



GLOBAL COMPLIANCE PROGRAM ON CORPORATE CRIMINAL LIABILITY

November 2025

INTRODUCTION

ENEL S.p.A. (“ENEL”) is the holding company of a multinational group operating 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 conducting business.

It requires all Group personnel to operate with loyalty, correctness, transparency and strict compliance with domestic and foreign legislation and regulations, international standards and guidelines. The “Enel Global Compliance Program” or “EGCP” is designed as a tool to reinforce ENEL commitment to the highest ethical, legal and professional standards for enhancing and preserving the Group reputation.

To this purpose, it sets a number of preventive measures for corporate criminal liability. In recent years, countries that have established a criminal or quasi-criminal corporate liability regime - enabling courts to sanction corporate entities for criminal behaviors by their representatives, employees or third parties acting on their behalf - have been steadily increasing.

In certain jurisdictions, applicable laws and regulations encourage companies to adopt corporate governance structures and risk prevention systems to make efforts to prevent managers, executives, employees and external consultants and contractors from committing crimes, also providing for an exemption or mitigation of applicable penalties in the event of the adoption of adequate preventing measures.

EGCP, inspired to the most relevant international regulations, aims at defining general standards of behaviour applicable to employees, directors and any other member of the management and control bodies (“Corporate Recipients”) as well as consultants or other contractors and, in general, third parties (“Third Parties” or “Other Recipients”) (hereinafter the Corporate Recipients and the Other Recipients will be jointly referred to as the “Recipients”) who are respectively employed or appointed or who deal with or act on behalf of the non-Italian subsidiaries (the “Non-Italian Subsidiaries” or “NIS”).

EGCP is intended to be applied globally to all NIS in accordance with the legal and corporate governance as well as the cultural, social and economic differences in the various countries where NIS operate.

When conflicts exist between EGCP and other private standards or technical standards EGCP will prevail. Where local laws and regulations contain specific requirements that differ from the provisions of EGCP, such requirements will prevail.

1. MISSION

The EGCP represents an opportunity to enhance the proactive prevention of corporate criminal liability by strengthening corporate governance and the internal control system, and its purpose is to support appropriate and lawful conduct within the Group.

The EGCP sets out the main rules of conduct expected of all Corporate Addressees and (where specified) Other Addressees in order to:

- a) provide the NIS with a system of core rules aimed at preventing corporate criminal liability in their respective countries;
- b) integrate all local regulatory compliance programs adopted by the NIS in accordance with legislation in force on corporate criminal liability.

The rules set out in the EGCP are integrated with the following:

- c) the provisions established in the Code of Ethics, which represents the Group's ethical principles that all Addressees are required to comply with;
- d) the provisions established in the Zero Tolerance Plan against Corruption adopted by the ENEL Group;
- e) the corporate governance provisions adopted by the NIS, which reflect legislation in force and international best practices;
- f) the internal control system adopted by the NIS;
- g) the provisions established in all local compliance programs adopted by the NIS to comply with local legislation on corporate criminal liability, and in all corresponding internal guidelines, policies or organizational documents.

2. STRUCTURE

The EGCP identifies:

- a) the arrangements for its adoption by the NIS and the corresponding update process;
- b) its dissemination to Addressees and training activities;
- c) the sanctioning regime in force in the event of a breach of any of its provisions;
- d) general control rules;
- e) the areas of activity to be monitored in relation to certain types of unlawful conduct (the "Areas Subject to Monitoring" or "ABM") — set out in Section 7 — which are generally regarded as criminal and could potentially be committed by the NIS, as well as the prevention of what ENEL considers a priority in conducting its business with honesty and integrity (the "Offenses");
- f) the main rules of conduct relating to the Areas Subject to Monitoring.

The EGCP is complemented by Annex 1, titled "Examples of Unlawful Conduct in the ABM."

3. ADOPTION, IMPLEMENTATION, RESPONSIBILITY AND CORRESPONDING AMENDMENTS

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

The board of directors or other governing body of each NIS, in accordance with its autonomy and independence:

- i. adopts the most appropriate measures for the implementation and oversight of the EGCP, taking into account the size and complexity of the activities carried out, the internal control system, as well as the specific risk profile of the NIS and its regulatory framework;
- ii. is responsible for the correct implementation of the Areas Subject to Monitoring and the main rules of conduct, as set out in Section 10.2 of the EGCP, as well as for the oversight provided by the Enel Global Compliance Program.

The NIS will implement the EGCP in accordance with applicable legislation, the type of activity they carry out, and the specific characteristics of their organizational structure.

Enel S.p.A.'s internal board committees evaluate amendments or additions to the Enel Global Compliance Program and submit them for approval by the Board of Directors. Any modifications or additions to the EGCP will subsequently be submitted to the relevant board of directors or governing body of the NIS.

Each NIS must report any change or specific interpretation made in accordance with local legislation or practices. Likewise, the Board of Directors or relevant governing body of the NIS will designate the structure (person or body) responsible for supporting the implementation and oversight of the EGCP, as well as for carrying out the relevant controls, in compliance with applicable regulations.

4 DISSEMINATION OF THE EGCP AND TRAINING ACTIVITIES

The EGCP will be available and downloadable from the ENEL Group Intranet.

Specific training activities will be carried out at the Country level for all personnel (including through e-learning) to ensure the dissemination and correct understanding of the EGCP, the ABM, and the types of conduct relevant to preventing such Offenses from being committed. Such training activities may also be organized as part of any training program adopted by an NIS in connection with compliance with local criminal law and local compliance programs.

5 COMMUNICATION TO THIRD PARTIES

Third Parties will receive information on the principles and content of the EGCP through appropriate and timely contractual documentation that will provide standard clauses which, depending on the activities governed by the contract, will be binding on the counterparty.

6 REPORTING OF COMPLAINTS BY EMPLOYEES OR THIRD PARTIES (WHISTLEBLOWING NOTIFICATION)

Corporate Addressees of the EGCP are required to report any possible misconduct, irregularity or breach of the Enel Global Compliance Program.

In compliance with applicable regulations and its "Whistleblowing Policy," ENEL has established a specific Reporting Channel, managed by the General Audit Department, designed to ensure the confidentiality of the identity of the whistleblower, of the persons named in the report, as well as of its content and related documentation. Reports may be submitted as follows:

- i. in writing, that is, through the website, or through the online reporting system available on the Group's website;
- ii. orally, by telephone, using the numbers indicated on the same website;
- iii. or through an in-person meeting, at the whistleblower's request, within a reasonable timeframe and using the channels mentioned above.

As already set out in this document, ENEL handles reports received within the timeframes provided for by applicable regulations, prohibits any form of retaliation, and guarantees that no act of retaliation will be taken as a result of a report.

ENEL applies disciplinary sanctions against:

(i) those who breach the protective measures for the whistleblower or other persons protected by the applicable law, or (ii) those who conceal or attempt to conceal the report; or (iii) those who breach the confidentiality obligations set out in applicable whistleblowing legislation; or (iv) those responsible for the failure to establish or properly manage reporting channels in accordance with the requirements set out in applicable whistleblowing regulations; or (v) those responsible for the failure to verify and analyze reports; or (vi) those who take retaliatory measures against the whistleblower or other persons protected by the applicable law, as a result of the same report; as well as (vii) the whistleblower or reporting party where it is established, even by a first-instance judgment, that they are criminally liable for defamation or slander, or civilly liable on the same grounds in cases of willful misconduct or gross negligence.

7 DISCIPLINARY SYSTEM

The relevant NIS functions will apply the appropriate disciplinary measures in the event of a breach of any rule of conduct set out in the EGCP, in accordance with the applicable sanctioning regime, under applicable rules or local compliance programs, and without prejudice to the protection afforded to employees under local legislation (e.g., the right of defense or the principle of adversarial proceedings). Disciplinary measures will be applied irrespective of the outcome of any potential criminal proceedings conducted by the competent judicial authority.

Contractual documentation will set out the appropriate sanctions, including, but not limited to, termination of contract, in accordance with applicable legislation, in the event of a breach by Third Parties of any of the provisions contained in the EGCP.

8 OFFENSES

The EGCP covers the following types of Offenses (hereinafter, "the Offenses," as described below):

- A. Bribery/corruption offenses
- B. Other offenses against public administration

- C. Accounting fraud
- D. Market abuse
- E. Terrorist financing and money laundering offenses
- F. Offenses against individuals
- G. Occupational safety and health offenses
- H. Environmental offenses
- I. Cybercrimes
- J. Copyright offenses
- K. Tax offenses

Section 10.2 below of the EGCP identifies the areas of activity that the NIS must monitor and the main applicable rule of conduct.

The list set out in section 10.2 does not exempt the NIS from carrying out their own risk assessment and defining the main rules of conduct, where deemed appropriate.

Accordingly, the NIS may identify:

- i. business activities that may pose a specific risk of committing an Offense, by carrying out an analysis of business processes, as well as of the possible ways in which crimes attributable to the types of offenses may be committed;
- ii. additional rules of conduct that all Corporate Addressees and (where expressly specified) Other Addressees must comply with in order to:
 - refrain from any behavior giving rise to any of the aforementioned Offenses; and
 - refrain from any behavior that, while not in itself constituting any of the aforementioned Offenses, could potentially develop into one of them.

9 EGCP CONTROL SYSTEM

The EGCP provides for the following two levels of control in relation to the Areas Subject to Monitoring:

- general control rules;
- main rules of conduct applicable to each ABM.

10.1 GENERAL CONTROL RULES

The NIS will adopt the following general control rules:

1. **segregation of duties:** the assignment of functions, tasks and responsibilities within an NIS is carried out in accordance with the segregation of duties, whereby no individual may execute an entire process alone (e.g., under this principle, no individual may automatically be responsible for carrying out an action, authorizing it, and subsequently verifying it); appropriate segregation of duties may also be ensured through the use of IT systems that grant access exclusively to identified and authorized Addressees to carry out certain operations;

2. **signing and authorization powers:** formal rules must be established governing the exercise of internal powers and signing powers. Signing powers will be consistent with the organizational and executive responsibilities assigned to each NIS representative;
3. **transparency and traceability of processes:** the identification and traceability of sources, information and controls carried out to support the formation and implementation of NIS decisions, as well as the management of financial resources, must always be guaranteed; appropriate storage of relevant data and information must be ensured, through information systems and/or paper records;
4. **appropriate management of relationships with Third Parties:**
 - (i) appropriate due diligence review of integrity requirements before entering into any type of relationship. The scope of each due diligence assessment (which may involve making inquiries through business contacts, local chambers of commerce, business associations, or internet searches, as well as verifying business references and annual financial statements) will be proportional to the actual or perceived risk that a potential partner, advisor or supplier does not meet the aforementioned requirements; in this regard, the following circumstances may be considered a "red flag":
 - the third party is located in a country which, according to international indices such as Transparency International's Corruption Perceptions Index, is known for widespread corruption, or in a country considered a "non-cooperative country" according to the FATF "blacklist" or other international lists prepared by international institutions concerning the global fight against terrorist financing and money laundering;
 - the third party is prohibited or has been prohibited from participating in tenders or contacting state-owned companies/public bodies/government agencies due to compliance investigations conducted by public authorities;
 - the third party is already subject to criminal prosecution;
 - the third party refuses to comply with the compliance program adopted by the company and does not adopt any code of conduct or similar rules;
 - the third party has a family relationship with a key official of the government agency or with a foreign official;
 - a public official is the owner, executive manager or principal shareholder of the third party;
 - the third party's company address is a virtual office;
 - the third party has an undisclosed beneficial owner.
 - (ii) supplementary controls in the event that any type of "red flag" arises during the due diligence phase;
 - (iii) periodic monitoring during the relationship to ensure that the counterparty continues to meet the requirements approved by the NIS; and
 - (iv) adoption of appropriate measures in the event that the Third Party fails to maintain such requirements or that any type of "red flag" arises during the contractual relationship, such as:
 - the third party insists on dealing directly with officials, without allowing the company's involvement;
 - the third party requests unusual advance payments;
 - the third party proposes to submit, or submits, inaccurate invoices or invoices for services that were not assigned to it or did not need to be performed;
 - the third party requests payments in cash or bearer instruments;
 - the third party requests that payments be made to it outside its own country, in a jurisdiction with no connection to the entities involved in or relevant to the transaction;
 - the third party requests that payments be made to an intermediary or another entity, or requests that payments be made to two or more current accounts;
 - the third party requests that funds be donated to a non-profit institution or foundation.

10.2 AREAS SUBJECT TO MONITORING AND MAIN RULES OF CONDUCT

A. BRIBERY/CORRUPTION OFFENSES

This type of Offense refers to offering, giving, soliciting or receiving money (or any other benefit, gain or advantage) with the purpose or intent of influencing the recipient (who may be an individual belonging to a private company or a public official) in a manner favorable to the third party paying the bribe or engaging in corruption.

Bribes consist of gifts or payments of money (other forms of bribery may include various goods, privileges, entertainment and favors) in exchange for favorable treatment.

The favorable treatment provided by the party being bribed could consist of:

- the briber's participation in an important contract (with a public administration or a private company);
- the award of a public tender;
- false testimony, favorable to the briber, given by a witness in a trial;
- a lenient report by a public official.

For more details, see the examples cited in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

- i. negotiation, execution and management of relevant contracts with all Parties (public administrations, companies, associations, foundations, etc.);
- ii. participation in public or private tenders;
- iii. management of relationships (other than contractual relationships) with community organizations and public administrations (e.g., with reference to health, safety and environmental requirements, personnel management and payment of taxes);
- iv. management of litigation (lawsuits, arbitration and out-of-court proceedings);
- v. selection of partners, intermediaries and advisors, as well as negotiation, execution and management of the corresponding contracts;
- vi. management of cash and financial resources;
- vii. management of non-profit initiatives;
- viii. management of gifts, entertainment and hospitality expenses;
- ix. reimbursement of employee expenses;
- x. personnel recruitment;
- xi. definition of incentives (e.g., Management by Objectives — MBOs) for NIS executives.

MAIN RULES OF CONDUCT

When doing business with private companies, as well as with public administrations, international, national, regional and local governments (the "Public Authorities"), the NIS and their representatives are committed to acting with integrity and honesty, and to complying with applicable legislation and regulations.

Corporate Addressees and Third Parties (under specific contractual clauses) are specifically prohibited from:

- a) offering money or granting any other type of advantage (promises of employment, etc.) to representatives of Public Authorities, as well as to individuals belonging to a private company, or to members of their family, with whom the NIS intend to establish or have already established a business relationship or, when dealing with representatives of Public Authorities, any other relationship that includes a request for public funds, the submission of a public authorization or permit, etc.;
- b) offering gifts, hospitality or other benefits to the persons mentioned in the preceding point, unless these are accepted practices in accordance with standard business customs. The following are not considered admissible, among others: (i) travel; (ii) gifts or entertainment offered to persons connected with tender processes in which an NIS or any ENEL group company participates. Only benefits constituting reasonable business courtesy are permitted, such as: (i) occasional low-value meals; (ii) occasional attendance at local sporting, theatrical or other cultural events; and (iii) low-value promotional items, such as pens, calendars or similar objects. Gifts offered — except low-value ones — must be documented to allow inspection in accordance with established internal controls;
- c) using cash as a means of payment except where regulations permit it (e.g., minor expenses);
- d) incurring promotional or sponsorship expenses, unless such expenses have been approved in advance and in writing by the competent function;
- e) making any type of donation to non-profit institutions, community service projects and professional associations unless such expenses have been approved in advance and in writing by the competent function;
- f) awarding services to Third Parties that are not sufficiently justified in relation to the NIS's needs;
- g) paying money to Third Parties that is not sufficiently justified in relation to the type of task to be performed and current local customs;

The NIS will assess the possibility of adopting appropriate organizational measures to prevent Addressees from engaging in any of the aforementioned activities. Likewise, the NIS will assess the possibility of adopting appropriate procedures to ensure that:

- h) appropriate evidence is kept with respect to significant relationships (e.g., administrative procedures aimed at obtaining an authorization, a license or similar act, joint ventures with public entities, processing of documents to obtain a certain public authorization) with Public Authorities and any significant business relationship;
- i) relationships with Public Authorities, when matters concerning the NIS's interests are at a standstill, are handled by at least two authorized Addressees;
- j) any personnel recruitment procedure is carried out exclusively based on a demonstrable, genuine business need; at least two functions will participate in the selection process, which will be based on criteria of objectivity, competence and professionalism, so as to avoid favoritism, nepotism and conflicts of interest;

- k) incentive plans for managers are adopted to ensure that the objectives set do not give rise to abusive conduct and, instead, are based on an achievable, determined, measurable outcome related to the time needed to achieve it;
- l) a realistic schedule is established for project planning;
- m) regarding expense reimbursement, the appropriate documentation — including original receipts for the payment of expenses or costs incurred — is submitted to the accounting department before payment and the subsequent payment or expense (or receipt thereof) is accurately described, being reflected in the accounting records of the relevant NIS.

B. OTHER OFFENSES AGAINST PUBLIC ADMINISTRATION

This type of Offense is mainly related to fraud against public institutions and occurs when a company uses a scheme or other deception to defraud the public entity or to obtain an economic advantage through false or fraudulent representations, promises or pretenses.

This type of Offense is usually related to the use of public funding and subsidies in a manner different from that provided for in the subsidy agreement.

This type of Offense may occur for a wide range of reasons, generally related to obtaining an economic advantage.

For more details, see the examples cited in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

- i. participation in public tenders and public procedures in general;
- ii. management of relationships with Public Authorities (e.g., with reference to health, safety and environmental requirements, personnel management and payment of taxes);
- iii. requests for public financing, grants, subsidies or guarantees granted by the Public Administration;
- iv. management of public financing received, grants, subsidies or guarantees obtained.

MAIN RULES OF CONDUCT

In addition to the main rules of conduct set out in section 10.2.A) above, Corporate Addressees and Third Parties (under specific contractual conditions) will refrain from:

- a) submitting false or altered documents, whether partially or wholly, when participating in public tenders;
- b) inducing Public Authorities in any way to make an incorrect assessment while reviewing applications for authorizations, licenses, permits, concessions, etc.;
- c) omitting relevant information in order to steer Public Authorities' decisions in favor of the NIS in relation to all the circumstances described in points a) and b) above;
- d) any type of conduct aimed at obtaining from the Public Administration any type of subsidy, financing, subsidized loan or any other similar disbursement, by presenting falsified financial statements or documents, or by omitting relevant information or, in general, through deception or fraud attempting to mislead the granting institution;

- e) using money received from Public Authorities as financing, contributions or loans for purposes unrelated to those for which they were granted.

Likewise, in order to apply the aforementioned rules of conduct, the NIS will assess the possibility of adopting appropriate organizational measures to ensure that:

- f) declarations submitted to national or international Public Authorities for the purpose of obtaining financing, grants or loans include only truthful information and are signed by authorized signatories, and, when such financing, grants or loans are obtained, they are properly recorded in the accounts;
- g) there is appropriate segregation of task controls, ensuring that the application, management and reporting phases regarding administrative procedures for obtaining financing, grants or loans are carried out by different Corporate Addressees within the organization;
- h) information gathering and analysis activities necessary for reporting are carried out with the support of the relevant functions;
- i) documentation and subsequent reporting carried out for the purpose of applying for financing, grants, loans and guarantees are approved at the appropriate hierarchical levels.

C. ACCOUNTING FRAUD

Accounting Fraud is a type of Offense that mainly consists of intentionally manipulating financial statements to create a false representation of a company's financial health to investors, creditors, shareholders and other stakeholders.

Accounting Fraud may occur for various reasons, including, but not limited to, the following:

1. continuing to obtain financing from a bank (for this purpose, financial statements could be altered to create a representation of financial health);
2. recording unrealistic profits or concealing losses;
3. concealing circumstances that could negatively affect the company;
4. causing an inflation of the share price;
5. concealing the creation of secret funds;
6. covering up wrongdoing (such as theft, committed by company managers);
7. omitting material facts that may mislead any interested party (e.g., stakeholders, creditors, stock exchange authorities, etc.).

For more details, see the examples cited in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

- i. preparation of documents intended for investors or the public (e.g., financial statements and periodic financial reports) concerning the NIS's assets and liabilities, income, expenses and cash flows, even where such documents are not periodic accounting documents;
- ii. management of relationships with external auditors and oversight bodies.

MAIN RULES OF CONDUCT

Non-Italian Subsidiaries must keep books, records and accounts that accurately and precisely reflect, with a reasonable degree of detail, all transactions and dispositions of company assets.

Non-Italian Subsidiaries will consider adopting appropriate measures, and the personnel assigned to maintain books, records and accounts must act appropriately to ensure that:

- a) data and information used to prepare periodic financial reports are accurate and diligently verified;
- b) all balance sheet items whose determination and quantification involve discretionary assessment are objective and supported by appropriate documentation;
- c) transactions are carried out in accordance with general or specific management authorizations;
- d) invoices, as well as other relevant documents related to transactions, are properly reviewed, recorded and filed;
- e) transactions are recorded as necessary to prepare financial statements, in accordance with generally accepted or applicable accounting principles or any other criteria applicable to such financial statements;
- f) access to such transaction records is permitted only under general or specific management authorizations.

Likewise, to ensure that complete and fair information is provided to the market, Non-Italian Subsidiaries may not engage in any conduct that prevents or, in any case, hinders control and audit activities by external auditors, by concealing documentation or using other fraudulent means.

Finally, Non-Italian Subsidiaries must make all communications to any public financial authority (as required by applicable local legislation) correctly, completely, appropriately and promptly, without in any way obstructing the performance of their duties, including during inspections (e.g., express denial, unreasonable refusal, obstructive conduct or lack of cooperation).

D. MARKET ABUSE

This category of Offenses mainly refers to three different types of conduct: (1) buying or selling financial instruments using information not available to the public ("Inside Information"), or unlawfully disclosing such information to third parties; (2) altering the price-setting mechanism of financial instruments by knowingly providing false or misleading information to influence the price of a financial instrument; (3) placing sell and buy orders that provide or are intended to (i) provide false or misleading signals regarding the supply, demand or price of financial instruments, (ii) fix the market price of one or more financial instruments at an abnormal or artificial level.

These types of conduct may occur to benefit the company, for a number of reasons, including, but not limited to, the following:

- deflating the share price of a given company before purchasing it;
- undermining the reputation of a rival company;
- altering the price of a certain financial instrument held in a portfolio before carrying out any related activity.

For more details, see the examples cited in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

- i. management of public information (e.g., with respect to investors, analysts and financial journalists and other media representatives) and organization of and participation in any type of meeting with the aforementioned Addressees;
- ii. management of Inside Information related to the Group's listed companies and relevant financial instruments (for example, new products, services and markets, periodic accounting data, forecast data and quantitative targets concerning the company's results, mergers and spin-offs, as well as new particularly significant commitments, such as, for example, discussions and agreements concerning the acquisition or sale of significant assets);
- iii. management of Inside Information related to energy derivatives (for example, information on the unavailability of facilities);
- iv. any type of transaction related to financial instruments held in a portfolio.

MAIN RULES OF CONDUCT

All Addressees are expressly prohibited from:

- a) using Inside Information to trade, directly or indirectly, financial instruments in order to obtain personal advantages or to benefit Third Parties, the NIS, or any other Group company;
- b) disclosing Inside Information to Third Parties, except where required by law or other regulatory provisions or specific contracts in which the counterparties are required to use the information only for the purpose for which it was originally intended, while maintaining its confidentiality;
- c) advising or inducing a person, based on certain Inside Information, to carry out any type of transaction in financial instruments;
- d) disclosing false or misleading information through the media (about the company or other companies), including the internet, or through any other means, in order to alter the price of shares, derivatives or any underlying activity supporting transactions already planned by the person disclosing the information in question;
- e) carrying out transactions in financial instruments (e.g., purchase or sale) in violation of market abuse rules.

E. TERRORIST FINANCING AND MONEY LAUNDERING OFFENSES

Terrorist financing involves soliciting, collecting or providing funds with the intent to use them to support terrorist acts or organizations. The primary objective of individuals or entities involved in terrorist financing is to conceal the financing, as well as the nature of the activity being financed.

Money laundering is the process by which proceeds derived from criminal activities are disguised in order to conceal their illicit origin. More specifically, it may involve three different and alternative types of conduct: (i) the conversion or transfer of funds, knowing that they represent proceeds derived from criminal activity; (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of, or rights with respect to, property, knowing that such property represents proceeds derived from criminal activity; and (iii) the acquisition, possession or use, knowing, at the time of receipt, that such property represents proceeds derived from criminal activity.

When the proceeds of criminal conduct are created by the same person who conceals their illicit origin, in certain countries such conduct is punishable as self-laundering.

Money laundering and terrorist financing often display similar characteristics, mainly related to the concealment of money. Money launderers channel illicit funds through legal channels to conceal their illicit origin, while those financing terrorism transfer funds — which may originally be legal or illicit — while concealing their source and ultimate use, which is to support terrorism.

These types of conduct may occur to benefit the company, for a number of reasons, including, but not limited to, the following:

- obtaining income or any other advantage derived from illegal activities carried out by the terrorist organizations financed (other advantages may consist of protection of the company in countries where such organizations have significant influence);
- concealing the illegal origin of proceeds derived from criminal activities.

For more details, see the examples cited in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

1. financial or commercial transactions carried out with individuals or corporations (and legal entities directly or indirectly controlled by the aforementioned parties) that are resident or have a registered office in a country representing a high-risk, non-cooperative jurisdiction (e.g., with strategic deficiencies in its framework for combating money laundering and the proliferation of terrorist financing) in accordance with the assessment carried out by international authorities (e.g., FATF).

MAIN RULES OF CONDUCT

The NIS will condemn the use of their resources to finance or carry out any activity aimed at achieving objectives related to terrorist financing, as well as any misuse of financial instruments and transactions intended to conceal the origin of company funds.

More generally, the NIS will condemn any conduct that could be aimed, even indirectly, at facilitating the offenses of receiving, laundering or using capital, assets or any other benefit of illicit origin; in this regard, the NIS undertakes to carry out all necessary controls, both prior and subsequent, to achieve this objective, likewise governing relationships with third parties through contractual provisions requiring compliance with applicable legislation on the matter.

In particular, the following is prohibited:

- a) using blank payment documents or cash for any collection, payment, or fund transfer transaction, etc.;
- b) making or receiving payments to or from anonymous current accounts or current accounts at banks located in high-risk jurisdictions;
- c) issuing or receiving invoices or issuing documents referring to non-existent transactions.

Likewise, to apply the aforementioned rules of conduct, the NIS must:

- d) carry out analytical checks of cash flows;
- e) verify the validity of payments, checking that the beneficiary is indeed the counterparty with which the contract was entered into;
- f) carry out a review of procedures, especially with regard to any transactions taking place outside the Company's normal processes;
- g) have evidence available for all transactions carried out;
- h) ensure the traceability of all financial transactions, as well as agreements or any other company investment or project;
- i) verify the economic consistency of such transactions and investments;
- j) check the international blacklist concerning terrorism and high-risk jurisdictions.

F. OFFENSES AGAINST INDIVIDUALS

The expression "offenses against Individuals" refers to various types of offenses that often involve personal injury, the threat of physical assault, or other actions committed against a person's will.

In any case, for purposes of this EGCP, Offenses against Individuals mainly refer to offenses that are more likely to occur in the administration of a company, such as those relating to forced labor practices, which mainly consist of forcing employees to work through violence or intimidation, or through other means such as withholding identity documents.

This type of Offense may occur for a number of reasons, including, but not limited to, the following:

- employing labor at minimal cost;
- employing fully subservient labor that could not refuse any request.

For more information, see the examples set out in Annex 1.

AREAS SUBJECT TO MONITORING

In relation to this type of Offense, the following areas must be monitored:

- i. entering into contracts with suppliers that do not use specialized personnel, or operating in countries where human rights are not fully protected by international or local legislation.

MAIN RULES OF CONDUCT

Non-Italian Subsidiaries must:

- a) select external Third Parties (e.g., partners, suppliers), especially those providing non-technical services, only after carefully verifying their reliability;
- b) prepare accurate contractual documentation with external contractors, requiring them, and requiring their subcontractors, to comply with applicable local and international legislation (e.g., ILO conventions on minimum working age and the worst forms of child labor) on forced labor, protection of child and women's labor, and compliance with hygiene and health conditions;
- c) include and apply contractual sanctions in the relevant contract should a contractor or any of its subcontractors breach any applicable local or international laws.

G. OCCUPATIONAL SAFETY AND HEALTH OFFENSES

Occupational safety and health offenses are usually related to non-compliance with local legislation and workplace labor standards aimed at preventing accidents and occupational illnesses.

These types of conduct may occur to benefit the company, for a number of reasons, including, but not limited to, the following:

1. reducing costs, since adopting the necessary measures entails additional costs for a company;
2. increasing productivity, since working without regard to precautionary procedures and policies could speed up the production process.

For more information, see the examples set out in Annex 1.

AREAS SUBJECT TO MONITORING

With respect to this type of Offense, the following areas must be monitored:

- i. compliance with applicable occupational safety and health regulations.

MAIN RULES OF CONDUCT

Regardless of the scope of local legislation on occupational safety and health, the NIS will promote and foster the protection of workplace safety, raising awareness of the risks and responsibilities associated with individual conduct.

To this end, notwithstanding compliance with applicable local occupational safety and health legislation, the NIS undertakes to adopt the necessary measures to protect the physical and moral integrity of its workers.

In particular, the NIS will ensure:

- a) compliance with the legislative provisions governing worker safety and health in the workplace as a priority;
- b) the assessment of worker risks, to the extent possible and thanks to advances in modern techniques, with the aim of protecting workers, choosing the most appropriate materials and safety equipment to eliminate or, where this is not possible, reduce risk at its source;
- c) that information and training for workers is comprehensive, up to date, and specific to the activity performed;
- d) periodic consultation with workers on matters concerning workplace safety and health;
- e) the application of an effective monitoring system to ensure the correct implementation of preventive measures. Any non-compliance or area for improvement detected during work activities or as part of periodic inspections will be addressed promptly and effectively;
- f) that the organization of work tasks is structured to protect the integrity of workers, Third Parties and the community in which the NIS operates.

To achieve the above, the NIS will allocate organizational, instrumental and financial resources to ensure full compliance with current provisions on the prevention of workplace accidents and to continuously improve worker safety and health in the workplace and appropriate preventive measures.

Corporate Addressees, each according to the role they play within the organization, must ensure full compliance with legislative provisions, company procedures and any other internal regulations aimed at protecting the safety and health of workers in the workplace.

H. ENVIRONMENTAL OFFENSES

Environmental offenses refer to a broad list of unlawful activities, including illegal trade in wildlife and flora, offenses related to water management, illegal trade and disposal of hazardous waste, and smuggling of substances that affect the ozone layer.

Environmental offenses typically affect the quality of air, water and soil, threaten the survival of species, may cause uncontrollable disasters, and pose a threat to the safety of a large number of Addressees.

Driven by enormous profits and facilitated by low detection rates and few convictions, criminal networks and organized crime groups are showing increasing interest in these unlawful transnational activities.

These types of conduct may occur to benefit the company, for a number of reasons, including, but not limited to, the following:

- reducing costs, since adopting the measures necessary to protect the environment often entails additional costs;
- increasing productivity, since working without regard to environmental issues could speed up the production process.

For more information, see the examples set out in Annex 1.

AREAS SUBJECT TO MONITORING

With respect to this type of Offense, the following areas must be monitored:

- i. compliance with applicable environmental legislation regarding the design, construction, management, maintenance, decommissioning/dismantling of plants, interconnections and distribution network infrastructure;
- ii. compliance with applicable environmental regulations in the provision of products and services related to energy, energy efficiency and electric mobility, both to residential customers and small, medium and large companies, as well as public sector entities; including the design, testing and development of electric mobility products and technological innovation.

MAIN RULES OF CONDUCT

In its activities, the NIS will follow the principle of protecting the environment. In particular, the NIS:

- a) contributes to raising awareness and disseminating information on environmental protection, and manages the activities entrusted to it in accordance with applicable legislation;
- b) promotes scientific and technological development aimed at protecting the environment and safeguarding resources by adopting modern environmental protection and energy efficiency systems during its operations;
- c) works to meet the expectations of its customers and shareholders with respect to environmental issues and adopts all appropriate means for protecting and preserving the environment, condemning any form of harm or damage to the ecosystem.

In contracts entered into with Third Parties where the Company's liability with respect to environmental regulations may arise, particularly regarding waste management and disposal, the Company will include provisions requiring such Third Parties to comply with applicable regulations and will provide for contractual sanctions in the event of a breach.

I. CYBER CRIMES

Cybercrimes may be of two types: those in which the target is a network or a computer, and those in which the offenses are carried out or transmitted by a computer.

For the purposes of the EGCP, Cybercrimes do not include offenses that may be facilitated by a computer-related crime such as fraud, theft, extortion, forgery and intimidation (e.g., intimidation or stalking over the internet).

Accordingly, Cybercrimes considered under the EGCP consist, for example, of:

- i. unauthorized intrusion into a protected network;
- ii. introduction of computer viruses into an information system;
- iii. interception of data from a computer network.

Cybercrimes may occur for various reasons, including, but not limited to, the following:

- stealing trade secrets from a rival company;
- compromising or damaging a rival company's computer system;
- obtaining confidential information about the market strategies of rival companies.

For more information, see the examples set out in Annex 1.

AREAS SUBJECT TO MONITORING

With respect to this type of Offense, the following areas must be monitored:

- i. digital activities carried out by Addressees, in both Information Technology and Operational Technology environments, including the use of resources such as the intranet, internet, corporate email, business applications, collaboration and data-sharing platforms, social media, and instant messaging tools;
- ii. management and protection of corporate devices (for example, workstations, smartphones, removable devices) and technology infrastructure (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, and management of privileged user profiles.

MAIN RULES OF CONDUCT

Non-Italian Subsidiaries will consider applying appropriate technical, physical and organizational measures to prevent, and all Addressees are required not to engage, for example, in:

- a) inappropriate use of personal credentials to access Information Technology and Operational Technology devices, systems or infrastructure;
- b) allowing unlawful access by Third Parties to such systems or infrastructure;
- c) the unauthorized exchange and disclosure of business information and data outside the company;
- d) unauthorized access to, extraction of, or modification of information and data;
- e) the use of personal or unauthorized devices to transmit or store company information or data;
- f) handing over company-provided devices to other persons;
- g) manipulating or altering configuration parameters of company devices or infrastructure;
- h) manipulating company systems, or the theft or destruction of files, data and programs;
- i) accessing corporate information systems without proper authorization;
- j) sending unsolicited communications (spam);
- k) connecting external devices (personal computers, peripherals, external hard drives, etc.) to company systems or infrastructure and installing software and databases without prior authorization;
- l) installing harmful software (e.g., worms and viruses) on Information Technology and Operational Technology systems or infrastructure;
- m) using unauthorized software and/or hardware that could be used to assess or compromise the security of company devices, systems and infrastructure (for example, systems to identify credentials, decrypt encrypted files, etc.).

In order to identify unusual conduct and potential vulnerabilities and weaknesses in company systems and devices, Non-Italian Subsidiaries will ensure periodic monitoring of activities carried out by NIS personnel on the company's information system, in accordance with applicable local legislation.

Likewise, the NIS will periodically remind Corporate Addressees of the correct use of the company devices, systems and infrastructure available to them, including through specific training sessions where necessary.

J. COPYRIGHT OFFENSES

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

For the purposes of the EGCP, copyright offenses mainly comprise conduct most likely to occur in the context of business management, such as the unlawful use of databases or software, and the unauthorized reproduction or distribution of protected materials, among others.

This type of Offense may occur for various reasons, including, but not limited to, the following:

- a) Lack of awareness: employees may infringe copyright unintentionally due to insufficient training on applicable regulations and the company's internal policies;
- b) Competitive pressure: in highly competitive markets, NIS could engage in the unauthorized use of copyrighted works in order to reduce development costs and gain business advantages.

Bad faith: employees who deliberately infringe copyright with the intention of harming a competitor of the NIS. For more information, see the examples set out in Annex 1.

AREAS SUBJECT TO MONITORING

With respect to this type of Offense, the following areas must be monitored:

- unauthorized use or disclosure of copyrighted works, research materials or content owned by third parties;
- 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 private domains and protected databases;
- infringements arising from outsourcing processes, joint venture agreements, or inadequate oversight of license agreements, content distribution rights or digital asset management under commercial agreements.

MAIN RULES OF CONDUCT

In addition to the main rules of conduct set out in section 9.2, section I) above, Non-Italian Subsidiaries will consider adopting appropriate technical, physical and organizational measures to prevent:

1. any unlawful use or public disclosure, through computer networks or any type of connection, of protected original works or parts thereof;

2. the use, distribution, extraction, sale or rental of database content in breach of the exclusive performance and authorization rights of the copyright holder;
3. the illegal download of any software without completing the appropriate contractual documentation;
4. the download of peer-to-peer software or any other software not directly related to the company's activity.

If the NIS has entered into a contract with external contractors for the performance of activities potentially affected by the risk of copyright infringement, such contract must contain provisions requiring compliance with applicable legislation and regulations.

Such measures must comply with the following pillars:

- respect for the copyright of third parties: obtaining the necessary authorizations before using protected materials, including images, videos, software and written content;
- compliance with internal policies and ongoing training: complying with internal policies regarding the use, licensing and protection of copyright, disseminating them within the organization, and promoting training programs updated in line with regulatory developments;
- internal oversight and reporting of infringements: fostering a culture of internal vigilance and encouraging employees to report any suspected copyright infringement or unauthorized use of protected content.

A proactive attitude must also be maintained with respect to all forms of intellectual property, including trademarks, patents and trade secrets. This involves:

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

K. TAX OFFENSES

Tax offenses comprise conduct carried out by a taxpayer that breaches provisions intended to protect the interests of the tax administration in exercising its assessment, control and tax collection functions.

From a criminal law perspective, tax offenses are mainly classified into three categories: declaratory offenses, document forgery, and offenses related to tax evasion:

- Declaratory offenses include: i) the filing of fraudulent returns through the use of invoices or other documents relating to non-existent transactions; ii) fraudulent returns through other schemes, 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;
- document forgery offenses consist of issuing invoices or other documents for non-existent transactions, with the aim of facilitating tax evasion;
- offenses related to tax evasion refer to non-compliance with applicable tax obligations.

Both declaratory and documentary offenses are considered offenses of specific intent, meaning that they require the subjective element of the offense to be aimed at evading income tax or value added tax.

Likewise, failure to meet the requirements established for accessing tax incentives or benefits granted under applicable legislation may constitute a tax offense.

AREAS SUBJECT TO MONITORING

In relation to this type of offense, the following areas must be specifically monitored:

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

MAIN RULES OF CONDUCT

In order to ensure fair, responsible and transparent taxation, the NIS are committed to acting with integrity and honesty, adopting an approach fully oriented toward compliance with applicable tax regulations in the countries where they operate. Likewise, they undertake to interpret such regulations responsibly, in order to mitigate tax risk and appropriately address the interests of all stakeholders.

To apply these standards of conduct, the NIS must:

- a. ensure honest and transparent conduct, in compliance with legislation and regulations, as well as internal procedures, in all activities related to accounting management, invoicing, maintenance of tax records, and tax management (including the preparation of returns and compliance with related obligations);
- b. verify the reliability of income tax and value added tax (VAT) return and payment forms, cross-checking them against accounting records, as well as the accuracy of the data recorded;
- c. verify the correctness of 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 amounts corresponding to income tax, VAT and withholdings certified by the company as a withholding agent have been correctly calculated and paid;
- f. confirm that economic and financial events with tax relevance correspond to actual, duly documented business events;
- g. ensure the complete, accurate and timely accounting record of invoices and other documents relevant for tax purposes;
- h. ensure the retention of mandatory records and documents by digital means that guarantee their availability and integrity;
- i. verify the integrity and accuracy of the data recorded on invoices, in accordance with what was contractually agreed with suppliers or customers, and in relation to the services actually rendered;
- j. ensure the utmost integrity, transparency and substantive and procedural correctness in transactions with other Group companies, ensuring that intercompany services are duly governed by contract and provided on market terms;

- k. define criteria for determining transfer prices, in accordance with applicable regulations;
- l. establish clear roles, duties and responsibilities regarding verification of compliance with the criteria adopted for transfer pricing;
- m. ensure the involvement of the relevant tax functions in assessing tax impacts and regulatory compliance in the context of extraordinary corporate transactions;
- n. verify compliance with procedures relating to the transfer and disposal of assets, ensuring their appropriate tax treatment;
- o. promote transparency, fairness and cooperation in relationships with tax authorities, including during audit processes. Likewise, encourage adherence to cooperative compliance regimes for those entities that meet local regulatory requirements, with the aim of strengthening institutional relationships;
- p. verify compliance with applicable regulatory requirements for offsetting direct and indirect taxes, as well as the accuracy and veracity of the certifications supporting tax credits.

10.3 FINAL PROVISIONS

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

ANNEX 1 EXAMPLES OF UNLAWFUL CONDUCT IN THE ABM

A. BRIBERY/CORRUPTION OFFENSES

Someone from the NIS:

- gives a gift to a public official to obtain the award of a tender;
- offers money to an official during an inspection at a plant to persuade them to "turn a blind eye" to certain irregularities;
- promises to hire an employee of a rival company in exchange for gaining access to confidential documents of that rival;
- offers money to a witness to persuade them to give false testimony in a trial in which the NIS is involved.

B. OTHER OFFENSES AGAINST PUBLIC ADMINISTRATION

Someone from the NIS:

- during the process of submitting documents or data to participate in a tender, provides false information to a Government Body in order to secure the award of the tender;
- misrepresents the NIS's financial and business situation in order to obtain public financing;
- by failing to comply with the subsidy agreement, misappropriates funds received from the public entity.

C. ACCOUNTING FRAUD

Someone from the NIS:

- fails to disclose significant losses incurred by the NIS in the financial statements;
- conceals the creation of secret funds by overstating the cost of advisory services received by the NIS.

D. MARKET ABUSE

Someone from the NIS (assuming the NIS is a listed company with respect to the first two examples):

- discloses Inside Information to a relative about an upcoming acquisition, inducing them to buy shares of the company;
- discloses false information about the NIS's financial situation in order to influence its share price;
- spreads false or misleading information about a rival company to harm its market reputation.

E. TERRORIST FINANCING AND MONEY LAUNDERING OFFENSES

Someone from the NIS:

- receives money from (or transfers money to) a company located in a tax haven or whose current account is held at a bank located in a tax haven, in order to conceal the criminal origin of such money;
- under the guise of paying a company for advisory services, transfers money to current accounts secretly held by an illegal organization that finances terrorist attacks;
- uses secret funds, the creation of which has been concealed by manipulating the company's financial statements, to finance political parties linked to terrorist organizations.

F. OFFENSES AGAINST INDIVIDUALS

Someone from the NIS:

- exploits a worker who is in a state of physical or psychological need;
- forces people to work, using threats, abuse of authority or violence;
- forces immigrant workers to work under threat of reporting them to immigration authorities.

G. OCCUPATIONAL SAFETY AND HEALTH OFFENSES

Someone from the NIS, acting in breach of applicable occupational safety and health legislation:

- fails to provide Personal Protective Equipment (PPE) in accordance with the risk assessment;
- fails to implement emergency measures in the workplace (organizational, training and technical measures);
- fails to provide workers with the necessary safety equipment and machinery;
- allows employees to work with machinery without instructing them on how to use it safely;
- fails to periodically subject workers to specialized medical examinations, as required by law, to monitor their health and assess whether the work they perform is harmful to them.

H. ENVIRONMENTAL OFFENSES

Someone from the NIS:

- fails to consider the impact on biodiversity when planning a plant expansion, harming the habitat of protected animal species and endangering their survival;
- operates a thermal power plant without regard for the legal thresholds for gas emissions, polluting the surrounding area;
- fails to properly dispose of company waste and, instead, organizes an unlawful waste disposal site;
- causes water pollution through improper use of the resource or improper use of water treatment systems;
- fails to properly manage atmospheric emissions, by not adopting appropriate prevention and control systems, thereby causing air pollution.

I. CYBER CRIMES AND COPYRIGHT OFFENCES

Within the NIS, the commission of cybercrimes or intellectual-property-related offenses will be considered to occur when a person:

- installs illegally copied software on work devices;
- gains access to a rival company's information system using malicious hacking techniques to steal information and trade secrets, and distributes malware to damage it.

J. TAX OFFENSES

Within the NIS, the commission of tax offenses will be considered to occur when a person, in order to evade income tax or value added tax (VAT):

- uses invoices or other documents relating to non-existent transactions, or declares fictitious liability items on their tax return;
- conceals or destroys documentation legally required to be kept, thereby preventing the reconstruction of income or turnover;
- issues invoices or other documents for non-existent transactions, for the purpose of enabling third parties to evade income tax or VAT;
- fails to pay taxes owed, using non-existent or improper tax credits as an offset mechanism.