Terna

LG054

检举

2026 年 3 月 24 日

指导方针

已批准

F. Salerni (SDS)

修订历史

2026 年 3 月 24 日 第 05 修订版	第六版发行，法规调整。
2023 年 12 月 14 日 第 04 修订版	第五版发行。
2023 年 7 月 12 日 第 03 修订版	第四版发行。
2018 年 12 月 21 日 第 02 修订版	第三版发行。
2017 年 1 月 27 日 第 01 修订版	第二版发行。
2016 年 9 月 30 日 第 00 修订版	初版发行。

管理体系及 / 或参考组织模式

	已获认证/认可的管理体系
☑	**SGQ** (质量)
☑	**SGA** (环境)
☑	**SGSL** (工作场所的安全与健康)
☑	**SGPIR** (预防重大事故—《塞维索指令》)
☑	**SGSI** (信息安全)
☑	**SGE** (自用能源消耗量)
☑	**SGQ LST** (LST 实验室)
☑	**SGQ TAR** (校准中心)
☑	**SGAC** (反腐败)
☑	**SGAM** (资产管理)
☑	**SGPCI** (感染预防与控制—生物安全)
☑	**SGC**(合规)
☐	**SGPG** (性别平等)
☐	**SGPAC** (行政与会计流程)

	组织模式
☑	**BCM** (业务连续性模型)
☑	**TCM** (税务合规模型)
☑	**PRV** (隐私政策模板)
☑	**M262** (262 模型)
☑	**M231** (231 模型)
☐	**MIMP** (公正客观模型)
☐	**SCIIS** (可持续发展信息核查系统)

(如需进一步了解经认证/认可的管理体系，请点击 此处)

目录

1. 总则

TERNA 集团始终高度重视预防可能影响其业务实现负责任与可持续管理的各类风险，且依托自身使命和内部控制体系，积极致力于及时洞察潜在的风险问题，同时予以纠正，从而进一步巩固与利益相关方之间的信任关系。

Terna 集团，为确保管理责任的履行以及符合法律规定，自 2016 年 9 月起，已建立并持续更新了一套接收及处理内部或外部违规举报的系统。该系统旨在保障业务及各项活动的正当性与透明度，同时维护公司声誉及形象，防范可能对公司造成损害或不利影响的各类风险，例如：欺诈、 一般性风险或潜在危险情况等可能对公司造成损害或不利影响的行为。上述确保这项体系的持续运行，同时符合 2017 年出台的法规要求，即“在公共或私营部门工作期间发现犯罪或违规行为并予以举报的保护举报人相关规定”，以及 2023 年颁布的《第 24/2023 号立法法令》，该法令涉及*举报*[1]，并包含*“实施欧洲议会和理事会 2019 年 10 月 23 日《第 2019/1937 号欧盟指令》的实施，其涉及保护举报违反欧盟法律行为的人员，并包含关于保护举报违反国家法规行为的人员的规定”*（以下简称**《举报人保护指令》**或**《24/2023号立法法令》**）以及国家反腐败局（**“ANAC”**）根据《举报人保护指令》第 10 条颁布的指导方针[2]。

该体系是集团道德规范（《道德准则》）及*企业责任*，其组织与管理模型依据前《231/01 立法法令》（**《231号模型》**），并适用于集团旗下海外公司的情况下亦包括《全球合规计划》（LG058）。

因此，Terna将“举报”作为内部控制工具之一，并将其纳入开展*业务*时所遵循的行为准则中。若能对检举行为加以适当规范，那么检举任何可能构成欺诈、为同事和股东带来损害风险，或是涉及公司利益与声誉之侵害和非法行为，皆将成为打击腐败的有力举措。

本指南旨在为 Terna 集团界定处理举报的程序，涉及在集团各公司范围内获悉的任何非法行为和/或不当行为（包括作为或不作为），此类行为须符合现行相关法规，并构成违规行为（包括涉嫌违规）：

(i)《道德准则》中已经确立的原则，

(ii) 内部规章制度，即：接收该举报的公司所制定的所有规定、程序、指导方针或操作说明，其中包括根据前《231/01指令》（**“231号模型”**）制定的组织与管理模型、 反腐败指南、《全球合规计划》，以及任何违反政策或公司规章的行为，其可能针对同事、股东及*利益相关方*，导致欺诈或造成实际或潜在损害，或构成损害公司利益及声誉的非法或有害行为，以及

[1] *举报*（*Whistleblowing*）这一英文术语源自比喻性表达*“to blow the whistle”*（意为突然中断某事），它是一种允许任何人举报非法行为（包括涉嫌行为）的机制

[2] 《举报人保护指令》第 10 条规定，国家反腐败局在征询个人数据保护专员意见后，应于《举报人保护指令》生效之日起三个月内，制定关于外部举报提交和管理程序的指导方针。国家反腐败局已在官网上公布了 2023 年 7 月 12 日第 311 号决议，该决议已于 2023 年 7 月 13 日提交至理事会秘书处，并通过 2023 年 7 月 25 日第 172 期《官方公报》发布的公告予以公布，其中包含“*关于保护举报欧盟法律违规行为人员及保护举报违反国家法规人员的相关指导方针。外部举报的提交与处理程序*”。*外部举报的提交与处理程序*”。
国家反腐败局亦在其官方网站上发布了 2023 年 7 月 12 日的第 301 号决议，该决议已于 2023 年 7 月 13 日提交至理事会秘书处，并自 2023 年 7 月 15 日起生效；具体依据为同日刊载于《官方公报》的公告，其标题为“*为落实 2023 年 3 月 10 日第 24 号立法法令，关于国家反腐败局外部举报管理及制裁权行使的条例*”。
随后，国家反腐败局在其官方网站上发布了 2025 年 11 月 26 日第 478 号和第 479 号决议，该决议已刊载于 2025 年 12 月 29 日第 300 期的《官方公报》，内容分别涉及关于内部和外部举报渠道的举报指导方针。

(iii)《24/2023 号指令》所规定的违规行为，“*损害公共利益或公共行政机构或私营实体诚信的国家或欧盟制度规定*”。

具体而言，特此声明，本文件的起草亦符合《举报人保护指令》之规定。该指令是针对打击和预防腐败、遏制不符合公共行政良好运作与公正原则的行为，以及预防公共和私营部门违法行为的立法依据。《举报人保护指令》特别针对公共和私营部门引入了一套综合性的规则体系，该体系协调了欧盟法律与国内法律，旨在鼓励举报损害公共利益或机构诚信的特定非法行为。新式制度提高了举报人所享有的保护层级。

2. 本文件的宗旨

本指南旨在规范违规举报（whistleblowing）的管理，明确并规范集团各公司用于受理举报的内部渠道及其运作方式，界定举报的对象及可进行举报的主体，明确收到举报后开展分析与调查活动的职责分工及管理方式 （职责与责任）及其相关时限、举报人的保护措施、进行外部举报及公开披露的条件，以及为开展举报管理活动而进行的数据保存方式和期限，同时亦需遵守隐私规章制度[3]。

此外，亦对以下方面作出了规定：关于举报渠道使用情况的信息披露方式、通过这些渠道进行举报的条件、负责处理举报的主体及相关程序、针对员工的宣传和培训举措，以及更新这些指导方针的具体方式。

此外，需说明的是，本指南是根据适用于特定范围意大利公司的相关规章制度起草的，其包括《举报人保护指令》及随之颁布的国家反腐败局指南[4]，其中对举报事宜的具体条件和方式作出规范，涉及：保护的客观范围；保护的客观适用范围；举报渠道及提交方式；保密、保护及防范 任何报复行为；对举报人、投诉人或进行公开披露者（“**相关举报**”）的责任限制。

因此，对于不属于上述规章制度范围的举报（“**常规举报**”），以下规定仅在有限范围内适用：关于举报的最低内容要求（第 6.2.1 节）；内部举报渠道（第 6.4 节）；以及对举报的处理（第 6.5 节），但《举报人保护指令》规定的核查和时限除外；以及潜在利益冲突的管理（第 6.6 节）。

无论如何，对于普通举报，也保证将按照适用的《隐私法规》处理数据，并遵守《道德准则》中关于禁止报复的一般性规定；对于出于善意且秉持对公司忠诚精神所作的举报，违反该规定将受到明确的处罚。

3. 适用范围

本指导方针适用于 Terna 及其集团旗下所有公司，包括境外受控公司，但下文第 7 节[5]的规定除外。

[3]隐私法规范围由以下国家及超国家层面的处置措施构成：2018 年 8 月 10 日第 101 号立法法令“关于使国家规章制度与欧洲议会和理事会之 2016 年 4 月 27 日《第 2016/679 号欧盟法规》的规定所调整的条款，*其涉及在处理个人数据方面对自然人的保护以及此类数据的自由流通，并且废除《第 95/46/EC 号指令》*”；欧洲议会和理事会 2016 年 4 月 27 日《第 2016/679 号欧盟法规》，关于在个人数据处理方面保护自然人以及此类数据的自由流通，并废止《第 95/46/EC 号指令》（GDPR）；2003 年 6 月 30 日《第 196 号立法法令》，“*《隐私统一法》*”及其后续修订和补充，以及个人数据保护监管机构颁布的与该法典相关的措施

[4]这是国家反腐败局指导方针，其最新版本已根据 2025 年 11 月 26 日第 478 号决议进行了更新

[5] 根据《举报人保护指令》第 24 条第 2 款的规定，本指导方针中援引的《24/2023号指令》的相关条款，仅自 2023 年 12 月 17 日起适用于 Terna 集团旗下在过去一年中平均雇请 249 名内之受雇员工（包括签订无固定期限或固定期限劳动合同者）的公司。根据 Terna 基金会在 2025 年 12 月 17 日董事会会议纪要，本指南的规定在适用范围内适用于 Terna 基金会。

4. 参考文献

4.1 外部参考文献

- 2023 年 3 月 10 日第 24 号落实了 2019 年 10 月 23 日欧洲议会和理事会颁布的《第 2019/1937 号欧盟法令》，其涉及保护检举违反欧盟法律的人员，同时包括保护举报违反意大利国家法规者的相关规定和后续修正和补充;
- 2017年11月30日第179号法律及其后续修订，“关于保护在公共或私营部门工作期间发现犯罪或违规行为并予以举报的人员的条款”[6];
- 2012年11月6日第190号法律及其后续修订，“关于预防和打击公共行政领域腐败及违法行为的规定”；
- 2001年6月8日第231号立法法令及其后续修订（或《231/01指令》），“关于法人、公司及协会（包括不具有法人资格的协会）行政责任的制度，依据2000年9月29日第300号法律第11条”；
- 2003年6月30日第196号立法法令《隐私统一法》及其后续修订，以及个人数据保护监管机构颁布的相关措施；
- 《第 2016/679 号欧盟法规》（或“**GDPR**”）：关于在个人数据处理方面保护自然人以及此类数据的自由流通，并废除《第 95/46/EC 号指令》（《通用数据保护条例》），以及数据保护监管机构关于个人数据保护的措施；
- 2018 年 8 月 10 日《第 101 号立法法令》及其后续修订，旨在将国家法规与 2016 年 4 月 27 日欧洲议会和理事会关于在个人数据处理方面保护自然人，以及此类数据自由流动的《第 2016/679 号欧盟法规》之规定相互协调，并废除《第 95/46/EC 号指令》；
- 2018 年 5 月 18 日《第 51 号立法法令》旨在实施欧洲议会和理事会于 2016 年 4 月 27 日通过的《第 2016/680 号欧盟指令》，其关于在主管当局为预防、调查、查明和起诉犯罪或执行刑事制裁，以及此类数据的自由流通，并废止理事会《第 2008/977/GAI 号》决定框架及其后续修订；
- 关于数据保护影响评估（Data Protection Impact Assessment 或“**DPIA**”）的，以及根据《第 2016/679 号欧盟法规》判定数据处理是否“可能构成高风险”的指南（第 248 工作小组的 01 修订版）；
- 国家反腐败局根据《举报人保护指令》第10条发布的指导方针，内容涉及保护举报欧盟法律违规行为的人员以及保护举报违反国家法规行为的人员—关于提交和管理外部举报的程序，已发布在国家反腐败局的官方网站上；
- 国家反腐败局关于外部举报管理及行使制裁权的条例（旨在落实《第 24/2023 号立法法令》），已发布于国家反腐败局官方网站；
- 欧洲议会和理事会 2019 年 10 月 23 日《第 2019/1937 号欧盟指令》，其与举报违反欧盟法律行为者的人员保护相关。

[6] 该法律的适用范围仅限于集团旗下在过去一年中已雇佣平均不超过 249 名签订无固定期限或固定期限劳动合同的雇员，由于根据《举报人保护指令》第24条第2款的规定，《24/2023号指令》所指的内部渠道设立义务自2023年12月17日起生效。

4.2 内部规定

- 《道德准则》；
- 前2001年6月8日第231号立法法令的组织与管理模型，和 TERNA S.p.A.及其部分受控公司；
- LG014 -《伦理委员会规章》；
- LG050 - Terna 集团旗下公司《道德准则》的实施
- LG018 - 信息安全政策战略方针；
- LG039 - Terna 公司的隐私政策；
- LG058 - 全球合规计划；
- LG059 - 反腐败指南；
- IO009SER - 电子文书登录管理服务；
- PL02 - Terna 集团综合管理体系政策；
- IO202SG - 根据 UNI ISO 37301:2021 标准开展合规活动管理

5. 术语定义与缩写

除了本指南之（或其附件）其他章节中所定义的术语和表述外，就本指南而言，下列术语和表述之含义如下所示。

- **系统管理员**：该主体可用 Whistle Editor 的所有功能，且与后者不同的是，其亦负责管理内部用户的权限。
- **其他主体**：本指南第 6.1.2 条中的主体，并且其是依据《24/2023号立法法令》第3条第5款界定。
- **审计** (或 **AU**)： Terna 审计部负责在收到举报后开展初步调查，并通过门户网站向伦理委员会通报调查结果。
- **CISO**：首席信息安全官。
- **《道德准则》**：一份记载积极原则和行为准则的文件，由 Terna 集团自愿采纳，并予以公开，以此具体体现集团之于其所接触的各主体所秉持的宗旨。
- **伦理委员会**：负责处理所接获的举报，并采取后续行动的公司内部机构。上述组成人员由 Terna S.p.A. 的首席执行官提名，其任命旨在体现多元化的视角，并在集团旗下各公司、企业职能及岗位之间保持平衡。
- **合规官** （或 **CO**）： 根据 LG058 号法律规定，在集团各海外公司中指定的负责人，其职责是在公司内部推动《全球合规计划》及/或相关国家附件中规定的《本地合规计划》与母公司指南的普及，并通过培训、信息传播以及建立专门的信息流机制，促进相关计划的有效实施。
- **工作背景**：指举报人于目前或过去，为 Terna 或本集团内其他收受此举报之公司所从事的工作或职业活动；无论此类活动的性质如何，举报人正是通过这些活动获取了违规信息，且在该背景下，若进行举报，其可能面临遭受报复的风险；
- **隐私法规**：此定义指现行关于个人数据保护的隐私法规，具体包括：2016年4月27日欧洲议会和理事会颁布的《第 2016/679 号欧盟法规》（关于在个人数据处理方面保护自然人以及此类数据的自由流通）， 意大利第196/2003号立法法令、2018年第101号立法法令，以及任何其他适用的个人数据保护法规，包括个人数据保护之监管人的各项措施。

- **公开披露**或**公开公布**：在《第 24/2023 号立法法令》规定的案件中，通过印刷媒体、电子媒体或其他能够覆盖大量人群的传播渠道，将违规信息公之于众。
- **ITD-ESP**：IT与数字化领域的“企业服务与平台”架构。
- **协助人**：指协助举报人进行举报的自然人，该自然人与举报人身处同一工作环境中，且根据第24/2023号立法法令的规定，其相关协助行为应予以保密。
- **举报管理人**或**管理人**：根据本指南中第 6.5 节规定，由公司指定的、负责管理举报事宜的人员，其遵循自主、公正和独立的原则。
- **违规行为的相关数据**： 有关违规行为的数据，包括合理怀疑，涉及已在或根据具体证据可能在以下组织内发生的违规行为：举报人或向司法或审计机关提出指控的人士，与其在工作环境中存在法律关系；以及为隐瞒此类违规行为的相关证据。明显毫无根据的消息、已完全为公众所知的信息，以及仅基于不可靠的传闻或谣言（即所谓的“道听途说”）所获得的信息，均不属于应可举报或可投诉的违规信息。
- **监督机构**或**OdV**：本公司根据《231/01指令》所设立、拥有独立主动权和监督权的机构，其负责监督运行、遵循《231模型》，及其相关更新事务。**主责人**：经正式授权并接受过培训的审计部员工，负责按照如第 6.5 节所述内容对举报进行核查。
- **PCE**：伦理委员会主席。
- **涉事人员**：指在内部或外部举报中，或在公开披露中被提及的自然人或法人，其被认定为违规行为的责任主体，或以任何形式涉入被举报事件或经公开披露的违规行为。
- **RU**：Terna 人力资源部。
- **信息门户**或**门户**：是为本集团旗下公司处理书面及口头违规举报研发专设，为一项*基于网络的*信息技术工具，可访问网址 https://whistleblowing.terna.it/ ，当中根据《举报人保护指令》为本集团各公司设立了专门的举报渠道。
- **举报联系人**或**联系人**：由相关受控公司指定的人员；当举报事项涉及该子公司时，则管理人将根据本指南第 6.5 节之规定使该人员参与处理。
- **文档库**： 指为信息门户上设立的每个内部渠道专门建立的*数据库*，其用于归档所有收到的举报，无论采用何种方式进行举报。
- **审计负责人**或“**RIA**”： Terna 的审计总监。
- **报复**：任何行为、作为或不作为，即使仅是企图或威胁，因举报、向司法或审计机关提出申诉或公开披露而实施，且直接或间接导致或可能导致举报人或提出申诉的人遭受不公正的损害（即无正当理由的损害）。尤其，根据《第 24/2023号立法法令》第 17 条第 4 款之规定以及国家反腐败局的指南，以下行为构成报复行为并纯属示例：
    - 解雇、停职或同等措施；
    - 降职或不予晋升；
    - 调岗、更换工作地点、降薪、调整工作时间；
    - 暂停培训或对培训活动设置任何限制；
    - 记过处分或负面推荐；
    - 采取纪律处分或其他处罚措施，包括罚款；
    - 胁迫、恐吓、骚扰或排挤；
    - 歧视或任何形式的不利待遇；
    - 未将固定期限劳动合同转为无固定期限劳动合同，而劳动者对该合同转换事宜具有合理预期；

- 不续签或提前终止固定期限劳动合同；
- 损害，包括对个人声誉的损害（特别是在社交媒体上），或经济或财务上的损失，包括经济机会的丧失和收入损失；
- 基于正式或非正式的行业或产业协议，将某人列入不当名单，其可能导致该当事人今后无法在该行业或产业中找到工作；
- 提前终止或解除商品或服务的供应合同；
- 吊销执照或许可；
- 要求接受精神或身体检查。
- 例如，以下行为也可能构成报复：要求以指定方式和在指定时间内达成无法实现的目标；蓄意给出负面绩效评估；无正当理由撤销工作任务；无正当理由不分配工作任务，同时将任务分配给他人；反复拒绝请求（例如休假、请假）； 无正当理由暂停资格证书、执照等。
- 此外，根据本指导方针，“报复”一词亦涵盖对举报行为的任何阻碍或阻碍企图。

- **反馈**：向举报人通报有关对举报事宜已采取或欲采取之后续措施的信息，此举亦符合《第24/2023号立法法令》的规定。
- **SE 或外国公司**：Terna 集团旗下的非意大利公司。
- **举报人**：指在 Terna 或集团内其他接收举报之公司的工作环境中，发现违规行为并提交相关信息举报的自然人。
- **被举报人**：指在举报事件中，被指认为违规行为责任人，或以任何形式涉及所举报违规行为的自然人或法人。
- **举报**：以书面或口头形式呈报违规信息之事件。
- **外部举报**：根据《第 24/2023 号立法法令》规定的情形，通过国家反腐败局设立的外部举报渠道提交的、关于违规行为信息的书面或口头报告。
- **内部举报**：通过 Terna 集团内设立的、针对举报接收方的内部举报渠道，以书面或口头形式提交的违规信息。
- **后续情况**：管理人为核实所举报事件是否属实而采取的行动、调查结果以及可能采取的措施。
- **纪律处分制度**：指企业内部现行的纪律处分制度，其在《231号模型》中有所阐述；对于各外国公司而言，则指各外国公司所采纳的《全球合规计划》中规定的纪律处分制度。公司会根据比例性和适当性原则，视相关措施是否适用于相关对象，以确定纪律措施和相关处分；在这当中，应考虑相关措施是否有效发挥吓阻作用和后续制裁作用，同时评估适用不同对象之资格、身份等因素。
- **无关的受控公司**：此类公司指根据《第 24/2023 号立法法令》第 4 条第 4 款规定，即员工人数少于 249 人，且总部位于意大利的 Terna 集团旗下公司；就本指导方针而言，亦包括海外公司。
- **相关受控公司**： 此处所指的公司系指根据《第24/2023号立法法令》第 4 条第 4 款规定，员工人数超过 249 人，且总部位于意大利的 Terna 集团旗下公司。
- **违规行为**：任何构成（或涉嫌构成）违反《道德准则》所确立原则的非法行为和/或行为（包括作为或不作为），以及违反内部规章制度的行为，该制度包括被举报公司的所有规定、程序、指导方针或操作说明，其中包括《231号模型》、反腐败指南、全球合规计划，以及违反可能导致欺诈或造成损害（包括潜在损害）的政策、公司规章的行为，这些行为是针对同事、股东及一般利益相关方，或构成损害公司利益及声誉的非法或有害行为，以及《举报人

保护指令》所规定的违规行为“*损害公共利益或公共行政机构及私营实体诚信的国内或欧盟法规规定*”；

- **举报事件编辑：** 由审计负责人在审计过程中识别出的对象，其经列入门户网站用户名单，用于将通过非门户渠道收到的举报信息录入举报门户。该编辑会更新门户网站各部分中的信息（包括免责声明、常见问题解答（FAQ）、数值列表、类型管理等…）。

6. 举报的条件、操作方式及相关保障措施

6.1 主体范围

根据《道德准则》的规定，Terna 集团旗下各公司均向举报人提供最高程度的保密和保护，确保那些出于善意、秉持对公司忠诚精神进行举报的人员免受报复，或对其职业地位产生负面影响，同时对实施报复行为的人员予以惩处。

而本指导方针根据《举报人保护指令》规定之保护机制，将相关主体合适地分为两类：

- “***举报人***;
- “***其他主体***”。

6.1.1 举报人

任何人都可以提交违规检举

至于《举报人保护指令》的具体规定及相关保障措施，凡是在 Terna 或举报事件所指涉的集团内其他公司之“*工作环境中*”任职的人员，均可作为以下身份提交举报：

- 本集团旗下某家公司的雇员；
- 在本集团旗下某家公司从事工作的自雇人士；
- 与那些存在专业合作关系的人员（例如：供应商）、自由职业者（例如：律师、会计师、公证人等），以及在集团旗下某家公司提供服务的顾问；
- 在本集团旗下某家公司工作的志愿者和实习生，无论是否领取报酬；
- 股东，即持有公共部门某主体股份的自然人，前提为该主体具有公司性质，例如：公部门控制公司、内部公司、合作社型公司等。此类人员包括：因作为公司股东而行使相关权利时，获悉违规行为举报事件的人员；以及在集团旗下任何一家公司中担任管理、领导、控制、监督或代表职务的人员，即使该等职务仅属事实状态的行使。

此外，符合以下条件的人员亦可进行举报：

- 如在与 Terna 集团的雇佣关系期间获取相关信息，且该雇佣关系现已终止，只要有关违规行为的信息是在雇佣关系终止前获取的，即可进行举报；
- 若劳动关系尚未建立，且有关违规行为的信息是在选拔过程中或合同签订前的其他协商阶段获取的，则应记录所获取的信息；
- 在本集团旗下某家公司于试用期间获取的信息。

6.1.2 其他主体

根据《举报人保护指令》的举报相关规定，在“其他应受保护主体”类别中则涵盖：

- 协助人；
- 与举报人共处于同个工作环境，且与其存在稳定情感关系或四亲等以内亲属关系的人员；

- 举报人的同事，且与举报人在同一工作环境中工作，并与该人保持着日常且密切的往来[7]；
- 举报人所属的机构或其供职的机构，以及在同一工作环境中运营的机构。

6.2 举报内容

所有违规行为均可举报。具体而言，根据《举报人保护指令》的规定，凡涉及可能损害公共利益或公共行政机构及私营实体诚信的所有行为、作为或不作为的违规举报，均被视为“重大举报”（即：允许采取下文第 6.3 节中所述的保护措施）。

具体而言，可以分为三类[8]：

1. ***违反国家及欧洲法规的行为，具体涉及以下领域的违法行为***：公共采购；金融服务、产品及市场，以及洗钱防治和反恐怖主义融资；产品安全与合规；交通安全； 环境保护；辐射防护与核安全；食品和饲料安全以及动物健康与福利；公卫保健；消费者保护；隐私保护与个人数据保护；网络与信息系统安全；
2. ***违反欧盟规定***，其具体表现为：i) 损害欧盟财政利益的行为或不作为；ii) 涉及内部市场的行为或不作为[9]；iii) 使欧盟在上述领域所颁布之法规宗旨或目的落空的行为或表现；iv) 违反《刑法典》第二卷第一章第一编第 I-bis章所规定的欧盟限制性措施，以及 1998 年 7 月 25 日第 286 号立法令第 12 条第 1-bis 项《*实施欧洲议会和理事会 2024 年 4 月 24 日第 2024/1226 号欧盟指令，其涉及界定违反欧盟限制性措施的犯罪及处罚，并修订第 2018/1673 号欧盟指令*》；(v) 违反《第 2024/1689 号欧盟法规》（即《人工智能法案》）[10]。
3. ***违反国家规定***，其包括：i) 行政、会计、民事或刑事的违法行为；ii) 根据《231/2001号立法法令》或《231号模型》规定构成重大违法之行为。此类违法行为不得隶属于前文第 1 点和第 2 点中所述的范畴。

6.2.1 举报的最低要求

举报必须包含以下所列的基本要素。

- **检举人：**检举内容应包含检举人的身份信息[11]。举报必须出于善意，且不得以匿名形式进行。
- **内容：**对举报所涉事实的清晰描述，包括发生或未发生各项事件的时间和地点，以及举报人获悉这些事件的途径。
- **举报内容及相关人员：**涉嫌实施违规行为的人员及相关人员的身份信息，或任何有助于明确识别其身份的要素（如职务/公司职责）。
- **集团所属公司：**举报应清晰指明所检举事项涉及集团内的特定公司，尤其是在多个集团公司使用相同检举渠道的情况下。

---

[7] *“以工作同事为例，立法者规定，此处所指的同事是指在举报的时间点处于与举报人共同工作（因此不包括前同事）的期间，且与举报人存在日常且持续工作关系的人员。因此，该规定所指的关系并非仅限于零星、偶发、片段或例外的情况，而是指当前存在、持续较长时间，且具有一定连续性的关系，其足以形成一种‘共同性’或友谊的关系。”*， 摘自 2023 年 7 月 12 日国家反腐败局第 311 号决议批准的 ANAC 第 22 页。

[8]根据《举报人保护指令》，针对上述各类违规行为，需根据以下情况加以区分：(i) 该实体为公共服务特许经营者（或从事此类活动的实体），在此情况下，所有类别的违规行为均适用；(ii) 该实体拥有 50 名以上员工,且已采用《231号模型》；在此情况下，违反欧洲法规及构成重大违法行为的类别均适用《第231/2001号立法法令》的规定或《231号模型》的违规行为。（Iii）员工人数少于 50 人但已采用《231号模型》，在此情况下，可根据《第231/2001号立法法令》的规定或《231号模型》的违规行为举报相关违规行为。

[9]该范畴涵盖所有违反欧盟竞争法和国家援助法规的行为，以及与违反公司税法规的行为相关的内部市场违规行为，或旨在获取税务优惠、从而使适用公司税法规之宗旨或目的落空的机制。

[10]根据《第 2024/1689 号欧盟法规》第 113 条， 第 87 条，该条规定将《第 2019/1937 号欧盟指令》适用于本条例违规行为的举报，以及对举报人的保护，并自 2026 年 8 月 2 日起生效

[11]系指以专门且保密的方式进行公司与举报人之间的沟通，并根据举报事件的后续情形发送反馈的个人数据

举报内容一旦符合受理条件、无明显缺乏依据、情况详实，且包含有助于查明和核实违规行为的要素，即将予以审查。根据具体案件情况，以及是否存在足以支持后续调查工作的相关证据，伦理委员会保留对举报进行评估的权利。

此外，举报人亦可提供以下补充信息：

- 可能知情并能提供举报事件相关情况之**其他人员**的信息；
- 发送可能实证该事件情形的**相关文件**；
- 有助于采集被举报事件之证据的**其他信息**。

举报人亦可提供相关文件，以便更详细地说明举报情况。

最后，为便于准确识别本指南第 6.1.2 节以及《第 24/2023 号立法法令》第 3 条所界定的其他涉事人员，并确保对其提供保密保护，以及下文第 6.3 节中所列并赋予其的相关保护，举报人宜明确指出这类主体的存在，并具体说明其是否具备相关条件。

6.2.2 举报内容的限制

以下情况不属于《举报人保护指令》的适用范围（因而不得适用下文中第 6.3 节所述的保护措施）：

- 举报人或向司法或审计机关提出举报者所提出之个人性质的主张、异议或请求，如：其仅关于自身个别劳动观秀，或关于其上级层级之间的劳动关系 — 在此情况下不属于本制度的涵盖范围[12]；
- 以下内容已由欧盟或国家层面的法规强制性规范：关于服务、产品和金融市场，洗钱防治、反恐怖主义融资，运输安全和环境保护等领域的违规举报或 作为欧盟法规[13]实施依据的国家法规，以及涉及国家安全、国防或国家安全相关采购方面的违规举报，除非此类方面属于欧盟相关衍生法的管辖范围；
- 匿名举报，由于本指南旨在保护举报人免受报复风险。

关于匿名举报，请注意：如果因匿名举报导致举报人身份暴露，则第 6.3 节中所述的保护措施可予以适用。为向举报人提供最高级别的保密保护，即使在普通举报的情况下，这类举报亦不得以匿名形式提交。

此外，请注意，根据《举报人保护指令》第 1 条第 3 款之规定，涉及以下事项的举报不属于该《举报人保护指令》及本指南中所规定之保护措施的适用范围：a）机密信息；b）律师和医生的职业保密义务；c）司法机关决议的保密性。

检举内容不得带有侮辱性言辞，也不得包含针对被检举人个人或职业荣誉及尊严的侮辱、攻击性评价。

在任何情况下，严禁：

- 出于纯粹诽谤或诬告目的提交检举；

[12] *“因此，以下范例情形均不包括：涉及劳动纠纷及诉前阶段的举报、同事间的歧视、举报人与另一名员工或具上下级关系者的人际冲突，以及在不损害公共利益或公共行政机构或私营实体诚信的情况下，针对个人劳动关系中数据处理行为的举报”*，此为国家反腐败局于 2023 年 7 月 12 日通过第 311 号决议批准之《ANAC指南》第 28 页的内容。

[13]其明载于《第 2019/193725 号欧盟指令》附件的第二部分。

“例如：欧洲议会和理事会《第 596/2014 号欧盟法规》以及欧盟委员会根据该条例通过的《第 2015/2392 号欧盟执行指令》中，关于市场滥用行为的举报程序，其中已包含关于保护举报人的详细规定”，此为国家反腐败局于 2023 年 7 月 12 日通过第 311 号决议批准的《ANAC指南》第 28 页的内容。

- 所提交的举报事件仅涉及个人隐私方面，且与被举报人的公司/职业活动并无任何直接或间接关联；
- 所提交的举报事件涉及与举报人个人利益相关的异议、权利主张或诉求；
- 所提交的举报事件涉及被举报人的性取向、宗教信仰、政治立场或族裔背景的歧视性举报；
- 仅以损害被举报人利益为目的而提交检举。

对于提交此类检举的集团员工，集团方面可能会对其采取纪律处分措施。同时，若检举人出于恶意或因重大过失提交了经查证并无事实依据的举报，同样可能面临处罚。

6.3 举报人的保护

举报制度在实施过程中可能会遭受一定程度的猜忌，由于潜在举报人对于进行举报感到担心，顾虑自己无法在工作中得到充分保护，从而面临报复或歧视的风险。Terna 及其集团旗下公司将根据前文中第 2 节之规定，对举报人的隐私加以保障，并保护其免受报复性质的举措。

特别依据《举报人保护指令》，通过专门设立的内部举报渠道，旨在确保在接收举报与处理阶段，检举人身份的保密措施得以切实落实。

关于这一点，有必要将“保密性”与“匿名性”的概念区分开来，由于前者以知晓举报人的身份为前提，这是确保提供充分保护所必需的。而事实上，匿名性则可能会妨碍举报真实性的核实工作。

此外，亦已采取了适当措施，以保障举报人免受与举报相关任何形式的报复、歧视或处罚，同时，考虑到《举报人保护指令》规定的条件和要求，在本指南第 6.1.2 节和《第 24/2023 号立法法令》第 3 条所界定，为保护其他涉事人员而采取此类措施，并且应在不损害法律义务以及保障公司或个人的相关权利的前提下。

此类保障措施一方面在于禁止公司对举报行为进行报复，另一方面在于规定任何违反该禁令而实施的报复行为均属无效[14]。

为享有《举报人保护指令》所规定的保护制度，必须满足以下条件：

- 举报人是否属于《第 24/2023 号立法法令》第 3 条所列人员（如前文第 6.1.1 节中所述）；
- 所举报的违规信息应符合《第 24/2023 号立法法令》所规定的客观范围，该范围已在前文第 6.2 节中列明；
- 举报人在向司法或审计机关进行举报或投诉，或进行公开披露时，有“充分理由”相信相关信息属实i[15];
- 举报事件应按照内部或外部渠道规定的程序进行（该渠道系根据本指南设立，其载于下文第 6.4 节，其由国家反腐败局管理并载于下文第 6.9 节)或依据《举报人保护指令》第 15 条关于公开披露之规定处理（其载于后续第 6.10 节）。6.10).

违反本指南第 6.1.2 节所指、并由《第 24/2023 号立法法令》第 3 条第 5 款所确立，个别为举报人和其他相关主体所实施的保护措施，即构成适用《纪律处分制度》所规定处罚措施的理由。具体而言，根据《第 24/2023 号立法法令》的规定，以下行为将受到纪律处分的处罚：

- 违反《第 24/2023 号立法法令》第 17 条的报复性行为，即：因举报而实施的、可能直接或间接对举报人造成不公正损害的行为、作为或不作为，即使仅是具有意图或威胁；
- 可能妨碍举报的行为；

[14]根据《举报人保护指令》第 19 条的规定，如有任何报复行为，可向国家反腐败局通报，以便其进行相关调查。

[15]基于可提交的具体事实和可获取的信息，而非单纯的推测。

- 违反关于保密义务的举报人保护措施。

在以下情况中，举报人的匿名性无法得到保障：

- 举报人已明确同意披露其身份；
- 一审判决已认定举报人因诽谤或诋毁等罪行，或因通过举报实施的任何其他犯罪行为，而需承担刑事和/或民事责任；
- 如果司法机关因举报而启动调查（刑事、税务或行政调查）或监管机构开展检查，并要求披露举报人的身份，则依据法律不予以承认匿名权。

6.3.1 举报人保护的限制及被举报人的保护

《举报人保护指令》中规定举报人无权获得保护的几类情况：

- 如果经查实（包括一审判决），举报人因诽谤或诬告罪负有刑事责任，或者在向司法或审计机关举报时实施了此类犯罪；
- 因同一事由而产生基于故意或重大过失的民事责任时。

对于上述两种情况，举报人或投诉人均将受到纪律处分。

此外，对于以下情况均不排除承担刑事、民事或行政责任（《第24/2023号立法法令》第 20 条第 4 款）：所有与举报、向司法或会计机关举报、公开披露无关，或并非揭露违规行为所必需的行为、作为或不作为。

违反《第 24/2023 号立法法令》关于举报违法行为的规定，将构成适用《纪律处分制度》所规定处罚措施的依据。特别是，在已查实举报人因诽谤或诬告而应承担民事责任（无论出于故意或重大过失），其包括一审判决的情况下，亦得对其采取纪律处分；然而，但若该举报人此前已因诽谤或诬告罪行（或因向司法或审计机关举报而实施的同类罪行）被判处有罪刑罚（包括一审判决），则不在此限。其不影响国家反腐败局依据前述根据《举报人保护指令》第 21 条规定另行科处行政处罚。

关于被举报人的保护，在根据本指南设立的举报渠道的管理过程中，亦将按照《举报人保护指令》的规定确保被举报人身份的保密性，旨在防止个人信息的不当传播，无论是向外界或所属公司内部遭受泄露，直至已启动之举报程序结束为止。

被举报人无权随时获知与之相关的举报进展情形。在对举报进行核查和分析后，如出现以下情况，即将被举报的涉案人员将获悉与之相关的举报消息：(i) 因对该举报进行核查和分析而对其启动了程序，且 (ii) 该程序全部或部分基于该举报。在这种情况下，得经请求听取被举报人的说明陈述，亦可通过书面程序，即收集书面意见和文件的方式进行听证。

最后，如果其指控或异议之全部或部分以该举报为基础，且知晓举报人的身份对被告的辩护至关重要时，则该举报仅在举报人明确同意披露其身份的情况下，方可用于纪律处分程序（参见第 6.4.1 节）。

6.3.2 禁止报复

报复行为一律严格禁止，若对举报人或向司法或审计机关举报违规行为的人员（其知悉《举报人保护指令》的规定）采取任何报复措施，均将受到处罚。

公司将保护举报人以及《第 24/2023 号立法法令》第 3 条所指的其他主体（详见前文第 6.1.2 节）免于遭受任何形式的报复，通过确立相关规则，以防止或消除为惩罚举报人披露信息的行为或措施所产生的影响，并防止这类行为或举动妨碍举报行为。

依据现行法规所规定之本项禁令不仅涵盖因举报而实施的、对举报人造成不公正损害的行为、作为或不作为，亦包括实施报复的企图或威胁。所造成的损害也可能是通过间接方式。

此外，就举报人而言，证明此类行为或举动系基于与举报、公开披露或投诉无关的理由的举证责任，应由实施该行为的公司承担；因此，该公司有义务证明其采取的措施是基于与举报无关的理由。
至于其他主体，则由其本身自行承担举证责任，证明其行为、作为或不作为系因举报而产生，因此具有报复性质。
为保障这一保护措施，现行法规规定，举报人可向国家反腐败局通报认为自身曾遭受的报复性措施。

6.4 内部举报渠道

已确定以下内部渠道用于进行举报（“**内部举报渠道**”），这些渠道能够确保举报人的身份保密性及信息安全性，并设有仅允许经特别授予访问权之人员的规定。具体而言，有以下渠道可供使用：

- **信息门户网站**，确保用户可有效访问Terna 集团公司专为意图提交举报设的所设立的渠道。该信息门户通过先进的通信加密系统，确保举报人身份数据的安全与保护，并保障相关人员及举报中受提及人员的隐私性，同时确保举报内容及相关文件的保密性遵循《举报人保护指令》的规定。
- **直接举报方式**，旨在允许通过事先约定的面谈进行举报，且此类会面仅限于与经特别授权的主体，其专为接收举报而安排进行。
- **普通邮件渠道**，其允许通过普通邮件提交举报，并在处理举报的过程中，在举报人提供的信息允许的情况下，按照《举报人保护指令》的规定对该信息进行处理，以便与举报人进行沟通。

已建立的内部渠道应被视为优先渠道。
根据相关法规的规定，该项原则一方面旨在“在组织内部倡导良好的沟通文化与企业社会责任”，另一方面，则在于让举报人藉由揭露违法行为、不作为或不当行为，为其所在组织的改善做出重要贡献[16]。
按照下文第 6.5 节的规定，内部渠道的管理应交由正式界定的主体执行。
如果举报被错误地提交给无权处理的对象（非正式指定的对象）或本集团内其他公司（而非相关公司）的渠道，且举报人明确表示希望接受《举报人保护指令》规定的举报保护，或者可从明确指向《举报人保护指令》的行为中清晰推断出来其具有该等意愿，在此情况下，则须在收到举报后 7 日内（通过审计负责人）将举报转交管理人，且不得保留副本，同时在可能的情况下立即通知举报人已转交举报的事宜。

6.4.1 信息门户

如需提交举报，举报人需登录门户网站，在该网站上可找到拟向本集团旗下公司提交举报的专用渠道。门户网站的访问链接如下：https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione。

公司的渠道

该门户网站根据《举报人保护指令》第 4 条第 4 款的规定，本集团内相关公司各自专用的举报渠道，以及 Terna 集团其余公司共用的举报渠道。具体而言，该门户网站内设有下列的举报渠道：

- Terna S.p.A.；
- Terna Rete Italia S.p.A.；
- Tamini Trasformatori S.r.l.；
- Altenia S.r.l.

[16]根据《第 1937/2019号欧盟指令》第 47 条的规定。

- Terna 集团的其他公司[17]/机构。

举报方式

举报人通过访问所选集团公司的渠道 （例如：Terna S.p.A. 的渠道、Terna Rete Italia S.p.A. 的渠道或其他渠道），既可以通过书面形式提交举报（其以手动编写内容），亦可通过口头形式提交，应在明确同意录音的前提下发送语音消息。检举人在发送前可以重新收听、保存或删除录音；提交后，针对口头检举，系统会对声音参数进行处理，使其人声特征无法被识别（见右侧图片）

举报必须出于善意，且不得以匿名形式进行。

如需进行举报，举报人在收到相关数据处理的说明后，需在指定字段中填写其个人信息。该注册流程要求提供个人电子邮箱地址和电话号码，以便接收后续登录所需的双重安全验证码，并为公司与举报人之间提供专属且保密的沟通渠道，以便就相关事宜做出进一步澄清，并就举报的后续处理情况发送相关*反馈*。

举报人的身份信息将存储于*信息技术工具*中，并通过加密系统进行保护（该加密机制可将举报信息处理为部分匿名化，并非完全匿名）。在调查所需且确有必要的情况下，可在保持数据保密的前提下对其进行解密；仅在《举报人保护指令》规定的情况下，且经举报人明确同意后，方可向负责接收或处理该举报的人员以外的其他人士披露相关内容（即，当仅基于该举报的纪律处分程序中，为使涉案人员能够进行辩护，且了解举报人的身份对涉案人员的辩护不可或缺时）。在这种情况下，在提出解密请求之前，审计负责人将通过同一平台向举报人说明理由，并努力征得其同意。

经伦理委员会主席（“**PCE**”）通过门户网站将已提交的、附有理由的解密请求交给 Terna[18] 的首席信息安全官（“**CISO**”），后者负责协助解密举报人的身份数据，但无权访问举报内容。届时，若根据《举报人保护指令》的规定认为有其必要，将会向首席信息安全官通报已获得举报人的同意。如果伦理委员会主席无法参与，则由审计负责人在知晓伦理委员会主席的情况下发起解密请求。

门户网站的管理

在处理举报事宜时，伦理委员会主席除了会履行审计部为调查目的而被明确赋予的职责外，亦负责监督和管理该门户网站（但因利益冲突或基于分配给其他类别用户的特定任务而明确排除的情况除外，例如：修改审查调查证据的伦理委员会会议记录）。

在门户网站的管理工作中，审计负责人负责将通过门户网站以外之渠道所收到的举报信息上传至门户网站，并通过门户网站对收到的举报进行分配；若审计负责人未直接处理，则授权**举报事件编辑**代为处理。

为开展门户网站的更新和管理工作，审计负责人可委托**门户网站编辑**负责相关事务，该人员由审计负责人在审计过程中选定，且须为门户网站的登记列档用户。“门户网站编辑”的职责并不具备查看“举报”信息的权限。

通过该门户网站，审计负责人（如存在与审计负责人有利益冲突的情况下，则交由伦理委员会主席）会在审计部门范围内，从已登记为门户网站用户的对象中，按照下文第 6.5 节中所述的方式，主责人作为经正式授权并接受过相关培训的人员，负责开展初步调查工作。在上述活动中，主责人负责将初步调查文件上传至相关渠道的文档库，并通过门户网站与举报人进行沟通，向其回复*反馈意见*。

[17]根据《第 24/2023 号立法法令》第 4 条第 4 款的规定，此类公司可以共享内部举报渠道及其管理。

[18]若涉及重要受控公司的举报，该请求也将抄送给根据第 6.5 节中所述，为该特定举报指定的联系人，供其知悉。

主责人在获得审计负责人（若存在与审计负责人有利益冲突时，则交由伦理委员会主席）的正式授权后，应在满足《举报人保护指令》规定条件时和/或 相关举报已超过其保存期限时，负责删除举报信息[19]；并应视情况必要，事先通知重要受控公司的联系人。
对门户网站的访问记录将被追踪，文件和报告的替换及删除操作也将被记录。
平台的技术功能管理及更新工作由 Terna 旗下*企业服务与平台*（“**ITD-ESP**”）部门指派的门户系统管理员负责，该管理员将根据审计反馈进行相关操作：该管理员不得查看或管理任何举报事件，其对平台所有功能的最高权限仅限于纯粹技术支持的职责。

6.4.2 直接面谈

除了上述举报渠道，检举人可以申请与审计负责人进行直接面谈，亲自说明举报事项。上述面谈事宜应由举报人通过门户网站（https://whistleblowing.terna.it/Segnalazioni/InvioSegnalazione）预约安排，或发送至指定邮箱 whistleblowing@terna.it，同时注明举报涉及的 Terna 集团旗下公司名称。该电子邮箱仅用于发送面谈申请，不得用于提交书面形式的举报事件。

6.4.3 普通邮件

使用信息化平台是保障检举信息保密性的最佳方式。任何举报（也可通过普通邮寄方式提交）须寄至本集团对应的相关公司，收件人为 TERNA S.p.A.审计负责人，地址：Viale Egidio Galbani, 70 – 00156 罗马，并使用以下标注：“*举报信，机密——请勿拆封*”且如举报内容详实，以便对事实进行评估，并依据《举报人保护指令》的规定，如举报基于准确且一致的事实依据，则将予以受理；虽然就与举报人的沟通管理及*反馈*层面来说，此类举报将不被视为《举报人保护指令》意义上的正式举报。若未包含上述明确表述，该举报将无法根据《24/2023 号立法法令》的规定予以受理和处置。一切必要措施将被采取，以确保包括通过此方式提交的举报信息内容和数据资料的机密性。

6.5 举报管理

6.5.1 权责主体

根据《24/2023 号立法法令》、《道德准则》以及有关个人数据保护的法规，已正式确定负责处理举报事宜的权责主体。
负责处理举报的公司权责机构包括：

- 审计负责人，负责接收和调查举报；
- 伦理委员会将针对该举报的受理资格、内容及初步调查进行分析，并对此进行妥善跟进。

伦理委员会的成员由 Terna 的首席执行官任命。
举报事宜由审计负责人与伦理委员会成员共同处理，并通过预先设定的流程以透明的方式进行。
在举报管理方面，上述相关的公司部门应在各自职责范围内确保：

- 对于根据《举报人保护指令》提交的举报，须在收到之日起七日内向举报人发出举报收讫通知；
- 如有可能，亦根据举报人选择的渠道与其保持沟通，并在必要时要求其提供进一步的信息和补充文件；

[19]根据《24/2023号立法法令》第 14 条第 1 款，举报及相关文件将按各内部渠道分别保存在文档库中，保存期限为该举报所需的处理时间，但自举报程序最终结果通知之日起不得超过五年，除非因司法程序、监管机构的要求或启动争讼而需进一步保存；同理，根据第 6.8 节下的规定，对于通过门户网站以外渠道收到的举报，其纸质文件亦按此方式处理。至于涉及《24/2023 号立法法令》未涵盖个案情形的举报，数据将始终存储在内部的文档库中，存储时长仅限于实现收集目的所必需的期限，且符合保护相关人员权利的规定，并遵守法律规定的时效期限。

- 认真跟进接获的举报；
- 应在收到举报确认通知之日起三个月内对举报作出答复；若未收到该通知，则应在提交举报后七天期限届满之日起三个月内作出答复。

Terna 集团旗下各公司的举报管理会依据与 Terna 签订之集团内部的合适协议进行，并规定了相关措施以确保重要受控公司的参与。对此，根据本节所述，此类情况下亦应由审计负责人参与，其职责是确保遵守关于接收、分析和核查所收举报的法规要求，且伦理委员会的核心作用以及各公司对所收举报进行单独收集、处理和管理的方式不受影响、保持不变。然而，如果举报事件是针对相关受控公司的渠道且涉及该子公司，审计负责人在初步调查阶段须邀请一名联系人（至少两名被提名者中的一名）参与，该联系人由举报接收方的相关受控公司指派，以确保举报处理工作与该公司本身保持密切联系。相关联系人可查阅所有调查证据，并将受邀参加伦理委员会会议：该委员会负责评估调查结果，并在综合考虑联系人意见的基础上，对举报进行后续处理。

负责处理举报事宜的人员，未经举报人明确同意，不得向任何未正式参与调查工作的人员透露举报人的身份，或任何可能推断出其身份的其他信息。

负责处理该举报的相关人员将通过审计负责人[20].获悉该举报事件的存在。举报将显示给必须参与处理该特定举报的相关人员（主责人、伦理委员会成员，包括委员会秘书），具体依据各渠道的个资剖析以及审计负责人所做的分配指派来决定。

- 若通过门户网站进行举报，审计负责人[21] 将收到由门户网站生成的警报通知，该通知将以电子邮件形式发送至其邮箱。若举报对象为无涉及利益冲突的受控公司，审计负责人将向该子公司的联系人发送相同的警报[22]。
- 如果举报是通过直接面谈进行，则必须至少收到两名相关人员的举报。审计负责人在审计部另一名成员的陪同下，根据第 6.4.2 节的规定，在商定面谈安排后接受面谈请求。协助举报人将举报信息录入相关集团公司的文档库，并启动本节所述的核查程序。
- 如果举报是通过普通邮件提交的，则将由审计负责人根据相关内部规定以及本指南第 6.4.3 节之规定予以受理。审计负责人在核查信封内容后，将（直接或通过举报事件编辑）将举报信息录入举报接收方的公司文档库，并启动本节所述的核查流程。

6.5.2 管理阶段与初步调查工作

在通过第 6.4 节所述的内部渠道之一收到举报后对该举报进行初步评估，以确定：

（i）该事项是否涉及违规行为；

（ii）是否具备重大举报的客观和主观要件。

审计负责人将根据举报内容，确定对举报进行深入调查的方式，并评估最合适的人选，以确定应参与调查的相关人员。具体而言，审计负责人（直接或通过门户网站编辑）将审核流程的管理工作委托给其机构内一名经过适当授权和培训的员工（即：“**主责人**”。）此外，如调查工作需要，应评估是否需就举报事项涉及其他部门（例如：欺诈管理、数据保护与隐私等），同时确保举报内容的保密性，并仅向其提供开展工作所需的数据[23]。在涉及其他公司部门时，将遵循数据最小化原则，仅

[20]如在与审计负责人存在潜在利益冲突的情况下，该举报将直接提交给伦理委员会主席接管。

[21]Terna 已指定审计负责人为接收举报的负责主体，而伦理委员会的核心作用不受影响。作出这一选择的原因在于该职位的组织定位：由于该职位不具备业务决策权，并且直接向董事会主席汇报，因此其便是能够确保在处理举报相关事务时保持最大独立性的角色。

[22]该项消息将不包含任何与举报人身份和/或举报内容相关的信息。本警报旨在确保相关受控公司知悉已收到的举报，并监控已收到的举报与已审查的举报之间的对应关系。

[23]如果举报人声明该举报涉及审计负责人（在门户网站上勾选相应选项），则信息系统将把该举报发送给伦理委员会主席，而主席将根据本指南关于举报处理

限于为完成所分配的调查工作所必需的信息。为了确保伦理委员会能够及时获取履行其职责所需的所有调查文件，研究机构负责人（审计负责人）亦将授权伦理委员会成员（及委员会秘书）查阅该特定举报信息，但排除任何可能涉及该举报事件的人员。
相关联系人（若该举报涉及某家相关受控公司）可查阅与该特定举报事件相关的所有调查证据。
审计负责人经主责人任命后，将启动初步调查工作，以识别、分析和评估能够证实所举报事实之真实性和重要性的相关要素[24]。相关结果应载于主责人编制、经审计负责人批准的初步报告（Report）中。在涉及“相关受控公司举报”的情况下，该报告（包括最终报告及任何补充报告）将与指定的联系人共享。

6.5.3 伦理委员会的作用

审计负责人将最终报告提交给伦理委员会，旨在：

- 就该举报的后续处理作出决议，包括在认为必要时补充调查；
- 确认该案的撤销，如果其由审计负责人提议。

审计负责人应向伦理委员会成员通报情况；若发生第 6.6 节所述情形，则由伦理委员会主席负责通报，并通过门户网站对每条收到的举报进行处理。
伦理委员会的运作方式由专门的《伦理委员会规章》予以规范[25]。
审计负责人作为 Terna 审计部的负责人（该部门负责开展初步调查），在未涉及该举报的情况下，可派代表（最好由负责该举报的主责人担任）参加伦理委员会的会议。
只有在管理活动的结果出来后，管理人方会通过联系人，向受控的非相关公司及相关子公司之最高管理层或相关职能部门通报情况，以便采取相应措施。事实上，管理人无权对个人责任以及由此可能采取的后续措施或程序进行任何评估。

6.5.4 关于违反《231号模型》的举报及向监督机构的报告

关于涉及私营部门且不涉及公共服务特许权的举报，根据《231/2001立法法令》所指法规以及《231号模型》的相关违规行为，仅可通过内部举报渠道进行举报。在遵守《举报人保护指令》规定的保密义务及适用公司程序的前提下，管理人（通过审计负责人）应及时将专门的接收通知发送给相关公司的监督机构的电子邮件地址，以及该公司所指定的监督机构技术秘书处；该通知系指关于任何涉及《231号模型》中的违规或可能违规的行为，及/或构成《231/2001立法法令》所列前提之不法行为相关内容的举报。在初步调查出来后，经伦理委员会评估，调查负责人应及时向监督机构发送一份通知，在遵守保密原则的前提下，通报以下内容：i) 已开展的初步调查工作，ii) 相关调查结果，以及 iii) 伦理委员会作出的决定。

的规定，代行审计负责人的职责

[24]显然与处理特定报告无关的数据不会被收集；若因意外被收集，则会立即予以删除，以此贯彻《24/2023 立法法令》第 13 条第 2 款规定的最小化原则，应对其作严格解释，即在该规定与所报告事项显然毫无关联的情况下，且不影响有关文件保存的行业规定。

[25] 参见 LG014《伦理委员会规章》。

若监督委员会误收举报，应在收到后7天内（通过审计负责人）将举报转交管理人，且不保留副本；同时，在可行的情况下，应立即通知举报人已转交的相关情况。

6.6 潜在利益冲突的管理

若审计负责人涉及该举报，则该举报将由伦理委员会主席负责处理，具体程序依照前文第 6.4.1 条的规定执行。

将根据各渠道的个资剖析和审计负责人的分配情况，向管理人展示举报内容。如果伦理委员会的某位成员涉及某项举报，该成员则将不会收到任何关于其涉及的举报的通知，也不会参与伦理委员会的相关活动（其根据《伦理委员会规章》[26]的规定）。

此外，关于涉及相关受控公司的举报处理，各子公司应按照前文第 6.5 节的规定，至少指定两名联系人：上述任务在审计负责人收到举报之前即已确定，以确保该工作能与收到报告的集团内公司保持密切联系。审计负责人在收到举报后，须从指定的联系人中选定一人。若某位联系人与该举报事件存在潜在利益冲突，审计负责人应从其他被提名人中另行选定一人，同时需注意：涉事联系人可查阅所有调查证据，并将受邀参加伦理委员会会议，其评估调查结果以及就举报事项采取后续行动。

6.7 个人数据的处理

在举报程序中收集的个人数据的处理，完全遵守《隐私法规》，并符合《24/2023 立法法令》的规定。在兼顾被举报人权利与举报人身份保密权之间取得合理平衡的同时，实施本指南中规定的技术和组织措施，以确保个人数据的安全，同时符合现行法规的要求。此类措施包括（但不限于）：访问权限的分离、身份识别数据的加密、对系统访问及操作的记录，以及针对相关人员的具体授权和培训程序。在举报系统框架内进行的个人数据处理，其法律依据在于履行数据控制者所承担的法律义务，其根据《第 2016/679 号欧盟法规》第 6 条第 1 节 c 项之规定，并依照《第 24/2023 立法法令》之要求。在举报管理过程中，可能会对《通用数据保护条例》（GDPR）第 9 条所指的特殊类别个人数据，以及《通用数据保护条例》（GDPR）第 10 条所指的刑事定罪和犯罪相关数据进行处理，但此类处理仅限于为查明举报事实所必需的范围，且须遵守现行法规规定的保障措施。但需说明的是，举报人或被举报人（根据《隐私法规》定义的“相关方”）就其在举报流程中被处理之个人数据所行使的权利，可能会受到限制[27]，旨在确保他人权利和自由的保护，并明确指出在任何情况下均不得允许被举报人利用其权利获取举报人的身份信息[28]。相关方行使权利的具体操作方式，由相关内部个人数据保护规定，以及向相关主体提供的隐私声明予以规范。

因此，举报管理系统在架构设计上旨在保障相关人员的权利和自由，并明确界定了与数据处理相关的职责分工及相应的背景文件材料。

特别是，在集团内部，根据《24/2023立法法令》的规定，相关受控公司[29],将作为独立的数据控制者处理其内部举报渠道的数据。对于 Terna 集团[30]，的其他公司，可使用由各公司作为数据共同控制者

[26]参见 LG014《伦理委员会规章》。

[27]根据《通用数据保护条例》第 23 条和《第 196/2003 立法法令》第 2-undecies 条 。

[28]根据《第 196/2003 立法法令》第 2-undecies 条的规定，相关方将不可行使权利，若行使，相关权利可能对受保护的利益造成实际且具体的损害（例如：开展辩护调查、在司法程序中行使权利、举报违法行为的员工身份保密等）。因此，数据控制者可在任何情况下，通过向相关当事人及时发出附有理由说明的通知，推迟、限制或拒绝行使上述权利。

[29]截至本指南发布之日：Terna S.p.A.、Terna Rete Italia S.p.A. 和 Tamini Trasformatori S.r.l.

[30]此处所指的公司系 Terna 集团旗下根据《举报人保护指令》第 4 条第 4 款规定，员工人数少于 249 人的公司。

共同管理的共享举报渠道，根据《通用数据保护条例》（GDPR）第 26 条，基于一份具体的共同控制协议，其当中规定了各方在遵守 GDPR 义务方面的责任，特别是关于行使数据主体权利，以及根据 GDPR 第 13 条和第 14 条履行信息通报职能的责任。根据《通用数据保护条例》（GDPR）第 28 条的规定，负责支持信息技术门户及其相关技术基础设施管理的供应商被指定为数据处理者，相关安排基于具体合同协议，该协议对处理指令、安全措施及处理范围作了明确规定。

因此，各公司作为“独立数据控制者”和“共同数据控制者”，特此提供相应的隐私声明，其中载明了与举报程序相关的数据处理目的、期限及方式。

根据《通用数据保护条例》（GDPR）第 29 条和第 32 条以及第《196/2003立法法令》第 2-quaterdecies 条明确授权处理该类数据，因此，负责接收和处理举报的相关主体，亦因而成为特定指示的接收对象。

此外，根据《24/2023立法法令》的相关规定，通过内部渠道接收和管理举报的系统是基于数据保护影响评估（DIPIA）制定的，该评估系统化地梳理了数据处理的范围及相关层面的风险概况，并明确旨在降低已识别风险的技术和组织措施。

6.8 举报的归档与保存

如果举报是通过第 6.4.1 节所述的内部电子渠道提交的，则该平台即作为官方文档库，用于举报事件的存档，同时保存与其相关的所有文件。

如果举报是通过普通邮件或当面提交的方式进行的，则由审计负责人负责将报告上传至门户网站，具体应上传至第 6.4.1 节所述之举报接收方公司的专门渠道，以便妥善归档，同时以适当的方式保存原始文件，尽可能确保其机密性。

最后，举报及相关文件必须保存至处理该举报所需的时间为止；此外，根据《举报人保护指令》的规定，举报的保存期限不得超过自通报最终结果程序之日起五年，或法律规定的其他保存期限，如第 6.4.1. 节中所述。保存期限的起算时间取决于举报的最终处理结果（即：直接结案归档、最终调查结果；移交主管机关等）；因此，将由审计负责人授权销毁和/或销毁根据第 6.4.1. 条所述所保存的任何纸质文件，必要时，应事先通知相关受控公司的联系人。

6.9 外部渠道

根据《举报人保护指令》的规定，举报人可通过国家反腐败局设立的外部举报渠道进行举报，该渠道可在国家反腐败局的网站上找到[31]，然而，其仅限于《举报人保护指令》所规定的违规行为（涉及私营部门，且与公共服务特许经营无关的违规行为除外），且须满足《举报人保护指令》规定的以下条件，即：

- 未启动内部举报渠道；
- 该举报是根据《举报人保护指令》及本指南的规定执行的，但未获跟进；
- 而具备充分理由认为，如果进行内部举报，该举报将不会得到处理，或者自己会遭到报复。关于合理理由，特此说明：举报人必须能够基于所附的具体情况及实际可获取的信息（而非单纯的推测），旨在做出合理认定，若其进行内部举报：

[31]有关向该机构提交、接收和管理举报的具体方式，可在国家反腐败局网站的相关栏目中查阅更多详情。根据《举报人保护指令》的规定，只有员工人数超过五十人的公司才有资格使用外部渠道和采取公开披露的方式。
如第 6.5.2 节所述，涉及私营部门、与公共服务特许经营无关，且根据《第231/2001立法法令》所指法规构成重大违规行为的举报，以及违反《231号模型》的行为，仅可通过内部举报渠道进行举报。

- 该举报将无法得到有效落实。例如：当工作场所的最终负责人涉及违规行为时，存在违规行为或相关证据可能被隐瞒或销毁的风险，或可能影响主管当局调查的有效性，抑或由于认为国家反腐败局更适合处理该具体违规行为（尤其是在其职权范围内的事项）；
- 这可能会导致带来报复风险（例如：也可能是因违反对举报人身份保密的义务所引发）。

- 该者有充分理由认为，该违规行为可能对公共利益构成迫在眉睫或明显的威胁。例如，可以设想这类情况：违规行为需要采取紧急措施，以保障人员健康与安全，或保护环境[32]。

举报人及其他相主体可根据《举报人保护指令》第 19 条第 1 款的规定向国家反腐败局进行举报，员工有权就其认为因举报、投诉或公开披露而在工作场所遭受的报复行为提出申诉。

若管理人收到有关报复措施的通知，将告知举报人可将该通知转交至国家反腐败局。必须向国家反腐败局提供客观证据，以便据此推断出举报、投诉、公开披露与所称报复行为之间的因果关系。

6.10 公开披露

根据《举报人保护指令》的规定，举报人[33]亦可就其在工作中获悉的、属于《举报人保护指令》所涵盖的违规行为（涉及私营部门，且与公共服务特许经营无关的情况除外）进行公开披露，但仅限于满足该法令规定的以下条件时，即：

- 举报人此前已通过内部或外部渠道进行举报，但未收到回复，或其举报未在规定时限内得到处理；
- 举报人确有理由认为，该违规行为可能对公共利益构成迫在眉睫且显而易见的威胁[34]；
- 举报人有充分理由认为，外部举报可能导致报复风险，或者由于具体案件的特殊情况，该举报可能无法得到有效处理[35]。

支持采取“公开披露”措施的正当理由，必须基于具体事实（其应随举报事宜一并提交）以及实际可获取的信息。

在公开披露中，若举报人自愿透露其身份，则不涉及保密保护，但《举报人保护指令》为举报人规定的其他所有保护措施仍不受影响。反之，若举报人使用化名或*昵称*等无法识别其身份的方式举报违规行为，为保障举报人的数据隐私，且在后续披露其身份的情况下，该举报将被视为匿名举报（因此则无法确保《举报人保护指令》中所规定的保护措施）；若后续举报人的身份遭到披露，则仍将向该举报人提供针对报复行为的法定保护。

举报人须通过专门设立的电子邮箱地址 whistleblowing@terna.it 向公司提交公开披露的举报信息，以便举报人能够享受相关保护措施（详见本指南第 6.3 节）。

[32]根据《第 1937/2019号欧盟指令》第 62 条的规定。

[33] “*如果该主体与新闻信息来源不同*”（参见第 2023 年 7 月 12 日第 311 号决议第 3.3 条，该决议已于 2023 年 7 月 13 日提交至理事会秘书处，并通过 2023 年 7 月 25 日第 172 期《官方公报》发布的公告予以公布，其中包含 “*关于保护举报欧盟法律违规行为人员及保护举报违反国家法规人员的相关指南。外部举报的提交与处理程序*”）。
如第 6.5.2 节所述，涉及私营部门，且与公共服务特许经营无关，并根据《231/2001 立法法令》所指法规构成重大违规行为的举报，以及《231 号模型》的违规行为，仅可通过内部举报渠道进行举报。

[34]其指一种紧急情况或存在造成不可逆损害的风险，甚至可能危及一人或多人的身体安全，因此必须及时揭露该违规行为并引起广泛关注，以防止其产生影响。

[35]例如，这么做可能导致证据被销毁，或者负责接收举报的机构与违规行为实施者之间存在串通之虞。换言之，其可能指向公司内部特别严重的疏忽或恶意行为

7. 外国公司

上述所提及的检举制度，涵盖检举渠道以及对检举人和被检举人的保护举措，同样适用于海外公司，前提是遵守当地法律。

在此特别说明，涉及来自第三国（非欧盟国家）人员的数据传输，必须依据具体案件所适用的法律规定，在法律允许的范围内开展。为此，集团内部协议可根据第 6.5 节的规定，对海外公司的报告管理作出规定，其将辅以其他具体协议，以确保数据处理符合适用法律。关于职责分配，在处理由管理人负责的举报时，可请求相关公司指定的合规官和/或外部顾问提供支持；合规官在此阶段的参与仅限于收集与初步调查相关的信息。

反之，如果外国公司无法按照本指南所述，通过内部举报渠道实施举报制度，则外国公司应制定符合《道德准则》中，关于举报人保护相关规定的违规信息举报机制，并采取以下措施：

- 向 Terna S.p.A. 通报（也可通过合规官）已设立或拟设立的监管措施，这些措施可能涉及根据《全球合规计划》（该计划是面向所有子公司的合规计划）任命的合规官。
- 确保就违规举报系统、使用方法以及已建立的保护机制提供充分的信息。

8. 批准、修订与发布

本指南中的各项原则属于 Terna 集团的核心价值观，并以此为指导开展组织和业务活动，同时亦是旨在落实《道德准则》的相关规定。基于这项原因，本指南由 Terna S.p.A.的首席执行官兼总经理批准，并适用于全体员工（包括签订固定期限合同的员工）、实习生及临时工作者。

本集团鼓励全体旗下公司采纳本指南，并予以推广。为此，公司开展了针对员工的宣传和培训活动，以普及举报机制的宗旨及其使用流程（例如：专项通知、培训活动、电子简报、内网等）。

对此，已经开展：

a）针对负责管理内部渠道的人员提供适当的培训，包括通过专门的培训和入职培训课程；

b）为实现信息沟通之目的，应就内部举报渠道、进行内部举报的程序及前提条件，以及根据《举报人保护指令》进行外部举报的渠道、程序及前提条件，做出适当的告知。关于最后一点，本集团旗下的意大利公司将在其官方网站（如有）的专门栏目公布上述信息。

关于第 a）点，培训应以相关法规和*最佳实践*为基础。

关于第 b）点，亦有开展宣传活动，旨在向外界普及举报机制的宗旨及其使用流程。本集团旗下各公司均应确保本举报指南已经公司内网发布、电子邮件发送或其他公司文件等共享方式在全体内部予以公布。

适用于第三方的举报制度的原则和内容，将通过合同文件予以明确。

信息传播和培训活动均经过记录、监控和评估，以确保其适当性和有效性。

若因法规和/或判例的发展，或为与*最佳实践*和国家反腐败局指南对齐，或因已采取的监督行动、新出现的运营或组织需求，均可由数字战略与可持续发展总监进行修订和补充。如有必要或仅出于适当考虑，该总监可提供操作指示，以规范本指南的具体应用场景，并向受控公司提供相关指导。上述修改和/或补充内容须事先通知伦理委员会；若涉及实质性变更，亦须通知工会组织。

9. 报告

每年以日历年为周期，由审计负责人编写专门报告，并提交至伦理委员会，其内容涉及本集团的层面；该报告应明确列出收到的举报数量、已归档的举报数量、相关调查的进展情况以及相关调查程序的进展状态，其中举报数据将进行匿名化处理，并以汇总形式呈现。而针对本集团的其他公司，亦应将该报告提交给首席执行官/唯一董事，旨在全面展示举报系统的运行状况；此外，在职责范围内，还将定期（通常每六个月）向监督委员会/合规官提交报告。如果审计负责人无法查阅有关利益冲突的报告，上述报告的补充工作将由伦理委员会通过其秘书负责完成。

10. 第三部门机构（ETS）提供的支持措施

举报人可随时向国家反腐败局根据《第 24/2023 立法法令》第 18 条规定公布的名单中所列的第三部门机构寻求帮助，其中规定了以下支持措施：

a) 关于举报法规的信息、协助和咨询；

b) 法律援助；

c) 心理支持。

根据各自章程的规定，开展 2017 年 7 月 3 日第 117 号立法立法令所列活动的签约机构名单，其已发布在国家反腐败局的官方网站上。本节描述了相关宏观流程或治理/风险/合规主题所处的脉络背景。

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.