehen, zur Kenntnis gebracht.

Über das Portal bestimmt der RIA (oder der PCE im Falle eines Interessenkonflikts des RIA) innerhalb des Audit-Bereichs und unter den als Portalbenutzer erfassten Personen – wie im folgenden Abschnitt 6.5 vorgesehen – den Owner für die Durchführung der Ermittlungsphase, als hierzu ordnungsgemäß befugte und geschulte Person. Im Rahmen dieser Tätigkeiten ist der Owner jene Person, die die Ermittlungsunterlagen im Repository des betreffenden Kanals ablegt und über das Portal die Kommunikation mit der hinweisgebenden Person führt, indem sie ihr die entsprechenden *Feedbacks* übermittelt.
Der Owner nimmt – sofern er vom RIA (oder vom PCE im Falle eines Interessenkonflikts des RIA) ordnungsgemäß dazu ermächtigt wurde – die Löschung der Meldungen vor, wenn die Voraussetzungen gemäß dem WB-Dekret vorliegen und/oder die Aufbewahrungsfrist[19] abgelaufen ist. Dabei informiert er vorab, sofern zutreffend, die Ansprechpersonen der betreffenden kontrollierten Gesellschaft.
Die Zugriffe auf das Portal werden protokolliert, ebenso wie das Ersetzen und Löschen von Dokumenten und Berichten.
Die Verwaltung der technischen Funktionen sowie die Aktualisierungen der Plattform obliegen dem vom Bereich *Enterprise Services and Platforms* (**ITD-ESP**) von Terna beauftragten Systemadministrator des Portals, der diese Tätigkeiten auf Grundlage der Vorgaben von Audit durchführt. Dieser Administrator kann keine Meldung einsehen oder bearbeiten und behält ausschließlich jene erweiterten technischen Berechtigungen, die für die Ausübung einer rein technischen Unterstützungsrolle erforderlich sind.

6.4.2 Direktes Treffen

Als Alternative zum oben genannten Meldekanal hat die hinweisgebende Person die Möglichkeit, ein Treffen mit dem Leiter Audit zu beantragen, um ihm den Gegenstand der Meldung direkt mitzuteilen. Dieses Treffen wird über eine Anfrage vereinbart, die die hinweisgebende Person über das Portal (https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione) oder per E-Mail an die Adresse whistleblowing@terna.it übermittelt, wobei der Name der zur Terna-Gruppe gehörenden Gesellschaft, auf die sich die Meldung bezieht, anzugeben ist. Diese E-Mail-Adresse darf ausschließlich zur Übermittlung des Antrags auf ein Treffen verwendet werden und nicht zur Übermittlung schriftlicher Meldungen.

6.4.3 Normale Post

Die Nutzung des Portals stellt die größte Garantie für Vertraulichkeit dar. Allfällige Meldungen, die alternativ per ordentlicher Post übermittelt werden, werden zugelassen, sofern sie an die betroffene Gesellschaft des Konzerns adressiert sind, zu Händen des Leiters Audit, c/o TERNA S.p.A., Viale Egidio Galbani 70 – 00156 Rom, und den Vermerk „*Whistleblowing-Meldung, vertraulich – nicht öffnen*“ tragen. Solche Meldungen müssen ausreichend detailliert sein, um eine Bewertung der Sachverhalte zu ermöglichen, und auf präzisen und übereinstimmenden Tatsachen beruhen, wie im WB-Dekret vorgesehen. Sie können zugelassen werden, gelten jedoch nicht als Meldungen im Sinne des WB-Dekrets, insbesondere im Hinblick auf die Kommunikation mit der hinweisgebenden Person

[19] Gemäß Art. 14 Absatz 1 des GvD 24/2023 werden die Meldungen und die dazugehörige Dokumentation im Repository des jeweiligen internen Kanals für die zur Bearbeitung der Meldung erforderliche Dauer aufbewahrt, jedenfalls jedoch nicht länger als fünf Jahre ab dem Datum der Mitteilung des endgültigen Ergebnisses des Meldeverfahrens, vorbehaltlich einer längeren Aufbewahrung im Falle von Gerichtsverfahren, Anfragen von Behörden oder der Einleitung von Rechtsstreitigkeiten. Entsprechendes gilt für die Papierdokumentation zu Meldungen, die außerhalb des Portals eingegangen sind, gemäß den Bestimmungen in Abschnitt 6.8. Bezüglich der Meldungen, die Sachverhalte betreffen, welche nicht in den Anwendungsbereich des GvD 24/2023 fallen, werden die Daten ebenfalls im Repository aufbewahrt – und zwar nur für den Zeitraum, der unbedingt erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben wurden, und in Übereinstimmung mit den Bestimmungen zum Schutz der Rechte der betroffenen Personen sowie unter Beachtung der gesetzlich vorgesehenen Verjährungsfristen.

und die Übermittlung von *Feedbacks*. Ohne den oben genannten ausdrücklichen Vermerk kann die Meldung nicht gemäß den Bestimmungen des GvD 24/2023 entgegengenommen und bearbeitet werden.
Es werden alle geeigneten Maßnahmen ergriffen, um auch bei dieser Übermittlungsart die Vertraulichkeit der Informationen und Daten der Meldung zu gewährleisten.

6.5 Verwaltung der Meldungen

6.5.1 Zuständige Stellen

Die für die Verwaltung der Meldung zuständigen Personen werden gemäß den Vorgaben des GvD Nr. 24/2023, des Ethikkodex sowie der Vorschriften zum Schutz personenbezogener Daten formell bestimmt.
Die für die Verwaltung der Meldungen zuständigen Unternehmensorgane sind:

- der Leiter Audit, hinsichtlich des Eingangs und der Durchführung der Ermittlungsphase der Meldungen;
- der Ethikausschuss, hinsichtlich der Prüfung der Zulässigkeit, des Inhalts und der Ermittlungsunterlagen der Meldung sowie für die pflichtgemäße Weiterverfolgung derselben.

Die Mitglieder des Ethikausschusses werden vom Chief Executive Officer von Terna ernannt.
Die Meldungen werden vom RIA, gemeinsam mit den Mitgliedern des Ethikausschusses, transparent und anhand eines vordefinierten Ablaufs bearbeitet.
Im Rahmen der Verwaltung der Meldungen gewährleisten die genannten zuständigen Unternehmensorgane – jeweils im Rahmen ihrer Aufgaben – Folgendes:

- die Übermittlung einer Eingangsbestätigung an die hinweisgebende Person innerhalb von sieben Tagen ab Eingang der Meldung, für Meldungen gemäß dem WB-Dekret;
- die Aufrechterhaltung – soweit möglich und abhängig vom gewählten Meldekanal – der Interaktionen mit der hinweisgebenden Person, einschließlich der Anforderung zusätzlicher Informationen oder ergänzender Unterlagen, falls erforderlich;
- die pflichtgemäße Weiterverfolgung der eingegangenen Meldungen;
- die Erteilung einer Rückmeldung zur Meldung innerhalb von drei Monaten ab dem Datum der Eingangsbestätigung oder, falls eine solche Bestätigung fehlt, innerhalb von drei Monaten nach Ablauf der Sieben-Tage-Frist ab Einreichung der Meldung.

Die Verwaltung der Meldungen für die Gesellschaften der Terna-Gruppe erfolgt auf Grundlage geeigneter Intra-Group-Vereinbarungen mit Terna und sieht Verfahren vor, die die Einbindung der relevanten kontrollierten Gesellschaften sicherstellen. In diesem Zusammenhang ist – auch in diesen Fällen und im Einklang mit den Bestimmungen dieses Absatzes – die Einbindung des Leiters Audit vorgesehen, der dafür verantwortlich ist, die Einhaltung der gesetzlichen Vorgaben hinsichtlich des Eingangs, der Analyse und der Rückmeldung zu den eingegangenen Meldungen zu gewährleisten. Dabei bleibt die zentrale Rolle des Ethikausschusses unberührt, ebenso wie die getrennte Erfassung, Bearbeitung und Verwaltung der für jede einzelne Gesellschaft eingegangenen Meldungen. Sollte die Meldung an den Meldekanal der betroffenen kontrollierten Gesellschaft gerichtet sein und diese selbst betreffen, so bezieht der Leiter Audit in der Ermittlungsphase auch einen Referenten ein (aus mindestens zwei ernannten Referenten), der von der betroffenen kontrollierten Gesellschaft benannt wurde, um die Nähe der Bearbeitung der Meldung zur jeweiligen Gesellschaft sicherzustellen. Der einbezogene Referent kann sämtliche Ermittlungsunterlagen einsehen und wird eingeladen, an den Sitzungen des Ethikausschusses teilzunehmen – jenes Organs, das das Ergebnis der Ermittlungen bewertet und die Meldung weiterverfolgt, wobei der

Standpunkt des Referenten berücksichtigt wird.
Die mit der Verwaltung der Meldung betrauten Personen dürfen die Identität der hinweisgebenden Person oder andere Informationen, aus denen diese abgeleitet werden kann, keiner anderen Person offenlegen, die nicht ordnungsgemäß in die Ermittlungsaktivitäten eingebunden ist, es sei denn, die hinweisgebende Person hat ausdrücklich zugestimmt.
Die für die Verwaltung der Meldung zuständigen Stellen werden über das Vorliegen einer Meldung durch den RIA informiert[20]. Die Meldungen werden den für die jeweilige Meldung unbedingt einzubindenden Personen angezeigt (Owner, Mitglieder des Ethikausschusses einschließlich des Sekretärs des Ausschusses), entsprechend der Profilierung im jeweiligen Kanal und den vom RIA vorgenommenen Zuweisungen.

- Im Falle einer Meldung über das Portal wird der Leiter Audit[21] durch einen vom Portal generierten Alert informiert, der ihm als E-Mail-Benachrichtigung in seinem Postfach zugeht. Der gleiche Alert wird vom RIA an die Referenten der betroffenen kontrollierten Gesellschaft weitergeleitet, sofern diese nicht in einem Interessenkonflikt stehen, wenn die Meldung an diese Gesellschaft gerichtet ist[22].
- Im Falle einer Meldung über ein direktes Treffen ist es erforderlich, dass die Meldung von mindestens zwei Personen entgegengenommen wird. Der Leiter Audit, begleitet von einer weiteren Person der Direktion Audit, nimmt die Anfrage für ein Treffen gemäß den Bestimmungen in Abschnitt 6.4.2 entgegen und unterstützt – nach Vereinbarung des Treffens – die hinweisgebende Person bei der Erfassung der Meldung im Repository der betroffenen Gesellschaft der Terna-Gruppe. Anschließend leitet er den Prüfprozess gemäß diesem Abschnitt ein.
- Erfolgt die Meldung hingegen per ordentlicher Post, so wird sie vom Leiter Audit gemäß den internen Vorschriften und den Bestimmungen in Abschnitt 6.4.3 dieser Leitlinie entgegengenommen. Der Leiter Audit prüft nach Erhalt den Inhalt des Umschlags und erfasst die Meldung (direkt oder über den Whistler Editor) im Repository der empfangenden Gesellschaft. Anschließend leitet er den Prüfprozess gemäß diesem Abschnitt ein.

6.5.2 Phasen der Verwaltung und Ermittlungsaktivitäten

Beim Eingang der Meldung über einen der in Abschnitt 6.4 genannten internen Kanäle wird eine vorläufige Bewertung der Meldung vorgenommen, um festzustellen:

(i) ob sie einen Verstoß zum Gegenstand hat;
(ii) ob sie die objektiven und subjektiven Voraussetzungen einer relevanten Meldung erfüllt.

Der Leiter Audit legt auf Grundlage des Inhalts der Meldung die Modalitäten der Vertiefung sowie die einzubeziehenden Stellen fest und bewertet, welche davon am geeignetsten sind. Konkret weist der RIA (direkt oder über den Editor des Portals) die Verwaltung des Prüfprozesses einem hierfür autorisieren und geschulten Mitarbeiter seiner Struktur zu (sog. **Owner**). Er bewertet zudem, ob – in Bezug auf den Gegenstand der Meldung – das Einbeziehen weiterer Strukturen erforderlich ist (z. B. Fraud Management, Data Protection & Privacy), soweit dies für die Ermittlungsaktivitäten notwendig

[20] Ausgenommen hiervon sind Fälle eines potenziellen Interessenkonflikts des RIA; in solchen Fällen wird die Meldung direkt an den Vorsitzenden des Ethikausschusses weitergeleitet.

[21] Terna hat den Leiter Audit als die für den Empfang der Meldungen zuständige Person bestimmt, unbeschadet der zentralen Rolle des Ethikausschusses. Der Grund für diese Wahl liegt in der organisatorischen Positionierung dieser Funktion: Da sie über keine operativen Befugnisse verfügt und direkt an den Präsidenten des Verwaltungsrats berichtet, ist sie jene Stelle, die im Rahmen der Tätigkeiten zur Verwaltung der Meldungen die größtmögliche Unabhängigkeit gewährleisten kann.

[22] Diese Mitteilung wird keinerlei Elemente enthalten, die Rückschlüsse auf die Identität der hinweisgebenden Person und/oder auf den Inhalt der Meldung zulassen. Der Alert dient dazu, sicherzustellen, dass die betroffene kontrollierte Gesellschaft Kenntnis vom Eingang der Meldung erhält und die Übereinstimmung zwischen den eingegangenen und den geprüften Meldungen überwacht werden kann.

ist. Dabei wird die Vertraulichkeit der Meldung gewahrt und es werden ausschließlich jene Daten weitergegeben, die für die jeweiligen Tätigkeiten erforderlich sind[23]. Die Einbindung weiterer Unternehmensstrukturen erfolgt unter Beachtung des Grundsatzes der Datenminimierung, wobei die Weitergabe auf jene Informationen beschränkt wird, die für die Durchführung der zugewiesenen Ermittlungsaktivitäten unbedingt erforderlich sind. Damit der Ethikausschuss zeitnah Zugang zu sämtlichen für die Erfüllung seiner Aufgaben erforderlichen Ermittlungsunterlagen hat, erteilt der RIA den Mitgliedern des Ethikausschusses (sowie dem Sekretär des Ausschusses) Zugriff auf die jeweilige Meldung, wobei allfällige Mitglieder, die in die Meldung involviert sind, ausgeschlossen werden.
Der einbezogene Referent (falls die Meldung eine relevante kontrollierte Gesellschaft betrifft) kann sämtliche Ermittlungsunterlagen zur jeweiligen Meldung einsehen.
Nach der Ernennung des Owners leitet der Leiter Audit Ermittlungsaktivitäten ein. Ziel ist es, die zur Bestätigung der Stichhaltigkeit und Relevanz der gemeldeten Sachverhalte erforderlichen Elemente zu identifizieren, zu analysieren und zu bewerten[24]. Die Ergebnisse werden in den vom Owner erstellten und vom RIA genehmigten Ermittlungsberichten (Reports) festgehalten. Der Report – sowohl der Abschlussbericht als auch allfällige ergänzende Berichte – wird im Falle einer Meldung, die eine relevante kontrollierte Gesellschaft betrifft, mit dem benannten Referenten geteilt.

6.5.3 Rolle des Ethikausschusses

Der RIA teilt den Abschlussreport dem Ethikausschuss mit, um:

- über die weitere Weiterverfolgung der Meldung zu beschließen, einschließlich – falls erforderlich – einer Ergänzung der Ermittlungen;
- die vom RIA gegebenenfalls vorgeschlagene Archivierung zu bestätigen.

Die Mitglieder des Ethikausschusses werden für jede eingegangene Meldung über das Portal informiert – entweder durch den Leiter Audit oder, in den in Abschnitt 6.6 genannten Fällen, durch den Vorsitzenden des Ethikausschusses.
Die Arbeitsweise des Ethikausschusses ist in einer eigenen Geschäftsordnung geregelt[25].
Der RIA, in seiner Funktion als Leiter der Direktion Audit von Terna, innerhalb derer die Ermittlungen durchgeführt werden, nimmt – sofern er nicht selbst von der Meldung betroffen ist – an den Sitzungen des Ethikausschusses teil, gegebenenfalls auch durch einen Delegierten (vorzugsweise den für die Meldung zuständigen Owner).
Erst nach Abschluss der Verwaltungstätigkeiten informiert der Bearbeiter die Unternehmensspitzen oder die zuständigen Funktionen der nicht relevanten Gesellschaften sowie der relevanten kontrollierten Gesellschaften (über den jeweiligen Referenten) über die erforderlichen Folgemaßnahmen. Dem Bearbeiter obliegt keine Bewertung individueller Verantwortlichkeiten und auch nicht die Entscheidung über etwaige nachfolgende Maßnahmen oder Verfahren.

[23] Hat die hinweisgebende Person im Portal angegeben, dass die Meldung den RIA betrifft (durch Setzen des entsprechenden Flags), so übermittelt das IT-System die Meldung direkt an den Vorsitzenden des Ethikausschusses, der für die Zwecke dieser Leitlinien die Funktionen des RIA in Bezug auf die Verwaltung der Meldung übernimmt

[24] Offensichtlich für die Bearbeitung einer spezifischen Meldung nicht erforderliche Daten werden nicht erhoben oder – falls sie versehentlich erfasst wurden – unverzüglich gelöscht, wobei der in Art. 13 Abs. 2 des GvD 24/2023 vorgesehene Grundsatz der Datenminimierung restriktiv ausgelegt wird, sofern deren absolute Irrelevanz für den gemeldeten Sachverhalt klar erkennbar ist. Unberührt bleiben dabei die sektorspezifischen Vorschriften zur Aufbewahrung von Unterlagen.

[25] vgl. LG014 – Regelwerk des Ethikausschusses

6.5.4 Meldungen betreffend Verstöße gegen das Modell 231 und Informationsflüsse an das OdV (Überwachungsorgan)

Hinsichtlich der Meldungen, die den privaten Sektor betreffen und nicht die Konzession eines öffentlichen Dienstes, können die gemäß dem GvD 231/2001 relevanten Verstöße sowie die Verstöße gegen die Modelle 231 ausschließlich über die internen Meldekanäle übermittelt werden. Unter Wahrung der im Whistleblowing-Dekret und in den einschlägigen Unternehmensverfahren vorgesehenen Vertraulichkeitspflichten übermittelt der Bearbeiter (über den Leiter Audit) unverzüglich an die E-Mail-Adresse des OdV der betroffenen Gesellschaft (sowie an das von der Gesellschaft benannte technische Sekretariat des OdV) die entsprechende Eingangsinformation, sofern eine Meldung tatsächliche oder potenzielle Verstöße gegen das Modell 231 und/oder rechtswidrige Verhaltensweisen betrifft, die die Vortatbestände gemäß GvD 231/2001 erfüllen. Nach Abschluss der Ermittlungsaktivitäten und nach der Bewertung durch den Ethikausschuss übermittelt der RIA dem OdV unverzüglich eine Mitteilung, in der – unter Wahrung des Vertraulichkeitsgrundsatzes – i) die durchgeführten Ermittlungsaktivitäten, ii) die entsprechenden Ergebnisse sowie iii) die vom Ethikausschuss getroffene Entscheidung dargelegt werden.
Erhält das OdV irrtümlich Meldungen, so leitet es diese innerhalb von 7 Tagen nach Eingang an den Bearbeiter (über den Leiter Audit) weiter, ohne eine Kopie zurückzubehalten, und informiert – soweit möglich – gleichzeitig die hinweisgebende Person über die Weiterleitung.

6.6 Verwaltung potenzieller Interessenkonflikte

Ist der RIA in die Meldung involviert, wird diese – wie in Abschnitt 6.4.1 vorgesehen – vom Vorsitzenden des Ethikausschusses verwaltet.
Die Meldungen werden den Bearbeitern entsprechend ihrer Profilierung im jeweiligen Kanal und den vom RIA vorgenommenen Zuweisungen angezeigt. Ist einer der Mitglieder des Ethikausschusses in die Meldung involviert, erhält dieses Mitglied keine Benachrichtigung über die betreffende Meldung und nimmt nicht an den entsprechenden Tätigkeiten des Ethikausschusses teil (gemäß den Bestimmungen der Geschäftsordnung des Ethikausschusses[26]).
Darüber hinaus wird im Hinblick auf die Verwaltung der Meldungen betreffend relevante kontrollierte Gesellschaften jede dieser Gesellschaften – wie in Abschnitt 6.5 vorgesehen – mindestens zwei Referenten benennen. Dieses Mandat wird bereits im Vorfeld, also vor dem Eingang der Meldung beim Leiter Audit, festgelegt, um die Nähe der Bearbeitung zur jeweils betroffenen Gesellschaft des Konzerns sicherzustellen. Der RIA hat, sobald die Meldung eingegangen ist, einen der benannten Referenten auszuwählen. Sollte bei einem der Referenten ein potenzieller Interessenkonflikt bestehen, muss der Leiter Audit einen anderen der benannten Referenten bestimmen, wobei zu berücksichtigen ist, dass der involvierte Referent sämtliche Ermittlungsunterlagen zur betreffenden Meldung einsehen kann und zur Teilnahme an der Sitzung des Ethikausschusses eingeladen wird, der das Ergebnis der Ermittlungen bewertet und über die weiteren Maßnahmen zur Meldung entscheidet.

6.7 Verarbeitung von personenbezogenen Daten

Die Verarbeitung der im Rahmen des Meldeverfahrens erhobenen personenbezogenen Daten erfolgt unter voller Beachtung der Datenschutzbestimmungen, in Übereinstimmung mit den Vorgaben des GvD 24/2023. Dabei wird ein angemessener Ausgleich zwischen den Rechten der gemeldeten Person und dem Recht auf Vertraulichkeit der Identität der hinweisgebenden Person

[26] vgl. LG014 – Regelwerk des Ethikausschusses

gewährleistet, indem die in dieser Leitlinie vorgesehenen technischen und organisatorischen Maßnahmen umgesetzt werden, die geeignet sind, die Sicherheit der personenbezogenen Daten gemäß der geltenden Rechtsvorschriften sicherzustellen. Diese Maßnahmen umfassen unter anderem – ohne Anspruch auf Vollständigkeit – die Zugangstrennung, die Verschlüsselung der identifizierenden Daten, die Protokollierung der Zugriffe und der im System durchgeführten Vorgänge sowie spezifische Autorisierungs- und Schulungsverfahren für das beteiligte Personal. Die Verarbeitung der personenbezogenen Daten im Rahmen des Whistleblowing-Systems stützt sich auf die Erfüllung einer gesetzlichen Verpflichtung, der der Verantwortliche unterliegt, gemäß Art. 6 Abs. 1 Buchst. c der Verordnung (EU) 2016/679, wie im GvD 24/2023 vorgesehen. Im Rahmen der Verwaltung der Meldungen können personenbezogene Daten, die besonderen Kategorien gemäß Art. 9 DSGVO angehören, sowie Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO gegebenenfalls und nicht systematisch verarbeitet werden – und zwar ausschließlich insoweit, als dies unbedingt erforderlich ist, um die gemeldeten Sachverhalte zu überprüfen, und unter Beachtung der in der geltenden Rechtsvorschrift vorgesehenen Garantien. Es bleibt vorbehalten, dass die Ausübung der Rechte durch die hinweisgebende Person oder die gemeldete Person (beides „betroffene Personen“ im Sinne der Datenschutzbestimmungen) in Bezug auf ihre im Rahmen des Whistleblowing-Verfahrens verarbeiteten personenbezogenen Daten eingeschränkt werden kann[27], um die Rechte und Freiheiten anderer Personen zu schützen. Dabei gilt ausdrücklich, dass der gemeldeten Person unter keinen Umständen gestattet werden darf, ihre Rechte so auszuüben, dass sie Informationen über die Identität der hinweisgebenden Person erlangt[28]. Die operativen Modalitäten für die Ausübung der Rechte der betroffenen Personen werden durch die unternehmensinternen Vorschriften zum Schutz personenbezogener Daten sowie durch die den betroffenen Personen zur Verfügung gestellten Datenschutzinformationen geregelt.

Das System zur Verwaltung der Meldungen ist daher so ausgestaltet, dass die Rechte und Freiheiten der betroffenen Personen gewährleistet werden, unter anderem durch eine klare Zuweisung von Rollen und Verantwortlichkeiten im Zusammenhang mit der Datenverarbeitung sowie durch die entsprechende Dokumentation des Kontextes.

Insbesondere werden im Rahmen des Konzerns gemäß GvD 24/2023 die relevanten kontrollierten Gesellschaften[29], die Daten ihres jeweiligen internen Meldekanals als eigenständige Verantwortliche verarbeiten. Für die übrigen Gesellschaften der Terna-Gruppe[30], kann ein gemeinsamer Meldekanal genutzt werden, dessen Verwaltung von den jeweiligen Gesellschaften selbst wahrgenommen wird, in ihrer Eigenschaft als gemeinsame Verantwortliche gemäß Art. 26 DSGVO. Dies erfolgt auf Grundlage einer Vereinbarung über die gemeinsame Verantwortlichkeit, in der die jeweiligen Pflichten und Verantwortlichkeiten hinsichtlich der Einhaltung der aus der DSGVO resultierenden Verpflichtungen festgelegt sind – insbesondere in Bezug auf die Ausübung der Rechte der betroffenen Personen sowie die jeweiligen Informationspflichten gemäß den Art. 13 und 14 DSGVO. Die Dienstleister, die die Verwaltung des IT-Portals und der zugehörigen technischen Infrastrukturen unterstützen, werden gemäß Art. 28 DSGVO als Auftragsverarbeiter bestellt. Dies erfolgt auf

[27] Gemäß Art. 23 DSGVO und Art. 2-undecies des GvD 196/2003.

[28] Gemäß Art. 2-undecies des GvD 196/2003 kann die betroffene Person ihre Rechte nicht ausüben, wenn deren Ausübung einen tatsächlichen und konkreten Nachteil für die geschützten Interessen verursachen könnte (beispielsweise die Durchführung von Verteidigungsermittlungen, die Ausübung von Rechten in einem Gerichtsverfahren, die Wahrung der Vertraulichkeit der Identität des Mitarbeiters, der einen Verstoß meldet, usw.). Daher kann der Verantwortliche in jedem Fall die Ausübung dieser Rechte aufschieben, einschränken oder ausschließen, wobei dies der betroffenen Person unverzüglich und begründet mitzuteilen ist.

[29] Zum Zeitpunkt der Veröffentlichung dieser Leitlinie: Terna S.p.A., Terna Rete Italia S.p.A. und Tamini Trasformatori S.r.l.

[30] Unter diesen Gesellschaften sind jene der Terna-Gruppe zu verstehen, die gemäß Art. 4 Abs. 4 des WB-Dekrets weniger als 249 Beschäftigte haben.

Grundlage spezifischer vertraglicher Vereinbarungen, in denen die Weisungen, die Sicherheitsmaßnahmen sowie die Grenzen der Verarbeitung eindeutig geregelt sind.
Daher stellen die Gesellschaften – sowohl in ihrer Eigenschaft als eigenständige Verantwortliche als auch als gemeinsame Verantwortliche – die jeweils erforderlichen Datenschutzinformationen zur Verfügung, in denen Zwecke, Fristen und Modalitäten der Datenverarbeitung im Zusammenhang mit dem Meldeverfahren angegeben sind.
Gemäß den Art. 29 und 32 DSGVO sowie Art. 2-quaterdecies des GvD 196/2003 sind ausdrücklich jene Personen zur Verarbeitung dieser Daten autorisert, die mit dem Empfang und der Verwaltung der Meldungen betraut sind; sie erhalten hierfür spezifische Weisungen.
Darüber hinaus wird – in Übereinstimmung mit den Vorgaben des GvD 24/2023 – das System zur Entgegennahme und Verwaltung der Meldungen über interne Kanäle auf Grundlage einer Datenschutz-Folgenabschätzung (DIPIA) ausgestaltet. In dieser werden die Verarbeitungsbereiche, die damit verbundenen Risikoprofile sowie die technisch-organisatorischen Maßnahmen zur Minimierung der identifizierten Risiken systematisch dargestellt.

6.8 Archivierung und Aufbewahrung der Meldungen

Falls die Meldung über den internen IT-Kanal gemäß Abschnitt 6.4.1 erfolgt, dient dieser als offizielles *Repository* und ermöglicht sowohl die Archivierung der Meldung als auch die Aufbewahrung sämtlicher damit verbundener Unterlagen.
Erfolgt die Meldung per Post oder alternativ im Rahmen eines persönlichen Gesprächs, so obliegt es dem RIA, die Meldung im Portal im entsprechenden Kanal der empfangenden Gesellschaft gemäß Abschnitt 6.4.1 hochzuladen, um eine ordnungsgemäße Archivierung zu gewährleisten. Gleichzeitig ist die Originaldokumentation in geeigneter Weise aufzubewahren, sodass deren Vertraulichkeit soweit wie möglich gewahrt bleibt.
Die Meldungen und die dazugehörige Dokumentation sind schließlich für den Zeitraum aufzubewahren, der für die Bearbeitung der Meldung erforderlich ist, und jedenfalls gemäß dem WB-Dekret nicht länger als fünf Jahre ab dem Datum der Mitteilung des endgültigen Ergebnisses des Meldeverfahrens oder für die gesetzlich vorgesehene abweichende Aufbewahrungsfrist, wie in Abschnitt 6.4.1 angegeben. Der Beginn der Aufbewahrungsfrist richtet sich nach dem endgültigen Ausgang der Meldung (z. B. unmittelbare Archivierung, Ergebnisse der abschließenden Prüfung, Weiterleitung an die zuständigen Behörden usw.). Der RIA ist daher befugt, die Löschung und/oder Vernichtung etwaiger in Papierform aufbewahrter Unterlagen gemäß Abschnitt 6.4.1 zu veranlassen und informiert gegebenenfalls vorab die Ansprechpersonen der relevanten kontrollierten Gesellschaft.

6.9 Externer Meldekanal

Gemäß den Bestimmungen des WB-Dekrets kann die hinweisgebende Person die von der ANAC eingerichteten externen Meldekanäle, die auf der Internetseite der ANAC[31], verfügbar sind, ausschließlich für jene Verstöße nutzen, die vom Dekret erfasst sind (mit Ausnahme der Verstöße im privaten Sektor, die nicht die Ausübung eines öffentlichen Dienstleistungsauftrags betreffen), und nur sofern die im Dekret vorgesehenen Voraussetzungen erfüllt sind, nämlich:

[31] In dem hierfür vorgesehenen Bereich auf der Internetseite der ANAC finden sich weitere Einzelheiten zu den Modalitäten der Übermittlung, Entgegennahme und Bearbeitung der Meldungen durch die Behörde. Gemäß den Bestimmungen des WB-Dekrets ist die Möglichkeit, den externen Meldekanal oder eine öffentliche Offenlegung zu nutzen, ausschließlich für Gesellschaften vorgesehen, die mehr als fünfzig Beschäftigte haben.
Wie in Abschnitt 6.5.2 angegeben, können Meldungen, die den privaten Sektor betreffen und nicht mit der Ausübung eines öffentlichen Dienstleistungsauftrags verbunden sind, sowie Meldungen über relevante Verstöße gemäß GvD 231/2001 oder Verstöße gegen die Modelle 231, ausschließlich über die internen Meldekanäle erstattet werden.

- fehlende Einrichtung der internen Meldekanäle;
- die Meldung, die gemäß dem WB-Dekret und der vorliegenden Leitlinie erstattet wurde, wurde nicht weiterverfolgt;
- die hinweisgebende Person hat begründeten Anlass zu der Annahme, dass eine interne Meldung keine Weiterverfolgung hätte oder sie Repressalien ausgesetzt wäre. Hinsichtlich der begründeten Gründe wird präzisiert, dass die hinweisgebende Person auf der Grundlage konkreter, belegter Umstände und tatsächlich erlangbarer Informationen – und somit nicht auf bloßen Vermutungen – vernünftigerweise annehmen können muss, dass, wenn sie eine interne Meldung erstatten würde:
    - dieser nicht wirksam nachgegangen würde. Dies ist beispielsweise der Fall, wenn die letztverantwortliche Person im Arbeitskontext an der Verletzung beteiligt ist, das Risiko besteht, dass die Verletzung oder die entsprechenden Beweise verborgen oder vernichtet werden könnten, die Wirksamkeit der Ermittlungen der zuständigen Behörden andernfalls beeinträchtigt würde oder wenn anzunehmen ist, dass die ANAC aufgrund ihrer Zuständigkeiten besser geeignet wäre, die spezifische Verletzung zu behandeln;
    - sie das Risiko von Repressalien mit sich bringen könnte (beispielsweise infolge einer Verletzung der Pflicht zur Vertraulichkeit der Identität der hinweisgebenden Person);
- die hinweisgebende hat Person begründeten Anlass zu der Annahme, dass die Verletzung eine unmittelbare oder offensichtliche Gefahr für das öffentliche Interesse darstellen könnte. Dies ist beispielsweise der Fall, wenn die Verletzung ein dringendes Eingreifen erfordert, um die Gesundheit und Sicherheit von Personen zu schützen oder um die Umwelt zu bewahren[32].

Die hinweisgebende Person und die sonstigen betroffenen Personen können gemäß Art. 19, Absatz 1, des WB-Dekrets der ANAC jene Repressalien melden, die sie nach eigener Einschätzung in ihrem Arbeitsumfeld infolge einer Meldung, Anzeige oder öffentlichen Offenlegung erlitten haben. Geht dem Bearbeiter eine Mitteilung über mutmaßliche Repressalien zu, so weist dieser die hinweisgebende Person darauf hin, dass sie die Möglichkeit hat, diese an die ANAC weiterzuleiten. Der ANAC sind jene objektiven Elemente zu übermitteln, aus denen sich der ursächliche Zusammenhang zwischen der erfolgten Meldung, Anzeige oder öffentlichen Offenlegung und der behaupteten Repressalie ableiten lässt.

6.10 Öffentliche Bekanntgabe

Gemäß dem WB-Dekret kann die hinweisgebende Person[33] eine öffentliche Bekanntgabe von Informationen über jene Verletzungen vornehmen, die im WB-Dekret vorgesehen sind (mit Ausnahme derjenigen, die den privaten Sektor betreffen und nicht mit der Ausübung eines öffentlichen Dienstleistungsauftrags verbunden sind), von denen sie im Arbeitskontext Kenntnis erlangt hat, ausschließlich unter den folgenden, im Dekret festgelegten Voraussetzungen, nämlich:

- die hinweisgebende Person hat zuvor den internen oder externen Meldekanal genutzt, jedoch weder eine Rückmeldung erhalten noch eine Weiterverfolgung der Meldung innerhalb

[32] Gemäß Art. 62 der Richtlinie (EU) 2019/1937.

[33] *„für den Fall, dass sie eine von der journalistischen Informationsquelle verschiedene Person ist“* (vgl. Abschnitt 3.3 des Beschlusses Nr. 311 vom 12. Juli 2023, hinterlegt bei der Geschäftsstelle des Rates am 13. Juli 2023 und veröffentlicht durch Hinweis im Amtsblatt Nr. 172 vom 25. Juli 2023, enthaltend die *„Leitlinien zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, sowie zum Schutz von Personen, die Verstöße gegen nationale Rechtsvorschriften melden. Verfahren zur Einreichung und Bearbeitung externer Meldungen“*).
Wie in Abschnitt 6.5.2 angegeben, können Meldungen, die den privaten Sektor betreffen und nicht mit der Ausübung eines öffentlichen Dienstleistungsauftrags verbunden sind, sowie Meldungen über relevante Verstöße gemäß GvD 231/2001 oder Verstöße gegen die Modelle 231, ausschließlich über die internen Meldekanäle erstattet werden.

der vorgesehenen Fristen erfahren;

- die hinweisgebende Person hat begründeten Anlass zu der Annahme, dass die Verletzung eine unmittelbare und offensichtliche Gefahr für das öffentliche Interesse darstellen könnte[34];
- die hinweisgebende Person hat begründeten Anlass zu der Annahme, dass die externe Meldung ein Risiko von Repressalien mit sich bringen könnte oder dass ihr aufgrund besonderer Umstände des konkreten Falls nicht wirksam nachgegangen würde[35].

Die triftigen Gründe, die eine öffentliche Bekanntmachung rechtfertigen, müssen auf konkreten Umständen beruhen, die der Meldung beizulegen sind, sowie auf tatsächlich ermittelbaren Informationen.

Bei der öffentlichen Offenlegung, wenn die betroffene Person ihre Identität freiwillig offenlegt, kommt der Schutz der Vertraulichkeit nicht zur Anwendung; alle übrigen Schutzmaßnahmen gemäß dem WB-Dekret für die hinweisgebende Person bleiben jedoch unberührt. Legt die Person hingegen Verletzungen unter Verwendung eines Pseudonyms oder *Nicknamens* offen, der ihre Identifizierung nicht ermöglicht, so kann die Meldung – im Hinblick auf den Schutz der Daten der hinweisgebenden Person und für den Fall einer späteren Offenlegung ihrer Identität – wie eine anonyme Meldung behandelt werden (wodurch die im Dekret vorgesehenen Schutzmaßnahmen nicht gewährleistet werden können). Der Person, die die Offenlegung vornimmt, werden jedoch im Falle einer späteren Identifizierung jedenfalls die Schutzmaßnahmen bei Repressalien gewährt.

Die hinweisgebende Person hat der Gesellschaft die jener öffentlichen Offenlegung zugrunde liegende Meldung an die hierfür eingerichtete E-Mail-Adresse whistleblowing@terna.it zu übermitteln, damit sie in den Genuss der vorgesehenen Schutzmaßnahmen gelangen kann (siehe hierzu Abschnitt 6.3 der vorliegenden Leitlinie).

7. Ausländische Gesellschaften

Die Whistleblowing-Regelung, sowohl hinsichtlich der internen Meldekanäle als auch der Schutzmaßnahmen für die hinweisgebende Person und die gemeldete Person, findet – wie oben beschrieben – auch auf ausländische Gesellschaften Anwendung, unter Beachtung der jeweils örtlich geltenden Rechtsvorschriften.

Diesbezüglich wird darauf hingewiesen, dass die Übermittlung personenbezogener Daten aus Drittländern im Sinne und im Rahmen des anwendbaren Gesetzes im Einzelfall zulässig ist. Zu diesem Zweck werden die konzerninternen Vereinbarungen, welche gemäß Abschnitt 6.5 die Bearbeitung der Meldungen für die ausländischen Gesellschaften regeln können, durch weitere spezifische Vereinbarungen ergänzt, um die Datenverarbeitung in Übereinstimmung mit dem jeweils anwendbaren Recht sicherzustellen. Was die Rollen und Verantwortlichkeiten bei der Bearbeitung der Meldungen durch den Bearbeiter betrifft, so kann dieser die Unterstützung des von der betroffenen Gesellschaft bestellten Compliance Officers und/oder externer Berater in Anspruch nehmen. In dieser Phase beschränkt sich die Einbindung des CO auf die Einholung der für die Sachverhaltsprüfung erforderlichen Informationen.

Ist es einer SE nicht möglich, die Whistleblowing-Regelung mit den in der vorliegenden Leitlinie beschriebenen internen Meldekanälen einzuführen, so richten die SE Meldemodalitäten für Informationen über Verletzungen ein, die mit den Bestimmungen des Ethikkodex hinsichtlich des

[34] Eine Notfallsituation oder ein Risiko eines irreversiblen Schadens liegt vor, wenn die körperliche Unversehrtheit einer oder mehrerer Personen betroffen ist und die Verletzung umgehend und mit breiter Resonanz offengelegt werden muss, um ihre Auswirkungen zu verhindern.

[35] Denn es könnte beispielsweise die Gefahr bestehen, dass Beweismittel vernichtet werden oder dass es zu einer Absprache zwischen der für den Empfang der Meldung zuständigen Stelle und dem Verfasser der Verletzung kommt. Es müsste sich mit anderen Worten um besonders schwerwiegende Situationen von Fahrlässigkeit oder um vorsätzliches Fehlverhalten innerhalb des Unternehmens handeln.

Schutzes der hinweisgebenden Person in Einklang stehen, und sie werden:

- Terna S.p.A., auch über den CO, über die bereits eingerichteten oder noch einzurichtenden Schutz- und Kontrollmechanismen informieren, welche das Einbeziehen des gemäß dem Global Compliance Program bestellten CO vorsehen können, als Programm der Compliance, das an alle SE gerichtet ist;
- eine angemessene Information über das System zur Meldung von Informationen über Verletzungen, über die Modalitäten seiner Nutzung sowie über das eingerichtete Schutzsystem sicherstellen.

8. Genehmigung, Überarbeitung und Verbreitung

Die Grundsätze der vorliegenden Leitlinie gehören zu den wesentlichen Werten der Terna-Gruppe und prägen deren Organisation und Tätigkeiten, auch im Rahmen der Bestimmungen des Ethikkodex. Aus diesem Grund und da sie sich an alle Mitarbeitenden (einschließlich der mit befristetem Arbeitsvertrag eingestellten Mitarbeitenden), die Praktikantinnen und Praktikanten sowie die Leiharbeitnehmenden richtet, wurde die vorliegende Leitlinie vom Chief Executive Officer (CEO) und Generaldirektor von Terna S.p.A. genehmigt.
Die Übernahme dieser Leitlinie durch alle Gesellschaften der Gruppe sowie ihre Verbreitung werden gefördert. Zu diesem Zweck werden Sensibilisierungs- und Schulungsinitiativen für das Personal gefördert, um die Ziele des Whistleblowing-Instruments und dessen Nutzungsvorgaben bekannt zu machen (wie etwa spezifische Mitteilungen, Schulungsveranstaltungen, Newsletter, Intranet usw.).
In diesem Zusammenhang werden folgende Maßnahmen durchgeführt:

a) eine angemessene Schulung für die mit der Verwaltung der internen Meldekanäle betrauten Personen, auch durch spezifische Schulungs- und Einführungssitzungen;
b) eine angemessene Kommunikation, um die erforderlichen Informationsziele zu erreichen, hinsichtlich der internen Meldekanäle, der Verfahren und der Voraussetzungen für die Abgabe interner Meldungen sowie hinsichtlich des Kanals, der Verfahren und der Voraussetzungen für die Abgabe externer Meldungen gemäß dem WB-Dekret. In Bezug auf Letzteres erfolgt für die italienischen Gesellschaften der Gruppe die Veröffentlichung der genannten Informationen in einem hierfür vorgesehenen eigenen Bereich der Website, sofern vorhanden.

In Bezug auf Punkt a) hat die Schulung unter Berücksichtigung der anwendbaren Rechtsvorschriften sowie der geltenden *Best Practices* zu erfolgen.
In Bezug auf Punkt b) werden Kommunikationsinitiativen gefördert, die auch der externen Verbreitung der Ziele des Whistleblowing-Instruments und des Verfahrens zu dessen Nutzung dienen. Jede Gesellschaft der Gruppe stellt sicher, dass die vorliegende Leitlinie zum Whistleblowing intern zugänglich gemacht wird, sei es durch Veröffentlichung im unternehmensinternen Intranet, durch Versand per E-Mail oder durch andere Formen der Weitergabe interner Unternehmensdokumente.
Die Grundsätze und Inhalte des Whistleblowing-Instruments, soweit sie für Dritte anwendbar sind, werden durch die vertragliche Dokumentation bekannt gemacht.
Die Informations- und Schulungsmaßnahmen werden dokumentiert, überwacht und hinsichtlich ihrer Angemessenheit und Wirksamkeit bewertet.

Etwaige Änderungen und/oder Ergänzungen, die sich aus gesetzlichen oder rechtsprechungsbezogenen Entwicklungen ergeben, zur Angleichung an *Best Practices* oder an die

Leitlinien der ANAC, im Zusammenhang mit durchgeführten Monitoring-Maßnahmen oder aufgrund neuer betrieblicher oder organisatorischer Erfordernisse als notwendig oder zweckmäßig erweisen, können vom Direktor für Digitale Strategie und Nachhaltigkeit vorgenommen werden. Dabei können, sofern erforderlich oder zweckmäßig, operative Anweisungen erteilt werden, um spezifische Anwendungsprofile der vorliegenden Leitlinie zu regeln und Vorgaben für die kontrollierten Gesellschaften festzulegen. Über die genannten Änderungen und/oder Ergänzungen ist der Ethikausschuss vorab zu informieren. Betreffen die Änderungen wesentliche Aspekte, ist auch die Gewerkschaftsorganisation zu informieren.

9. Reporting

Die Meldungen werden mit jährlicher Periodizität und Bezug auf das Kalenderjahr einer spezifischen Berichterstattung unterzogen, sofern sie im entsprechenden Zeitraum eingegangen sind (mit Angabe der Anzahl der eingegangenen Meldungen, der Anzahl der archivierten Meldungen sowie des Stands der jeweiligen Prüfverfahren). Diese Berichterstattung wird vom RIA erstellt, wobei die Daten der Meldungen anonymisiert und in aggregierter Form zusammengefasst werden. Die Berichterstattung wird dem Ethikausschuss in Bezug auf Terna S.p.A. vorgelegt. Für die übrigen Gesellschaften der Gruppe wird sie auch dem CEO/Alleinverwalter übermittelt, um eine umfassende Darstellung der Funktionsweise des Whistleblowing-Systems zu gewährleisten. Soweit zuständig, erfolgt eine periodische Übermittlung an die OdV/CO, in der Regel alle sechs Monate. Sollte der RIA in Fällen eines Interessenkonflikts keine Einsicht in die Meldungen gehabt haben, wird die Ergänzung der vorgenannten Berichterstattung vom Ethikausschuss über den Sekretär des Ethikausschusses vorgenommen.

10. Unterstützungsmaßnahmen durch Einrichtungen des Dritten Sektors (ETS)

Die hinweisgebende Person kann sich jederzeit an die im von der ANAC gemäß Art. 18 des GvD 24/2023 veröffentlichten Verzeichnis aufgeführten Einrichtungen des Dritten Sektors wenden, die folgende Unterstützungsmaßnahmen anbieten:

a) Informationen, Unterstützung und Beratung zu den Whistleblowing-Vorschriften;
b) Rechtsbeistand;
c) Psychologische Unterstützung.

Das Verzeichnis der vertraglich gebundenen Einrichtungen, die gemäß den Bestimmungen ihrer jeweiligen Satzungen die in dem GvD vom 3. Juli 2017, Nr. 117 vorgesehenen Tätigkeiten ausüben, ist auf der institutionellen Website der ANAC verfügbar. Dieser Absatz beschreibt den Kontext, in den der betreffende Makro-Prozess bzw. das Governance-/Risk-/Compliance-Thema einzuordnen ist.

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".

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, 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.

- 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

[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 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

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

[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.