STATKRAFT ITALIA S.r.l.

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

adopted pursuant to

Legislative Decree no. 231 of 8 June 2001

GENERAL SECTION

Status of revisions			
Rev.	Subject	Approval	Date
00	1a First publication	BoD resolution	October 2023
	2a issue of the document reflecting organisational and regilatory changes	BoD resolution	March 19, 2026

CONTENTS

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS

DEFINITIONS

Code of Conduct: Code of Conduct adopted by the Company, which is binding for partners, suppliers and all the individuals and organizations acting on behalf of the Company. This Code of Conduct outlines the fundamental ethical values and rules for business conduct which the Company's entire personnel are required to observe in carrying out their activities.

Collective Bargaining Agreement or CBA: the Italian national collective bargaining agreement applicable to the Company's employees.

Corporate Entities: entities, companies and associations, including those without legal status, to which administrative liability may be attributed pursuant to Decree 231.

Decree 231 or **Decree**: Legislative Decree n. 231 dated 8 June 2001, published on Official Journal no. 140 of 19 June 2001 and subsequent amendments.

Disciplinary System: the set of sanctions or disciplinary actions applicable to Recipients in cases of non-compliance with the Decree 231 or Model 231.

Employees: each person employed by the Company.

Employment Act: Italian Law no. 300/1970

Guidelines: guidelines for the drafting of organizational, management and control models pursuant to the Decree 231 and published by Confindustria, as they were updated in June 2021.

Model or **Model 231**: systems and controls organisational model set up by Statkraft Italia, for the prevention of the Crimes and Administrative Offences, as it is provided by articles 6 and 7 of the Decree.

Procedures: the set of internal procedures, policies, guidelines and internal regulations adopted by Statkraft Italia to which all the Recipients are bound, that define the guidelines and rules to be followed by them in performing their business activities.

Recipients: (a) managers; (b) members of the board or other committees; (c) any other individual holding positions of representation, management or control of the company or a business unit of the institution or in any event de facto exercise management and control functions over the same; (d) employees or external associates who are under the direction and supervision of any one of the persons specified in (c).

Risk Areas: in the light of the analysis of the corporate context and the activities at potential risk of crime, have been identified:

a) The areas of activities that are "sensitive" to the committing of offences, i.e., the activities in the scope of which opportunities for committing the unlawful behaviours set forth in the Decree may hypothetically be created;

b) The processes that are "instrumental" to the commission of the offences set forth in the Decree, i.e., the processes within the scope of which, in principle, conditions and/or tools for committing offences could be created.

Statkraft Italia or **SKI** or **the Company:** Statkraft Italia S.r.l. with registered office in Via Caradosso, no. 9, 20123, Milan Italy

Supervisory Board or SB: *Organismo di Vigilanza*, *i.e.* the board established pursuant to article 6 of the Decree by resolution of the Board of Directors.

GENERAL SECTION

It should be noted that the Italian text of this Model shall be considered the official version and shall prevail in any case over the English text

1. INTRODUCTION

The Decree introduced into the Italian legal system the administrative liability of the Corporate Entities for offences committed in the interests of or for the benefit of the Company, by persons holding a top executive position therein or subordinate to such persons (art. 5 of the Decree). According to the requirements of the Decree, the Company has integrated and strengthened the Corporate Governance System long adopted by the Group to which it belongs and where required adapted it to comply with Italian laws and regulations.

The Model 231 has the aim to ensure an integrated system of controls and procedures aimed at minimising the risk of commission of illicit in the corporate context, being also a tool of communication of company's values and ethics towards internal functions (managers or employees) and external (clients, third parties, supplies, external partners).

Statkraft Italia – as an entity operating in renewable energy, particularly sensitive to compliance topics – has already adopted, in relation to the activities carried out in Italy, an integrated system of controls and procedures adequate to ensure the compliance with corporate strategies and the acquisition of effectiveness and correctness of business processes and ethical principles.

The Mode 231 is part of the system and controls regulating the performance of activities presenting risks profile with regard to criminal offences included in the scope of the Decree, through protocols and controls aimed at preventing behaviours of the corporate representatives which may be in contrast with the law.

This Model 231 is adopted on the basis of the Guidelines, as last amended in June 2021.

2. LEGISLATIVE DECREE NO. 231/2001

2.1 Requirements of the corporate vicarious liability

The Decree introduced in the Italian legal system the *"Discipline of administrative responsibility of Corporate Entities"*, thus adapting the Italian legislation to the European regulation.

Pursuant to article 5 of the Decree, in order for the vicarious liability to arise, the following conditions should be met:

(a) One of the criminal offences listed in the Decree has been committed;

(b) The criminal offence must be committed in the interest or for the benefit of the Corporate Entity;

(c) The individual who committed the offence is a manager of the entity (*Soggetto Apicale*) or a person subject to their direction and supervision (*Soggetto Sottoposto*).

More in detail, the Decree sets forth a vicarious liability for relevant offences committed in the interest or for the benefit of the company by:

- managers, executives and persons who hold positions of representation, management or control of the company or a business unit of the company or who in any event de facto exercise management and control functions over the corporate entity;
- individuals who are under the direction and supervision of any one of the persons specified above.

By "*interest*" and "*benefit*" two different concepts are meant, and the presence of only one of them is sufficient for the corporate entity to be held liable.

In particular:

(a) The **benefit** consists in the concrete acquisition of an economic gain for the entity;

(b) The **interest**, on the other hand, only implies that the illegal conduct is aimed at receiving such gain.

Consequently, vicarious corporate liability is excluded when the individual acted only for the interest of himself or of third parties (art. 5, para. 2 of the Decree).

Vicarious corporate liability and criminal liability of the individual are both assessed during the same proceedings before the criminal court.

The corporate entity may be held liable even if the individual who directly committed the misconduct was not identified, or if this person cannot be punished for any reasons (art. 8 of the Decree).

2.2 Penalties

The Decree provides for specific penalties that can be imposed to the Corporate Entities which are held liable for the administrative offence linked to the crime committed. In particular, the sanctions provided are the following:

(a) Monetary penalties, which are applicable to all the offences, and are quantified through a shares system (the number of shares may vary between 100 and 1000 and their value is between a minimum of Euro 258 and a maximum of euro 1.549,000. Furthermore, in cases provided by law, the monetary penalty is determined based on the specific percentage indicated for each offense of the entity's total global turnover for the financial year preceding the one in which the crime was committed or, if lower, the financial year preceding the application of the monetary penalty. When it is not possible to ascertain the entity's total global turnover, the monetary penalty is applied in the amount determined in relation to each offense;

(b) Industry Bans, which may last between 3 months and 2 years, and may consist of disqualification from carrying out business, prohibition from contracting with the Public Administration, suspension or revocation of authorizations, licenses, or concessions; exclusion from facilitations, financing, contributions and subsidies, and/or revocation of those already granted, prohibition from advertising goods or services. The ban sanctions may be applied only in the cases indicated by the Decree, if at least one of the following conditions is met:

(i) The Entity has derived a significant profit from the crime and the crime has been committed by persons in top positions, or by persons subject to the direction and supervision of others when the commission of the crime was determined or facilitated by serious organizational deficiencies;

(ii) In case of reiteration of the commission of the criminal offences.

In place of applying industry bans, the judge may order that the entities' activities are continued by a judicial commissioner.

(c) Industry bans can be applied to the Corporate Entity as a precautionary measure when there are serious elements to deem that the Corporate Entity is responsible for the commission of the crime and there are well-founded and specific elements that make it appear that there is a concrete danger that crimes of the same nature as the one being prosecuted will be committed (art. 45 of the Decree). Also in this case, instead of the ban precautionary measure, the judge can appoint a judicial commissioner to continue the activity if the Corporate Entity provides a service of interest to the community, or if the interruption of its activity could have significant repercussions on employment. In this case, any profit deriving from the continuation of the activity is subject to confiscation.

Failure to comply with the industry bans imposed constitutes an autonomous crime foreseen by the Decree also as a source of possible administrative liability of the Entity (art. 23 of the Decree).

(d) With reference to crimes against the Public Administration, in cases of conviction for one of the crimes indicated in paragraphs 2 and 3 of art. 25 of the Decree, the bans provided for in article 9, paragraph 2, are applied for a duration of no less than four years and no more than seven years, if the crime was committed by one of the top management representatives, and for a duration of no less than two years and no more than four years, if the crime was committed by one of the subordinates. In the latter case, if before the first degree judgement the Corporate Entity has effectively taken measures to (i) prevent the criminal activity from having further consequences, (ii) ensure the evidence of the offences and the identification of the persons responsible, or (iii) seize the sums or other benefits transferred, as well as having eliminated the organisational deficiencies that caused the offence by adopting and implementing organisational models suitable for preventing offences of the same type as the one that has occurred, the ban sanctions have the duration established by article 13, paragraph 2 of the Decree.

(e) Disgorgement of profits, also for equivalent amounts, of the price or profit of the crime, i.e., the utility obtained by the Entity in relation to the commission of the crime;

(f) Publishment of the judgement, which applies the sanction to the Corporate Entity;

2.3 The function of the Model 231 – Exemption from liability

With the intention of enhancing the preventive function of the system introduced, the legislator has foreseen the exclusion of liability in the event that the Corporate Entity has adopted and effectively implemented Model suitable for preventing offences of the same type of the one committed.

More in particular, pursuant to articles 6 and 7 of the Decree, Corporate Entities shall not be liable for the offence committed in their interests or for their benefit by a senior person if they are able to prove that:

- The management body had adopted and effectively implemented an organisational and management model able to prevent the commission of crimes of the type occurring prior to its commission;
- The task of monitoring the functioning and observance of the Model and of updating it was entrusted to a specific body with independent powers of initiative and control (i.e. the Supervisory Board – *Organismo di Vigilanza*);

- the persons committed the offence fraudulently breaching the Model 231[1], provided that this person is part of the top management;
- the offence was not committed as a result of non- or insufficient vigilance by the SB.

The Decree also provides that the Model shall:

(a) Identify activities in the context of which relevant offences may be committed;

(b) Provide specific protocols aimed at planning training acitivities and the execution of Corporate Entities' decisions with regard to offences that must be prevented;

(c) Identify procedures for the management of financial resources able to prevent the occurrence of situations favouring the commission of offences;

(d) Provide for information duties towards the Supervisory Board;

(e) Include an internal disciplinary system adequate to sanction the failure of complying with the measures indicated in the Model.

2.4 Criminal Offences listed in the Decree 231

As of today, the corporate vicarious liability may arise in relation to the following types of offences:

(a) Crimes against Public Administration (artt. 24 e 25)[2];

(b) IT Crimes and unlawful data processing (art. 24-*bis*)[3];

(c) Offences related to organised crime (art. 24-*ter*)[4];

[1] The fraudulent evasion of the 231 model is linked to the notion of acceptable risk, a key concept in the construction of a preventive control system. In the context of the 231 model, the conceptual threshold of acceptability for malicious offences is represented by a prevention system such that it cannot be circumvented except fraudulently. As clarified by case law (cf. Cass. Sez. V Pen. no. 4677 of 2014), the fraud alluded to by Legislative Decree no. 231/2001 does not necessarily require actual artifice and deception, which would in fact make it almost impossible to predicate the exemptive effectiveness of the 231 model. At the same time, however, neither can fraud consist in the mere violation of the prescriptions contained in the 231 model. It presupposes, therefore, that the violation of the latter is in any case determined by a circumvention of the "security measures", suitable for forcing their effectiveness.
For culpable offences, on the other hand, the fraudulent evasion of the 231 models appears incompatible with the subjective element (there is a lack of intention to cause damage, for example, to the physical integrity of workers or the environment). In these hypotheses, then, the acceptable risk threshold is represented by the implementation of a conduct in violation of the 231 model (and, in the case of crimes regarding health and safety, of the underlying obligatory fulfilments prescribed by the prevention regulations), despite the punctual observance of the supervisory obligations provided for by Legislative Decree no. 231/2001 by the Supervisory Board.
[2] As supplemented and amended, most recently, pursuant to Law no. 68 of May 22, 2015, as amended by Law no. 3/2019, and most recently by Legislative Decree no. 75/2020 implementing Directive (EU) 2017/1371 of the European Parliament and of the Council of July 5, 2017, "on the fight against fraud affecting the financial interests of the Union by means of criminal law".
[3] Introduced by article 7, Law no. 48 of March 18, 2008. More specifically, these are offences relating to computer falsification and certification relating to electronic signatures (articles 491-bis and 640-quinquies); offences against the security and integrity of data and systems (articles 615-ter, -quater, -quinquies ; 617-quater and quinquies ; 635-bis, ter, quater, quinquies of the Italian Criminal Code). With reference to the crime referred to in Article 491-bis the same was amended by Legislative Decree no. 7/2016, which decriminalized the computer forgery relating to acts between private individuals..
[4] Introduced by article 2, paragraph 29, of Law no. 94 dated July 15, 2009, subsequently amended by Law 69/2015. More specifically, these are crimes of criminal association aimed at enslavement, human trafficking or the purchase or sale of slaves (art. 416, para. 6 of the Italian Penal Code); mafia-type criminal association (art. 416-bis c.p.); mafia-style criminal conspiracy (art. 416-bis c.p.); political-mafia electoral exchange (art. 416-ter c.p.); kidnapping for the purpose of extortion (art. 630 c.p.); crimes committed by taking advantage of the conditions of subjugation and silence deriving from the existence of a
association aimed at the illegal trafficking of narcotic drugs or psychotropic substances (art. 74, Presidential Decree no. 309 of 9 October 1990); criminal association (art. 416 of the Italian Criminal Code).) offences of illegal manufacture, introduction into the State, sale, transfer, possession and carrying in a public place or a place open to the public of weapons of war or warlike weapons or parts of them, explosives, illegal weapons as well as more common firearms (art. 407, para. 2, lett. a) no. 5 of the Italian Criminal Code).

(d) Offences involving the counterfeiting of money, of public credit cards, of revenue stamps and falsification of distinctive marks (art. 25-*bis*)[5];

(e) Crimes against trade and industry (art. 25-*bis*.1)[6];

(f) Corporate offences (art. 25-*ter*)[7];

(g) Crimes committed to facilitate terrorism or to subvert the democratic order (art. 25-*quater*)[8];

(h) Female genital mutilation practices (art. 25-*quater.*1)[9];

(i) Crimes against individuals - related to slavery, trafficking of slaves, child prostitution, child pornography, and sexual exploitation (25-*quinquies*)[10];

(j) Crimes and administrative offences concerning Market Abuse (artt. 184 e 185 TUF) (art. 25-*sexies*)[11];

(k) Manslaughter or serious harm in violation of health and safety at workplace laws and regulations (artt. 589 e 590, para. 3 of the Italian Criminal Code) (art. 25-*septies*)[12];

[5] Introduced by art. 6 of Law no. 409 of November 23, 2001, containing "Urgent provisions in view of the introduction of the Euro" and subsequently amended (with specific regard to the cases covered by articles 473 and 474 of the Criminal Code) by art. 15 of Law no. 99 of July 23, 2009.

[6] Introduced by art. 15 of Law no. 99 of July 23, 2009. More specifically, these offences include: disturbance of the freedom of industry or trade (art. 513 of the Italian Penal Code); fraud in the exercise of trade (art. 515 of the Italian Penal Code); sale of non-genuine foodstuffs as genuine (art. 516 of the Italian Penal Code); sale of industrial products with misleading signs (art. 517 of the Italian Penal Code); manufacture and sale of goods made by usurping industrial property rights (art. 517 ter of the Italian Penal Code); counterfeiting of goods made by usurping industrial property rights (art. 516 of the Italian Penal Code).); Manufacture and commerce of goods made by usurping industrial property rights (art. 517 ter penal code); Counterfeiting of geographical indications or designations of origin of agro-food products (art. 517 quater penal code); Unlawful competition with threats or violence (art. 513 bis); Fraud against national industries (art. 514 penal code).

[7] The article was added by Legislative Decree no. 61/2002, amended by Law no. 190/2012, Law no. 69/2015, Legislative Decree no. 38/2017 and Law no. 3/2019. More specifically, these are the crimes of false corporate communications (art. 2621 civil code); minor facts (art. 2621-bis civil code); false corporate communications in listed companies (art. 2622 civil code); false prospectus (art. 2623 civil code); falsehood in the reports or communications of the Auditing Company (art. 2624 Italian Civil Code); impediment to control (art. 2625 Italian Civil Code); undue restitution of contributions (art. 2626 Italian Civil Code); unlawful distribution of profits and reserves (art. 2627 Italian Civil Code); unlawful transactions on shares or quotas of the company or of the parent company (art. 2628 c.c.); transactions to the detriment of creditors (art. 2629 c.c.); fictitious capital formation (art. 2632 c.c.); unlawful distribution of corporate assets by liquidators (art. 2633 c.c.); unlawful influence on the shareholders' meeting (art. 2636 c.c.); market rigging (art. 2637 c.c.); failure to communicate the financial statements of the company (art. 2637 c.c.); unlawful distribution of corporate assets by liquidators (art. 2633 c.c.). c.); failure to communicate a conflict of interest (art. 2629 bis c.c.); obstruction of the exercise of the functions of public supervisory authorities (art. 2638 c.c.); bribery among private individuals (art. 2635 c.c.) and incitement to bribery among private individuals (art. 2635-bis c.c.).

[8] Introduced by Law no. 7/2003.

[9] Introduced by Law no. 7/2006.

[10] Introduced by Law no. 228 of August 11, 2003 and subsequently amended by Legislative Decree no. 39/2014. More specifically, these are the crimes of reduction or maintenance in slavery and child pornography, namely: reduction or maintenance in slavery or servitude (art. 600 c.p.); child prostitution (art. 600-bis c.p.); child pornography (art. 600-ter criminal code); possession of pornographic material (art. 600-quater) tourist initiatives aimed at the exploitation of child prostitution (art. 600-quinquies criminal code); people trafficking (art. 601 criminal code); purchase and sale of slaves (art. 602 criminal code).

[11] Introduced by Law no. 62/2005, Law no. 262/2005 of Legislative Decree no. 107/2018. More specifically, these are the crimes of abuse of privileged information (art. 184 TUF) and market manipulation (art. 185 TUF).

[12] Introduced by Article 9 of Law No. 123/2007 Subsequently, Law No. 41 of March 23, 2016 increased the penalty provided for in Article 589 of the Criminal Code. (culpable homicide resulting from violation of accident regulations), bringing it to a maximum of 7 years.

(l) Receiving stolen goods, money laundering and use of unlawfully obtained money, assets or profits and self-money laundering (artt. 648, 648 *bis*, 648 *ter*, art. 648 ter.1 c.p.) (art. 25-*octies*)[13];

(m) Crimes committed by non-cash payments tools (art. 25-*octies.1*);

(n) Crimes against EU foreign policy and common security (art. 25-*octies*.2);

(o) Crimes regarding breaches of intellectual property (art. 25-*novies*)[14];

(p) Obstruction of justice (art. 25-*decies*)[15];

(q) Environmental crimes (art. 25-*undecies*)[16];

(r) Crime of employment of extra UE citizens without permission; (art. 25-*duodecies*)[17];

(s) Racial and xenophobic crimes (art. 25-*terdecies*)[18];

(t) Sport frauds; unlawful gambling (art. 25-*quaterdecies)*[19]*;*

(u) Tax crimes (art. 25-*quinquiesdecies*)[20];

(v) Smuggling (art. 25-*sexiesdecies*)[21];

(w) Offences relating to instruments of payment other than cash (art. 25-*octies*.1)[22];

(x) Crimes against the cultural heritage (Art. 25-*septiesdecies*)[23];

(y) Laundering of heritage assets and devastation and looting of cultural and landscape assets (Art. 25-*duovedecies*) [24];

(z) Crimes against animals (art. 25-*undevicies*)[25];

[13] Introduced by Legislative Decree no. 231/2007 and subsequently amended by Law no. 186/2014.
[14] Introduced by art. 15 of Law no. 99 of July 23, 2009.
[15] Introduced by Law no. 116/2009.
[16] Introduced by Legislative Decree No. 121/2011 and amended by Law No. 68/2015.
[17] Introduced by Legislative Decree No. 109/2012 and Law No. 161/2017.
[18] Introduced by Act No. 167/2017.
[19] Introduced by Act No. 39/2019.
[20] Introduced by Law no. 157/2019, which converted into law, with amendments, Law Decree no. 124/2019, containing "urgent provisions on tax matters and for unavoidable needs" and by D. Lgs. 75/2020 transposing Directive (EU) 2017/1371 of the European Parliament and of the Council of July 5, 2017, "on the fight against fraud affecting the financial interests of the Union by means of criminal law".
[21] Introduced by Legislative Decree 75/2020 transposing Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 "on the fight against fraud affecting the financial interests of the Union by means of criminal law".
[22] Introduced by Legislative Decree no. 184/2021.
[23] Introduced by L. no. 22/2022.
[24] Introduced by L. no. 22/2022.
[25] Introduced by L. no. 82/2025.

(aa) Transnational crimes regarding matters of organised crimes; migrants smuggling; obstruction of justice (art. 10, Law. 16 March 2006 no. 146)[26].

With regard to the other types of offences, whose risk of commission has been estimated to be low as a result of the Risk Self-Assessment conducted, the Company has in any case adopted a series of organisational and procedural measures aimed at ensuring the correct performance of company activities, which are in theory suitable for minimising the risk of committing such offences, referring first of all to the set of values and principles contained in the Code of Conduct as well as to the Procedures established with specific regard to the prevention of the offences indicated in the Special Part of the Model.

The Corporate Entity is also liable for administrative offences related to attempted crimes: in this case, pecuniary sanctions and bans are reduced by between one third and one half, while the imposition of sanctions is excluded in cases where the Entity voluntarily prevents the action from being carried out or the event from taking place.

2.5 Criminal Offences committed abroad

Pursuant to art. 4 of the Decree, the Corporate Entity may be held liable in Italy in relation to crimes listed in the Decree even if they are committed abroad, provided that the State of the place where the act was committed does not take action against it.

The prerequisites on which the Entity's liability for offences committed abroad is based, as provided for by Law no. 146 of 16 March 2006 and by the Decree are the following:

(a) The crime was committed abroad by a subject functionally connected to the Corporate Entity (art. 5, para. 1 of the Decree);

(b) The Corporate Entity has its main premises in Italy (art. 4 of the Decree);

(c) The Corporate Entity is liable for specific offences and only if conditions provided for by articles 7, 8, 9, 10 of the Italian Criminal Code are met, provided that this is requested by the Ministry of Justice also against the Company.

3. COMPANY'S GOVERNANCE

3.1 The Group and the Company

Statkraft Italy is part of the Statkraft Group, founded in Oslo and wholly owned by the Norwegian state. The Statkraft Group is a generator of energy from renewable sources since 1895, as well as the largest energy producer in Norway and the third largest in the Nordic region. Statkraft develops and generates hydropower, wind energy, gas and district heating, and is also a player in international energy markets. The Group is headquartered in Oslo and operates in approximately 19 countries.

[26] Introduced by Law no. 146/2006 which, in ratifying the Convention and Protocols of the United Nations against transnational organized crime adopted by the General Assembly on 15 January 2000 and 31 May 2001, has provided for the responsibility of entities for the transnational crimes of criminal association (art. 416 c.p.); mafia-type criminal association (art. 416-bis form of induction not to make statements or to make false statements to the Judicial Authority and personal aiding and abetting (art. 377-bis and 378 c.p.). A transnational crime is considered to be a crime punishable by imprisonment of no less than a maximum of four years, if
years, if an organized criminal group is involved in it and it is committed in more than one State, or it is committed in one State, but a substantial part of its preparation, planning, direction and control takes place in another State; or it is committed in one State, but an organized criminal group engaged in criminal activities in more than one State is involved in it; or it is committed in one State but has substantial effects in another State.

In this context, Stratkraft Italia, established in 2019 and headquartered in Milan, carries out, directly or through subsidiaries (SPVs), activities in the promotion and development (as well as eventually also the construction and operation) of renewable energy plants in the, wind, storage and solar sector on an industrial scale in the Italian territory.

Statkraft Italia's share capital is fully subscribed and paid-up by the Norwegian company Statkraft European Wind and Solar holding A.S is subject to management and coordination pursuant to Article 2497-bis of the Italian Civil Code by Statkraft A.S.

The Company's corporate governance system is structured as follows:

(a) Ownership: 100% by the Norwegian-registered company Statkraft European Wind and Solar holding A.S, the sole shareholder owning the share capital.

(b) Shareholders' Meeting: is competent to decide on matters reserved to it by law and the Company's Articles of Association. For the manner in which shareholders' meetings are convened and decisions are made, please refer to the provisions of the Articles of Association.

(c) Board of Directors: vested with all powers of ordinary and extraordinary administration except for those reserved to shareholders in accordance with the provisions of the Company Bylaws.

(d) *Statutory auditor:* the statutory audit of the accounts is entrusted to an external firm. The auditing firm carries out the audits required by auditing standards to express an opinion on the appropriateness of the financial statements to give a true and fair view of the company's economic and financial situation, as well as on the correctness of the administrative and accounting procedures adopted by the company.

Statkraft Italia also has intercompany service contracts in place, which formally regulate the provision of services within the Group, ensuring transparency in the objects of the services provided and the relative fees.

3.2 Power of attorney and proxies system

The autonomy, power of attorney and financial limits, assigned to the various holders of proxies and powers of attorney within the Company, are always identified and fixed in a manner consistent with the hierarchical level of the recipient of the proxy and power of attorney, within the limits of what is necessary to carry out the tasks and duties subject to delegation. According to the system of proxies with which the Company is equipped, the representation of the Company is delegated to single subjects, with the power to sign individually and/or jointly, for the performance of specific activities (for further information on the identification of these activities, reference should be made to the Company's Business Description).

In the event of investigations for a predicate offense against one of the legal representatives, the non-investigated director or an ad hoc attorney shall arrange for the entity to be provided with a defense counsel, different from the defense counsel of the legal representatives.

3.3 Manual and IT procedures

As part of its organisational system, the Company has adopted a system of manual and IT Procedures aimed at regulating the performance of corporate activities, also in compliance with the principles indicated in the Guidelines.

In particular, the Procedures already adopted and their subsequent additions or amendments describe the rules of conduct that must be followed by internal resources in the various processes, providing for the necessary control points for the correct performance of corporate activities.

These operating procedures ensure compliance with the following principles:

(a) encourage the involvement of more than one person in order to achieve an adequate separation of duties;

(b) adopt measures to ensure that every operation, transaction and action is verified, documented, consistent and appropriate;

(c) document the control phases carried out with reference to the individual operations and/or actions performed.

The Procedures, in addition to being disseminated to the functions concerned through specific communication and, where necessary or appropriate, training, are collected and made available to all company subjects by means of publication on the company intranet and/or distribution of the relative documentation/manuals.

4. METHODOLOGY

4.1 The project of drafting Statkraft Italia's Model 231

Statkraft Italia, in order to ensure fairness and transparency in the management of its activities considered it a priority to prepare and adopt the Model 231 which, together with the Procedures and the other policies and provisions issued by the Company, constitutes the internal system of controls to ensure effective prevention and detection of any possible violation of the law.

4.2 The objectives of the Model 231

The purpose of the Model 231 is to establish procedures for the activities that trigger a criminal (with particular regard to one of the Relevant Offences), in order to prevent such offences from being committed.

The Model 231 has therefore the function of:

(a) Identifying the activities carried out by each function, which due to their particular type may trigger a criminal risk pursuant to the Decree;

(b) Analysing the potential risks with regard to the possible ways in which crimes may be committed in relation to the internal and external operating context in which the Company operates;

(c) Evaluating the existing system of preventive controls and adapting it to ensure that the risk of commission of offences is reduced to an "acceptable level", i.e., a level that is suitable for excluding the perpetration of one of the underlying

offences set forth in the Decree by the Company's top management and employees;

(d) Defining a system of rules that sets out the general lines of conduct, as well as specific organizational procedures aimed at regulating activities in so-called "sensitive" sectors;

(e) Defining a system of authorisation and signatory powers that guarantees accurate and transparent representation of the process of forming and implementing decisions;

(f) Defining a control system capable of promptly reporting the existence and emergence of general and/or specific critical situations;

(g) Defining a communication and training system for employees that makes the Code of Conduct, authorization powers, hierarchical reporting lines, Procedures, information flows and everything that contributes to the transparency of the activity known;

(h) Establishing and assigning to a Supervisory Board specific responsibility for monitoring the effectiveness, adequacy and updating of the Model;

(i) Defining a system of sanctions for violations of the provisions of the Code of Conduct and of the Procedures and Protocols foreseen by the Model.

The updating and the implementation of the Model is aimed not only at allowing the Company to benefit from the exemption provided for by art. 6 of the Decree, but also, and primarily, at improving the internal control system, significantly limiting the risk of committing the offences provided for by the Decree 231.

The Model 231, together with the Code of Conduct, constitutes the way for icreasing the awareness within all the Company's Stakeholders, and aims at determining a full awareness in these subjects of the seriousness in case of commission of an offence and of the criminally relevant consequences not only for themselves, but also for the Company, allowing them, in the presence of such situations, to act promptly and effectively.

4.3 The drafting of the Model

The Company has completed a project aimed at adopting and implementing the Model and, to this end, has carried out a series of preparatory activities, divided into phases, aimed at developing a risk prevention and management system.

In particular, here below are summarised the phases of the project, from the identification of the Risk Areas to the subsequent updating of the Model.

(a) Phase 1: Analysis of the Risk Areas

In this phase the collection of documentation and information aimed at knowing the activities and the organization of the Company took place.

(i) In particular, in this phase were carried out the collection and analysis of internal documentation such as, but not limited to, organization charts, delegations and procedures, policies, visas, CBA ect.;

(ii) **Outcomes:** as an outcome of this phase, a plan of interviews with key officers was prepared, as well as the preliminary mapping of the risk areas.

(b) Phase 2: Risk Assessment

This phase was carried out according to the *Control Risk Self-Assessment* (CRSA) techniques.

(i) The following activities were carried out as part of this phase: (i) confirmation by the management of the corporate processes and areas most exposed to the risk of irregularities and identification of additional areas/processes at risk; (ii) assessment by the management of the risk associated with each risk area identified pursuant to the Decree; (iii) identification and/or confirmation of the organizational changes necessary and appropriate for the purposes of the Decree for more effective protection against the relevant risks; (iv) analysis of the control system in place in each sensitive activity identified during the Control & Risk Self-Assessment activities;

(ii) **Outcomes:** as an outcome of this phase, the Risk Areas were mapped as well as the relevant activities and the Document of *Risk Self Assessment* (potential risk / control level / nett risk) was prepared.

(c) Phase 3: Gap Analysis and Action Plan

This phase was carried out as follow:

(i) Following the results that emerged from the Risk Self-Assessment activity, the following activities were carried out with respect to the relevant control principles, market benchmarks and best practices: (i) identification and/or confirmation of the organisational changes necessary and appropriate for the purposes of the Decree, for more effective protection against the relevant risks; (ii) company-wide self-assessment of the adequacy of the design of the internal control system by some members of the company management; (iii) more detailed critical analysis for each relevant activity at risk pursuant to the Decree, of what was highlighted during the previous phase and of the design of the internal control systems in place;

(ii) **Outcomes:** as an outcome of this phase, the Gap Analysis of the internal control system was prepared as well as a detailed Action Plan referred to the corrective actions needed.

(d) Phase 4: Drafting of the Model

The outcomes of the mentioned activities are summarised in the present Model, which is indeed based on such activities and on market benchmark and best practice.

These phases have been scrupulously followed – with the exception of the gap analysis, during the updating of this Model (in the course of the year 2025).

5. THE STRUCTURE OF THE MODEL

5.1 General and Special Sections

The Company has decided to draw up a Model which, on the basis of its own experience and the indications deriving from case law on the subject, constitutes adequate protection against the possibility of the commission of offences, in line with the system of governance and ethical values which have always inspired the Company.

The Model consists of a General Section and a Special Section.

(a) The General Section is aimed at defining general principles that the Company sets as reference for the management of its own activities and that are applicable to the Company business, not only in relation to risk activities. The following parts are summarized or attached hereto and form an integral part thereof:

(i) Code of Conduct;

(ii) List of the relevant offences

(iii) Organisational chart

(b) The Special Sections, which identifies the control system for the prevention of criminal offences.

In particular, the Special Sections have the function of:

(i) Identifying the control system with particular reference to:

a) The principles of conduct;

b) General protocols of control;

c) Specific control protocols to be followed by the individual departments in carrying out their activities.

(ii) Establishing information flows towards the Supervisory Board.

Statkraft Italia's Model 231 is constituted by the following Special Sections:

A. PROCUREMENT
B. PERSONNEL
C. DEVELOPMENT
D. COMMUNICATION, REPRESENTATION EXPENSES, VALUE-SHARING MECHANISMS
E. ACCOUNTING, TAXATION, CORPORATE TRANSACTIONS AND FINANCIAL FLOWS
F. IT SYSTEMS
G. LEGAL AND REGULATORY SUPPORT

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS

H. HEALTH AND SAFETY AT WORK

I. ENVIRONMENT

J. CONSTRUCTION

(c) all the Procedures and Policies adopted by the Company and existing at a Group level, which are a prerequisite and an integral part of this Model, being aimed at preventing the risk of offences, and which have been the subject of specific information and training activities directed at the Recipients, each one in relation to the function exercised.

The Model has been structured in this way in order to ensure the more effective drafting process. In fact, if the General Part contains the formulation of principles of law that are considered substantially invariable, the Special Part, in consideration of its particular content, is instead susceptible to periodic updates.

Moreover, the growth of the Company and the legislative evolution – such as, for example, a possible extension of the types of criminal offences that are included in or anyway connected to the scope of application of the Decree - may make it necessary to integrate / update the Model 231.

In view of the above, the Supervisory Board has the task of adopting any type of measure so that the Company's Board of Directors can carry out the updates and additions deemed necessary from time to time.

5.2 Relationship between the Organisational Model and the Code of Conduct

In addition to the control tools provided for in the 231 Decree, the Company has adopted the Statkraft Group Code of Conduct, which is an expression of a corporate context where the primary objective is to satisfy, in the best possible way, the needs and expectations of stakeholders.

The Code of Conduct aims, among other things, to foster and promote a high standard of professionalism and to avoid behavioural practices that are not in the company's interest or that deviate from the law, as well as being in conflict with the values that the Company and the Group to which it belongs intend to maintain and promote.

The Code of Conduct must therefore be considered as the essential foundation of the 231 Model, since together they constitute a systematic body of internal rules aimed at disseminating a culture of ethics and transparency within the company and is an essential element of the control system; the rules of conduct contained therein complement each other, although the two documents have different purposes:

- → the Code of Conduct represents an instrument adopted independently and liable of being generally applied by the Company in order to express a series of principles of business ethics that the Company recognises as its own and on which it intends to call for the observance of all its employees and of all those who cooperate in the pursuit of the Company's aims;
- → The Model, on the other hand, complies with specific requirements contained in the 231 Decree, aimed at preventing the commission of particular types of offences that may entail the liability of the Company.

5.3 The organizational and authorization system

5.3.1 *Organizational system*

The organisational system must be sufficiently formalised and clear, especially as regards the assignment of responsibilities, the lines of hierarchical dependence and the description of tasks, with specific provision for control principles.

The Company's organisational structure is formalised and graphically represented in an organisational chart, which clearly defines the lines of hierarchical dependence and the functional links between the various positions making up the structure itself. In this way it is intended to ensure management that is consistent with the strategic objectives set by the Company's top management.

5.3.2 *Authorization system*

The powers of authorisation and signature must be assigned in line with the organisational and management responsibilities assigned, providing, when required, for a precise indication of the approval thresholds for expenses, especially as regards those activities considered at risk of crime.

The powers of authorisation and signature with which the Company has been endowed are consistent with the organisational and management responsibilities assigned and provide for an indication of the approval thresholds for expenditure

5.4 Control Principles

The Company, by this Model, has intended to provide for the process of implementing the new system of controls centred on the principles set out below.

The control principles that must inspire the management of all the activities potentially at risk contained in the so-called risk mapping, as well as in all the internal processes, are the following:

(a) Guaranteeing integrity and ethics in the performance of activities, through the provision of appropriate rules of conduct aimed at regulating each specific activity considered at risk of crime;

(b) Identifying each Company function involved in activities at risk of offence;

(c) Allocating decision-making responsibilities in a way commensurate with the level of responsibility and authority conferred;

(d) Properly defining, assigning and communicating authorization and signatory powers, including, when required, a precise indication of the approval thresholds for expenses, so that no person is granted unlimited discretionary powers;

(e) Ensuring the principle of separation of duties in the management of processes/activities, assigning to different subjects the crucial phases of which the process/activity is composed and, in particular, those of:

(i) authorization;

(ii) execution;

(iii) control.

(f) Regulate at-risk activities by means of appropriate protocols, providing for the appropriate control points (checks, reconciliations, etc.);

(g) Ensure the verifiability, documentation, consistency and congruity of every operation or transaction. For this purpose, the traceability of the activity must be guaranteed through adequate documentary support on which controls can be carried out at any time. Therefore, for each transaction, the following must be easily identified:

(i) Who authorized the transaction;

(ii) Who executed it;

(iii) Who recorded it;

(iv) Who carried out controls.

The traceability of operations is ensured with a higher level of certainty through the use of computer systems;

(h) Ensure the documentation of the controls carried out; to this end, the procedures with which the controls are implemented must guarantee the possibility of retracing the control activities carried out, in such a way as to allow the evaluation of the consistency of the methodologies adopted and the correctness of the results obtained.

These control principles have been taken as a reference when drawing up internal procedures and the Special Part.

5.5 The system of management of financial flows

Art. 6, paragraph 2, letter c) of the Decree establishes that the models must provide for "*methods of managing financial resources suitable for preventing the commission of offences*". The rationale of this provision is based on the fact that many of the underlying crimes can be committed through the company's financial flows (e.g.: constitution of non-accounting funds for the performance of acts of corruption).

The Guidelines recommend the adoption of mechanisms for the proceduralisation of decisions which, by making the various phases of the decision-making process documented and verifiable, prevent the improper management of such financial flows.

On the basis of the principles indicated in the Guidelines, the control system relating to administrative processes, and in particular, to the process of managing financial flows, is based on the separation of duties in the key phases of the process, a separation that must be suitably formalised and for which a good traceability of the acts and authorisation levels to be associated with the individual operations must be envisaged.

In particular, the specific control elements are as follows:

(a) Different subjects operating in the different phases/activities of the process;

(b) Preparation and authorization of the payment proposal to discharge the obligation duly formalized;

(c) Control over the execution of payment;

(d) Reconciliations on final accounts;

(e) Existence of authorization levels for payment requests that are articulated according to the nature of the transaction (ordinary/extraordinary) and amount;

(f) Systematically performing reconciliations of internal accounts and relationships maintained with lending institutions to the accounting records;

(g) Traceability of acts and documents that have already resulted in a payment.

5.6 General Prevention Principles and Protocols

5.6.1 *General Prevention Principles*

The protocol system for the prevention of offences has been implemented by applying the following General Principles of Prevention to individual sensitive activities, which inspire the General Prevention Protocols referred to in the following paragraph, as well as the Preventive Controls of the Special Section:

(a) Regulation: existence of internal provisions and formalised protocols suitable for providing principles of conduct and operating procedures for carrying out sensitive activities, as well as procedures for archiving the relevant documents;

(b) Traceability: 1) every operation relating to the sensitive activity must, where possible, be adequately documented; 2) the process of decision-making, authorisation and performance of the sensitive activity must be verifiable ex post, also by means of appropriate documentary supports;

(c) Segregation of duties: application of the principle of separation of duties between those who authorise, those who execute and those who control. This separation is guaranteed by the intervention, within the same macro-process of the Company, of several subjects, in order to guarantee independence and objectivity of the processes;

(d) **Proxies and powers of attorney**: the authorization and signatory powers assigned must be: 1) consistent with the organizational and managerial responsibilities assigned, including, if required, an indication of the approval thresholds for expenditure; 2) clearly defined and known within the Company. The roles within the Company to which the power to commit the Company to certain expenses must be defined, specifying the limits and nature of the expenses. The act of assigning functions must comply with any specific requirements that may be required by law (e.g., delegation of authority in relation to the health and safety of workers);

(e) **Code of Conduct**: activities must be carried out in accordance with the principles set out in the Code of Conduct.

5.6.2 *General prevention protocols*

In the context of the sensitive activities identified for each type of criminal offence (see the Special Part of the Model), the general prevention protocols provide that:

(a) All the activities, as well as the formation and implementation of the Company's decisions comply with the principles and the provisions contained in the provisions of the law, in the memorandum and articles of association, in the Code of Conduct and in the Procedures;

(b) Internal provisions are defined and adequately communicated to provide principles of conduct and operating procedures for carrying out sensitive activities, as well as procedures for filing the relevant documentation;

(c) For all the transactions:

(i) The management, coordination and control responsibilities within the Company must be formalised, as well as the levels of hierarchical dependence and the description of the relative responsibilities;

(ii) The phases of formation of the acts and the relative authorization levels must be documented and traceable;

(iii) The Company must adopt means of communicating the signatory powers granted to ensure that they are known within the Company;

(iv) The allocation and exercise of authority within a decision-making process must be consistent with positions of responsibility and the significance and/or criticality of the underlying economic transactions;

(v) Access to the Company's data must comply with Legislative Decree no. 196/2003 and subsequent amendments and additions and EU Regulation 2016/679 on the protection of personal data;

(vi) Access to Company's data is permitted only to authorized persons;

(vii) Confidentiality in the transmission of information is guaranteed;

(viii) Documents relating to the formation of decisions and the implementation of the same must be archived and kept by the competent function in such

a way as not to allow subsequent modification, except with appropriate evidence;

(ix) Access to documents already archived is allowed only to persons authorized under internal rules.

5.6.3 *General principles of the control standards relating to intentional crimes*

The general control standards at the basis of the tools and methodologies used to structure the specific control systems can be summarized as follows:

(a) Sufficiently up-to-date, formalized and clear organizational system: The standard refers to the allocation of responsibilities, hierarchical reporting lines and job descriptions, with specific provision for control principles such as, for example, the segregation of functions. In the context of the organizational system, attention should be paid to employee reward systems: these are necessary to direct the activities of operational and managerial staff towards the achievement of company objectives. However, if they are based on clearly unjustified and unattainable performance targets, they could constitute a veiled incentive to commit some of the offences provided for by the Decree.

(b) Manual and computer procedures (information systems): the standard refers to the use of procedures that regulate the performance of activities by foreseeing the appropriate control points (balancing, in-depth information on particular subjects such as agents, consultants, brokers). It is advisable to evaluate over time the separation of duties within each process at risk, verifying that the company procedures and/or operating practices are periodically updated and constantly take into account the variations or novelties that have occurred in the company processes and in the organisational system.

(c) Authorization and signature powers: these powers must be assigned in line with organizational and managerial responsibilities. Certain functions may be delegated to a person other than the original holder. It is necessary to define in advance, in a clear and unequivocal manner, the company profiles that are entrusted with the management and responsibility of the activities at risk of crime, also with regard to the profile of the effect of the proxies against third parties. The delegation must be the instrument for a more effective fulfilment of the obligations imposed by law on the complex organisation, not for an easy transfer of responsibility. This can be achieved through a clear indication of the approval thresholds for expenditure by the delegate. It is also important to provide for a coherent and integrated system that includes all the company's delegated or proxy powers (including those for accident prevention and environmental matters), periodically updated in the light of both regulatory changes and any changes in the company's organizational system. It would also be advisable to ensure that the delegation system can be documented in order to facilitate any subsequent reconstruction.

(d) Integrated control system: the standard requires that these systems must take into account all operational risks, in particular those relating to the potential commission of alleged offences, in order to provide timely warning of the existence and emergence of general and/or specific critical situations. It is necessary to define appropriate indicators for the individual types of risk detected and the internal Risk Self Assessment processes of the individual company departments.

5.6.4 *General principles of the control standards relating to the Risk Areas of culpable offences regarding the protection of health and safety at work and the environment.*

(a) Organizational Structure: with reference to offences relating to the health and safety of workers, an organisational structure is required with tasks and responsibilities formally defined in line with the organisational and functional scheme of the company.

A system of functions that ensure the adequate technical competences and the necessary powers to evaluate, manage and control the risk for the health and safety of the workers (art. 30, paragraph 3 Legislative Decree n. 81/2008) must be provided.

The level of articulation of functions will be adapted to the nature and size of the company and the characteristics of the activity carried out.

In order to guarantee the effective and appropriate exercise of these functions it is possible to resort to the institution of the delegation of functions, in compliance with the limits and requirements envisaged by articles 16 and 17 of Legislative Decree no. 81/2008.

Particular attention must also be paid to the specific figures working in this area (RSPP, Prevention and Protection Service staff (ASPP, *Addetti al Servizio di Prevenzione e Protezione*), Doctor, where applicable and, if present, RLS, first aid staff, emergency staff in case of fire).

This approach, in essence means that:

(i) the duties of the company management, managers, supervisors, the workers, RSPP, Competent Doctor and all other subjects present in the company and foreseen by the Legislative Decree no. 81/2008 regarding the safety activities of their respective competence, as well as the related responsibilities, must be explained;

(ii) the duties of the RSPP and of any personnel assigned to the same service, of the RLS, of the emergency management personnel and of the Doctor must be documented.

In order to prevent environmental offences, the company's organisation must include specific operating procedures to effectively manage the environmental risks that may contribute to the commission of the offences referred to in article 25-*undecies* of the Decree.

Among the many initiatives and measures to be promoted, it would therefore be necessary to:

(i) Proceduralize and monitor the activity of environmental risk assessment according to the regulatory framework and the naturalistic-environmental context in which the company operates;

(ii) Formalize appropriate organizational arrangements, to identify those responsible for compliance with environmental regulations and those

operationally responsible for the management of environmental issues, in light of the risk assessment above;

(iii) Monitor the activities of planning and accounting for environmental expenditures, qualification, evaluation and monitoring of suppliers (e.g., workers in charge of waste characterization and classification, rather than transporters, disposers, brokers in charge of waste management);

(iv) Ensure that the Model is updated to comply with the legislation on environmental offences, which is complex and constantly evolving.

With particular reference to the issue of delegation, it must be considered that, unlike the delegation of functions governed by Legislative Decree no. 81/2008, the "environmental" delegation is not codified. Therefore, it is necessary to refer to the jurisprudential judgements, including those of legitimacy (see Court of Cass, Criminal Section III, October 12, 2009, no. 39729), which have clarified the specific nature of the so-called *environmental delegation* with respect to the delegation on accident prevention, foreseeing the need for the content of the delegation to be clear and unequivocal and to expressly refer to the measures for compliance with environmental regulations.

(v) From this point of view, the most recent interventions of jurisprudence admit the validity of the "environmental delegation" in the presence of the following conditions: (i) specificity and unequivocal indication of the delegated powers; (ii) size of the company (in a complex organization it is crucial); (iii) technical capacity and suitability of the delegated subject; (iv) autonomy (of management and finance) and effective powers of the delegate; (v) express acceptance of the delegation.

(vi) Moreover, the principles elaborated by jurisprudence in relation to the delegation of functions are also valid in this sector: in the event of structural deficiencies, the involvement of top management will be inevitable, but at the same time it is to be excluded that liability for non-compliance with the duty of control can be affirmed in the abstract, which must be verified in concrete terms with reference to the company's organization, the type of delegation and the high level of dispute.

(b) Communication and Involvement: sharing information within the company takes on significant value in fostering the involvement of all stakeholders and enabling appropriate awareness and engagement at all levels.

This involvement, with reference to occupational health and safety, should be achieved through:

(i) The preventive consultation of the RLS, if any, and of the Competent Doctor, if any, regarding the identification and assessment of risks and the definition of preventive measures;

(ii) Periodic meetings that take into account not only the requirements set forth in applicable law, but also reports received from workers and operational needs or problems encountered.

With reference to environmental offences, the communication and involvement of stakeholders should be carried out through periodic meetings of all competent

figures to verify the proper management of environmental issues, after which there should be adequate dissemination of results (e.g. performance, accidents and lack of environmental incidents) within the organization and, therefore, also to workers.

(c) **Operational management:** the control system should be integrated and congruent with the overall management of company processes.

The analysis of company processes and their interrelationships and the results of the risk assessment (whether they relate to health and safety at work or environmental risks) lead to the definition of the methods for the correct performance of the activities that have a significant impact on these issues.

Having identified the areas of intervention associated with the aspects of health and safety and the environment, the Company should exercise regulated operational management. In this sense, particular attention should be paid to:

(i) Recruitment and qualification of personnel;

(ii) Organization of work (and work stations for worker health and safety); and

(iii) Acquisition of goods and services used by the Company and communication of appropriate information to suppliers and contractors;

(iv) Normal and extraordinary maintenance;

(v) Qualification and selection of suppliers and contractors;

(vi) Emergency management;

(vii) Procedures for dealing with non-compliance with the objectives and rules of the control system.

In addition to the indications mentioned above, the model for the prevention and management of the risks of environmental offences should instead identify, on the basis of the results of the risk analysis, appropriate measures for the prevention, protection and mitigation of the risks identified. Similarly, all the management issues of the company fleet (vehicles, boats, aircraft, etc.), of the plants containing ozone-depleting substances, as well as the treatment and disposal of special or even hazardous waste, which must be governed by specific company protocols aimed at guiding the work of the employees, in line with the articulated reference regulations (e.g.: respect of time constraints, respect of time limits, respect of the rules of conduct, etc.), are also relevant, compliance with time constraints, volumes and dedicated physical spaces for the temporary storage of materials intended for disposal; checks to be implemented on the accesses of third-party companies assigned to transport and disposal).

(viii) Still on the subject of waste management and disposal, particular attention must also be paid to the controls - both during the contractual phase, with the use of specific precautionary clauses, and during the actual performance of the service - regarding the suppliers entrusted with these activities.

Lastly, it should be noted that some areas of attention in terms of environmental protection have clear points of contact with similar areas of risk, considered from a different perspective, relevant to health and safety at work (e.g. management of emergencies, maintenance, etc.). Therefore, the controls implemented in this regard within the Company may assume a synergic value, covering both profiles of attention.

(d) Monitoring system: Occupational health and safety management should include a phase to verify that the risk prevention and protection measures adopted and assessed as suitable and effective are being maintained. The technical, organizational and procedural prevention and protection measures implemented by the company should be subject to planned monitoring.

The setting up of a monitoring plan should be developed through:

(i) Temporal scheduling of reviews (frequency);

(ii) Assignment of tasks and responsibilities;

(iii) Description of methodologies to be followed;

(iv) Procedures for reporting any non compliance.

Systematic monitoring of these measures should therefore be envisaged, the procedures and responsibilities for which should be established at the same time as the procedures and responsibilities for operational management are defined.

The above can be summarised in the table below[27].

[27] It should be noted that the Guidelines are not mandatory and non-compliance with specific points of the Guidelines does not in itself affect the validity of the Model. In fact, the Company has created its own 231 Model on the basis of best practice and the Confindustria Guidelines, whose indications - which are, however, not mandatory and necessarily general and standardised in nature - have been taken into account, integrated or disregarded in order to prepare an effective organisational model in light of the corporate structure, core business and the company reality of Statkraft Italia S.r.l.

PREVENTIVE CONTROL SYSTEMS INTENTIONAL OFFENCES	PREVENTIVE CONTROL SYSTEMS NON-INTENTIONAL OFFENCES (SAFETY AND ENVIRONMENT)	PRINCIPLES OF CONTROL
Code of Conduct Organisational system sufficiently up-to-date, formalised and clear Manual and IT procedures (information systems) Powers of authorization and signature Communication to and training of personnel Integrated control systems	Code of Conduct Organisational structure Education and training Communication and involvement Operational management Monitoring system	è*"Each transaction and action must be verifiable, documented, consistent and appropriate"* è*"No one can manage an entire process on their own"* è *"Controls must be documented"* 

6. SUPERVISORY BOARD

6.1 Requirements

Art. 6, lett. b), of the Decree requires the Corporate Entity to set up a Body with autonomous powers of initiative and control (Supervisory Board), which will supervise the functioning of and compliance with the Model and which will ensure that it is updated.
Each member of the Supervisory Board must possess the capacity and qualifications to carry out the duties and tasks assigned to the Supervisory Board by the Model and must satisfy the following conditions/requirements of:

(a) Autonomy and independence;

(b) Adequate experience in corporate governance matters;

(c) Good reputation;

(d) Continuity, i.e., maintaining a continuous presence and participation in activities throughout the mandate.

The members of the Supervisory Board are considered ineligible and unsuitable and, consequently, if already appointed, must be revoked, in the following cases:

(a) Conviction:

(i) To imprisonment for a term not less than one year for any of the crimes or administrative offences referred to in the Decree;

(ii) To imprisonment for a period of not less than one year for any non-culpable offence;

(iii) To imprisonment for a period of not less than one year for any of the offences set out in Title XI of Book V of the Civil Code, as amended by the provisions of Legislative Decree 61/2002;

(iv) Disqualification, including temporary disqualification, from holding public office, or temporary disqualification from holding managerial positions in legal persons and companies.;

(b) Definitive application of one of the prevention measures provided for in Article 10, paragraph 3, of Law 575/1965, as replaced by Article 3 of Law 55 of 19 March 1990 and subsequent amendments;

(c) Incapacitation and judicial liquidation.

Any member of the Supervisory Board may be removed from office by the Board of Directors only if he/she can be challenged on the following grounds:

(a) Serious misconduct in the performance of their activities or violations of the Regulations, including the violation of confidentiality obligations with regard to information acquired as a result of the mandate;

(b) Occurrence of one of the causes of ineligibility, prior to appointment as a member of the SB.

Each member of the Supervisory Board shall be removed from office if a personal precautionary measure is applied.

Each member of the SB may be suspended from office in the event of inclusion in the register of persons under investigation by the Prosecutor.

Each member of the SB must promptly notify the Board of Directors of any circumstances that determine the need to replace one of the other members of the SB.

If the majority of the members of the SB do not remain in office, all the members of the SB will be removed from office.

The replacement of the individual member must take place as soon as possible by the Board of Directors, and in any case, no later than one month.

The Company shall ascertain, prior to the appointment of the members, that they meet the requirements established by the Model in addition to those provided for by the legal and regulatory framework.

6.2 Composition of the Supervisory Board

The SB is appointed by the Board of Directors and may have a collegiate composition of three members or may be composed by a sole member.

Each member of the Supervisory Board must have the skills and professional qualification to carry out the tasks and duties assigned to the SB by the Company.

The members of the Supervisory Board remain in office for the period defined by the Board of Directors.

When appointing the members, the Board of Directors also appoints a Chairman, who is responsible for:

(a) Promote the convening and direct the meetings of the Supervisory Board;

(b) Coordinate relations and manage relations between the Supervisory Board and the Board of Directors;

The office of Chairman lasts from the date of appointment until the expiry of the corresponding term of the Supervisory Board's mandate.

The Supervisory Board identifies from among its own staff, or from among the Company's employees or consultants, a figure dedicated to carrying out the functions of drafting the minutes of the Supervisory Board's meetings, preparing and processing the documentation subject to the decisions of the Supervisory Board and carrying out the tasks concerning the organisational aspects of the Supervisory Board itself.

6.3 Duties and activities of the Supervisory Board

The SB is in charge of, among other things:

(c) Promoting and supervising the dissemination and knowledge of the Model and the implementation of the personnel training plan through training plans for Recipients;

(d) Report to the Board of Directors any violations of the Model and/or of the regulations in force of which he/she becomes aware in the performance of the above duties;

(e) Supervise the effectiveness, adequacy and compliance with the provisions of the Model by the Recipients. The SB carries out these activities:

(i) Maintaining relations and ensuring information flows to the Board of Directors, guaranteeing adequate liaison with the external auditors, as well as with the Company's other control bodies;

(ii) Formulating expenditure forecasts for the performance of its activities;

(iii) Coordinating and promoting training initiatives for personnel and periodic communications to Employees and (where necessary) to outsourcers and consultants in order to inform them about the provisions of the Model;

(iv) Conducting inspections, including through the analysis of documents and/or requesting information from departments, employees and non-employee personnel;

(v) Verifying periodically the implementation and effective functionality of proposed corrective solutions/actions;

(vi) Ensuring the confidentiality of any information in their possession.

The Board of Directors periodically ascertains the adequacy of the SB , in terms of both its organisational structure and its powers, and adopts the appropriate amendments and/or additions.

The SB is assigned an annual budget, endorsed by the Board of Directors.

6.4 Information flows from the Supervisory Board

The Supervisory Board reports to the Board of Directors on the implementation of the Model and the emergence of any critical aspects, and communicates the outcome of the activities carried out in the exercise of the tasks assigned to it periodically in an annual report.

In particular, the reporting activity concerns:

(a) The overall activity carried out during the reporting period, with particular reference to the audit activity;

(b) Critical issues that emerged both in terms of conduct or events within the Company, and in terms of the effectiveness of the Model;

(c) The activities that could not be carried out for justified reasons of time and/or resources;

(d) The necessary and/or appropriate updating, corrective and improvement actions of the Model and their implementation status;

(e) The state of implementation of the Model;

(f) The identification of the activity plan for the following (annual) period.

In addition, the Supervisory Board shall promptly report to the Board of Directors on:

(a) Any violation of the Model which is deemed to be well-founded, which has come to the attention of the Supervisory Board or which has been ascertained by the Supervisory Board itself;

(b) Detected organizational or procedural deficiencies capable of determining the concrete danger of commission of crimes relevant to the Decree;

(c) Regulatory changes that are particularly relevant to the implementation and effectiveness of the Model;

(d) Lack of cooperation by company structures (in particular, refusal to provide the SB with requested documentation or data, or obstruction of its activity, also determined by the denial of conduct due on the basis of the Model);

(e) Existence of criminal proceedings against individuals who work on behalf of the Company, or proceedings against the Company in relation to relevant crimes under the Decree;

(f) Result of the investigations ordered following the start of inquiries by the judicial authorities into crimes pursuant to the Decree;

(g) Any other information deemed useful for the purposes of the Board of Directors taking urgent resolutions; (m) Any other information deemed useful for the Board of Directors taking urgent resolutions..

6.5 Supervisory Board and Privacy Policy

In accordance with the opinion issued by the Guarantor of the Protection of Personal Data of May 12, 2020, at the request of the Association of the Components of the Supervisory Bodies (AODV 231), on the subjective qualification of the Supervisory Bodies for privacy purposes, the external members of the SB will be required to process the data of subjects in any capacity working at the Company, acquired through the information flows, in accordance with the instructions given by the Data Controller in accordance with the provisions of art. 29 Regulation no. 679/2016 (hereinafter, GDPR) so that the processing takes place in accordance with the principles established by art. 5 of the same GDPR.

The Data Controller will be required to adopt the technical and organizational measures suitable to ensure the protection of the processed data, ensuring at the same time to the Supervisory Board the autonomy and independence with respect to the corporate management bodies in the performance of its duties in the manner provided for by the cited legislation.

Furthermore, the Company will designate - within the scope of the technical and organisational measures to be put in place in line with the principle of accountability (art. 24 GDPR) - the individual member(s) of the Supervisory Board as subjects authorised to process personal data (articles 4, no. 10, 29, 32 par. 4 GDPR; see also art. 2 quaterdecies of the Privacy Code).

7. INFORMATION FLOWS TO THE SB AND WHISTLEBLOWING

7.1 Information flows

The Supervisory Board must be informed by the subjects required to comply with the Model about events that could generate liability for the Company pursuant to Decree 231. To this end, the SB supervises the preparation of a procedure relating to information flows (periodical and occasional) or provides directly for the structuring of the same, the implementation of which is carried out by the Company.
The specific control protocols indicate some of the information flows to the SB which, in any case, can be derogated autonomously by the SB itself.
Within the company, the Company's Function Managers must communicate to the SB:

(a) At the request of the Supervisory Board and in accordance with the methods defined by the latter, information and control activities carried out, at the level of its own operational area, which are useful for the exercise of the activity of the Supervisory Board in terms of verifying compliance with, effectiveness and updating of this Model, and from which facts, acts, events or omissions may emerge with critical profiles with respect to compliance with the provisions of Decree 231;

(b) On a periodical basis, the information identified in this Model, as well as any other information identified by the Supervisory Board and requested by it to the individual organizational and managerial structures of the Company through internal directives;

(c) Any other information, also coming from third parties and pertaining to the implementation of the Model in the Risk Areas and the compliance with the

provisions of Decree 231, which may be considered useful for the purposes of carrying out the duties of the Supervisory Board. In particular, by way of example but not limited to, the following information must be obligatorily and promptly transmitted to the Supervisory Board:

(i) Measures and/or news coming from judicial police bodies, or from any other authority, from which it can be inferred that investigations are being carried out for the offences set out in the Decree, also against unknown persons;

(ii) Requests for legal assistance made by managers and/or Employees in the event of legal proceedings being initiated against them for the offences set out in Decree 231;

(iii) Transactions on the share capital, allocation of profits and reserves, purchase and sale of shareholdings in Companies or their branches, mergers, demergers, spin-offs, as well as all transactions that could potentially damage the integrity of the share capital;

(iv) Any assignment conferred or intended to be conferred on the Independent Auditors in addition to the certification of the financial statements;

(v) Decisions relating to the application for, disbursement and use of public funds;

(vi) Information on the effective implementation of the Model at all levels of the company, with evidence of any disciplinary procedures carried out and any sanctions imposed or measures taken to dismiss such procedures and the relative reasons;

(vii) The system of directors' proxies and any subsequent amendments and/or additions thereto, as well as the organisational structure;

(viii) The system of company signature powers and any subsequent amendment and/or integration thereof;

(ix) Reports and/or news relating to offences committed in breach of accident prevention regulations and the protection of hygiene and health at work;

(x) Other documents from which facts, acts, events or omissions may emerge that are critical with respect to compliance with the provisions of Decree 231.

Finally, it should be noted that such information may also be collected directly by the Supervisory Board during its periodic control activities through the methods that the Supervisory Board deems most appropriate (such as, purely by way of example, the preparation and use of special checklists).

7.2 Whistleblowing System

Legislative Decree No. 24/2023, transposing Directive (EU) 2019/1937 concerning the *"protection of persons who report breaches of Union law and on the protection of persons who report breaches of national laws"* ("**Whistleblowing Decree**") has replaced the previous national regulations on

whistleblowing by bringing together in a single regulatory text - for the public and private sectors - the provisions on the protection of persons who report unlawful conduct of which they have become aware in a work context.

Article 2(1)(a) of the Whistleblowing Decree defines the "violations" that may be subject to reporting as follows:

(a) infringements of national and European provisions consisting of offences in the following areas: public procurement, services, products and financial markets, prevention of money laundering, financing of terrorism product safety and compliance, transport safety, protection of the environment, radio and nuclear safety food and feed safety and animal health and welfare; public health; consumer protection; protection of privacy and protection of personal data and security of networks and information systems, EU restrictive measures;

(b) acts or omissions affecting the financial interests of the Union;

(c) acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union, including violations of Union competition and State aid rules, as well as violations relating to the internal market linked to acts in breach of corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law;

(d) administrative offences provided for therein, accounting, civil or criminal offences not covered by the above;

(e) **unlawful conduct relevant under Legislative Decree No. 231 of 8 June 2001, or violations of the organisation and management models that do not fall within the above (*i.e.* breaches of Decree 231 and Model 231).**

With reference to the subjective scope, the Whistleblowing Decree identifies the scope of application of the regulation more broadly than the previous one. This includes, amongst other, all persons who are even only temporarily in a working relationship with the Entity, even if they do not have the status of employees (such as volunteers, trainees, whether paid or unpaid), those in probationary periods, as well as those who do not yet have a legal relationship with the above-mentioned entities or whose relationship has ended if, respectively, the information on violations was acquired during the selection process or in other pre-contractual stages or in the course of the employment relationship. The reporting person is thus the natural person who makes the report or public disclosure of information on breaches acquired in the context of his/her work context.

7.3 Reporting channels

The Whistleblowing Decree, in transposing the indications of the European Directive, has provided for a diversified channels for submitting reports.

- **Internal channels;**
- **External channel managed by ANAC;**
- **Public disclosure;**

- Reporting to the Judicial Authority.

7.3.1 Internal channels

The Whistleblowing Decree provides that private sector entities are required to activate an internal channel for the transmission and management of reports. With regard to the internal channel, the Whistleblowing Decree provides that:

(a) they must guarantee, also through the use of encryption tools, the confidentiality of the identity of the person making the report, of the person involved and of the person in any event mentioned in the report, as well as the content of the report and the related documentation;

(b) the management of the reporting channel is to be entrusted to a dedicated autonomous internal person or department with specifically trained staff for the management of the reporting channel, or to an external entity, also autonomous and with specifically trained staff;

(c) reports are made in written form, also in computerised form, or in oral form;

(d) internal reports in oral form are made by means of telephone lines or voice messaging systems or, at the request of the reporting person, by means of a face-to-face meeting set within a reasonable period of time;

(e) private-sector entities that have employed, over the last year, an average of no more than two hundred and forty-nine employees, under permanent or fixed-term employment contracts, may share the internal reporting channel and its management;

(f) the internal report submitted to a person other than the person in charge is transmitted, within seven days of its receipt, to the competent person, with simultaneous notification of the transmission to the reporting person.

7.3.2 External Channels

Without prejudice to the preference for the internal channel - as clarified above - the Whistleblowing Decree provides for the possibility for persons in both the public and private sectors to make a report through an external channel. Italian Anti-Corruption Authority (ANAC) is the competent authority to activate and manage this channel, which guarantees, also through the use of encryption tools, the confidentiality of the identity of the person making the report, the person involved and the person mentioned in the report, as well as the content of the report and the relevant documentation.

The conditions under which Statkraft Italia employees may use ANAC's external channel are as follows:

(a) if the mandatory internal channel - is not active - is active but does not comply with the legislator's provisions on the subjects and methods of submitting reports

(b) the person has already made the internal report but it has not been followed up;

(c) the person making the report has reasonable grounds to believe that if he or she made an internal report - which would not be effectively followed up - this could lead to a risk of retaliation;

(d) the reporting person has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

7.3.3 Public Disclosure

The Whistleblowing Decree introduces an additional reporting modality consisting of public disclosure. With public disclosure, information on violations is brought into the public domain through the press or electronic media or in any case through means of dissemination capable of reaching a large number of people. The conditions for public disclosure are the following:

(a) an internal report to which the administration/entity has not replied within the prescribed time limits has been followed by an external report to ANAC, which, in turn, has not replied to the reporter within a reasonable time;

(b) the person has already directly made an external report to ANAC which, however, has not provided feedback to the reporter as to the measures envisaged or taken to follow up the report within a reasonable timeframe;

(c) the person directly makes a public disclosure because he/she has reasonable grounds for believing, on the basis of concrete circumstances and thus not on mere inferences, that the breach may represent an imminent or obvious danger to the public interest;

(d) the person directly makes a public disclosure because he or she has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up.

7.3.4 Reporting to the judicial authorities

The Whistleblowing Decree also recognises the possibility for protected persons to turn to the judicial authorities, in order to file a report of unlawful conduct of which they have become aware in a work context.

7.4 Protective and support measures

A key pillar of the entire discipline is the system of protections offered to whistleblowers, who make a public disclosure or report violations, protections which also extend to persons other than the whistleblower and complainant who, precisely because of their role in the whistleblowing process and/or the relationship that binds them to the whistleblower, could be the recipients of retaliation.

The Whistleblowing Decree has provided for a protection system which:

(a) includes the protection of the confidentiality of the whistleblower, the facilitator, the person involved and the persons mentioned in the report

(b) the protection against any retaliation taken by the entity on account of the report, public disclosure or whistleblowing made and the conditions for its application

(c) limitations of liability with respect to the disclosure and dissemination of certain categories of information operating under certain conditions.

Such protection is reflected in the Disciplinary System of the Model 231.

7.5 Internal Reporting Channels implemented by Statkraft Italia

In compliance with the provisions of the Whistleblowing Decree, Statkraft Italia has implemented the following reporting channels, via outsourcing to the parent company Statkraft AS (also regulating potential conflict of interest cases regarding the manager of the channel). Internal reports can be summitted – not only by the recipients of this Model 231 but also by seconded personnel and agency workers, suppliers, contractors and sub-contractors, freelancers and consultants, volunteers (paid or unpaid), trainees, apprentices and interns (paid or unpaid):

(a) in written form through the IT platform managed by the Head of the Corporate Audit Function: https://statkraft.whistleblowernetwork.net or by e-mail at the following address: compliance@statkraft.com (the first method is preferable and allows identification of the country where the incident occurred);

(b) orally via the hotline available at: +47 24 06 86 76 (also managed by the Head of the Corporate Audit Function).

Employees may, in any case, report concerns to their line manager (who will act in accordance with a dedicated procedure for managing reports).

When filing a report, it is necessary to at least indicate the following elements:

- clear and complete description of the facts being reported;
- circumstances of time and place where the reported facts occurred (if known);
- general information or other elements that allow the identification of the subject who carried out the reported facts;
- any documents or other useful information to confirm the reported facts. In any case, the whistleblower is guaranteed to receive a receipt of the report within seven days from its submission.

The whistleblower will be also provided with an update on the investigation within 3 months from the receipt above.

The Compliance unit – also in its capacity as an internal member of the Supervisory Body – will be informed by Corporate Audit regarding 231-relevant reports and involved, where necessary, in their management (e.g., in the case of a local investigation).

7.6 Regulations

In order to regulate the performance of its activities, the Supervisory Board adopts its own regulations.

8. DISCIPLINARY SYSTEM

8.1 Introduction

Pursuant to and for the purposes of articles 6 and 7 of the Decree, the Entity adopts and effectively implements - prior to the commission of the crime - "an organization, management and control model suitable to prevent crimes of the kind that have occurred". A fundamental requirement for guaranteeing the effectiveness of the implementation of the Model is the introduction of a disciplinary system to be applied in the event of violation of the rules of conduct foreseen by the Model. The Disciplinary System must impose appropriate disciplinary measures within the framework of the current legislation and labour laws. The system of disciplinary measures, applied in the event of violations of the Model and the Code of Conduct, operates in compliance with the principle of proportionality between the violation detected and the sanction imposed, in accordance with current legislative and contractual regulations.
In defining the disciplinary measure to be applied, the following criteria must be considered:

(a) Seriousness of the violation;

(b) Type of violation perpetrated;

(c) Circumstances in which the unlawful conduct took place;

(d) Position, content of the assignment and duties of the worker and of the persons involved in the facts constituting the disciplinary case;

(e) Any recidivism on the part of the individual.

Any impediment to the legitimate performance of the duties attributed to the Supervisory Board on the part of the Recipients will be sanctioned in accordance with the provisions of the Disciplinary System. The activation by the Company of the mechanisms foreseen by the Disciplinary System is irrespective of the opening of any criminal proceedings and/or the outcome of investigations or proceedings conducted by judicial authorities.
The Company expresses unequivocally that no unlawful conduct will be justified in any way, even if carried out in the alleged "interest" or "advantage" of the Company itself.
Any unlawful conduct will lead to the imposition on the Employees of the disciplinary measures provided for by the CBA and by the employment contract of each single Employee.

Following communications to the Supervisory Board of violations of the rules contained in the Model or in the Code of Conduct, the Supervisory Board directly investigates and ascertains the actual commission of a violation of the type described and reports the violation detected to the HR function, in order to initiate disciplinary proceedings; unless the report of commission of violations concerns the HR function itself.

The HR function, having heard the hierarchical superior of the author of the conduct in question, is called upon to initiate disciplinary proceedings and, if the misconduct is confirmed, to determine and adopt the relative disciplinary measure, in compliance with the provisions of law, CBA, the corporate collective complementary agreements and the applicable internal Procedures.

The HR function will inform the Supervisory Board of the imposition of the disciplinary measure or the different outcome of the proceedings.

The Employer will impose on the Employee the most appropriate disciplinary measure among those listed below.

8.2 Sanctions applying to the employees

About Employees, the Decree provides that the system of disciplinary measures must comply with the limits related to the sanctioning power imposed by the Workers' Statute and by the CBA, both with regard to the disciplinary measures that can be imposed, and with regard to the form of exercise of such power. Therefore, the disciplinary measures that may be adopted against Employees based in Italy are those envisaged in the CBA (and in any amendments and renewals of said contracts, always considering the seriousness of the conduct, the possible recidivism or the degree of guilt).
In this context, in accordance with the provisions of the CBA, the applicable disciplinary measures, based on the seriousness of the violation, in addition to the different, appropriate, and legitimate actions that the Company may take pursuant to the Company's Procedures and Guidelines, are as follows:

(a) verbal warning

(b) written warning

(c) fines in compliance with the Italian National Labor-Agreement and only where applicable, up to 4 hours pay

(d) suspension from work and pay up to 10 days

(e) dismissal.

An employee shall incur the measure of a verbal warning if, in the event of a minor infraction, they violate the internal procedures set forth in the Model 231 (for example, by failing to correctly record working hours on a project in the Zalaris application), or adopt, in performing activities within sensitive areas, behavior that slightly deviates from the provisions of Model 231 itself or the Code of Conduct. Violations that do not constitute a concrete threat to the integrity of the Company or to the proper implementation of the Model are punishable by a verbal warning. Such conduct constitutes a minor non-compliance with the Model or with the provisions issued by the Company[28].
In particular, by way of example and not limitation, an employee shall incur a verbal warning if they:

- have used the company email address to register on websites unrelated to work activities, provided that such registrations have not compromised the integrity of the Company or the proper implementation of the Model and the employees have promptly proceeded with deregistration;

- have modified the configuration of their workstations, whether fixed or mobile, without causing any harm to their own safety or that of others.

[28] Tier 3 cases according to the Group-level disciplinary system.

Employees shall incur the measure of a written warning if, while committing a minor infraction by violating the internal procedures set forth in Model 231 or by adopting, in performing activities within sensitive areas, behavior that is slightly non-compliant with the provisions of Model 231, they expose the integrity of the Company to an objectively dangerous situation, without causing any damage (even minor) to the Company and without in any way (even slightly) compromising the implementation of the Model[29]. In particular, by way of example and not limitation, employees are punishable with a written warning if they:

- have already received a verbal warning during the two-year period for committing the same infraction;
- violate, in the event of a minor infraction, the provisions of Model 231 or the Code of Conduct, as well as the company procedures referenced in this Model, where such violation constitutes a concrete threat to the integrity of the Company or to the proper implementation of the Model (for example, fail to provide accurate and timely information to a competitor invited to a procurement procedure);
- violate, in the event of a minor infraction, the obligation to inform the Supervisory Body (for example, delay in sending reports to the Body).

Such conduct, resulting from non-compliance with the provisions issued by the Company, creates a situation of risk for the integrity of the Company or for the proper implementation of the Model and/or constitutes acts contrary to its interests.

Employees shall incur the measure of a fine not exceeding four hours of normal pay if, through non-compliance and omissions of medium severity, they violate the internal procedures set forth in Model 231 or adopt, in performing activities within sensitive areas, behavior that is not compliant with the provisions of the Model, causing minor harm to the integrity of the Company or slightly compromising the proper implementation of the Model, or if they are repeat offenders in the violations described above[30]. In particular, by way of example, employees are punishable with a fine if they:

- are repeat offenders (once) during the two-year period in committing infractions for which a written warning applies;
- undermine the effectiveness of the Model through behaviors such as: repeated failure to comply with the obligation to inform the Supervisory Body (e.g., delayed or inaccurate submission of reports to the Body);
- violate the provisions of Model 231 or the Code of Conduct, as well as the company procedures referenced in this Model, where such violation constitutes minor harm to the integrity of the Company or to the implementation of the Model (e.g., receiving from or

[29] Tier 3 cases according to the Group-level disciplinary system.

[30] Tier 3 or 2 cases according to the Group-level disciplinary system.

giving to private parties, without prior authorization in accordance with internal procedures, gifts or hospitality of modest value).

Such conduct, resulting from non-compliance with the Model or with the provisions issued by the Company, causes minor harm to the integrity of the Company, slightly compromises the proper implementation of the Model and/or constitutes acts contrary to its interests.

Employees shall incur the measure of suspension from work and pay for up to a maximum of 10 days if, through a medium-level infraction, they violate the internal procedures set forth in Model 231 or adopt, in performing activities within sensitive areas, behavior that is not compliant with the provisions of Model 231 and that may lead to the commission of an offense punishable under Legislative Decree 231, causing medium-level harm to the integrity of the Company or to the proper implementation of the Model. Suspension also applies to employees who are repeat offenders in the violations described above[31]. In particular, by way of example, employees are punishable with suspension if they:

- are repeat offenders (three times) during the calendar year in committing infractions for which a fine of up to four hours of pay applies;
- violate provisions concerning signing authority and the current system of delegations and powers of attorney;
- violate, through a medium-level infraction, the provisions of Model 231 or the Code of Conduct, as well as the company procedures referenced in this Model (e.g., near-miss caused by failure to comply with health and safety regulations).

Employees shall incur the measure of dismissal (with or without notice) if they engage in conduct of serious gravity in violation of the provisions of Model 231, or if they engage in conduct unequivocally aimed at committing an offense punishable under Legislative Decree 231, or conduct that results in the actual application to the Company of the measures provided for by Legislative Decree 231. The sanction of dismissal also applies to employees who commit one of the infractions mentioned in the previous points, causing serious harm to the integrity of the Company or to the proper implementation of the Model, as well as employees who are repeat offenders in the violations described above[32]. In particular, by way of example, employees are punishable with dismissal if they:

- fraudulently circumvent the provisions of Model 231 or the Code of Conduct, as well as the company procedures referenced in this Model 231, through conduct unequivocally aimed at committing one of the offenses included among those provided for by Legislative Decree 231 (e.g., in the context of a permitting process, act in conflict of interest with the official responsible for the services conference in order to unlawfully obtain an authorization);

[31] Tier 2 or 1 cases according to the Group-level2 disciplinary system.

[32] Tier 1 cases according to the Group-level disciplinary system.

- remove, destroy, or alter documentation, or prevent the Supervisory Body from controlling or accessing information and documentation, thereby obstructing transparency and verifiability (e.g., documentation relating to the hiring of employees in conflict of interest, documentation proving the exceeding of the value threshold for the acceptance or giving of gifts);

- violate measures adopted by the Company to ensure the protection of the identity of whistleblowers under the Whistleblowing Decree, thereby generating retaliatory behavior or any other form of discrimination or penalization against the whistleblower;

- obstruct or attempt to obstruct a report and/or the process of managing a report under the Whistleblowing Decree;

- are found responsible for defamation or slander committed through a report under the Whistleblowing Decree;

- commit a retaliatory act against a whistleblower or against other persons to whom the Whistleblowing Decree extends protection against retaliation (e.g., facilitators or persons with a qualified connection to the whistleblower);

- are repeat offenders (three times) during the calendar year in committing infractions for which suspension applies;

- make, with gross negligence or intent, false or unfounded reports concerning violations of Model 231 or the Code of Conduct.

The aforementioned disciplinary measures may vary in compliance with the amendments and/or integrations of the CBA.

8.3 Sanctions for directors

In addition to the provisions of the preceding paragraph, the failure of managerial staff to supervise the proper application by their subordinate workers of the rules and provisions laid down in the Model and in the Code of Conduct, which leads to an actual violation thereof, constitutes a disciplinary offence.

The Company will, therefore, ascertain the infringements and impose the most suitable measures in proportion to the seriousness of the conduct and in accordance with the rules set out in the previous paragraph. In the event of particularly serious violations of the principles contained in the Model, the measure applied could go as far as dismissal.

8.4 Sanctions for managers

In the event of failure to comply with the Model or the Code of Conduct on the part of the Company's directors who are also employees of the same, the most appropriate disciplinary measures will be applied, if and to the extent that the conduct also relates to the managerial role covered.

Violations of the Model and of the Code of Conduct shall give rise to the application of specific sanctions for the role of director, ranging from a written reprimand, to revocation of office, to liability action pursuant to art. 2393 of the Civil Code, in consideration of the intentionality and seriousness of the conduct (assessable also in relation to the level of risk to which the company is exposed) and of the particular circumstances in which the said conduct occurred.
The measure of a written warning shall be applied in the event of minor non-compliance with the principles and rules of conduct provided for by this Model.
The above-mentioned measure shall also be specifically applied, for example, in cases of:

(a) Delay in taking action on reports, Including those under the Whistleblowing Decree;

(b) Delayed preparation of the documentation required by the Model or Procedures;

(c) violation of the confidentiality obligations provided for by the Whistleblowing Decree, including those relating to the report and the identity of the whistleblower;

(d) obstruction of the reporting process or violation of the confidentiality obligation in the context of managing reports under the Whistleblowing Decree;

(e) retaliatory acts against anyone who has made a report under the Whistleblowing Decree, or against other persons to whom the Whistleblowing Decree extends protection against retaliation (e.g., facilitators or persons with a qualified connection to the whistleblower);

Depending on the seriousness of the infringement, the Shareholders' Meeting, convened by the Board of Directors, will apply the protective measures it deems most appropriate, in compliance with the regulations in force.

8.5 Sanctions for third parties

Violations of the Model by non-employee collaborators of the Company shall be sanctioned by the competent bodies on the basis of the internal rules of the Company in accordance with the provisions of the collaboration contracts, and in any case with the application of conventional penalties and/or the automatic termination of the contract (pursuant to art. 1456 of the Italian Civil Code), without prejudice to the compensation for damages.

8.6 Application of whistleblowing regulations in the disciplinary procedure

Pursuant to Article 21 of the Whistleblowing Decree, Within the disciplinary procedure initiated following a report, the identity of the whistleblower may not be disclosed unless strictly necessary, that is, if the disciplinary charge is based on findings that are separate and additional to the report.

Conversely, if:

i. the charge is based, in whole or in part, on the report; and

ii. ii. knowledge of the whistleblower's identity is indispensable for the defense of the accused,

the report may only be used for the purposes of the disciplinary procedure with the whistleblower's consent to the disclosure of their identity. In particular, the whistleblower will be contacted by the

Head of the Corporate Audit Function, who will provide written communication explaining the reasons that make disclosure of confidential data necessary and will request the whistleblower's consent to reveal their identity. The whistleblower may refuse consent; in such case, the report cannot be used in the disciplinary procedure.

The whistleblower is further protected by a limitation of liability regarding the disclosure and dissemination of certain categories of information that would otherwise expose them to criminal, civil, and administrative liability. Specifically, the whistleblower shall not be held liable, either criminally, civilly, or administratively, for:

- disclosure of professional secrets (excluding legal and medical privilege);
- disclosure of trade secrets;
- breach of the duty of loyalty and fidelity;
- violation of provisions relating to copyright protection;
- violation of provisions relating to personal data protection;
- disclosure or dissemination of information on violations that harm the reputation of the reported party.

However, these limitations of liability are subject to certain conditions:

- at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to reveal the violation subject to the report;
- the report is made in compliance with the conditions set out in Legislative Decree 24/2023 to benefit from protection against retaliation, meaning (i) there are reasonable grounds to believe the reported facts are true, (ii) the violation falls within the scope of reportable matters, and (iii) the reporting channels and conditions are respected.

It is important to emphasize that the limitation applies only if the reasons for disclosure or dissemination are not based on mere speculation, gossip, or motives that are retaliatory, opportunistic, or sensationalistic. In any case, liability is not excluded for conduct that:

- is unrelated to the report;
- is not strictly necessary to reveal the violation;
- involves the unlawful acquisition of information or access to documents. If such acquisition constitutes a criminal offense (e.g., unauthorized access to an IT system), criminal liability and any other civil, administrative, and disciplinary liability of the whistleblower remain unaffected. Conversely, the extraction (e.g., copying, photographing, removal) of documents to which the whistleblower has lawful access is not punishable.

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS

Waivers and settlements of rights and means of protection provided by Legislative Decree 24/2023 for the whistleblower and related parties are prohibited unless carried out under specific conditions. In particular, the whistleblower and/or related parties may waive their rights and means of protection or settle them only if this occurs in protected venues pursuant to Article 2113 of the Civil Code, such as before a judge, following a mandatory conciliation attempt, or through mediation and conciliation agreements arranged in a trade union setting.

9. DISSEMINATION AND TRAINING

For the purposes of the effective implementation of the Model, it is Statkraft Italia's duty to make the rules of conduct contained within the Model known to all Recipients thereof.

The Compliance Function or the HR Function or the Office Manager makes the Model available to all Recipients by publishing the entire document on the company shared drive and, on the website, the Code of Conduct and an extract of the Model.

All subsequent amendments and/or information concerning the Model will be communicated to Recipients through official information channels, including e-mail communications and the company sharepoint.

The Compliance department, in coordination with the Office Manager and the Supervisory Board, will define and implement the training program, establishing the content and frequency of the courses and documenting the attendance.

10. MODEL'S UPDATING

Since the Model is an "act of issuance by the management body" (in compliance with the specifications of art. 6, paragraph 1, letter a) of the Decree), any subsequent substantial amendments and additions to it are the responsibility of the Company's Board of Directors. However, the SB has the task of promoting the necessary and continuous updating and adjustment of the Model.
The updating of the Model is to be considered necessary in the following cases:

(a) Changes in the internal structure of the Company and/or the way in which its activities are carried out;

(b) Changes in legislation or significant interpretations of case law;

(c) Significant violations of the Model;

(a) Commission of the offences referred to in the Decree by the Recipients;

(b) Identification of new sensitive activities, or variation of those previously identified, also possibly related to the start-up of new business activities;

(c) Identification of shortcomings and/or gaps in the provisions of the Model following checks on its effectiveness.

The Company's Board of Directors has the power to make changes or additions of a formal nature to the text of the Model (such as, for example, those necessary to adapt the text of the Model to any changes in regulatory references).

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS

Once the changes have been approved, the Company's Board of Directors will proceed to communicate the contents of said changes internally (and externally, as necessary).

The Model will, in any case, be subjected to a periodic review procedure to be arranged by the Company's Board of Directors.

11. SUBSIDIARIES

Statkraft Italia promotes the adoption of the organisation, management and control model provided for in the 231 Decree by its subsidiaries (SPVs). However, it is the responsibility of the management bodies of the individual companies to assess and, if necessary, to adopt their own organisational, management and control model and to set up their own supervisory body, as provided for in Article 6, paragraph 1, letter b) of the 231 Decree or to take a formal resolution to formally ratify the Model 231 of Statkraft Italia.

12. ANNEXES

(a) Annex 1 – Code of Conduct

(b) Annex 2 – List of relevant criminal offences

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS

Registro delle Imprese di Milano, C.F 11061330962
P.IVA 11412940964, R.E.A. MI – 2576468
Società con socio unico soggetta all'attività di direzione e coordinamento di Statkraft AS