COMPLIANCE PROGRAM ON CORPORATE CRIMINAL LIABILITY

May 2025

INTRODUCTION

Enel S.p.A. ("**ENEL")** is the parent company of a multinational group ("**Group**") that operates in a complex and highly regulated business sector, and in different economic, political, social, and cultural environments. In this context, integrity is conceived as a fundamental value for the performance of business activity. It requires all Group personnel to act with loyalty, integrity, transparency and strict compliance with national and international laws and regulations, as well as applicable standards and guidelines.

The "**Enel Global Compliance Program**" or "**EGCP"** is conceived as a tool to reinforce ENEL's commitment to the highest ethical, legal, and professional standards, with the aim of enhancing and preserving the Group's reputation. To this end, it establishes a series of preventive measures aimed at avoiding corporate criminal liability.

In recent years, there has been a steady increase in the number of countries that have established corporate criminal liability regimes in their legislation, which allows courts of law to sanction corporate entities for criminal conduct by their representatives, employees or third parties acting on their behalf.

In certain jurisdictions, applicable laws and regulations encourage companies to adopt corporate governance structures and risk prevention systems, to prevent their directors, employees, consultants, or external contractors from engaging in criminal conduct. Likewise, these regulations provide for the possibility of exempting or mitigating the applicable penalties when companies have implemented adequate preventive measures to prevent the commission of actions that may result in criminal liability of legal people.

The EGCP, inspired by the most relevant international regulations, aims to define **general standards** of conduct applicable to employees, management personnel and other members of the management and control bodies ("**Corporate Recipients**"), as well as to consultants or other contractors and, in general, to third parties ("**Third Parties**" or "**Other Recipients")**") (hereinafter referred to as the Corporate Recipients and the Other Recipients shall be jointly referred to as the "**Recipients**") of the Group companies of non-Italian nationality (hereinafter referred to as "**NIS"),** and must at all times comply with the local legislation and cultural, social and economic idiosyncrasies of the different countries in which the NIS operate, which, in the event of contradiction with the EGCP, they will always prevail.

1 MISSION

The EGCP represents an opportunity to strengthen the initiative-taking prevention of corporate criminal liability by strengthening governance and the internal control system. a stand designed to encourage the development of appropriate conduct in accordance with the legislation in force and applicable to the entire Group.

The EGCP sets out the key standards of conduct expected of all Corporate Recipients and, where specified, of all other Recipients, too:

i. provide NIS with a uniform set of rules aimed at preventing corporate criminal liability in their respective countries.
ii. integrate any local compliance program adopted by NIS in accordance with applicable corporate criminal liability laws.

The standards contained in the EGCP are aligned with:

i. the provisions contained in the Code of Ethics, which sets out the ethical principles of the ENEL Group and which all Recipients are obliged to respect.
ii. the provisions of the Zero Tolerance Plan against Corruption, of the ENEL Group; iii. the corporate governance standards adopted by LSS NIS, in accordance with the local legislation applicable in each case and best international practices.
iv. the internal control systems implemented by each of the NIS.
v. The provisions contained in any local compliance program adopted by NIS to comply with their respective local corporate criminal liability laws, as well as any related internal guidelines, policies, or organizational documents.

2 STRUCTURE

The EGCP states:

a. The processes of implementation of the EGCP adoption by the NIS, as well as the corresponding process of updating it, as appropriate.
b. EGCP dissemination mechanisms to Target Audiences, together with associated training activities.

c. the disciplinary system applicable in the event of non-compliance with any of the provisions contained in the EGCP.
d. the general standards of control.
e. the areas of activity subject to supervision in relation to certain types of unlawful conduct (the "**Areas to Supervise**" or "**ABMs**"), listed in Section 8. The prevention of which is a priority for ENEL in its commitment to conduct its operations with honesty and integrity (the "**Crimes**").
f. the key standards of behavior applicable to the "Areas to Supervise".

The EGCP is complemented by **Annex 1**, entitled "Examples of unlawful conduct committed in the ABM".

3 ADOPTION, APPLICATION, REPONSIBILITY AND SUBSEQUENT MODIFICATION

The EGCP has been approved by ENEL's Board of Directors and will be subject to the mandatory approval of the Board of Directors, or other corresponding administrative body of each NIS.

The Board of Directors or other governing body responsible for each NIS, within the framework of its autonomy and independence:

i. adopt the most appropriate measures for the implementation and supervision of the EGCP, considering the size, complexity of the activities conducted, the internal control system and the relative specific risk profile of the NIS and its regulatory framework.
ii. will be responsible for the correct application of the "Areas to Supervise" and the "Key Standards of Behavior", as provided for in section 10.2 of the EGCP, as well as for the controls established in Enel's Global Compliance Program.

NIS will apply to the EGCP in accordance with the local legislation in force, the nature of the activities they conduct and the specific characteristics of their organizational structure.

The internal committees of the Enel S.p.A. Board of Directors evaluate the amendments or extensions of Enel's Global Compliance Program and submit them to the Board of Directors for approval. Amendments or integrations of the EGCP shall subsequently be submitted to the board of directors or relevant governing body of the NIS.

Each NIS shall report on any specific changes or interpretations made in accordance with local law or practice. Likewise, the Board of Directors or corresponding administrative body of the NIS will designate the structure (person or body) responsible for providing support in the implementation and supervision of the EGCP, as well as for executing the relevant controls, in compliance with the applicable regulations.

4 DISSEMINATION OF THE EGCP AND TRAINING ACTIVITIES

The EGCP will be available for consultation and download through the ENEL Group Intranet.

At the local level, specific training activities will be developed for all staff, including digital training tools, with the aim of ensuring adequate dissemination and understanding of the EGCP, the Areas to Be Supervised (ABM), as well as the relevant behaviors to prevent the commission of Crimes. These training activities may be integrated into the training programs that each NIS adopts within the framework of compliance with local criminal law and their respective regulatory compliance programs.

5 COMMUNICATION TO THIRD PARTIES

Third Parties will be informed about the principles and contents of the EGCP, adhering to it by signing the corresponding documentation.

6 GENERAL PRINCIPLES

EGCP Corporate Recipients are obliged to report any misconduct, irregularity, and non-compliance with Enel's Global Compliance Program.
In compliance with current regulations and its "Whistleblowing Notification Policy “people has established a specific Reporting Channel, managed by the General Directorate of Audit,

designed to guarantee the confidentiality of the identity of the informant, of the persons mentioned in the report, as well as of the content and related documentation. Reports may be submitted as follows:

i. in writing, i.e., via the web, or via the online notification system available on the Group's website.
ii. orally, through the telephone numbers indicated on the same website; iii. or, through a face-to-face meeting, at the request of the complainant, within a reasonable period and using the channels mentioned above.

In accordance with what is already defined in the current document, ENEL handles reports received within the timeframe provided for by the regulations in force, prohibits any form of retaliation and ensures that no act of retaliation is conducted by reason of a report.

ENEL will apply disciplinary sanctions in the following cases:

(i) those who violate the protection measures of the whistleblower or other persons protected by the relevant law, or (ii) who conceal or attempt to conceal the report; or (iii) who violates the confidentiality obligations provided for in the legislation in force regarding the notification of complaints; or (iv) whoever is responsible for the non-establishment or improper management of the notification channels in accordance with the requirements established in the regulations in force on notification of complaints; or (v) whoever is responsible for the failure to verify and analyze the reports; or (vi) those who take retaliatory action against the complainant or other persons protected by relevant law, because of the same report; as well as (vii) the informant or complainant when it is established, even by means of a judgment of first instance, the criminal liability of the same for the crimes of defamation or slander, or his civil liability for the same title in cases of intent or gross negligence.

7 SYSTEM DISCIPLINARY

The competent functions of the NIS will apply the corresponding disciplinary measures in case of non-compliance with any of the standards of behavior established in the EGCP, in accordance with the disciplinary system in force, applicable regulations and local compliance

programs. All this without prejudice to the legal guarantees recognized to employees by local legislation, such as the right to defense and the principle of due process.

Disciplinary measures shall be applicable regardless of the outcome of any criminal proceedings that may be initiated by the competent judicial authority.

Likewise, the contractual documentation must provide for appropriate sanctions in the event of non-compliance with the EGCP by Third Parties, including – but not limited to – the possibility of contractual termination, in accordance with applicable law.

8 CRIMES

The EGCP applies to the following types of Crimes (hereinafter referred to as "Crimes", as described below):

A. Bribery Crimes
B. Other Crimes Against Public Entities
C. Accounting Fraud
D. Market Abuse
E. Terrorist Financing and Money Laundering
F. Crimes against Individuals
G. Crimes against Health and Safety
H. Environmental Crimes
I. Cybercrime
J. Crimes against Intellectual Property
K. Tax Crimes

Section 10.2 of the EGCP identifies the areas of activity that should be subject to oversight by the NIS, as well as the applicable key standards of behavior.

The list in paragraph 10.2 does not exempt Non-Italian Subsidiaries from conducting their own risk assessment and defining additional key standards of behavior, where deemed appropriate.

Accordingly, NIS may identify:

i. business activities that may involve a specific risk of committing crimes, through an analysis of the operational processes and modalities of commission associated with the diverse types of crimes.
ii. additional standards of behavior to be met by all Corporate Recipients and, where expressly specified, by other Recipients to: refrain from any conduct that may result in the commission of any of the Offenses described above; and to refrain from any conduct that, without directly constituting one of these crimes, could reasonably lead to its commission.

9 SYSTEM OF CONTROL OF THE EGCP

The EGCP establishes two main levels of control in relation to the Areas to be Supervised:

- general standards of control.
- key standards of behavior, specific to each ABM.

10.1 GENERAL CONTROL STANDARDS

NIS must comply with the following general control standards:

1) **separation of duties**: the assignment of roles, tasks, and responsibilities within an NIS is done in accordance with the separation of duties according to which no one person can autonomously perform the entirety of a process (i.e., in accordance with this principle, no person can autonomously undertake to perform an action, authorize it, and subsequently verify it); appropriate separation of duties can also be granted using systems computer computers that allow certain transactions to be carried out only by identified and authorized persons;
2) **Delegation of signature and authorization**: There should be formal rules on the exercise of internal powers and delegation of signature. Signature delegations shall be consistent

with the organizational and managerial responsibilities assigned to each power holder in the NIS.

3) **Transparency and traceability of processes**: The identification and traceability of sources, information and controls conducted to support decision-making and the execution of actions by NIS, as well as the management of financial resources, should always be ensured. Likewise, the adequate storage of relevant data and information must be guaranteed, either through electronic information systems and/or paper support.

4) **Proper management of relations with Third Parties**:

(i) before entering any relationship with a Third Party, an appropriate due diligence assessment must be conducted with respect to the requirements of good repute. The scope of such assessment shall be proportionate to the actual or perceived risk that the prospective partner, consultant, or supplier will not meet the required standards. This evaluation may include, but is not limited to, inquiries into business contacts, local chambers of commerce, business associations, Internet searches, and reviews of business references and financial statements:

- the following circumstances will be considered red flags: the Third Party is constituted in a country with high levels of corruption according to international indices, such as the Transparency International Corruption Perceptions Index, or in a country classified as a "non-cooperative country" according to the FATF blacklist or other international list related to the fight against money laundering and the financing of terrorism;
- The Third Party has been suspended or excluded from participating in tenders or contracts.
  with state entities, public bodies, or government agencies due to compliance investigations conducted by public authorities.
- the Third has been the subject of criminal proceedings.
- The Third Party refuses to adhere to the company's compliance program and lacks a code of conduct or equivalent ethical standards.
- the Third maintains family ties with key officials of domestic or foreign government agencies.
- A public official appears as the owner, director, or main shareholder of the Third Party.
- The direction of the business activity of the Third Party is a virtual office.
- The Third Party has an undisclosed beneficial owner.

(ii) additional checks, in case red flags emerge during the due diligence phase,

(iii) continuous monitoring throughout the contractual relationship to ensure that the counterparty continues to comply with the requirements set out in the NIS; and

(iv) Corrective measures, if during the contractual relationship the third party fails to comply with the established requirements or new warning signs arise, appropriate measures must be adopted. Situations that could trigger these measures include:

- The third-party requests unusual advance payments.
- The third party submits inaccurate invoices or invoices for services not rendered.
- The third-party requests that payments be made in cash or by bearer instrument.
- The third-party requests that payments be made outside their country of origin, in jurisdictions unrelated to the transaction.
- The third-party requests that payment be made to an intermediary or other entity or requests that payments be made to two or more bank accounts.
- The third-party requests funds to be donated to a non-profit institution or foundation.

10.2 AREAS TO MONITOR AND KEY STANDARDS OF BEHAVIOUR

A. Bribery offences

These types of Crimes refer to the offering, giving, solicitation or receipt of money (or any other type of benefit, gain or advantage) for the purpose or with the intention of influencing the recipient (who may be a person belonging to a private company or a public official) in a way that acts in favor of the person providing the bribe.

Often, bribes consist of gifts or payments of money (other forms of bribes may include various goods, privileges, entertainment, and favors) in exchange for favorable treatment. Such favorable treatment, which triggers bribery, may consist, for example, of:

- the hiring of the briber in a relevant contract (either with a public administration or a private company); or the award of a public tender.
- a false statement, favorable to the briber, by a witness in a judicial proceeding.
- the preparation of a lenient report by a public official.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of Crime, it is necessary to supervise the following areas of activity:

(i) negotiation, execution, and management of relevant contracts with any Party (Public Authorities, companies, associations, foundations, among others).
(ii) participation in tenders, both public and private.
(iii) management of non-contractual relationships with community organizations and Public Authorities (e.g., in relation to health, safety, environment, personnel management and tax compliance requirements).
(iv) dispute management, including litigation, arbitration, out-of-court proceedings.
(v) selection of partners, intermediaries, and consultants, as well as the negotiation, execution, and management of the corresponding contracts.
(vi) cash and financial resource management.
(vii) management of non-profit initiatives.
(viii) management of gifts, entertainment, and hospitality expenses.
(ix) reimbursement of expenses incurred by employees.
(x) hiring of personnel.
(xi) definition of compensation incentives, such as results-based target plans (e.g., MBOs) for NIS executives.

KEY STANDARDS OF BEHAVIOR

When conducting business with private companies, as well as international, national, state, and local governments and public administrations (hereinafter referred to as the "**Public Authorities**"), NIS and its representatives are committed to acting with integrity and honesty and must comply with all applicable laws and regulations. In addition, Corporate Recipients and Third Parties (subject to specific contractual terms) are expressly prohibited from:

a) offering money or granting any other type of advantage of any kind (including promises of employment, among others) to representatives of Public Authorities, as well as to natural persons belonging to a private company -or their relatives (hereinafter, the "**Individuals**")- with whom the NIS maintain or intend to establish a commercial relationship, or in the

framework of any other interaction, such as requests for public funds, processing of authorizations or licenses, among others;

b) offer gifts, hospitality or other benefits to the people mentioned in the previous point, except in the case of accepted practices in accordance with customary business standards. The following are not considered admissible, among others: (i) travel; (ii) gifts or entertainment offered to people linked to bidding processes in which a NIS or any company of the ENEL group participates. Only those benefits that constitute reasonable business courtesy are permitted, such as: (i) occasional low-value meals; (ii) occasional attendance at local sporting events, theaters, or other cultural events; and (iii) promotional gifts of low value, such as pens, calendars, or similar objects. Gifts offered - except those of low value - must be documented to allow inspection in accordance with established internal controls.

c) using cash as a means of payment, except in cases permitted by current regulations (e.g., money for petty expenses).

d) incur any promotional or sponsorship expenses, unless the expenses have been approved, in advance, in writing by the competent area.

e) make any contribution to non-profit institutions, community projects, or professional associations, unless the expenses have been approved, in advance, in writing by the competent area.

f) assign services to Third Parties without adequate justification in relation to the needs of NIS.

g) make payments to Third Parties that are not sufficiently justified with respect to the type of service provided and local practices in force.

Non-Italian subsidiaries will evaluate the advisability of adopting appropriate organizational measures to prevent any Recipient from engaging in the conduct described above. In addition, NIS shall consider adopting specific procedures aimed at ensuring that:

h) There is adequate documentation supporting all material relationships established with Public Authorities (e.g., administrative procedures for obtaining authorizations, licenses or similar acts, joint ventures with public entities, applications for public authorizations) and any relevant business relationships.

i) Theations with Public Authorities, when issues relating to the interests of the NIS are at stake, are managed by at least two authorized people, in order to ensure transparency and control's contracting procedures are carried out exclusively on the basis of a real and demonstrable business need, thatinterest.ction process involves at least two different

areas and is based on criteria of objectivity, competence and professionalism, in order to avoid favoritism, nepotism and conflicts of interest;

j) incentive plans aimed at management are designed in such a way that contingent objectives do not encourage abusive behavior, but focus on specific, measurable, and achievable results of a given period.

k) in relation to project planning, realistic deadlines are established, commensurate with the nature and complexity of the planned activities.

l) In relation to the reimbursement of expenditures, relevant documentation, including original receipts supporting the expenditure incurred, must be submitted to the relevant accounting department prior to payment. In addition, the relevant payment or expense (or receipt thereof) is accurately described and reflected in the relevant NIS accounting records.

B. Other offences against public authorities

This type of crime refers to fraud against public entities and occurs when a company uses illicit artifices or schemes to defraud a public entity or obtain an economic advantage through false or fraudulent statements, promises or pretensions.

Often, these types of crimes are related to public funding and grants and occur when a company applies for public funding or grants without being entitled to them, or misuse them, other than as provided for in the grant agreement.

This type of crime can occur for multiple motivations, which are usually related to obtaining any undue economic advantage.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to these crimes, it is necessary to pay special attention to the following areas:

(i) participation in public tenders and in administrative procedures of a public nature in general.

(ii) management of relations with Public Authorities, especially in relation to health, safety, environment, personnel management, and tax compliance requirements.

(iii) application for public funding, grants, subsidies or guarantees issued by Public Authorities.
(iv) management of public funds received, including grants, subsidies or guarantees obtained.

KEY STANDARDS OF BEHAVIOR

In addition to the standards established in section 10.2. A), Corporate Recipients and Third Parties (in accordance with the specific contractual terms), will refrain from engaging in the following conduct:

a) submitting false or altered documents, in whole or in part, during participation in public bidding bids.
b) misleading the Public Authorities, by any means, during the evaluation of applications for authorizations, licenses, authorizations, concessions, or other administrative acts.
c) omitting relevant information held by NIS that may influence the decisions of Public Authorities, in relation to the circumstances described in paragraph a) and b) above, in favor of NSIs.
d) any conduct aimed at obtaining from a Public Authority any type of public subsidy, financing, loans or other public disbursements, by means of altered or falsified statements or documents, the omission of relevant information or, by any other artifice or fraud, with the intention of misleading the relevant public entity;
e) use money received from Public Authorities as funds, contributions, or loans for purposes other than those for which they were granted.

In addition, to implement the standards of behavior described above; the non-Italian Subsidiaries shall assess the desirability of adopting appropriate organizational measures to ensure that:

f) all declarations submitted to public authorities, both national and international, for the purpose of obtaining funds, grants or loans contain only truthful information and are signed by duly authorized persons and, in the event of obtaining such funds, grants or loans, they are duly accounted for;
g) adequate separation of duties controls is put in place, ensuring that the application, management and notification phases related to public procedures for obtaining funds, grants or loans advantaged by different Corporate Recipients within the organization's information collection and analysis activities, necessary for reporting purposes, are carried

out with the support of the competent functions, ensuring the quality and veracity of the data;

h) Subsequent documentation and notifications related to applications for subsidies, subsidies or guarantees are approved by appropriate hierarchical levels, in accordance with internal control and supervision procedures.

C. Accounting fraud

Accounting fraud is a type of crime that consists of the intentional manipulation of financial statements with the aim of presenting a false image of the economic and financial situation of a company to investors, creditors, shareholders, and other interested parties.
Accounting fraud can occur for a number of reasons, including, but not limited to:

i. obtaining bank financing, by altering financial statements to appear non-existent economic solidity.
ii. reporting unrealistic profits or concealing losses.
iii. omitting relevant information, which could negatively affect the valuation or reputation of the company.
iv. cause inflation of the share price.
v. concealing the creation of funds intended for illicit purposes.
vi. covering up misconduct, such as theft or embezzlement committed by managers or employees.
vii. omit material facts that may mislead any interested party, including stock exchange authorities, regulators, creditors, and investors.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

(i) the preparation of documents addressed to investors or the public, including, but not limited to, financial statements and periodic financial reports, containing information on assets, liabilities, income, expenses or cash flows of non-Italian subsidiaries, even where such documents do not constitute formal periodic accounting reports.

(ii) management of relations with external auditors and supervisory bodies.

KEY STANDARDS OF BEHAVIOR

Non-Italian Subsidiaries will assess the desirability of implementing appropriate measures, and accounting, records and accounts staff are required to act appropriately to ensure that:

a) The data and information used in the preparation of periodic financial reports are accurate and diligently verified.

b) All balance sheet items, the determination and quantification of which involve discretionary judgments, are objective and are duly supported by the corresponding documentation.

c) transactions are executed in accordance with general or specific authorizations granted by the management.

d) invoices and other relevant documentation related to transactions are properly monitored, recorded, and filed.

e) Transactions are recorded as necessary to enable the preparation of financial statements in accordance with applicable or acceptable accounting principles or any other criteria applicable to such statements.

f) Access to such transaction records is permitted only pursuant to general or specific authorizations from the Directorate.

In addition, in order to ensure that complete and truthful information is provided to the market, non-Italian Subsidiaries are prevented from engaging in any conduct that hinders or, in any case, obstructs the verification of external auditors, whether through the concealment of documentation or the use of other fraudulent means.

Finally, non-Italian Subsidiaries are obliged to make all communications with any public financial authority (as provided by applicable local law) in a correct, complete, adequate and prompt manner, without impeding them, in any way, from performing their duties, including in the context of any inspection (e.g. by express opposition, unjustified refusal, obstructive behavior or lack of cooperation).

D. Market abuse

This category of offences mainly refers to three different types of conduct: (1) selling or buying financial instruments using information that is not publicly available ("Inside Information"), or illegitimately communicating it to third parties; (2) altering the pricing mechanism of financial instruments through the deliberate dissemination of false or misleading information in order to influence the price of such instruments; (3) execute buy and sell orders that have the object or effect of: (i) providing false or misleading indications regarding the supply, demand or price of financial instruments, (ii) fixing the market price of one or more financial instruments at an anomalous or artificial level.

This type of conduct can take place for the benefit of a company for multiple reasons, including, but not limited to:

- artificially reduce the share price of a target company before an acquisition.
- damage the reputation of a competing company.
- alter the price of a certain financial instrument in the portfolio before conducting commercial operations related to it.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

(i) Public information management includes interactions with investors, financial analysts, journalists, and other representatives of the media, as well as the organization and participation in meetings of any kind with such ppersons.management of inside information related to the Group's listed companies and relevant financial instruments. This includes, among other things, information on new products, services and markets; accounting data for the period; forecasts and quantitative objectives on business performance; mergers/spin-offs; and, in particular, relevant new commitments such as negotiations and/or agreements related to the acquisition and/or sale of significant assets;

(ii) management of Privileged Information linked to energy derivatives, such as information on the unavailability of plants or facilities.

(iii) any type of transaction related to financial instruments in the portfolio.

KEY STANDARDS OF BEHAVIOR

Each Recipient is expressly prohibited from:

a) use Inside Information to negotiate, directly or indirectly, financial instruments for the purpose of obtaining personal advantages or in favor of Third Parties or an NIS or any other company in the Group.

b) disclose Inside Information to Third Parties, except as required by law, or other regulatory provisions or specific contracts in which counterparties are required to use the information only for its originally intended purpose and to maintain its confidentiality.

c) recommend or induce a person, based on certain Inside Information, to enter any type of transaction in financial instruments.

In addition, each Recipient is expressly prohibited from:

d) disseminate false or misleading information through the media (whether about the company itself or about any other company), including the Internet, or by any other means, only to alter the process of actions, derivatives or underlying activities that support the transaction previously planned by the subject who disseminates the information contained herein;

e) conduct any transaction on a financial instrument (e.g., buying or selling) against market abuse regulations.

E. Terrorist financing and money-laundering offences

The financing of terrorism involves the solicitation, collection, or provision of funds with the intention of using them to support terrorist acts or organizations.

The primary purpose of the persons or entities involved in terrorist financing is to conceal both the financing and the nature of the financed activity.

Money laundering is the process by which the illicit origin of funds from criminal activities is concealed. This process can manifest itself through three different and alternative conducts: (i) the conversion or transfer of funds, knowing that they are proceeds of crime, (ii) the concealment or concealment of the true nature, origin, location, disposition, movement or ownership of property or rights with respect to them, knowing that such property is the

proceeds of a crime; and (iii) the acquisition, possession, or use of property, knowing, at the time of receipt, that such property is derived from criminal activity.

When the proceeds of crime are generated by the same person who conceals their illicit origin, such conduct is punishable in some countries as self-employment money laundering.

Money laundering and terrorist financing often share similar transactional characteristics, related to concealment. Money launderers send illicit funds through legal channels to conceal their criminal origins, while those who finance terrorism transfer funds that may be of legal or illicit origin in such a way as to conceal their origin and end use, which is the support of terrorism.
This type of conduct can take place for the benefit of a company for multiple reasons, including, but not limited to:

- obtaining products or any other advantage derived from illegal activities conducted by terrorist organizations that have been financed (the other advantages may consist of the protection of business activity, in countries where such organizations have considerable influence).
- Concealing the illegal origin of the proceeds of crime.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

- financial or commercial transactions carried out with individuals, corporations, or legal entities controlled directly or indirectly by the aforementioned subjects, who have their residence or registered office in a country that represents a high-risk and non-cooperative jurisdiction (i.e., with strategic deficiencies in its legal and regulatory frameworks to combat money laundering and terrorist financing) as assessed by the competent international authorities, such as the Financial Action Task Force (FATF).

KEY STANDARDS OF BEHAVIOR

The NIS expressly condemns the use of its resources for the financing or execution of any activity aimed at achieving objectives associated with the financing of terrorism, as well as any improper use of financial instruments and/or operations aimed at concealing the origin of the company's funds.

More generally, NIS rejects any possible conduct aimed, even indirectly, at facilitating crimes such as the receipt, laundering and use of money, property or any assets of illicit origin; in this regard, the NIS undertakes to implement all the subsequent preventive and control measures required to achieve this objective, also regulating relations with third parties through contractual provisions that require compliance with the applicable laws on the matter.
It is expressly forbidden:

a) use blank or cash payments for any collection operation, payments, transfer of funds, etc.
b) making or receiving payments into anonymous bank accounts or bank accounts located in high-risk jurisdictions.
c) issue or receive invoices or issue documents in relation to non-existent transactions.

In addition, to apply the standards of behavior described above, NIS must:

d) perform analytical controls of cash flows.
e) verify the validity of payments, checking that their beneficiary is indeed the counterparty involved in the transaction.
f) conduct procedural checks about transactions that occur outside the normal processes of the company.
g) keep documentary evidence of all transactions conducted.
h) guarantee the traceability of each financial operation, as well as agreements or any other investment or business project.
i) verify the economic coherence of such operations and investments.
j) Review the international blacklist on terrorism and high-risk districts.

F. Offences against private individuals

The term "crimes against private individuals" refers to several types of criminal offenses that typically involve personal injury, threats of physical harm, or other actions committed against a person's will.

However, for the purposes of this EGCP, crimes against individuals mainly refer to crimes that are most likely to occur in the management of an enterprise, such as those relating to forced labor practices, consisting mainly of forcing employees to work through the use of violence, intimidation, or other coercive means, such as the retention of identity documents.
This type of crime can occur for a number of reasons, including, but not limited to:

- employ labor at minimal cost.
- employ a submissive workforce, which does not question orders or reject requests.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

(i) entering contracts with suppliers employing non-skilled personnel and/or operating in countries where individual rights are not fully protected by local or international law.

KEY STANDARDS OF BEHAVIOR

Non-Italian Subsidiaries are required to:

a) select external third parties (e.g., partners, suppliers), especially those providing non-technical services, only after having rigorously verified their reliability.
b) formalize appropriate contractual documentation with external contractors that require them to comply, and that their subcontractors comply with any applicable international and local laws. This includes, inter alia, the International Labor Organization (ILO) conventions on the minimum age for employment, the worst forms of child labor, forced labor, the protection of child and women's labor, as well as compliance with adequate hygiene and sanitary conditions.
c) apply and enforce the contractual sanctions provided for in the relevant agreements in the event of non-compliance by a contractor or any of its subcontractors with any applicable international or local legislation.

G. Health and safety offences

Health and safety crimes are related to the failure to comply with local laws and labor standards that must be conducted in the workplace to prevent accidents and illnesses of employees.
This type of conduct can occur for the benefit of a company for multiple reasons, including, but not limited to:

i. reduce costs, as the implementation of the required measures often entails additional costs for a company.
ii. increase productivity, since working without considering preventive procedures and policies could speed up the production process.

For more details, see the examples in Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

(i) compliance with applicable health and safety laws.

KEY STANDARDS OF BEHAVIOR

Regardless of the scope of local occupational health and safety legislation, NIS will promote and consolidate a strong culture of protection in the workplace, fostering risk awareness and individual responsibility for safe behavior.

In this sense, and beyond strict compliance with the applicable local regulations, the NIS undertakes to adopt all necessary measures to safeguard the physical and moral integrity of its workers.

NIS shall ensure that:

a) Compliance with the legal provisions on occupational health and safety is a priority.
b) occupational risks are assessed and managed, as far as possible and in accordance with the development of the best available techniques, through the selection of appropriate

and safe materials and equipment, with the aim of eliminating or, where this is not possible, reducing the risk at its source.

c) The information and training of workers is extensive, updated, and specific according to the activities conducted.

d) Workers are regularly heard on issues related to health and safety in the work environment.

e) An effective monitoring system is in place to ensure the correct implementation of preventive measures. Any non-compliance or area for improvement detected during work activity or within the framework of periodic inspections will be addressed in a timely and effective manner.

f) The organization of work is structured in such a way as to protect the integrity of workers, third parties and the community in which the NIS operates.

To achieve these objectives, the NIS will allocate the organizational, technical, and economic resources necessary to ensure full compliance with the regulations in force on the prevention of occupational risks, as well as to continuously improve the health and safety conditions of workers.

Corporate Recipients, depending on the role they play within the organization, must ensure strict compliance with applicable legislation, internal procedures and any other corporate regulations aimed at protecting the health and safety of workers.

H. Environmental crimes

Environmental crime comprises a wide range of illicit activities, including illegal wildlife trade, mismanagement of water resources, unauthorized trafficking, and disposal of hazardous waste, and smuggling of ozone-depleting substances.

This type of crime usually has a direct impact on the quality of air, water and soil, puts biodiversity at risk, and can trigger environmental disasters of great magnitude, representing a threat to the health, safety, and well-being of large sectors of the population.

Driven by high economic benefits and facilitated by a minimal risk of detection and low conviction rates, these illicit activities are attracting more criminal networks and criminal organizations, especially in transnational contexts.

These behaviors can occur for the benefit of a company for a variety of reasons, including:

- Cost reduction: avoiding the implementation of environmental protection measures can represent immediate economic savings.
- Increased productivity: Operating without considering environmental impacts can speed up production processes, although at the cost of regulatory compliance and sustainability.

For specific examples, see Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to supervise the following areas:

(i) compliance with applicable environmental regulations in the design, construction, operation, maintenance and dismantling of plants, interconnections, and distribution network infrastructures.

(ii) compliance with environmental regulations applicable in the provision of products and services related to energy, energy efficiency and electric mobility, both to residential customers and to small, medium and large companies, as well as public sector entities, including the design, testing and development of electric mobility products and technological innovation.

KEY STANDARDS OF BEHAVIOR

In the development of their business activities, NIS undertakes to act in accordance with the principle of protection and preservation of the environment.

NIS:

a) actively contributes to the awareness and dissemination of good practices in environmental protection, managing their activities in compliance with applicable legislation.

b) promote scientific and technological development aimed at protecting the environment and conserving natural resources, through the adoption of advanced systems that favor sustainability and energy efficiency.

c) They strive to meet the expectations of their customers and other stakeholders in relation to environmental issues, adopting all necessary measures for the protection and preservation of the environment and condemning any form of damage to the ecosystem.

Agreements entered with third parties that may imply environmental liability for the Company --especially in relation to waste management and disposal-- will include specific clauses that impose compliance with the applicable environmental standard, as well as contractual sanctions in the event of non-compliance.

I. Cybercrime

Cybercrimes are criminal offenses that fall into two main categories.

(i) those in which the target is a network or a computer system.
(ii) those in which crime is executed or facilitated using a computer system.

For the purposes of the EGCP, Cybercrimes do not include those crimes that, although they can be facilitated by computer means, constitute separate criminal categories, such as fraud, theft, extortion, forgery, or harassment (for example, cyberbullying). Therefore, the Cybercrimes considered within the framework of the EGCP include, among others, the following examples:

(i) unauthorized intrusion into a protected computer network or systems.
(ii) introduction of viruses or other malicious programs into computer systems.
(iii) Unauthorized interception of data transmitted over computer networks.

These crimes can have a variety of motivations, including:

- theft of trade secrets of competing companies.
- sabotage or intentional damage to a competitor's computer systems.
- Illicitly obtaining confidential information on other companies' market strategies.

For additional examples, see Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, it is necessary to monitor the following key areas:

(i) digital activities conducted by the Recipients, both in Information Technology and Operational Technology environments, including the use of resources such as the intranet, internet, corporate email, business applications, collaboration and data exchange platforms, social networks, instant messaging tools.

(ii) management and protection of corporate devices (e.g., workstations, smartphones, removable devices) and technology infrastructures (such as servers, switches, routers, firewalls, and storage systems).

(iii) planning and implementation of preventive measures to mitigate the risk of data and information loss, as well as to ensure the confidentiality, integrity, and availability of digital assets.

(iv) Privileged user profile management.

KEY STANDARDS OF BEHAVIOR

The advisability of applying appropriate technical, physical, and organizational measures to prevent improper conduct must be evaluated, and each Recipient is obliged to refrain from engaging in the following practices:

a) improper use of personal credentials to access Information Technology and Operational Technology devices, systems, or infrastructures.

b) allow or facilitate unauthorized access by third parties to such systems or infrastructure.

c) unauthorized disclosure or sharing of business information or data outside the corporate environment.

d) unauthorized access, extraction, or modification of information or data.

e) use of personal or unauthorized devices to transmit or store company information or data.

f) sharing corporate devices with unauthorized people.

g) manipulation or alteration of configurations in corporate devices or infrastructures.

h) manipulation of systems, theft or destruction of files, data, or programs of the company.

i) access to corporate information systems without proper authorization.

j) sending unsolicited communications (spam).

k) connection of external devices (personal computers, peripherals, hard drives, etc.) to corporate systems or installation of software and databases without prior authorization.

l) installation of malicious software (e.g., viruses or worms) in Information Technology and Operational Technology systems or infrastructures.

m) Use of unauthorized software or hardware that may be used to assess or compromise the security of corporate devices, systems, and infrastructure (e.g., tools to identify credentials or decrypted encrypted files).

Regular monitoring of the activities conducted by NIS personnel in corporate computer systems to identify unusual behavior, vulnerabilities or deficiencies must be ensured, always in accordance with the applicable local legislation.
Likewise, it will be necessary to periodically remind Corporate Recipients of the obligation to use the devices, systems and infrastructures made available to them appropriately, including the realization of specific training sessions when necessary.

J. Copyright offences

Copyright infringement in the corporate environment may manifest itself through the unauthorized use, reproduction, distribution, or adaptation of works protected by intellectual property legislation, such as software, databases, videos, images, literary and musical works.

For the purposes of the EGCP, copyright offences comprise those conducts that are most likely to occur in the context of corporate governance, such as the unlawful use of databases or software, unauthorized reproduction, or distribution of protected materials, among others.

This type of crime can originate from various causes, including, but not limited to:

a) Lack of knowledge: employees may infringe copyrights unintentionally due to insufficient training in the applicable regulations and internal policies of the company.
b) Competitive pressure: in highly competitive markets, NIS could incur the unauthorized use of copyrighted works to reduce development costs and obtain commercial advantages.
c) Bad faith: employees who deliberately infringe copyright with the aim of harming a competitor of the NIS.

For specific examples, see Annex 1.

AREAS TO SUPERVISE

In relation to this type of crime, the following behaviors or situations should be specially monitored:

- unauthorized use or disclosure of copyrighted works, research materials, or content owned by others.
- use of copyrighted images, videos, or music in promotional campaigns without proper authorization.
- unauthorized use of software, digital piracy, or unauthorized extraction of data from protected databases.
- infringements arising from outsourcing processes, joint venture agreements or deficient supervision of licensing agreements, content distribution rights, or management of digital assets within the framework of commercial agreements.

KEY STANDARDS OF BEHAVIOR

In addition to the key standards of behavior set out in section 10.2 (I), the appropriateness of appropriate technical, physical, and organizational measures to prevent:

1. the unlawful use or dissemination to the public, through computer networks or any other type of connection, of original works protected by copyright, in whole or in part.
2. the use, distribution, extraction, sale, or lease of database contents in violation of the exclusive rights of exploitation and authorization of the owner of the rights.
3. the unauthorized downloading of software without the corresponding contractual documentation.
4. the downloading of peer-to-peer software or other programs not linked to corporate activity.

If the NIS enters contracts with third parties for the execution of activities that may involve risks of copyright infringement, such contracts must include specific clauses that require compliance with the applicable legislation and regulations on the matter.
The measures taken should be based on the following fundamental principles:

- respect for the copyrights of third parties: obtain the necessary authorizations before using protected materials, including images, videos, software, and written content.
- compliance with internal policies and continuous training: respect internal policies regarding the use, licensing and protection of copyright, disseminate them within the organization and promote training programs updated in accordance with regulatory evolution.

- Internal oversight and infringement reporting: Foster a culture of internal vigilance and encourage employees to report any suspected copyright infringement or unauthorized use of protected content.

Likewise, an initiative-taking attitude must be maintained with respect to all forms of intellectual property, including trademarks, patents, and trade secrets. This implies.

- comply with internal policies aimed at protecting intangible assets.
- fostering an organizational culture based on regulatory compliance.
- continuously monitor developments in intellectual property regulations, to adapt business practices accordingly.

K. Tax Crimes

Tax crimes include conduct conducted by the taxpayer that violates provisions to protect the interest of the tax administration in the exercise of its functions of tax assessment, control, and collection.

From a criminal point of view, tax crimes are classified into three categories: declaratory, document forgery and related to tax evasion:

- Declaratory offences include: (i) Filing fraudulent declarations through the use of invoices or other documents relating to non-existent transactions; (ii) Fraudulent declarations by means of other devices, such as simulated transactions (objectively or subjectively) or the use of false documentation other than that mentioned above; iii) Any other form of deception that may mislead the tax administration;
- The crimes of document forgery consist of the issuance of invoices or other documents for non-existent operations, to facilitate tax evasion.
- Crimes related to tax evasion refer to the failure to comply with the corresponding tax obligations.

Both declaratory and documentary offences are considered offences of specific intent, i.e., they require that the subjective element of the offence be geared towards the evasion of income tax or value added tax.

Likewise, non-compliance with the requirements established to access tax incentives or benefits granted in accordance with current legislation may be configured as a tax crime.

AREAS TO SUPERVISE

In relation to this type of crime, the following areas should be specially monitored:

(i) tax management (including the preparation of tax returns and compliance with related obligations).
(ii) preparation, conservation and filing of accounting records and other documents with tax relevance.
(iii) corporate billing.
(iv) accounting and invoicing between Group companies.
(v) transfer of assets and extraordinary corporate operations; **(vi)** management of relations with tax authorities; **(vii)** management of tax offsets.

KEY STANDARDS OF BEHAVIOR

With the aim of ensuring fair, responsible, and transparent taxation, NIS is committed to acting with integrity and honesty, adopting a fully compliance-oriented approach to the tax regulations applicable in the countries in which they operate. They also undertake to interpret these regulations responsibly, to mitigate tax risk and adequately address the interests of all interested parties.
To apply these standards of behavior, NIS must:

a. ensure integrity and transparent conduct, in compliance with laws and regulations, as well as internal procedures, in all activities related to accounting management, invoicing, tax record-keeping and tax management (including the preparation of returns and compliance with related obligations).
b. verify the reliability of the forms for the declaration and payment of income tax and value added tax (VAT), comparing them with the accounting records, as well as the accuracy of the data recorded.
c. to verify the correctness of the calculations relating to direct and indirect taxes.
d. ensure the timely implementation of legislative developments in tax matters and, consequently, update internal procedures and policies.

e. verify that the amounts corresponding to income tax, VAT and withholding tax certified by the company as a withholding agent have been correctly calculated and paid.
f. confirm that the economic and financial facts with tax relevance correspond to real and duly documented business events.
g. ensure complete, accurate and timely accounting records of invoices and other relevant documents for tax purposes.
h. ensure the preservation of mandatory records and documents through digital means that guarantee their availability and integrity.
i. verify the completeness and accuracy of the data contained in the invoices, as contractually agreed with suppliers or customers, and in relation to the services effectively provided.
j. to ensure maximum integrity, transparency, and substantive and procedural correctness in transactions with other companies in the Group, guaranteeing that inter-company services are duly regulated by contract and are provided under market conditions.
k. define criteria for the determination of transfer prices, in accordance with the applicable regulations.
l. establish clear roles, duties, and responsibilities in relation to the verification of compliance with the criteria adopted for transfer pricing.
m. ensure the participation of relevant tax functions in the assessment of tax impacts and regulatory compliance in the context of extraordinary corporate transactions.
n. verifying compliance with the procedures relating to the transfer and disposal of assets, ensuring their appropriate tax treatment.
o. to promote transparency, equity, and cooperation in relations with tax authorities, including during audit processes. Likewise, to promote adherence to cooperative compliance regimes for those entities that comply with local regulatory requirements, with the aim of strengthening institutional relations.
p. verify compliance with the regulatory requirements applicable to the compensation of direct and indirect taxes, as well as the veracity and accuracy of the certifications that support the tax credits.

10.3 FINAL PROVISIONS

To ensure compliance with the legal provisions, ENEL has established a system of internal policies and procedures that clearly assigns specific functions and responsibilities to the GROUP.

ANNEX 1 EXAMPLES OF ILLEGAL BEHAVIOR COMMITTED IN THE ABM

A. Bribery offences

Within the scope of the NIS, the commission of bribery offences shall be considered when a person:

- gives a gift to an official to obtain the award of a tender.
- Offer money to an official during an inspection at a plant to persuade him to ignore certain irregularities.
- promises to hire an employee of a competing company in exchange for access to confidential documents of that company.
- offers money to a witness for the purpose of inducing him or her to make a false statement in a judicial proceeding in which the NIS is involved.

B. Other offences against public authorities

Within the scope of the NIS, the commission of other offences against public authorities shall be considered when a person:

- Submit false information to a government agency during the bidding process to secure the award.

- provides a false representation of the financial or business situation of NIS to obtain public funding.
- breaches the terms of a grant agreement by misusing funds received from a public entity.

C. Accounting fraud

Within the scope of the NIS, the commission of accounting fraud shall be considered when a person:

- fails to record in the financial statements the material losses suffered by the NIS.
- conceals the creation of funds intended for illicit purposes, by overestimating the cost of consultancy services contracted by NIS.

D. Market abuse

In the event that the NIS is a listed company, it will be considered market abuse when a person:

- discloses inside information to a family member about an upcoming acquisition, inducing them to buy shares in the company.
- disseminates false information about the financial situation of NIS with the aim of influencing its share price.
- Disseminates false or misleading information about a competing company to damage its reputation in the market.

E. Terrorist financing and money-laundering offences

Within the scope of NIS, the commission of offences related to the financing of terrorism or money laundering shall be considered when a person:

- receives or transfers funds from or to a company located in a tax haven, or with bank accounts in such jurisdictions, for the purpose of concealing the illicit origin of the money.
- simulates the payment of consulting services to a company, transferring funds to bank accounts secretly controlled by an illegal organization that finances terrorist activities.
- uses funds intended for illicit purposes--the creation of which has been concealed through the manipulation of the company's financial statements--to finance political parties linked to terrorist organizations.

F. Offences against private individuals

Within the scope of the NIS, the commission of offences against private individuals shall be considered when a person:

- takes advantage of a worker's situation of physical or psychological vulnerability to exploit him or her for work.
- forces a person to work through threats, abuse of authority and/or violence.
- coerces migrants to work under threat of being reported to the immigration authorities.

G. Health and safety offences

Within the scope of NIS, the commission of health and safety offences shall be considered when a person acts in breach of applicable law, including, but not limited to, the following cases:

- fails to provide Personal Protective Equipment (PPE) as set out in the risk assessment.
- omits the implementation of emergency measures in the workplace, including organizational, training, and technical measures.
- fails to provide workers with the safety equipment or machinery necessary for the safe performance of their duties.
- allow employees to operate machinery without having received proper training on its safe use.
- omits to conduct the periodic medical examinations required by the regulations, necessary to evaluate the state of health of workers and detect effects derived from their work activity.

H. Environmental crimes

Within the scope of the NIS, the commission of environmental crimes shall be considered when a person:

- omits to consider the impact on biodiversity when planning the expansion of a plant or causes damage to the habitat of protected animal species, putting their existence at risk.

- operates a thermal power plant without respecting the legal thresholds for gas emissions, causing air pollution in the surrounding area.
- fails to effectively manage the company's waste disposal and instead establishes an illegal waste disposal site.
- contaminates water bodies due to improper use of the resource or water treatment systems.
- does not implement adequate systems for the prevention and control of atmospheric emissions, generating air pollution.

I. Cybercrime and intellectual property crime

Within the scope of the NIS, cybercrime or intellectual property-related crime will be considered when a person:

- Illegally copied software to work devices.
- Gain unauthorized access to computer systems of competing companies through malicious hacking techniques, steal confidential information, trade secrets, or spread malware with the intention of causing damage.

K. Tax Crimes

Within the scope of NIS, tax offences shall be considered to have been committed when a person:

- for the purpose of evading income tax or value added tax (VAT):
    - uses invoices or other documents relating to non-existent transactions or declares fictitious passive items in their tax return.
    - conceals or destroys documentation that must be legally preserved, thus preventing the reconstruction of revenue or turnover.
- issues or issues invoices or other documents for non-existent transactions, with the purpose of allowing third parties to evade income taxes or VAT.
- does not pay the taxes due, using non-existent or undue tax credits as a compensation mechanism.