Global Compliance Program
on
Corporate criminal liability

Table ofcontents

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 the business. It requires all Group personnel to operate with loyalty, correctness, transparency and strict compliance with domestic and foreign legislations 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 Company 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 ECGP 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

EGCP represents an opportunity to reinforce a proactive prevention of corporate criminal liability by strengthening the governance and internal control system and it is designed to support proper and legal conducts throughout the Group.

EGCP identifies the key standards of behavior expected from all Corporate Recipients and – where specified – from Other Recipients in order to:

(i) provide NIS with a standard set of rules aimed at preventing a corporate criminal liability in their own country;

(ii) integrate any local compliance program adopted by a NIS in accordance to any applicable law on corporate criminal liability.

The rules contained in EGCP are integrated by:

i. the provisions set out in the Code of Ethics, which represents the Group's ethical principles to which all Recipients are required to comply;

ii. the provisions set out in the Zero Tolerance of Corruption Plan adopted by the entire ENEL Group;

iii. the provisions of corporate governance adopted by NIS, reflecting the applicable legislation and international best practice;

iv. the internal control system adopted by NIS;

v. the provisions set out in any local compliance program adopted by NIS to comply with their own local legislations on corporate criminal liability and in any related guidelines, policy or internal organizational documents.

2. STRUCTURE

EGCP identifies:

a) the modalities of its adoption by NIS and relevant update process;

b) its dissemination to Recipients and training activities;

c) disciplinary system applicable in the event of breach of any provision contained therein;

d) general standards of control;

e) areas of activity to be monitored in relation to certain types of illicit behaviors (the "Areas to be Monitored" or "ABM") - as listed in Section 7 - which are broadly considered crimes and might be potentially committed by NIS and the prevention of which ENEL considers to be a priority to run its business with honesty and integrity (the "Crimes");

f) key standards of behavior connected to the Areas to be Monitored.

EGCP is then completed by Annex 1 regarding "Examples of illicit behaviors committed in the ABM".

3. ADOPTION, IMPLEMENTATION, RESPONSIBILITY AND SUBSEQUENT AMENDMENTS

EGCP has been approved by the Board of Directors of ENEL on 20 September 2016 and shall be approved by the board of directors, or other governing body, of NIS.

The Board of Directors or other governing body of each NIS, in compliance with their own autonomy and independence:

(i) adopts the most appropriate measures for the implementation and monitoring of EGCP, taking into account the size, the complexity of the activities carried out, the internal control system and the specific risk profile concerning the NIS and its regulatory framework;

(ii) is responsible for the correct implementation of the Areas to be monitored and the Key Standards of Behaviour, as set forth by section 9.2 of EGCP, as well as of the controls provided by Enel Global Compliance Program.

EGCP shall be applied by NIS in accordance with the applicable legislation, type of business they run, as well as to the specific features of their organizational structure.

Further substantive changes in and additions to EGCP shall be entrusted to the Board of Directors of ENEL and shall be thereafter approved by the board of directors, or other governing body, of Non-Italian Subsidiaries.

Each NIS will report changes or particular interpretations made in accordance with local legislation or customs.

The Board of directors/governing body of NIS shall identify the structure (individual or body) in charge of providing support in the implementation and monitoring of EGCP and of executing the related controls.

A specific reporting system for suspected or known violations of EGCP shall be identified by NIS.

4. DISSEMINATION OF EGCP AND TRAINING ACTIVITIES

EGCP shall be available and may be downloaded from ENEL Group's Intranet.

At Country level specific training activities shall be provided to all personnel (also through e-learning) to ensure the dissemination and correct understanding of EGCP, the ABM as well as the relevant behaviors to prevent the commission of the Crimes. These training activities can be organized also in the context of any training program adopted by a NIS in connection with compliance with local criminal law and local compliance programs.

5. COMMUNICATIONTOTHIRDPARTIES

Third Parties will be informed of the principles and contents of EGCP through proper contractual documentation which shall provide for standard clauses that, based on the activity regulated by the contract, shall be binding to the counterparty.

6. DISCIPLINARYSYSTEM

Proper disciplinary measures shall be applied by the competent NIS functions in the event of breach of any standard of behavior set out in EGCP, in accordance with the disciplinary system already in force, pursuant to applicable rules or local compliance programs and without prejudice for the protection afforded to employees under local legislation (e.g. the right to defense or the principle of an adversarial process).

The disciplinary measures shall be applied despite the results of any possible criminal procedure carried out by the relevant judicial authority.

Contractual documentation shall provide for adequate sanctions, including but not limited to the termination of the contract, in accordance with applicable laws in case of a breach of any provision contained in EGCP by Third Parties.

7. CRIMES

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

A. Bribery Crimes
B. Other Crimes against Public Entities
C. Accounting Fraud
D. Market Abuse
E. Financing of Terrorism and Money Laundering Crimes
F. Crimes against Individuals
G. Health and Safety Crimes
H. Environmental Crimes
I. Cyber Crimes
J. Copyrights Crimes

Section 9.2 below of EGCP identifies the areas of activity to be monitored by NIS and the applicable key standard of behavior.

The list included in paragraph 9.2. does not exempt Non-Italian Subsidiaries from carrying out their own risk assessment and definition of key standards of behaviour if deemed appropriate.

Therefore, NIS might identify:

(i) the business activities which may entail specific risk of committing a Crime through an analysis of business processes and the possible ways of commission attributable to the types of offences;

(ii) additional standards of behaviour which all Corporate Recipients and – where expressly specified – Other Recipients have to deal with in order to:

- abstain from any behaviour that gives rise to any of the Crimes described above; and
- abstain from any behaviour that, even though does not constitute itself any of the Crimes listed above, could potentially turn into.

8. EGCP's CONTROL SYSTEM

EGCP provides for the following two main levels of control in relation to the Areas to Be Monitored;

- general standards of control;
- key standards of behaviour applicable to each ABM.

9.1 GENERAL STANDARDS OF CONTROL

NIS shall comply with the following general standard of control:

- ☒ segregation of duties: the assignment of roles, tasks and responsibilities within a NIS is made in compliance with segregation of duties according to which no individual may autonomously perform an entire process (i.e. in accordance with this principle, no individual can be autonomously in charge of performing an action, authorizing it and subsequently check it); an adequate segregation of duties can be granted also using IT systems enabling only identified and authorized persons to perform certain transactions;
- ☒ power of signature and authorization: formal rules must be in place regarding the exercise of internal powers and powers of signature. Powers of signature shall be consistent with the organizational and managerial responsibilities assigned to each proxy holder within the NIS;
- ☒ transparency and traceability of processes: the identification and traceability of sources, information and controls carried out supporting formation and implementation of NIS's decision, as well as the management of financial resources must always be guaranteed; proper storage of data and relevant information must be guaranteed, through information systems and /or paper support.
- ☒ proper management of Third Parties' relationships:

  (i) appropriate due diligence on honourability requirements before any relationship is established. The extent of each due diligence assessment (which could include making enquiries through business contacts, local chambers of commerce, business associations, or internet searches and following up any business references and financial statements)

shall be proportional to the actual or perceived risk that any prospective partner, consultant or supplier can be not in possession of the above mentioned requirements; in this regard, the following circumstances can be considered red flags

- the third party is incorporated in a country that, according to international indices, such as the Transparency International Corruption Perceptions Index, is known for widespread corruption, or in a country which is considered as a "non-cooperative country" according to FATF blacklist or other international list prepared by international institutions in relation to the global fight against terrorism financing and money-laundering;

- the third party has or had been suspended to join tenders or enter into contract with state-owned companies/public bodies/governmental agencies due to compliance investigations carried out by the public authorities;

- the third party has been already subject to criminal proceedings;

- the third party refuses to comply with the compliance program adopted by the company and does not have in place any code of conduct or similar set of rules;

- the third party has a family relationship with a key officer of the government agency or with a foreign official;

- a public official is the owner, executive manager or major shareholder of the third party;

- the address of the third party's business is a virtual office;

- the third party has an undisclosed beneficial owner;

(ii) additional checks, in the event that, during the due diligence phase, any "red flags" come up;

(iii) periodical monitoring during the course of the relationship to ensure that the counterparty continues to meet the requirements approved by the NIS, and

(iv) appropriate measures to be applied in the event that a Third Party does not maintain these

requirements or any other "red flag" arise during the course of the contractual relationship such as:

- the third party insists on dealing with government officials by itself, not allowing any participation of the company;

- the third party requests uncommon advance payments;

- the third party offers to submit or submits inaccurate invoices or invoices for services which have not been assigned or have not been carried out;

- the third party requests payments to be made in cash, or bearer instrument;

- the third party requests payments be made outside its home country, in a jurisdiction that has no relationship to the entities involved in the transaction or to the transaction;

- the third party requests payment be made to an intermediary or to another 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.

9.2 AREAS TO BE MONITORED AND KEY STANDARDS OF BEHAVIOUR

A. Bribery Crimes

This type of Crimes refer to the offering, giving, soliciting or receiving of money (or any other profit, gain or advantage) for the purpose or with the intention of influencing the recipient (which can be an individual belonging to a private company or a public official) in any way that is favourable to the party which provides the bribe.

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

Such favourable treatments, which triggers the briber, may consist, for example, in:

- ☒ the engagement of the briber for a relevant contract (either with a public administration or a private company);
- ☒ the award of a public tender;
- ☒ a false deposition, favourable to the briber, by a witness in a trial;
- ☒ a lenient report by a public official.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) negotiation, execution and management of material contracts with any Party (Public Authorities, companies, associations, foundations, etc.);

(ii) participation to public or private tenders;

(iii) management of relationships – different from contractual relationships – with community organizations and Public Authorities (e.g. with reference to health, safety and environment requirements, management of personnel, payment of taxes);

(iv) management of disputes (lawsuits, arbitration, out-of-court proceedings);

(v) selection of partners, intermediaries and consultants and negotiation, execution and management of the relevant contracts;

(vi) management of cash and financial resources;

(vii) management of non-profit initiatives;

(viii) management of gifts, entertainments and hospitality expenses;

(ix) reimbursement of expenses incurred by employees;

(x) hiring of personnel;

(xi) definition of compensation incentives (e.g. MBOs) addressed to NIS' executives.

KEY STANDARDS OF BEHAVIOUR

In conducting business with private companies as well as public administrations, international, national, state and local governments (the "Public Authorities"), NIS and their representatives are committed to act with integrity and honesty and shall comply with all applicable laws and regulations.

Corporate Recipients and Third Parties (pursuant to specific contractual terms), are specifically forbidden to:

a) offer money or grant other benefits of any kind (promises of employment, etc.) to Public Authorities' representatives as well as to individuals belonging to a private company - or to members of their families (collectively, the "Private Individuals") - with which the NIS intends to engage in or already manages a business relationship with or, when dealing with Public Authorities' representatives, any other relationship including the request of public fund, submission of any public clearance or authorization, etc.;

b) offer gifts or entertainment activities to the individuals listed at lett. a) above other than what it is admitted according to standard corporate practice. Admitted gift and entertainment benefits include, but are not limited to: (i) modest occasional meals; [(ii) occasional attendance at local sports events, theatre or other cultural events]; and (iii) gifts of low nominal value such as pens, calendars, or other small promotional items. Gift and entertainment benefits that are not admitted include, but are not limited to: (i) weekend trips or trips with no longer duration; (ii) gift or entertainment involving parties, with whom a NIS or any other company belonging to ENEL's group is currently engaged in a tender, a competitive bidding process or other public proceedings. Gifts offered - except those of modest value - must be documented in order to allow the required inspections;

c) use cash as means of payment other then the cases allowed by regulations (e.g. petty cash);

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

e) make any contributions to non profit institutions, community service projects, and professional associations unless the expenses have been

approved, in advance, in writing by the competent function;

f) assign services to Third Parties that are not sufficiently justified in relation to the NIS needs;

g) pay money to Third Parties that is not sufficiently justified with regard to the kind of assignment to be performed and to local practices at the time;

The Non-Italian Subsidiaries shall evaluate the opportunity to adopt proper organizational measures for preventing any Recipient from carrying out any of the activities described above. Furthermore, NIS shall evaluate the opportunity to adopt adequate procedures in order to ensure that:

h) adequate evidence is given in relation to any material relationships (e.g. administrative proceedings aiming at obtaining an authorization, a license or similar act, joint ventures with public entities, submission of a filing to obtain a certain public clearance) entered with Public Authorities and any material commercial relationship;

i) relationships with Public Authorities, when issues concerning NIS' interest are at stake, are managed by at least two authorized persons;

j) any recruitment procedure is carried out solely on the basis of a real and demonstrable business need, the selection process involves at least two distinct functions and is based on criteria of objectivity, competence and professionalism aimed at avoiding favoritism or nepotism and conflict of interest;

k) management incentive plans are adopted in a way to ensure that the objectives set thereto do not to lead to abusive behaviour and are, instead, focused on a possible outcome, determined, measurable and related to the time required to achieve them;

l) in relation to the planning of projects, realistic timeframes are set;

m) in relation to expenses' reimbursement, proper documentation, including original receipts supporting the payment of the expenses or incurring the cost, needs to be submitted to the appropriate accounting department before payment and that the subsequent payment or expense (or receipt thereof) is accurately

described and reflected in the relevant NIS accounting records.

B. Other Crimes against Public Authorities

This type of Crimes mainly relates to fraud against public entities and occurs when a company executes an artifice or another illicit scheme in order to defraud a public entity or to obtain any economic advantage through false or fraudulent representations, promises or pretences.

Such type of Crimes are often connected to public funding and grants and occurs when a company claims for public funding or grants that it is not eligible for or misuse them in a manner different than outlined in the grant agreement.

This type of Crime can take place for a number of reasons, which are normally related to obtaining of any economic advantage.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) participation to public tenders and public procedures in general;

(ii) management of relationships with Public Authorities (e.g. with reference to health, safety and environment requirements, management of personnel, payment of taxes);

(iii) application for public funding, grants, subsidies or guarantees issued by Public Authorities;

(iv) management of the received public funding, grants subsidies or guarantees obtained.

KEY STANDARDS OF BEHAVIOUR

In addition to key standards of behaviour set out in paragraph 9.2. A) above, Corporate Recipients and Third Parties (pursuant to specific contractual terms), shall abstain from:

a) submit false or altered documents, either fully or in part, during the participation in public tender offers;

b) induce in any form Public Authorities to make a wrongful assessment during the examination of requests for authorizations, licenses, authorizations, clearances, concessions, etc.;

c) omit due information in order to direct in the NIS favor a Public Authorities' decisions in relation to any of the circumstances described at let. a) and b) above in favour of NIS;

d) any conduct aimed at obtaining from a Public Authority any type of grant, funding, facilitated loan or other disbursements of the same type, through altered or falsified statements and/or documents, or the omission of relevant information or, more in general, by means of artifice or deception, aimed at leading the grantee institution into error;

e) use money received from Public Authorities as funds, contributions or loans for purposes other than those for which they were granted.

Furthermore, in order to implement the behavioural standards described above, the Non-Italian Subsidiaries shall evaluate the opportunity to adopt proper organizational measures in order to ensure that:

f) all the statements rendered to national or international public authorities for the purpose of obtaining funds, grants or loans includes only true information and be signed by authorized signatories and, when said funds, grants or loans are obtained, these are appropriately accounted for;

g) proper segregation of duties controls are in place, ensuring that request, management and reporting phases in relation to public proceedings for the purpose of obtaining funds, grants or loans are managed by different Corporate Recipients within the organization;

h) the activities of collecting and analysing the information which are necessary for reporting purposes are carried out with the support of the competent functions;

i) the documentation and the subsequent reporting to be submitted in relation to the request of subsidies, grants, loans and guarantees need are approved by adequate hierarchical levels.

C. Accounting Fraud

Accounting Fraud is a type of Crime mainly consisting in intentionally manipulating financial statements to create a false representation of a company's financial health towards investors, creditors, shareholders and other stakeholders.

Accounting Fraud can take place for a number of reasons, including but not limited to:

- ☒ keep obtaining financing from a bank (for this purpose, one could alter the financial statement in order to create a representation of financial health);
- ☒ report unrealistic profits or to hide losses;
- ☒ hide circumstances which could affect negatively the company;
- ☒ cause the inflation of the share price;
- ☒ disguise the creation of slush funds;
- ☒ cover up misconducts (such as theft, carried out by company's managers);
- ☒ omitting material facts which may mislead any interested party (i.e. stakeholders, creditors, stock exchange authorities etc.).

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) drafting documents to be released to shareholders or to the public (e.g. financial statements, periodic financial reporting) regarding the assets and liabilities, revenues and expenses or cash flows of the Non-Italian Subsidiary, even if such documents are other than the periodical accounting ones;

(ii) management of relationships with the external auditors and supervisory boards.

KEY STANDARDS OF BEHAVIOUR

The Non-Italian Subsidiaries are required to keep books, records and accounts in a reasonable detail, duly and accurately also to

properly reflects the transactions and disposals of the assets of the companies.

The Non-Italian Subsidiaries shall evaluate the opportunity to apply appropriate measures and personnel assigned to keep books, records and account are required to properly act to ensure that:

a) data and information used for the preparation of periodic financial reporting are accurate and diligently verified;

b) all balance items, whose determination and quantification entail discretional valuations, are objective and supported by appropriate documentation;

c) transactions are executed in accordance with the management's general or specific authorizations;

d) invoices and other relevant documentation related to the transactions are properly vetted, recorded and stored;

e) transactions are recorded as necessary to permit the preparation of financial statements in conformity with the applicable or generally accepted accounting principles or any other criteria applicable to such statements;

f) access to such transactions records is allowed only in accordance with management's general or specific authorizations.

Furthermore, in order to ensure that complete and fair information is provided to the market, the Non-Italian Subsidiaries are prevented to perform any conduct which impedes and, in any case, obstructs the checking and auditing activities by the external auditors through the concealment of documentation or the use of other fraudulent means.

Finally, the Non-Italian Subsidiaries are required to make all communications towards any public financial authority (as provided for by the local applicable law) in a correct, complete, proper and expeditious manner, not preventing them, in any way, from performing their duties, even in the context of any inspection (e.g. express opposition, unreasonable refusal, obstructive conduct or failure in giving cooperation).

D. Market Abuse

This category of Crimes mainly refers to three different types of conducts: (1) sell or buy financial instruments using information which is not publicly available ("Inside Information") or illegitimately communicate them to third parties; (2) alter the price-setting mechanism of financial instruments by knowingly giving out false or misleading information in order to influence the price of a financial instrument; (3) execute sale and purchase orders which provide or are aimed at (i) providing false or misleading indications with regard to the offer, demand or price of financial instruments, (ii) set the market price of one or more financial instruments at an anomalous or artificial level.

These types of conducts can take place for the benefit of a company for a number of reasons, including but not limited to:

- ☒ deflate the share price of a target company before an acquisition;
- ☒ weaken the reputation of a competitor company;
- ☒ alter the price of a certain financial instrument in portfolio before carrying out any trading activity relating to it.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) management of public information (e.g. in relation to investors, financial analysts and journalists and other representatives of the mass media) and organization of and participation in meetings of any kind with the aforesaid persons;

(ii) management of Inside Information connected to listed companies and, particularly, listed companies of the Group and the relevant financial instruments (for example, new products/services and markets, period accounting data, forecast data and quantitative targets concerning corporate performance, mergers/de-mergers, and particularly significant new undertakings, i.e., talks and/or

agreements regarding the acquisition and/or sale of significant assets);

(iii) management of Inside Information connected to energy derivatives (for example information on plants' unavailability);

(iv) any kind of transactions relating to financial instruments in portfolio.

KEY STANDARDS OF BEHAVIOUR

Each Recipient is expressly prohibited to:

a) use Inside Information to negotiate, directly or indirectly, financial instruments to obtain personal advantage, or to favour Third Parties or a NIS or any other Group company;

b) disclose Inside Information to Third Parties, except when this is required by law, or other regulatory provisions or specific contracts in which the counter-parts are obliged to use the information only for the purpose originally intended and maintaining its confidentiality;

c) recommend or induce a person, on the basis of certain Inside Information, to carry out any kind of transactions on financial instruments.

Furthermore, each Recipient is expressly prohibited to:

d) spread false or misleading information through the media (whether about the company itself or about any other companies), including the Internet, or by any other means, just to alter shares' process, derivatives, or underlying activities which support already planned transaction by the subject which spreads the hereof information;

e) perform any transactions on a financial instrument (e.g. sale or purchase) against the market abuse regulations.

E. Financing of Terrorism and Money Laundering Crimes

Financing of terrorism involves the solicitation, collection or provision of funds with the intention to use them to support terrorist acts or organizations.

The primary goal of individuals or entities involved in the financing of terrorism is to conceal both the financing and the nature of the financed activity.

Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. More precisely, it may encompass three different, alternative conducts: (i) the conversion or transfer of funds, knowing that are proceeds of crime (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 is the proceeds of a crime; and (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime.

When the proceeds of a crime are created by the same person concealing their illicit origin, such a conduct is punished in certain countries as self-money laundering.

Money laundering and financing of terrorism often display similar transactional features, mostly having to do with concealment. Money launderers send illicit funds through legal channels so as to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is the support of terrorism.

These types of conducts can take place for the benefit of a company for a number of reasons, including but not limited to:

- ☒ obtain proceeds or any other advantage arising from illegal activities carried out by the terroristic organizations which have been financed (the other advantages may consist in protection of the business, in countries where such organizations are rather influential);
- ☒ disguise the illegal origin of criminal proceeds.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) financial or commercial transactions carried out with individuals or corporations - and legal entities controlled

directly or indirectly by the above-mentioned subjects – having their residence or a registered office in a country representing a high-risk and non-cooperative jurisdiction (i.e. with strategic deficiencies in their frameworks to combat money laundering and the financing of terrorism proliferation) according to the assessment made by international authorities (e.g. FATF).

KEY STANDARDS OF BEHAVIOUR

NIS shall condemn the use of its resources for the financing or execution of any activity aimed at reaching objectives associated with the financing of terrorism as well as any misuse of financial instrument and/or operation aimed at concealing the source of company's funds.

More generally, NIS shall condemn any possible conduct aimed at, even indirectly, facilitating offences such as receiving, laundering and use of money, goods or any other utility of unlawful origin; in this regard NIS is committed to implement all the requested preventive and subsequent control activities necessary to achieve that goal, regulating also relations with third parties by means of contractual provisions requiring the observance of the applicable laws on the matter.

In particular, it is specifically forbidden to:

a) use blank payment or cash for any operation of collection, payment, funds transfer et cetera;

b) make or receive payments on anonymous bank accounts or on bank accounts located in tax havens;

c) issue ore receive invoices or release documents in relation to non-existent transactions.

Furthermore, in order to implement the behavioural standards described above, the NIS must:

d) perform analytical controls of the cash flows;

e) verify the validity of payments, by controlling that its beneficiary actually is the counterparty involved in the transaction;

f) carry out procedural controls, in particular regarding possible transactions occurring outside the normal Company processes;

g) retain evidence of all of the transactions carried out;

h) ensure the traceability of every financial operation, as well as agreement or any other investment or business project;

i) verify the economic consistency of such operations and investments;

j) always check the international black list regarding terrorism and tax havens.

F. Crimes against Individuals

The term "crimes against individuals" refers to several types of criminal offenses which usually involve personal injuries, the threat of bodily harm, or other actions committed against the will of an individual.

However, for the purpose of this EGCP, Crimes against Individuals mainly refer to those crimes which can more likely occur in the management of a company such as those referring to forced labor practices, mainly consisting in coercing employees to work through the use of violence or intimidation, or by other means such as retention of identity papers.

This type of Crime can take place for a number of reasons, including but not limited to:

- ☒ employ workforce with minimal expenses;
- ☒ employ fully subservient workforce, to which no request would meet a refusal.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) entering into contracts with suppliers that utilize unskilled personnel and/or operating in countries where individual rights are not fully protected by international or local legislation.

KEY STANDARDS OF BEHAVIOUR

The Non-Italian Subsidiaries are required to:

a) select external Third Parties (e.g. partners, suppliers) – especially those providing for non-technical services – only after having accurately verified their reliability;
b) execute proper contractual documentation with external contractors requiring them to comply, and requiring their subcontractors to comply, with any applicable international and local legislation (e.g. ILO conventions on the minimum age for employment and on the worst forms of child labour) on forced labor, protection of child labour and of women and compliance hygienic-sanitary conditions;
c) implement and enforce any contractual penalties in the relevant agreement in the event of breach by a contractor or any of its subcontractors of any international or local legislation applicable .

G. Health and Safety Crimes

Health and safety crimes are mainly related to the non-compliance with local legislations and labor standards to be granted in the workplace in order to avoid employees' accidents and illnesses.

These types of conducts can take place for the benefit of a company for a number of reasons, including but not limited to:

- ☒ reduce costs, since the adoption of the required measures often entails additional expenses for a Company;
- ☒ increase productivity, given that working without considering precautionary procedures and policies might speed up the production process.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) compliance with applicable health and safety laws.

KEY STANDARDS OF BEHAVIOUR

Notwithstanding the local dimension of local legislation of health and safety in the workplace, NIS shall foster and enhance a strong culture of workplace safety protection, increasing awareness regarding risks and responsibilities of individual behaviours.

For this purpose, notwithstanding the compliance with applicable local legislation on health and safety in the workplace, NIS is committed to adopt all the necessary measures, in order to protect its workers' physical and moral integrity.

In particular NIS shall ensure that:

a) the respect of the provisions of law governing the safety and health of workers on the workplace is a priority;

b) the risks for workers, as far as possible and allowed by the best techniques' evolution, are evaluated with the aim of protection, also by choosing the most adequate and safe materials and equipment, in order to reduce the risk at the source;

c) the non-avoidable risks are correctly evaluated and adequately mitigated by the appropriate individual and collective safety measures;

d) the information and training of workers is widespread, up to date and specific with reference to the activity performed;

e) the workers are periodically heard on matters regarding health and safety on the workplace;

f) any non-compliance or improvement area, emerged during the working activity or during inspections, is timely and effectively considered;

g) the organization of the working activity is structured in order to protect the integrity of workers, Third Parties and the community within which the NIS operates.

In order to achieve the above, NIS assigns organizational, instrumental and economic resources both to ensure the full compliance with the current provisions of law on industrial accidents prevention and to continuously improve the health and safety of workers in the workplace and the relevant preventive measures.

Corporate Recipients, each according to the role within the organization, must ensure the full respect of the provisions of law, corporate procedures and of any other internal regulation aimed at protecting the safety and health of workers in the work place.

H. Environmental Crimes

Environmental Crimes refer to a broad list of illicit activities, including illegal trade in wildlife, water management crimes, illicit trade and disposal of hazardous waste substances and smuggling of ozone-depleting substances.

Environmental Crimes usually affect the quality of air, water and soil, threaten the survival of species and may cause uncontrollable disasters and might have a security and safety threat to a large number of people.

Led by huge financial gains and facilitated by a low risk of detection and scarce conviction rates, criminal networks and organized criminal groups are becoming increasingly interested in such illicit and more likely transnational activities.

These types of conducts can take place for the benefit of a company for a number of reasons, including but not limited to:

- ☒ reduce costs, since the adoption of the measures needed to safeguard the environment often entails additional expenses;
- ☒ increase productivity, given that working without considering the environmental issues might speed up the production process.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) compliance with applicable environmental laws in connection with the design, construction, management and maintenance of plants and related infrastructures.

KEY STANDARDS OF BEHAVIOUR

In its business, NIS shall follow the principle of safeguarding the environment.

In particular, NIS:

a) contributes to dissemination and awareness-raiseon environmental protection and manages the activities that are entrusted to it, in compliance with applicable legislation;

b) promotes scientific and technological development aimed at protecting the environment and safeguarding resources through the adoption in operations of advanced systems for safeguarding the environment and energy efficiency;

c) works to meet the expectations of its customers/stakeholders in relation to environmental issues and adopts all appropriate instruments for protection and preservation, and condemns any form of damage and harm to the eco-system.

In the agreements entered into with Third Parties where the Company's liability under environmental law may arise, concerning, in particular, waste management and disposal, the Company shall include provisions imposing to such Third Parties the compliance with applicable laws and shall provides for contractual sanctions in the event of violation.

I. Cyber Crimes

Cyber Crimes are criminal offenses that involve two separate categories of crimes: one in which the target is the network or a computer, and one in which crimes are executed or expedited by a computer.

For the purpose of EGCP, Cyber Crimes do not include those crimes that can be facilitated by a computer crime such as fraud, theft, blackmail, forgery and harassment (eg. cyber-bullying or cyber-stalking).

Therefore, Cyber Crimes considered by EGCP consist, for example, in: (i) unauthorized intrusion into a protected network; (ii) introducing computer viruses into a computer system; (iii) interception of data from a computer network.

Cyber Crimes can take place for a number of reasons, including but not limited to:

- ☒ steal a competitor company's business secret;
- ☒ jeopardy or damage a competitor company's computer system;
- ☒ obtain confidential information about competitor companies' market strategies.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) company activities carried out by Recipients using Intranet, Internet, the mail system or any other IT instruments;

(ii) management and protection of workstations;

(iii) management of storage devices;

(iv) planning of the measures to be adopted on telematics system and security, classification and processing of information and data;

(v) management of system administrators profiles.

KEY STANDARDS OF BEHAVIOUR

The Non-Italian Subsidiaries shall evaluate the opportunity to apply proper technical, physical and organizational measures in order to avoid and each Recipient is obliged not incur into:

a) an improper use of IT credentials;
b) the illicit access of Third Parties to the IT systems;
c) the unauthorized sharing of business information outside of the company;
d) the using of personal or unauthorized devices to transmit or store company information or data;
e) the tampering or alteration of the NIS's computer system;
f) the illicit pulling of NIS's data;
g) the tampering, theft or destruction of the NIS's information assets (files, data and programs);
h) the use of any lacks in the security measures of corporate information system for access to the information without proper authorization;
i) spamming practices;

j) the access to the NIS's computer systems of external devices (personal computer, peripherals, external hard drives etc.) and installation of software and databases without prior authorization;
k) the installation of harmful software (e.g. worms and virus);
l) the use of unauthorized software and/or hardware that could be used to evaluate or compromise the security of computer systems (e.g. systems to identify the credentials, decrypt encrypted files, etc.).

The Non-Italian Subsidiary, in order to identify unusual behaviour, potential vulnerabilities and deficiencies in corporate systems, shall ensure a periodical monitoring on the activities carried out by the NIS personnel on the corporate IT system, in compliance with the local applicable law.

Furthermore, the NIS shall periodically remind Corporate Recipients to use the IT tools in their possession appropriately, also through specific training sessions where needed.

J. Copyrights crimes

Copyright infringement might consist in the use of works (e.g. softwares, databases, videos, images) protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, including but not limited to the right to use, distribute or to develop derivative works.

For the purpose of EGCP, Crimes against Copyrights mainly refer to those crimes which can be more likely contemplated in the management of a company such as those referring to illicit use of softwares and data bases.

This type of Crime can take place for a number of reasons, including but not limited to:

- ☒ reduce costs, by refraining from paying for software licenses.

For further details, see the examples provided in Annex 1.

AREAS TO BE MONITORED

In relation to this type of Crimes, the following areas need to be monitored:

(i) company activities carried out by Recipients utilizing Intranet and any IT tool made available by the NIS.

KEY STANDARDS OF BEHAVIOUR

In addition to the key standards of behaviour set forth in paragraph 9.2 section I) above, the Non-Italian Subsidiaries shall evaluate the opportunity to adopt proper technical, physical and organizational measures in order to avoid:

1. any illegal use or dissemination to the public, through computer based networks or through connection of any type, of protected original work, or part thereof;
2. use, distribution, extraction, sale or lease of the contents of a database breaching the exclusive right of execution and authorisation from the copyright holder;
3. illegal download of any software without the execution of any proper contractual documentation;
4. the download of peer to peer software or any other software not directly connected to the corporate activity.

If the NIS has entered into a contract with external contractors for the performance of activities potentially affected by the risk of violating any copyrights rights, such contract must contain provisions requiring the compliance with applicable laws and regulations.