Organisational Model pursuant to Legislative Decree no. 231 dated 8th June 2001

Rev.	Approval	Change Type
00	Board of Directors 22/09/2021	Adoption
01	Board of Directors 13/09/2023	Update

INDEX

GENERAL SECTION

SECTION 1

LEGISLATIVE DECREE 231/2001

1.1 The Administrative Liability of Entities

Enacted on 8th June 2001, in execution of the delegation of authority under Article 11 of Law no. 300 dated 29th September 2000, was Legislative Decree no. 231 dated 8th May 2001 (hereinafter, also "Legislative Decree 231/2001" or merely the "Decree"), which came into force the following 4th July, seeking to bring domestic legislation on the liability of legal persons into line with a number of international conventions to which Italy had long since acceded and, in particular:

- The Brussels Convention of 26th July 1995 on the Protection of the European Communities' Financial Interests;
- The Convention also signed in Brussels on 26th May 1997 on combating corruption by officials of the European Community or its Member States;
- The OECD Convention of 17th December 1997 on Combating Bribery of Foreign Public Officials in International Business Transactions.

The Decree introduced into the legal system the administrative liability of Entities for offences resulting from crime. Its provisions apply to "*Entities with legal personality and companies and associations, including those without legal personality*" (hereinafter, also "Entities").

This new form of liability, although defined as "administrative" by the legislator, nevertheless presents certain characteristics of criminal liability since, for instance, the competent criminal court is responsible for ascertaining the offences from which this derives and extends to the Entity the guarantees of criminal proceedings.

However, the Decree not only outlines a strict repressive scheme but also foresees a clear mitigation of this rigidity for the Entity that has adopted suitable systems for preventing the offences from which the liability of legal persons derives. The aim is to

encourage legal persons to avail of an internal organisation capable of preventing criminal conduct. Indeed, the Entity is not liable if able to prove the measures, as indicated by the legislature, have been adopted and are presumed to be suitable for the scope of prevention.

There are three basic conditions for the Entity's liability to be incurred:

- An offence has been committed to which the law attaches liability to the Entity;
- The offence was committed in the interest or to the advantage of the Entity;
- The perpetrator of the offence, being the person who causes the "administrative liability" of the Company in which or for which they works, is:
    - An apical subject, being the person who holds representation, administration or management functions for the Company, as well as the person who exercises – even de facto – the management and control thereof;
    - A person subject to the direction or supervision of senior persons.

The Entity's liability thus arises from the commission by persons belonging to said Entity of offences peremptorily specified by Decree no. 231 or, according to the provisions of Article 2, if the Entity's liability is established by another law to have come into force before the act was committed.

In addition, Legislative Decree 231/2001 differentiates the regulation of the imputation criterion operating on a subjective level according to whether the offence is committed by a person in an apical position or by a subordinate.

The Decree additionally enshrines the principle of the autonomy of the Entity's liability from that of the natural person, specifying that the Entity's liability also persists when:

- The offender has not been identified or cannot be charged;
- The offence is extinguished by a cause other than amnesty.

Such liability also applies in relation to offences committed abroad, provided that the State in which they were committed does not prosecute them and that the Entity is headquartered in the territory of the Italian State.

As such, the Entity is at risk of prosecution when:

- Its headquarters – so where administrative and management activities are carried out, which may be different from the place where the business or registered office is located (for Entities with legal personality) or else the place where the activity is carried out on a continuous basis (Entities without legal personality) – are in Italy;
- The State of the location where the act was committed is not taking action against the Entity;
- The request of the Ministry of Justice, to which the punishment may be subject, is also referred to the Entity itself.

These rules concern offences committed entirely abroad by senior or subordinate persons. For criminal conduct that took place even only partially in Italy, the principle of territoriality pursuant to Article 6 of the Italian Criminal Code applies, according to which "*the offence shall be deemed to have been committed in the territory of the State when the act or omission constituting the offence has taken place there in whole or in part, or when the event that is the consequence of the act or omission has occurred there*".

1.2 Adopting Organisation, Management and Control Models as exemptions from the Entity's administrative liability

In view of Article 5(II) of Legislative Decree 231/2001, the Entity is not liable if the active parties have acted solely in their own interest or in the interest of third parties.

Moreover, Article 6 specifies that the Company shall not be liable if it proves that:

- The governance body adopted and effectively implemented, before the occurrence of the criminal event, Organisation and Management Models capable of preventing the occurrence of crimes such as the one committed;
- The task of supervising the functioning of and compliance with the models and ensuring that they are updated has been entrusted to a body endowed with autonomous powers of initiative and control;
- The persons committed the offence by fraudulently circumventing the Organisation and Management Models;

- There has been lacking or insufficient supervision by the body responsible for such purpose.

Legislative Decree 231/01 also defines the requirements for the effective implementation of organisational models, which must:

- Identify specific protocols aimed at planning the formation and implementation of the Entity's decisions in relation to the offences to be prevented;
- Identify ways of managing financial resources that are suitable for preventing the commission of such offences;
- Provide for information obligations vis-à-vis the body in charge of supervising the functioning of and compliance with the Model;
- Periodically check and, if necessary, amend the Model when significant violations of the requirements are discovered or when changes occur in the organisation and activity;
- Establish a suitable disciplinary system to sanction non-compliance with the measures indicated in the model;
- Provide for one or more channels for reporting misconduct, one of which is able to guarantee the confidentiality of the reporter's identity by computerised means;
- Prohibit retaliation or direct or indirect discriminatory deeds against any whistleblower for reasons directly or indirectly connected to reports being made.

The mere adoption of a Model is not sufficient to exclude the Entity's liability, since it is necessary that the Model be effectively and efficiently implemented. In particular and in addition to the concrete application of the disciplinary system, the effective implementation of the model requires a periodic verification of the Model itself and its updating/amendment if significant violations of its provisions are discovered or when changes occur in the organisation or activity of the Entity.

1.3 Offences under the Decree

The offences, the commission of which may give rise to the administrative liability of the Entity, are those expressly referred to by the Legislative Decree 231/2001, as amended and supplemented.

The types of offences that may give rise today to the administrative liability of the Company, if committed in its interest or to its advantage by the aforementioned persons,

are expressly referred to in Articles 24 to 26 of Legislative Decree no. 231/01, as well as Law 146/2006 and Law 9/2013.

A complete list of offences able to give rise to the administrative liability of the Company is set out in **Annex 1** to this Model, with details of the applicable offences and a description of the legislation of reference.

1.4 The Sanctions under the Decree

Jurisdiction for administrative offences committed by the Entity falls within the competence of the criminal courts. A finding of liability may lead to the application of sanctions that are serious and prejudicial to the life of the Entity, such as:

- Financial penalties;
- Disqualifying sanctions;
- Confiscation;
- Publication of the ruling.

The financial penalties are calculated according to: (i) the seriousness of the offence; (ii) the degree of the Entity's liability; (iii) the action, if any, carried out by the Entity to eliminate or mitigate the consequences of the offence and to prevent the commission of further offences; (iv) the Entity's assets and economic conditions.

The interdictory sanctions (which can also be applied as a precautionary measure) of a duration of no less than three months and no more than seven years (with the clarification that, pursuant to Article 14[1] of Legislative Decree no. 231/01, "*interdictory sanctions are aimed at the specific activity to which the Entity's offence relates*") which, in turn, may consist of:

- Disqualification of the activity;
- Suspension or revocation of authorisations, licences or concessions functional to the commission of the offence;
- A ban on contracting with the Public Administration, except for the provision of public services;
- Exclusion from facilitations, financing, contributions and subsidies and/or the revocation of those already granted;

- A ban on advertising goods or services.

It should also be noted that pursuant to Legislative Decree no. 2/2023, if the conditions persist for the application of an interdictory sanctions that may lead to the interruption of the activity of an installation of national strategic interest, the judge shall order the continuation of the Entity's activity through a commissioner instead of applying the ban. Disqualification sanctions may not be applied if the Entity has adopted an organisational model consistent with those outlined in the measures pertaining to the procedure for recognition of national strategic interest aimed at achieving the necessary balance between the requirements of continuity of production activities and the safeguarding of other legal assets protected by the law.

SECTION 2

CY4GATE'S ORGANISATION, MANAGEMENT AND CONTROL MODEL

2.1. The Company

CY4GATE is active in the design, development and production of technologies in the areas of cyber security and cyber intelligence for institutional bodies and corporate companies.

With reference to cyber intelligence, the Company implements programmes aimed at the collection and analysis of information present online and conveyed through the Internet, as well as the collection of information produced through electronic and digital devices.

With regard to cyber security, the Company produces products aimed at protecting its customers' computer systems but also at analysing and cataloguing threats and proposing countermeasures.

The Company's commercial offer is in turn split into three different business lines of decision intelligence, cyber security and forensic intelligence, with the latter exclusively dedicated to institutional clients.

2.2. Internal Organisational Context

The organisational system defines the organisational breakdown of the Company's structure, namely the units, roles and organisational positions, identifies the persons in charge and describes their assigned areas of responsibility in compliance with the principle of segregation of duties as well as other compliance and governance principles.

The Company's human resources are divided into the main areas described below, within which the functions of the managers issuing the directives are identified.

In detail, reporting directly to the Chief Executive Officer (hereinafter, also the “CEO”) are the following structures and functions:

- **Technical Organisational Structures –** Cyber & Decision Intelligence Engineering and Forensic Intelligence Engineering;
- **Operations Structures –** Cyber Security Operations and Portfolio & Planning Management;
- **Commercial Structures –** Marketing & Sales Italy, Defence & Security Sales Italy, Defense & Security Sales Italy, International Sales;
- **Staff Structures –** Group Accounting, Finance, Controlling and Procurement and Group HR, Legal & Shared Services.

Finally, due to the particular characteristics of the role, responsibilities and mandates entrusted thereto, the Chief Information Security Officer and the Chief Security Officer functionally report to the CEO.

Acting as Advisor to the Managing Director are:

- The Data Protection Officer (hereinafter, also the “DPO”);
- The Manager of the Prevention and Protection Service.

2.3. Internal Powers and Delegations

Pursuant to the Articles of Association, all powers for the ordinary and extraordinary administration of CY4GATE are vested in the Board of Directors (hereinafter, also the “BoD”), which has delegated some of its powers to the Chief Executive Officer (hereinafter, also the “CEO”), in order to ensure unity in the day-to-day management, in implementation of the Board’s resolutions. Moreover, the Board of Directors has defined the scope of the decision-making and spending powers granted to the heads of the organisational structures, in line with the organisational and management responsibilities assigned, predetermining the limits and also establishing the procedures and limits for the exercise of sub-delegation.

The right to sub-delegate is exercised through a transparent and constantly-monitored process, graded according to the role and position held by the “sub-delegate”, in any case foreseeing the obligation to inform the delegating function.

In addition, the procedures for signing external and internal deeds, contracts, documents and correspondence are formalised whilst the relevant powers are granted to managers or employees in combined or individual form.

All structures operate on the basis of specific procedures, which define their respective areas of competence and responsibility. These procedures are issued and brought to the attention of CY4GATE.

Operating procedures that regulate how the various business processes are conducted are also branched out within CY4GATE through specific procedures. Thus, the main decision-making and implementation processes concerning CY4GATE's operations are codified, monitorable and knowable by the entire structure.

2.4. The Model 231 Adopted by CY4gate

It is CY4GATE's policy to disseminate a general culture of compliance and internal control at all levels, as defined in the Code of Ethics (Annex 3). The adoption and continuous updating of this Organisation and Management Model pursuant to Legislative Decree 231/01 responds to the need to direct the Company's work in this direction, as far as it specifically relates to "sensitive processes" connected with offences – namely the predicate offences pursuant to Legislative Decree 231/01.

CY4GATE adopts this Organisation, Management and Control Model with the aim of preventing the commission of such predicate offences by members of the Company, whether senior or subordinate to the management of others.

The purpose of this Model is to build a structured and organic internal control system, able to prevent the commission of the offences set out in the Decree.

The Model is inspired by the most advanced principles and best practices in the field of combating corporate crime and conforms to the control principles elaborated by the Confindustria Guidelines.

In implementing the above indications, the Model prepared by CY4GATE:

- Independently identifies specific areas of risk in relation to the particular activity carried out, following an analysis of its organisational structure and business operations;
- Defines an internal regulatory system aimed at preventing offences;

- Adopts a Code of Ethics that expresses the ethical commitments and responsibilities in the conduct of Company business and activities undertaken by employees, directors and associates;
- Sets a system of delegations and proxies aimed at ensuring transparent representation of the decision-making and implementation process;
- Establishes formalised procedures aimed at defining roles, responsibilities and operating methods in identified areas of risk;
- Formalises an organisational structure consistent with the Company's objectives and the activities to be performed by drafting and issuing the Company's Organisation Chart and service orders listing the main responsibilities;
- Foresees an Internal Control and Risk Management System and identifies the processes for controlling and managing financial resources, able to prevent their inappropriate use, with particular reference to the offences covered by Legislative Decree no. 231/01;
- Entrusts the Supervisory Board (hereinafter, also the "SB") with the task of supervising the functioning of the Model 231, monitoring its compliance and updating opportunities.

With this document, CY4GATE has updated the Model in order to make it responsive to CY4GATE's new business situation, including the acquisition of new companies plus the move to the regulated market Euronext Milan – STAR segment – organised and managed by Borsa Italiana S.p.A., to new legislation, to the evolution of case law and to national and international best practices.
This Model takes effect on the date of its approval by CY4GATE's Board of Directors.

The Model is addressed to all Addressees. Any violations thereof may give rise to the application of specific measures, as set out under section five of this General Section.

2.5. Structure of the Model

This Model consists of a General Section composed of five parts containing, in order:

- A summary description of the legal framework, supplemented by the offences listed in a specific annex;

- A brief presentation of the Company, the nature, methodology and structure of the Model 231 adopted by CY4GATE, its key elements, its annexes, including the Code of Ethics, the Addressees, as well as the Internal Risk Management and Control System and the rules governing the manner in which the Model is disseminated and updated;
- The rules concerning the constitution of the SB;
- The sanctions applicable in the event of violations of the rules and prescriptions contained in the Model;
- The whistleblowing system for reporting violations.

There are then Special Sections containing a description relative to:

- The various predicate offences that are concretely and potentially relevant in the Company, identified on the basis of the specific characteristics of the activity carried out by CY4GATE;
- Risk-crime activities;
- Behavioural rules, specific control principles and organisational safeguards.

2.6. Addressees

Addressees of the provisions of the Model (hereinafter, the “Addressees”), pursuant to the Decree and within the scope of their respective competences, are the members of the CY4GATE corporate bodies, management and employees, as well as all those who, for various reasons, collaborate in and/or work towards the achievement of the Company’s purpose and objectives (such as associates, partners, suppliers and so on).

2.7. Methodology

2.7.1 Analytical Identification of Sensitive Activities and Critical Areas

Article 6(2)(a) of the Decree expressly establishes that the Entity’s Model should identify the corporate activities within the scope of which the offences referred to in the Decree may potentially be committed.

The mapping of areas exposed to the risk of predicate offences being committed is carried out by means of a self-assessment process (Risk Assessment) following the following steps:

- Analysis of the Company's reality, the characteristics of the Company and the types of activities actually carried out;
- Analysis of sensitive activities, aimed at identifying areas and processes at risk;
- Analysis of the existing internal control system;
- Analysis of internal standardisation (internal procedures);
- Analysis of reporting systems (such as reports, minutes, alerts);
- Analysis of the organisational set-up (organisational chart, proxies, existing documents);
- Interviews with persons with decision-making and spending powers/department heads.

The identification of the specific areas of the Company's activities considered to be at risk in relation to the issue in question, and that of the individual offences, amongst those taken into consideration, which may hypothetically be linked thereto, is contained in the Tables of activities at risk and relative controls.

On the basis of the indications and results of the overall analysis activity outlined above, the individual corporate functions implement – after assessing the risks identified and defining the policies for managing them – the internal rules and regulatory and organisational tools that govern the processes relating to the activities at risk (such as the procedures, policies and guidelines).

These represent the conceptual starting point for the implementation of the Risk Management System, since the internal preventive measures that the agent, if determined to commit a crime, must necessarily violate in order to give rise to the Entity's administrative liability have also been identified on the basis of their findings.

As better described in Section Four of this Model, prior knowledge constitutes an important component for any person working for the Company and their cognitive reading is thus a permanent basic tool for any possible preventive intervention by all internal bodies.

As such, the identification and description of the activities at risk is in direct relation to the various types of offences referred to in Decree 231/2001 and taken into account by the Model, which can, in abstract terms, be configured with reference to the same activities.

Therefore, the connection between the activity carried out, on the one hand, and the predicate offence on the other, has been identified through the factor of abstract potentiality referring to possible deviant conduct of the individual operator, the theoretical feasibility of which is also emphasised, on a case-by-case basis, by reason of the absence of checks or simultaneous findings of third parties in any way present at the transactions.

2.7.2. Implementation of the Model and Risk Assessment

The implementation methodology of the Organisational Model follows the structuring in phases on the basis of best practice and the guidelines of the main trade associations (the principal reference being the Confindustria guidelines), in order to guarantee the quality and authority of the results.

Based on the aforementioned CY4GATE Code of Ethics and Guidelines, the work phases followed are:

- The identification, amongst the offences set out in the 231 Catalogue, of those that can be considered inherent risks and those that are not inherent with respect to the Company's processes, activities and business activities in general, distinguishing crimes relating to the end behaviour from the conduct;
- Identification of sensitive activities ("as-is analysis"), so as to identify the processes and activities within the scope of which the offences referred to in the Legislative Decree 231/01 may be committed and the activities instrumental to the commission of offences;
- Carrying out a Gap Analysis, reporting on risk mapping activities and interview outcomes, as well as reporting on audit activities conducted – here, the areas of risk considered relevant in the individual special sections indicated. Improvement or corrective measures are identified (the creation or implementation of internal procedures, preparation of new delegations and/or proxies or revision of the pre-existing structure) and finally, a summary document is prepared in an excel file (Risk Mapping).

2.8. CY4GATE's Internal Control and Risk Management System

The Internal Control and Risk Management System (hereinafter, also the "ICRMS") consists of the set of rules, procedures and organisational structures aimed at the effective and efficient identification, measurement, management and monitoring of the main risks, in order to contribute to the sustainable success of the Company.

An effective Internal Control and Risk Management System contributes to the conduct of business consistent with the corporate objectives defined by the Board of Directors, fostering informed decision-making. This contributes to ensuring the safeguarding of the Company's assets, the efficiency and effectiveness of corporate processes, the reliability of information provided to corporate bodies and the market, compliance with laws and regulations as well as with the Articles of Association and internal procedures.

The people involved in the Internal Control and Risk Management System act according to a three-tier model of control:

- The first level of control identifies, assesses, manages and monitors the risks for which it is responsible, in relation to which it identifies and implements specific treatment actions. The responsibility for defining and implementing these controls lies with management, operates at every level of the organisational structure, and is carried out within the framework of day-to-day management;
- The second level of control monitors the main risks to ensure the effectiveness and efficiency of their treatment, monitors the adequacy and operability of the controls put in place to oversee the main risks and, in addition, provides support to the first level in the definition and implementation of adequate management systems for the main risks and relative controls;
- The third level of control provides independent and objective assurance on the adequacy and effective operation of the first and second levels of control and, in general, on the Internal Control and Risk Management System as a whole, carried out by independent, non-operational units, such as by an Internal Audit.

CY4GATE adopts the traditional Administration and Control Model, also in line with the 2020 Corporate Governance Code of Listed Companies to which CY4GATE has adhered, which is able to pursue the objective of an appropriate balance of powers and a precise distinction of the functions of: (i) strategic supervision, entrusted to the Board of Directors and assisted by Board Committees; (ii) management, entrusted to the Chief

Executive Officer (hereinafter, also the “CEO”); (iii) control, carried out by the Board of Statutory Auditors.

In particular:

(i) the Board of Directors (hereinafter, also the “BoD”): a) defines the guidelines of the Internal Control and Risk Management System in line with the Company’s strategies and assesses, at least once a year, the adequacy of said system with respect to the characteristics of the business and the risk profile assumed, as well as its effectiveness; b) appoints and revokes the head of the Internal Audit Function, defining their remuneration in line with corporate policies and ensuring that the same is provided with adequate resources to perform their duties – if it is decided to entrust the Internal Audit Function, as a whole or for certain categories of operations, to a person external to the Company, it shall ensure that such person meets the prerequisites of professionalism, independence and organisation and shall provide adequate justification for such choice in the report on corporate governance; c) approves, at least once a year, the work plan drawn up by the head of the Internal Audit Function, after consulting with the control body and CEO; d) assesses the appropriateness of adopting measures to ensure the effectiveness and impartiality of the judgement of the other corporate functions, verifying that they are endowed with adequate professionalism and resources; e) assigns to the body specifically established for this purpose the supervisory functions pursuant to Article 6(1)(b) of Legislative Decree no. 231/2001 – if the body does not coincide with the control body, the Board of Directors shall assess the advisability of appointing at least one non-executive Director and/or one member of the control body and/or the holder of legal or control functions of the Company to the body, in order to ensure coordination between the various parties involved in the Internal Control and Risk Management System; f) assesses, after consulting the control body, the results set out by the Statutory Auditor in the Letter of Recommendations, if any, and in the additional report addressed to the control body; g) describes in the report on corporate governance the main characteristics of the Internal Control and Risk Management System and the methods of coordination between the subjects involved therein, indicating the national and international models and best practices of reference, expressing an overall assessment on the adequacy of the system itself and giving an account of the choices made regarding the composition of the Supervisory Board referred to in point e) above, all in addition to examining and approving ordinary and extraordinary operations, as well as the Company’s strategic

plans. Following the changeover to the regulated market Euronext Milan – STAR segment – organised and managed by Borsa Italiana S.p.A., the Board of Directors may consist of 7 to 9 members of which at least one third is independent and at least 40% are of the least represented gender.

It should also be noted that CY4GATE's Board of Directors has set up four Board Committees with advisory and proposal-making functions to guarantee additional control, being:

- ***The Risk and Sustainability Control Committee (hereinafter, also the "RSC Committee")***, composed of at least three non-executive Directors, the majority of whom are independent in accordance with the independence requirements of the Corporate Governance Code, with the Chair being chosen from amongst the independent Directors.

  Specifically, the Risk and Sustainability Control Committee is responsible for:

  (i) Assisting the Board of Directors, in an investigative, propositional and advisory capacity, in its assessments and decisions pertaining to the Internal Control and Risk Management System, as well as those concerning sustainability issues;

  (ii) Assisting the Board of Directors to: a) assess the Statutory Auditor and the auditing body, the correct use of accounting standards and, in the case of groups, their homogeneity for the purposes of drawing up the Consolidated Financial Statements; b) assess the suitability of periodic financial and non-financial information to correctly represent the Company's business model, strategies, the impact of its activities and the performance achieved, examining the content of periodic non-financial information relevant to the Internal Control and Risk Management System; d) express opinions on specific aspects relating to the identification of the Company's main risks and support the evaluations and decisions of the Board of Directors relating to the management of risks arising from prejudicial facts of which the latter has become aware; e) examine the periodic reports and those of particular relevance prepared by the Internal Audit Function; f) monitor the autonomy, adequacy, effectiveness and efficiency of the Internal Audit Function; g) possibly entrust the Internal Audit Function with the performance of audits on specific operational areas, simultaneously notifying the Chair of the

control body; h) report to the Board of Directors, at least on the occasion of the approval of the annual and half-yearly Financial Report, regarding the activities performed and the adequacy of the Internal Control and Risk Management System.

Additionally, the Committee examines and evaluates:

(i) Communications and information received by the Board of Statutory Auditors and its members concerning the Internal Control and Risk Management System;

(ii) The annual reports issued by the Supervisory Board, as well as the timely information provided by the same, after informing the Chair of the Board of Directors and the Managing Director, on any facts of particular materiality or significance ascertained in the performance of the tasks assigned thereto.

- ***The Appointments and Remuneration Committee*** assists the Board of Directors with tasks of a preliminary, propositional and advisory nature in the field of appointments and remuneration, with the Committee consisting of at least three non-executive Directors, the majority of whom are independent according to the independence requirements of the Corporate Governance Code, whilst the Chair is chosen from amongst the independent Directors;
- ***The Related Parties Committee*** is tasked with expressing an opinion on Related-Party Transactions, in accordance with specific procedures approved by the Board of Directors, with the Committee being composed of non-executive Directors, the majority of whom are independent according to the independence requirements of the Corporate Governance Code;
- ***The Strategic Committee*** assists the Board of Directors and the Company's delegated bodies with investigative, proposing and advisory functions in its assessments and decisions in accordance with the specific powers attributed thereto, it being understood that the assessment regarding the approval of the possible transactions proposed by the Committee is the exclusive responsibility of the Board of Directors. The Committee consists of at least three members. The CEO is a member of the Committee by right, whilst the remaining members of the Committee are appointed by the Board of Directors and chosen from amongst its members.

(ii) The Chief Executive Officer in charge of establishing and maintaining the Internal Control and Risk Management System: a) identifies the main corporate risks, taking into account the characteristics of the activities carried out by the Company and its subsidiaries, periodically submitting them to the Board of Directors for review; b) implements the guidelines defined by the Board of Directors, taking care of the design, implementation and handling of the Internal Control and Risk Management System and constantly verifying its adequacy and effectiveness, as well as taking care of its adaptation to the dynamics of the operating conditions and the legislative and regulatory framework; c) may entrust the Internal Audit Function with the performance of checks on specific operating areas and on compliance with internal rules and procedures in the execution of corporate transactions, simultaneously notifying the Chair of the Board of Directors, the Chair of the Control and Risk Committee and the Chair of the control body; d) promptly reports to the Control and Risk Committee problems and critical issues to have emerged in the performance of their activities or of which they have in any case become aware, so that the Committee may take the appropriate initiatives.

(iii) The Board of Statutory Auditors monitors compliance with the law and the Articles of Association along with compliance with the principles of proper administration and, in particular, the adequacy of the organisational, administrative and accounting structure adopted by the Company and its proper functioning. Supervision of the general corporate risk management processes is carried out through meetings with the heads of the main business and functional areas, participation in meetings of the Board of Directors and other Board Committees, and the exchange of information with the External Auditors. The Board also periodically collaborates with the Supervisory Board.

2.8.1. Main Parties in the Internal Control and Risk Management System

Below is a description of the tasks and responsibilities of the main parties involved in Internal Control and Risk Management System and 231.

The Internal Audit Function

Following the move from the Euronext Growth Milan segment to the STAR segment, CY4GATE decided to set up its own Internal Audit Function (hereinafter, also “IA”), which reports hierarchically to the Board of Directors. In line with the provisions of the Corporate

Governance Code, CY4GATE has decided to outsource this function to an external party with the prerequisites of professionalism, independence and organisation. The Internal Audit assesses the effectiveness and adequacy of the Internal Control and Risk Management System through an audit plan approved by the Board of Directors and the Risk and Sustainability Control Committee, based on a structured process of analysis and prioritisation of the main risks. It prepares and shares periodic reports containing adequate information on the activities conducted, on the manner in which risk management is handled and on compliance with the plans defined for containment. As part of the audit plan, the Internal Audit Function also checks the reliability of information systems and facilitates coordination with the Level II control functions and maintains direct information channels with the Managing Director, the appointed Executive, the Risk and Control and Sustainability Committee, the Board of Statutory Auditors and the Supervisory Board, having direct access and with which they communicate without restrictions or intermediation.

The Internal Audit Function thus has the task of: (i) verifying the operation and adequacy of the Internal Control and Risk Management System, both on an ongoing basis and in relation to specific needs, and providing assessments and recommendations in order to promote its efficiency and effectiveness; (ii) providing specialist support to management on matters regarding the Internal Control and Risk Management System in order to foster the effectiveness, efficiency and integration of controls into business processes and to promote the continuous improvement of governance and risk management.

The Coordination and Consultation Board for Preventing Corruption

This Board recommends to the Board of Directors any updates or amendments to the Anti-Bribery Code (**Annex 3**) with particular regard to the evolution of emerging best practices and legislation of reference or in the event of any critical issues. Subsequent amendments and additions to the Anti-Bribery Code are thus the responsibility of the Board of Directors, with the exception of formal amendments and additions to be made by the Corruption Prevention Coordination and Consultation Board with the help of the Human Resources, Legal, Anti-Bribery and Finance organisational units.

The Anti-Money Laundering Function

This Function works in line with CY4GATE's Anti-Money Laundering Policy (**Annex 4**), which verifies on an ongoing basis that the Company's procedures are in line with the objective of preventing and countering the violation of money laundering, terrorist

financing, embargo violations, arms regulations and anti-corruption. For the pursuit of the purposes set out in Legislative Decree 231/2001, the Anti-Money Laundering Function, limited to the management of risks in the areas of anti-money laundering, financing of terrorism, violation of embargoes, arms regulations and anti-corruption:

- Participates in defining the structure of the Model and in its updating;
- Promotes organisational and procedural changes aimed at ensuring adequate protection against the risk of money laundering and terrorist financing;
- Receives and forwards the periodic reports and information flows required by the “Guidelines for Combating Money Laundering and Terrorist Financing and Managing Embargoes”;
- In liaison with the other corporate functions responsible for training, ensures the preparation of appropriate training activities aimed at achieving the continuous updating of employees and associates.

The Finance Function

The Chief Financial Officer (CFO) coordinates and defines the management guidelines in the administrative-financial area for all Group companies in consultation with the other management functions. Their role consists in:

- Overseeing the administrative/financial management process and the underlying controls in order to ensure the proper functioning of the companies in such a way as to coordinate and support the Group companies and the departments that manage the core business;
- Ensuring compliance with the relevant tax and civil laws by coordinating internal and external resources.

The functions of the position are to:

- Administer the Group’s Legal Entities (LEs) in terms of the civil, tax, economic, financial and reporting aspects;
- Supervise and monitor the operation of administrative, management and tax procedures for proper management information and evaluation;
- Supervise the fulfilment of tax obligations and the keeping of all compulsory books and their fiscal regularity, also with the help of external qualified professionals chosen by them;
- Oversee the activities required to perform the statutory audit of the Financial

Statements of the Group's LEs and Consolidated Financial Statements;

- Supervise the activities necessary to provide a prompt response to requests from the Board of Statutory Auditors and the Supervisory Board;
- Take care of the legal, patrimonial and corporate aspects affecting the Company, being able to rely on the advice and input of qualified external personnel when necessary.
- Carry out continuous monitoring of compliance with Company procedures in the administration sector, with prompt notification regarding any anomalies to the appropriate functions;
- Ensure the correct interface with Borsa Italiana and the relevant supervisory bodies;
- Assist the auditors/consultants involved in specific corporate transactions (such as mergers and acquisitions, due diligence, new incorporations, share/asset transactions and so on);
- Define long-term Company policies and strategies;
- Define the directions and objectives of the underlying corporate structures;
- Implement general control over the management of the Company;
- Entrust special assignments to its members or outsiders.

It should also be noted that the Finance Function is responsible for drafting the simplified prospectus pursuant to Article 14(d) of Regulation (EU) no. 1129/2017, Delegated Regulation (EU) 979/2019 and Delegated Regulation (EU) 980/2019, filed with Consob and available on the Company's website, which provides the key information investors need to understand the nature and risks of CY4GATE, the Group and the ordinary shares that are admitted to trading on the regulated market of the Euronext Milan-STAR segment organised and managed by Borsa Italiana S.p.A.

The Appointed Manager

In compliance with the provisions of Article 154-bis of the Consolidated Law on Financial Intermediation (Law no. 262 dated 28th December 2005 on "Provisions for the protection of savings and the regulation of financial markets"), the Board of Directors appointed the CFO of the Company's manager in charge of preparing the corporate accounting documents with the functions set by the aforementioned article of the Consolidated Law on Financial Intermediation and to whom suitable powers and means were conferred for the exercise of the duties attributed by the applicable laws and regulations at the time,

also in consideration of the requirements set forth by the applicable laws and by-laws coming into force upon the listing on Euronext Milan – STAR Segment.

The Appointed Manager prepares a report on the activities carried out during the reporting period, which is submitted to the Board of Directors at the time of approval of the Draft Financial Statements and issues, jointly-signed with the CEO, the Certifications on the Financial Statements and the Consolidated Financial Statements pursuant to Article 154-bis, in accordance with the Consob structure. In particular, they attest to:

- The adequacy of administrative and accounting procedures for drawing up the Annual and Consolidated Financial Statements;
- The effective application of the procedures during the period covered by the Financial Statements;
- The correspondence of the Financial Statements with the books and records;
- The suitability of the Financial Statements to provide a true and fair view of the financial position, results of operations and cash flows of the Company and the investees included in the consolidation;
- The Management Report including a reliable analysis of the development and results of operations, together with the situation of the issuer and the undertakings included in the consolidation, along with a description of the main risks and uncertainties to which they are exposed.

In addition, it should be noted that the Finance Function and the Appointed Manager are integrated with the other Control and Risk Management Models implemented within CY4GATE and the Group, with a view to an increasingly-integrated Internal Control and Risk Management System such as, for example, with the Management Control Model referred to in section 2.8.2.

The Legal Function

For the pursuit of the purposes set out in Legislative Decree 231/2001, they provide legal assistance and advice to corporate structures, following the evolution of specific legislation and jurisprudential orientations on the subject. The Legal Function is also responsible for interpreting legislation, resolving questions of law and identifying conduct that may constitute criminal offences. The Legal Function cooperates with the Internal Audit, Human Resources and Anti-Money Laundering functions, with the Employer

pursuant to Legislative Decree 81/2008, in the adaptation of the Model, also pointing out any extensions of the scope of the Entities' administrative liability.

The DPO

In compliance with the provisions of EU Regulation 2016/679 (General Data Protection Regulation – "GDPR"), CY4GATE has set up its own Data Protection Management System. This privacy system defines the set of internal rules, methodologies, roles and responsibilities assigned to all structures involved in processing personal data. As per EU Regulation 2016/679, the Data Protection Officer is obliged to supervise compliance with the Regulation and other legal provisions on data protection, effectively being a component of the Internal Control and Risk Management system.

The privacy management system provides for other internal rules that address the activities to be enacted to ensure compliance with the provisions of the Regulation. Aspects relating to data protection by design and by default, the data protection impact assessment process, handling data breaches, the implementation of data erasure times and the management of data subjects' rights are all regulated.

The Statutory Auditing Company

CY4GATE is also subject to a statutory audit by the auditing firm appointed by the Shareholders' Meeting pro-tempore in regards to both financial and non-financial information.

In addition to carrying out the Statutory Audit of the Annual Financial Statements, the aforementioned Company also audits the financial reporting package in order to assess the appropriateness of the accounting principles adopted, as well as to assess the accuracy of the Annual Financial Statements.

The auditing activities are recorded in the special book kept at the registered office.

2.8.2. Management and Control Systems for Specific Risks

On a more strictly operational level, the various Management and Control Systems for specific risks adopted in the Company cannot be overlooked as being fundamental prevention tools that Model 231 avails of for precautionary purposes are:

- ***Management Control System (hereinafter, also the "MCS")*** – the structured and integrated set of information and processes used by management to support planning and control activities, consistent with the CY4GATE Group (hereinafter, also the "Group") Business Model, with the System designed to support management in planning and monitoring economic-financial objectives through the Finance function.

  The CFO and the parent company's Planning and Management Control Function, through their various activities, provide the necessary support and tools to:

  - ❖ Define objectives and support decisions on:
    - Identification of business strategy and objectives;
    - Identification of the guidelines and action plan to achieve the objectives;
    - Evaluation of Critical Success Factors (CSFs) and Critical Risk Factors (CRFs);
  - ❖ Monitor the following aspects:
    - Achievement of the strategic objectives formalised in the Business Plan;
    - CSFs that enable the achievement of these objectives;
    - CRFs that influence their achievement;
    - Effectiveness and efficiency of processes and functions;
  - ❖ Implement corrective actions following any deviations – positive or negative – between the final balance and the targets.

  The Management Control System has various levels and dimensions:

  - ❖ Control objects, which represent the "*what to control*" and consist of:
    - Indicators and metrics;
    - Dimensions of analysis (as described below);
  - ❖ Control instruments, which represent the "*how to control*" and consist of:
    - Organisation;
    - Planning and control processes;
    - Technical-accounting tools used to process the information;
    - Supporting information systems;
  - ❖ Timing, production responsibilities, frequency and Addressees.

- ***The Occupational Health and Safety Management System*** is adopted pursuant to Legislative Decree no. 81/2008 and elaborated on the basis of the guidelines of

the Italian National Unification-National Institute for Insurance Against Workplace Accidents (UNI-INAIL), better detailed in the relevant paragraphs of Special Section L under “Occupational Health and Safety Crimes”;

- ***The Quality Management System*** sees the Company’s activities also subject to a series of controls resulting from the application of quality procedures. Through this Quality Management System, in particular, an external body (the Certification Board) certifies that the internal management system of the Company is structured according to certain, correct and effective rules of conduct, as well as in line with a certain system of division of responsibilities and controls, compliance with which leads to the achievement of certain objectives in the market.
  CY4GATE has been awarded ISO9001:2015 certification, which marks the Company’s precise and detailed way of operating to provide a quality product and service in the following areas:

  - Design, implementation and after-sales support of ICT software and solutions, also based on Artificial Intelligence technologies, for the Cyber Security market, big data analytics plus digitisation and automation processes;
  - Provision of cyber security products, including the training of people for specialised roles in terms of their use in organised teamwork;
  - Provision of Security Operation Centre (SOC) services;
  - Real-time monitoring and incident response support;
  - Marketing of ICT SW and HW products for public and private customers.

  CY4GATE has obtained ISO9001:2015 certification in the following IAF sectors:

  - 29a. Wholesale, retail and intermediary trade;
  - 33. Information technology;
  - 37. Education.

- ***Information Security Management System***: The information security policy in CY4GATE aims to protect information assets from all threats, be they organisational, technological, internal or external, accidental or intentional, by setting the following corporate objectives:

- Ensure an appropriate level of awareness amongst staff, associates and external suppliers;
- Keep the Information Security Management System (ISMS) aligned with changes in CY4GATE's internal procedures and service delivery methods;
- Ensure adequate governance of suppliers to guarantee compliance with information security requirements;
- Ensure an adequate level of confidentiality, integrity and availability requirements in the services provided.

CY4GATE has obtained ISO/IEC 27001:2013 certification that delineates a precise and detailed way of operating the Company, capable of providing a quality product and service with regards to information security in the following areas:

- Design, development, installation, service and maintenance of HW and SW systems in the field of cybersecurity and cyber intelligence;
- Design and delivery of specialised MSS (Managed Security Services) for cyber security;
- Network security, monitoring VA/PT security systems, SOC Management, Incident Management & Analysis and Security Advisory.

A more detailed description of the system is available in the relevant paragraphs under Special Section B – "Computer Crimes".

2.9. Audit Plans

In particular, CY4GATE conducts internal audits at planned intervals on the systems described above, taking into consideration the status and importance of the processes and areas to be audited.

CY4GATE has defined the criteria, field of application, frequency and methods of the audit.

The methods include:

- Spot checks on activities related to all Company processes to assess their compliance with the defined procedures;

- Spot checks on the effectiveness of the controls carried out on the activities (self-control, control by the department manager, control by software applications – when applicable);
- Spot checks on the effectiveness of audit activities (ability of audits to intercept anomalies or deficiencies or events that do not comply with the rules established and documented through procedures or other documents).

The Company is subject to specific audits in relation to: (i) statutory audits and account checks; (ii) maintenance of the ISO 9001:2015 Corporate Quality System; (iii) maintenance of the ISO/IEC 27001:2013 Management System.

The audits are conducted, with regard to point (i) by the auditing firm as per the Audit Plan and by the Board of Statutory Auditors on a quarterly basis as well as at the time of approval of the Financial Statements. In addition, concerning points (ii) and (iii), audits by the Systems Certification Board are conducted on an annual basis for maintenance of certification through surveillance audits and on a three-yearly basis for renewals.

The results of audits relating to the Quality and Information Security system are recorded and archived on the Certification Board's portal and, consequently, on the CY4GATE corporate intranet.

Finally, the set-up of the Internal Audit Function involves a 4-step plan:

1- Audit Universe – definition of the Audit Universe (being a set of auditable units potentially subject to Internal Audit activities) with document collection and analyses, industry experiences, hot topics of the Internal audit profession;
2- Prioritisation – definition of criteria (in first application, mainly subjective) and prioritisation of auditable units (strategic drivers, specific risks);
3- Integration – internal revisions and additions to the audit plan (discussions with Risk and Sustainability Control Committee, talks with selected Top Management for the collection of management concerns);
4- 2023–2024 Audit Plan – drafting of the proposed 2023–2024 Audit Plan (highlighting the types of intervention, objectives and risks, associated effort and timing).

2.10. Other Certifications/Qualifications

a) CY4GATE is in possession of the NATO Commercial and Governmental Entity (NCAGE) code.

This five-character alphanumeric code, assigned by the Central Coding Board, identifies:

- Each individual Manufacturer and/or Supplier of supply items with a direct or indirect contractual relationship (sub-supplier) with the Defence Administration of countries under the NATO Codification System (NCS);
- A company, association, person, etcetera, that provides services to the Defence Administrations of countries adhering to the NCS;

b) The Company also holds the Licence ex. Article 28 of the Consolidated Text of Public Security Laws, for the design, manufacture, possession and sale of electronic equipment specially designed for military use intended for utilisation by domestic and foreign Armed Forces and Police Forces;
c) The Company is additionally listed in the National Register of Businesses and Consortia of Enterprises for export, import, transit and intermediation of armament materials in whole or in part, in certain categories, as better defined by the Ministerial Decree of 29th September 2021 (Official Gazette of 9th October 2021, no. 242);
d) The Company holds NOSI (Industrial Security Clearance) for the premises in Rome at Via Coponia 8;
e) The Company keeps an up-to-date register of employees who have been granted Security Clearance and who need to process information with a secrecy classification higher than “Confidential” in the context of certain projects;
f) CY4GATE is certified with the “Cybersecutity Made-In Europe” label.

2.11. Prerequisites of the Model

In preparing the Model, CY4GATE has taken into account its Internal Risk Management Control System as well as the control systems for more specific risks handled through the Management Control, Occupational Health and Safety, Quality and Information Security, in order to verify its ability to prevent the offences listed in the Decree in the activities identified as being at risk, as well as the ethical and social principles to which it adheres in the performance of its activities.

More generally, the definition of an adequate Internal Control and Risk Management System, oriented to guarantee with reasonable certainty the achievement of operational, information and compliance objectives, makes it possible to:

- Identify the risks that may affect the pursuit of the objectives defined by the Board of Directors;
- Encourage informed decision-making consistent with the Company's objectives, in the context of a broad knowledge of risks and the level of tolerance thereto, of the legality and corporate values;
- Safeguard the Company's assets, the efficiency and effectiveness of processes, the reliability of information provided to corporate bodies and the market, along with compliance with internal and external regulations.

CY4GATE's Internal Control and Risk Management System is guided by the following principles:

- Integration of the Internal Control and Risk Management System into the general organisational structure of corporate governance, administration and accounting;
- The direction and coordination of CY4GATE as parent company vis-à-vis its subsidiaries;
- Integrity and values that inspire the daily actions of the entire Company;
- Formalised and clear organisational system in the allocation of powers and responsibilities consistent with the achievement of assigned objectives;
- Attention to the staff competence system, in view of the objectives pursued;
- Identification, assessment and management of risks that could jeopardise the achievement of corporate objectives;
- Definition of corporate procedures, as part of the Company's overall regulatory system, which spell out the controls put in place to protect against risks and the achievement of set objectives;
- Suitable information systems to support business processes and the overall internal control system (IT, reporting, etcetera);
- Internal communication processes and staff training;
- Monitoring systems to supplement line controls;

- Periodic internal audits carried out by the quality audit team and/or direct audits or other audits, the frequency of which is defined by the Supervisory Board.

Within the scope of their functions, all Addressees are responsible for the definition and proper functioning of the control system through line controls, consisting of all the control activities that individual offices perform on their processes.

2.12. Fundamental Elements of the Model

With reference to the requirements identified in the Decree, the key elements developed by CY4GATE in defining the Model can be summarised as follows:

- Identification of the corporate activities within the scope of which it is conceivable that predicate offences could give rise to the liability of Entities pursuant to Legislative Decree 231/2001 (“Activities at Risk” or “Sensitive activities”), carried out by analysing corporate processes and the possible ways in which offences may be committed;
- Drafting and updating regulatory instruments relating to the processes considered to be at potential risk of offences being committed, aimed at expressly regulating the formation and implementation of the Company’s decisions, in order to provide precise directions on the system of preventive controls in relation to the individual offences to be prevented;
- Business process management according to its Internal Control and Risk Management System as well as certifiable ISO standards for specific risk management systems such as for quality and information security;
- Adoption of ethical principles and rules of conduct aimed at preventing conduct that may constitute the types of offences envisaged, set out in CY4GATE’s Code of Ethics and, more specifically, in this Model;
- Establishment of a Supervisory Board to which specific tasks are assigned in order to monitor the effective implementation and application of the Model pursuant to Article 6(b) of the Decree;
- Implementation of an appropriate penalty system to ensure the effectiveness of the Model, containing the disciplinary provisions applicable in the event of non-compliance with the measures indicated in the Model;

- Conducting information, awareness-raising, dissemination and training activities on the contents of the Model, as well as on the Rules of Conduct valid across all Company levels, characterised by capillarity, compulsory participation, verification of learning and constant updating;
- Procedures for the adoption and effective application of the Model as well as for any necessary amendments or additions thereto;
- Identification of 'at risk' activities.

2.13. Special Parts and General Principles and Safeguards of Internal Control

For all risk activities described in the individual special sections, the following general control principles apply:

- Explicit formalisation of behavioural norms;
- Clear, formal and knowable description and identification of the activities, tasks and powers attributed to each Function and to the different professional qualifications and roles;
- Precise descriptions of control activities and their traceability;
- Adequate segregation of operational and control roles;
- Integrated information systems oriented not only towards the segregation of functions but also to the protection of the information they contain, with reference both to management and accounting systems and to the systems used to support business-related operational activities.

In particular, the following general organisational/managerial safeguards must be pursued.

Behavioural standards

Adoption and adherence to the Code of Ethics in which the general rules of conduct governing the activities conducted are set out.

Definition of roles and responsibilities

The internal regulations must spell out the roles and responsibilities of organisational structures at all levels, describing the activities of each structure in a uniform manner.

These regulations must be made available and known within the organisation.

Internal protocols and rules

Sensitive activities must be regulated in a consistent and congruous manner through the Company's regulatory instruments so that at all times, the operating procedures for carrying out the activities, the relevant controls and the responsibilities of those who have acted can be identified.

Segregation of tasks

Within each sensitive business process, the functions or persons in charge of the decision and its implementation must be separated from those who record and who control such.

There must be no subjective identity between those who make or implement decisions, those who prepare accounting evidence of the operations decided upon, and those who are required to carry out the controls set by law and by the procedures laid out in the internal control system.

Authorisation and signatory powers

A delegation system must be defined within which there is a clear identification and specific assignment of powers and limits for the persons whose work involves committing the Company and manifesting its will.

Organisational and signatory powers (delegations, proxies and associated spending limits) must be consistent with the organisational responsibilities assigned.

Proxies must be consistent with the internal proxy system.

There must be mechanisms for publicising the first-level proxies granted to external stakeholders.

Mechanisms for reporting on delegated powers and relative proxies must be in place.

Provision must be made for the revocation of proxies and delgations assigned.

The delegation process must identify, inter alia:

- The organisational position held by the delegate due to the specific scope of the delegation;
- The express acceptance by the delegate or sub-delegate of the delegated functions and the consequent assumption of the obligations conferred;

- The expenditure limits allocated to the delegate;
- Delegations must be granted in accordance with the principles of decision-making and financial autonomy of the delegate;
- The technical and professional suitability of the delegate;
- The autonomous availability of resources adequate to the task and continuity of performance;
- The control and traceability activities.

Code of Ethics

The Code of Ethics (**Annex 2**) circulated to all Company employees sets out the guiding principles and fundamental directives to which the activities and conduct of the Addressees of the Code must conform, including the rules of conduct that Suppliers and Partners are required to observe specifically within the scope of their contracted activities, as well as the relevant system of sanctions in the event of any breach thereof.

The relevant sanctions system, applicable in the event of violation, is described in the aforementioned Code.

Although the Code has its own autonomous value, it complements the overall system for the prevention of offences as set out in Legislative Decree no. 231/2001 and constitutes a fundamental and supporting element of the Model itself.

This Code is also a reference for all specific policies and regulatory instruments governing activities potentially exposed to the risk of offences.

2.14. Updating and Implementing the Model

In a logic of continuous improvement, CY4GATE's Model 231 is subject to updates upon:

- New developments and/or evolutions with reference to: (i) the regulation of the liability of Entities for administrative offences dependent on crime, including new areas of application of Decree 231; (ii) the regulatory framework in the areas of interest and the principles expressed by further legislation of reference; (iii) case law and doctrine on the subject; as well as (iv) the practice of Italian and foreign companies with regard to compliance models;
- Significant changes in CY4GATE's organisational structure or areas of activity;

- Considerations arising from the application of Model 231, including experiences from criminal litigation.

The Board of Directors is responsible for the effective implementation of the Model, by evaluating and approving the actions necessary for its execution or amendment. For the identification of such actions, the Administrative Body is supported by the Supervisory Board.

The Board of Directors delegates the individual structures to implement the contents of the Model and to take care of the constant updating and application of internal regulations and corporate processes, which form an integral part of the Model, in compliance with the control and conduct principles defined in relation to each sensitive activity.

The effective and concrete implementation of the Model is also ensured:

- By the Supervisory Board, in the exercise of the powers of initiative and control conferred to it over the activities carried out by the individual organisational units in sensitive areas;
- By the heads of the various organisational units in relation to the activities at risk carried out by them.

The Board of Directors must additionally ensure, also through the intervention of the Supervisory Board, that the sensitive areas and the Model are kept up-to-date, in relation to any adaptation requirements.

The updating activity, intended both as integration and amendment thereto, is aimed at ensuring the adequacy and suitability of the Model, assessed with respect to the preventive function of the commission of the offences established by the Legislative Decree 231/2001.

On the other hand, the Supervisory Board is responsible for concretely verifying the need or advisability of updating the Model, as well as promoting this need to the Board of Directors or the Managing Director. The Supervisory Board, within the scope of the powers conferred upon it in accordance with Article 6(1)(b) and Article 7(4)(a) of the Decree, is responsible for formulating reasoned proposals for updating and adapting this Model, submitting them to the Board of Directors for approval.

In any case, the Model must be promptly amended and supplemented by the Board of Directors, also upon proposal and after consultation with the Supervisory Board, upon the occurance of:

- Violations and circumventions of the requirements contained therein that have revealed their ineffectiveness or inconsistency for the purpose of preventing offences;
- Significant changes to the internal structure of the Company and/or the way in which it carries out its business activities;
- Regulatory changes and jurisprudential developments.

Amendments, updates and additions to the Model must always be communicated to the Supervisory Board.

All such amendments and additions shall then be promptly communicated to the Addressees.

2.15. Group Company Models

CY4GATE acts as the parent company in respect of all Entities in which it holds at least a majority shareholding and exercises management and coordination functions (of the Group). Management and coordination activities are exercised through strategic control, the issuance of Group directives and regulations and through Group operational functions that ensure homogeneity of management along with product and process integration.

The CY4GATE Group, following recent acquisitions, has initiated a project to integrate its Control and Management System in order to enable constant monitoring of Company performance and the achievement of business objectives, as well as to address the Internal Control and Risk Management System, which applies to all Group companies with the aim of:

- Providing guidance to the various people involved in the Internal Control and Risk Management System, so as to ensure that the main risks – including those of sustainability in the medium- to long-term – are correctly identified and adequately measured, managed and monitored;
- Identifying the principles and responsibilities for governing, managing and monitoring the risks associated with the Company’s activities;

- Providing for control activities at each operational level and clearly identifying the tasks and responsibilities, so as to avoid any duplication of activities and ensure coordination between the main people involved in the Internal Control and Risk Management System.

Without prejudice to the autonomous responsibility of each company belonging to the Group regarding the adoption and effective implementation of its own “Organisation, Management and Control Model pursuant to Legislative Decree no. 231 dated 8th June 2001”, CY4GATE, in the exercise of its particular function as Parent Company, has the power to issue criteria and directives of a general nature and to verify the compliance of the Models of the companies belonging to the Group with these criteria and directives through the functions of Group Accounting, Finance, Controlling and Procurement, Group Human Resources, Legal & Shared Services, Internal Audits, each to the extent of their respective competence.

In order to standardise at Group level the methods through which to transpose and implement the contents of the Decree, the companies in which CY4GATE holds a majority stake must comply with the principles and contents of the Parent Company’s Model unless there are specific situations relating to the nature, size or type of activity carried out as well as the corporate structure, organisation and/or articulation of internal delegations that impose or suggest the adoption of alternative measures in order to more effectively pursue the objectives of the Model, in compliance with the aforementioned principles as well as those expressed in the Code of Ethics.

SECTION 3

SUPERVISORY BOARD

PREAMBLE

Article 6 of the Decree foresees that the function of supervising and ensuring the updating of the Model is entrusted to a Supervisory Board within the Entity which, endowed with autonomous powers of initiative and control, continuously exercises the tasks assigned to it.

The CY4GATE Supervisory Board consists of members of proven experience and competence, satisfying the requirements of honour, professionalism and independence.

They are appointed by the Board of Directors, which also determines their remuneration.

The Supervisory Board remains in office for three years and, in any case, until the date of the Shareholders' Meeting convened for approval of the Financial Statements for the last year of office.

A member of the Supervisory Board may be one of the heads of the functions who are not assigned management or, in any case, operational roles and who meets the appropriate requirements of independence, professionalism and honourableness.

Nonetheless, upon expiry of the term of office, each member of the Supervisory Board remains in office until the appointment of a new Supervisory Board by the Board of Directors.

This is, however, without prejudice to cases of resignation of a member of the Supervisory Board, which takes immediate effect.

The Supervisory Board has autonomous powers of initiative and control along with its own rules of procedure.

The Board exercises all supervisory powers, including preventive powers, in relation to the operating and internal control procedures, as well as to the protocols established in

compliance with Article 6(2) of Decree no. 231/2001 and in relation to anti-money laundering (where applicable), in the application of which it may also request internal assistance from the Entity through the heads of each individual function concerned.

For the exercise of its supervisory powers over corporate activities, the Board may commission third parties to conduct investigations or checks also on the records or other acts of the Entity.

Amongst the requirements that the Model must meet, the Decree sets out in Article 6(2)(d) the establishment of information obligations vis-à-vis the Supervisory Board.

Constitutive and Operating Rules of the Supervisory Board

The Supervisory Board operates in accordance with the requirements set out below.

Article 1

SUPERVISORY BOARD

CY4GATE's Supervisory Board (hereinafter, also the "Board") is the management-appointed body established within the Entity pursuant to Article 6(1)(b) of Legislative Decree no. 231 dated 8th June 2001, endowed with autonomous powers of initiative and control with reference to the application of the provisions of the aforementioned Decree, the Model and the Company procedures contained and/or referred to therein. The Board's operational functionality is ensured by the mandatory application of these rules.

Article 2

Appointment and Composition of the Supervisory Board

The Board consists of three members appointed by the Board of Directors of the same Company for a term of three financial years.

Individuals with valid and recognised experience in legal, economic or business management matters may be members of the Board, provided that together they guarantee that the Board bears the characteristics of autonomy, independence, professionalism and continuity of action.

Upon appointment, the Board of Directors also appoints the Chair of the Board. No employee or internal person may be appointed as Chair of the Board.

Article 3

Causes of Ineligibility, Disqualification and Revocation

The following constitute grounds for ineligibility and/or disqualification of the members of the Supervisory Board:

- Having held the position of Executive Director, in the three fiscal years preceding the appointment as member of the Supervisory Board, in companies subject to bankruptcy, compulsory liquidation or similar procedures;
- Having been convicted with a ruling which has the force of res judicata, also resulting from a request for application of the penalty (plea bargaining), in Italy or abroad, in relation to offences of the same nature as those set out in the Decree;
- Having been convicted by a ruling which has the force of res judicata, to a penalty which entails the disqualification (even temporary) from public office or the temporary disqualification from the executive offices of legal persons and companies;
- Failure to attend at least three consecutive meetings without a justified reason;
- During the three-year term of office, any shortcoming in the requirements that determined the identification of the members at the time of their appointments and, by virtue of the corporate office or organisational role held.

The following constitute grounds for revocation of the members of the Supervisory Board:

- Lacking and/or insufficient supervision by the Supervisory Board resulting from a ruling which has the force of res judicata, issued against the Company pursuant to Decree 231, even following a request for application of the penalty (plea bargaining);
- Serious breach of the functions and/or duties of the Supervisory Board.

Removal is ordered by resolution of the Board of Directors approved by a two-thirds vote of those present and after consulting the other members of the Supervisory Board and the Board of Statutory Auditors.

In the event of the loss or revocation of one of the members of the Supervisory Board, the Board of Directors shall promptly replace them.

The dismissal of one or all members of the Board may be ordered, exclusively by resolution of the Board of Directors passed with the favourable vote of as many Directors as represent at least two-thirds of the entire Board. In addition to the cases indicated above, the members of the Board may be revoked for those cases exhaustively indicated in the resolution of the Administrative Body nominating and appointing them.

If, throughout the three financial years, one or two members of the Board should relinquish their office or otherwise cease to perform their function, the Board may replace them with other members of the same function (provided that they comply with the provisions of this Article), until the natural expiry of the term of office for the Board.

Even before the ruling becomes final, CY4GATE's Board of Directors may opt for the revocation or suspension of the individual member's powers and the possible appointment of an *interim* member if said member of the Supervisory Board has been convicted of particularly serious crimes at first instance and/or if a personal precautionary measure has been ordered against them.

Article 4

Duties and Powers of the Supervisory Board

Constituting the institutional tasks of the Board are:

- Supervision of the functioning of the Model established pursuant to Decree 231/2001;
- Supervising compliance with the Model, both inside and outside the Entity;
- Drafting periodic updates of the Model;
- Supervising compliance with the rules (where applicable) against money laundering.

In addition to the tasks assigned pursuant to Decree no. 231/2001 as indicated above, the Supervisory Board is also assigned the task of directly or indirectly monitoring the compliance of appointed personnel with internal operating procedures and applicable regulations.

Upon request and according to the needs expressed by the Supervisory Board, the Board of Directors makes available adequate corporate resources in relation to the tasks entrusted to it and, in preparing the corporate budget, approves – on the basis of the

proposal made by the Supervisory Board itself – an adequate endowment of financial resources that the Supervisory Board may use for the proper performance of its tasks.

The Board is also required to formally communicate the Company's Model to each member of the management and control bodies.

In relation to sensitive activities, the Supervisory Board prepares and executes a plan of activities and checks aimed at assessing, monitoring and supervising the actual application, adequacy and functionality of the regulatory instruments, in terms of safeguards aimed at preventing the commission of the offences covered by the regulatory framework.

The Board establishes a mutual communication plan with the corporate bodies and with all internal or external persons entrusted with carrying out internal control activities. The Board also has the power to consult all the books and registers of the Entity established pursuant to any law.

Taking into account the specific nature of the powers of the Board and its professional content, the Board may avail of the collaboration of other management and control functions of the Entity that may be necessary on occasion, as well as of external professionals and consultants, within the framework of the availability provided for and approved by a specific budget.

With reference to the aforesaid supervisory powers, the Board – taking into account the particular structure of the CY4GATE Model as a document also linking and integrating the corporate compliance systems already in force within the Company – may exercise part of the same also by requesting, as a body of reference, the assistance of the persons in charge of the control systems already adopted by the Company, in order to coordinate and maximise the activities already carried out by the latter, if necessary, also by preparing special checklists to be used in the performance of the respective cited control activities.

To this end, the Board may periodically organise individual or collective meetings with the various persons in charge of the different control functions, in order to receive from them the reports of their respective control activities and, in particular, their reports on any anomalies and critical issues, along with any suggestions on possible amendments to the Model. Upon the outcome of the aforementioned coaching and coordination of the

persons in charge of the various control functions mentioned, any further organisational measures to be modified and/or adopted may be assessed.

The Board may hear the Chair, the Managing Director or another Director (each individually).

As an alternative to the foregoing, the Board may proceed with obtaining the aforementioned information by means of appropriate written reports delivered, duly signed by the person issuing the information.

Article 5

Reporting by the Supervisory Board to the Corporate Bodies

The Supervisory Board reports to the Board of Directors and the Board of Auditors regarding its activities and in particular:

- On an ongoing basis, directly to the Chair of the Board of Directors and/or the Chief Executive Officer, also by sending the Minutes of their meetings or extracts thereof, concerning the overall activity performed, the critical issues to have emerged, the analysis of the reports and the relevant initiatives adopted, the proposals for revising and updating the Model, and information on the Activity Plan for the following year;
- On a regular basis, at least once a year, to the Board of Directors and/or the Managing Director and the Board of Statutory Auditors, by means of a report on the Company's implementation of the Model, any shortcomings, as well as on relevant and general elements concerning the adoption of the Organisational Model. By means of this report, the Board also details and/or summarises any non-compliance and violations of the Model, indicating all appropriate corrective actions to be taken. Any repeated and particularly serious violations must be promptly reported to the Chair and Managing Director, the Board of Directors and the Board of Statutory Auditors;
- Promptly informs the Board of Directors whenever it comes across particularly serious situations.

The Supervisory Board may be convened at any time by the Board of Directors or the Board of Statutory Auditors to report on the operation of and compliance with the Model or on specific situations.

Article 6

Information Flows to the Supervisory Board

In order to meet the requirements set out in the Decree (Article 6[2][d]), specific information obligations are imposed on the Supervisory Board.

To this end, the following are foreseen:

Periodic information flows, such as:

- Those relating to procedural changes that are significant for the purposes of Model 231;
- Periodic reporting on the most significant risk activities and the status of preparation and updating of internal regulatory instruments;
- Any communications from the auditing company;
- Budgets and reports;

Ad hoc flows of information relating to:

- Current or potential critical issues that, by way of example, may emerge from occasional news from the structure or corporate bodies relating to business activities along with organisational changes that are significant for the purposes of Model 231;
- Updates to the system of powers;
- News relating to proceedings or investigations concerning offences under Decree 231;
- Disciplinary proceedings against the Addressees for violation of Model 231 or the Code of Ethics.

The information flows that must be mandatorily and promptly transmitted to the Supervisory Board include information concerning:

- Measures and/or information from judicial or tax police bodies or any other authority, including administrative authorities, involving the Company or apical persons, from which it can be inferred that investigations are being conducted, even against unknown persons, for offences under the Decree, without prejudice to the legally-imposed obligations of confidentiality and secrecy;
- Requests for information or the sending of provisions, reports and any other documentation resulting from inspection activities carried out by the same and falling within the scope of Legislative Decree 231/2001;

- Communications to the Judicial Authority concerning potential or actual unlawful events that can be referred to in the hypotheses set out in Legislative Decree 231/2001;
- Requests for legal assistance made by managers and/or employees in the event of legal proceedings being initiated, in particular for offences covered by the Decree;
- Results of the control activities carried out by the heads of the various corporate functions from which critical facts, deeds, events or omissions have emerged with respect to compliance with the provisions of the Decree or the Model;
- Changes in the system of delegated and proxy powers, amendments to the Articles of Association or changes to the Company Organisation Chart;
- Information on the actual implementation of the Model across all levels of the Company, with evidence of the disciplinary proceedings carried out and any sanctions imposed, or of the orders to dismiss such proceedings with the relevant reasons;
- Reporting serious injuries (fatal accidents or accidents with a prognosis of more than 40 days) occurring to employees, contractors and/or associates present in the Company's workplaces;
- Reports of the Internal Audits carried out within the framework of the Quality System, the Risk Management System and the Control System, carried out according to the programme defined by the Supervisory Board.

Article 7

Procedure for Reporting to the Supervisory Board

The new whistleblowing regulation under Legislative Decree 24/2023 acts on Article 6(2a), stipulating that organisational models must provide for internal reporting channels, the prohibition of retaliation and the disciplinary system.

In order to protect the integrity of the Company, employees are required to transmit circumstantiated reports of relevant unlawful conduct, pursuant to Decree 231 and based on precise and concordant factual elements, or of violations of this Organisational Model of which they have become aware by reason of their duties, through the following communication channels:

- Reporting via a web platform

The whistleblower visits the **Integrity Line** web page, which can be reached via a link from the company's website or at CY4GATE Group | Home (integrityline.com), submits a message in Italian or English and receives a unique identification number for the report. The system deposits a copy of the message in a digital space accessible by the Company's legal department and the members of the Supervisory Board, who will deal with the message in accordance with the Company's reporting instrument.

The reporting party also has the option to record a voice message, upload documents or take a photo to support the report.

- Reporting in verbal, written or paper form

Whistleblowers can submit the communication, drawn up in paper form according to the principles contained in the internal procedure, in the dedicated box located at the Company's headquarters and marked "Internal Reporting".

In the context of the Model 231, reports are to be addressed to the Supervisory Board via:

- Verbal communication to the Supervisory Board;
- Email to OdV231@cy4gate.com, also available in the Company Directory;
- Regular mail to Via Coponia 8 – 00131 Rome, Italy.

The confidentiality of the reporter's identity is guaranteed in the handling of reports.

The Company guarantee of the prohibition of retaliation or direct or indirect discriminatory deeds against any whistleblower for reasons directly or indirectly connected to reports being made is reaffirmed.

In any case, should the Supervisory Board deem it necessary to proceed with a further investigation of the facts, it may call upon the support of the corporate control functions.

All information, documentation and reports collected in the performance of institutional tasks must be filed and kept by the Supervisory Board for a period of time not exceeding that necessary for the purposes for which the data was collected or subsequently processed and, in any case, in compliance with internal policies and procedures on personal data processing.

(a) Prohibited reports

Reports must always contain information from which a loyal spirit of participation in the control and prevention of facts harmful to the general interests emerges and may in no way be the instrument to vent disagreements or disputes between employees.

Likewise forbidden is:

- The use of insulting expressions;
- The submission of reports for purely defamatory or slanderous purposes;
- The submission of reports that relate exclusively to aspects of private life, without any direct or indirect connection with the Company's business – such reports will be considered even more serious when they refer to sexual, religious, political or philosophical habits and orientations.

(b) Content of the reports

The reporting person is obliged to provide all elements known to them that are useful to verify the facts reported.

In particular, the report must contain the following essential elements:

- The object – a clear description of the facts to be reported required with an indication (if known) of the circumstances regarding the time and place in which the facts were committed/permitted;
- The reported party – the whistleblower must indicate the personal details or, in any case, other elements (such as the function/role of the Company) enabling easy identification of the alleged perpetrator of the unlawful conduct.

In addition, the reporter may indicate the following further elements:

- Their personal details;
- An indication of any other persons who may report on the facts narrated;
- Details of any documents that may confirm these facts;
- Any other information that may facilitate the gathering of evidence on what has been reported.

(c) Management of reports

The principles of reference guiding the handling of reports are those laid out in Legislative Decree no. 24/2023 as well as the ANAC Guidelines and subsequent updates, including:

- Guarantee of confidentiality and protection of whistleblowers – the Supervisory Board will act in such a way as to ensure absolute confidentiality and non-disclosure of the whistleblowers' names;
- Bad faith reports – the Supervisory Board guarantees adequate protection against bad faith and/or unsubstantiated reports, censuring such conduct and informing the persons/companies concerned of such cases, as established by the general principles of the sanctions system;
- Data security and integrity requirements – the Supervisory Board and the Company shall act in such a way as to ensure that the channels and methods for handling reports guarantee compliance with the requirements of confidentiality, integrity and availability of data through the security measures in place for corporate IT tools.

Article 8

Meetings

The Supervisory Board meets quarterly, or at the request of the Board of Directors due to any operational need connected to the provisions of Decree 231/2001, or in any case when deemed appropriate.

Convening of the Board is arranged by the Chair availing of appropriate means to ensure that that the Board is informed at least 5 (five) days before the scheduled meeting. The convening of the Board is not deemed necessary if all its members are present.

Meetings of the Board are presided over by the Chair or, in their absence, by the oldest member in terms of age. Under no circumstances may an employee or, in any case, an internal person preside over the meeting.

The Meetings of the Board are considered valid with the presence of the majority of its members. Resolutions are passed by a majority of the members present. In the case of a tie, the Chair's vote prevails.

Before the start of each meeting, the Board appoints a Secretary from amongst its members to take the Minutes.

The Meeting Minutes, drawn up by the Secretary and signed by them together with the Chair, are then retained in a special register.

Article 9

Confidentiality and Secrecy

The Board undertakes to ensure that any information, data or news relating to CY4GATE that it becomes aware of and acquires in the course of the performance of its duties will be: (i) deemed and kept confidential; (ii) used exclusively for the performance of the assignment itself; (iii) retained for a time that is limited and, in any case, strictly necessary for the fulfilment of the purpose for which it is intended.

Article 10

Archiving

All the findings of the audits carried out by the Board must be formalised in documents kept, together with the Meeting Minutes, in special paper or electronic files.

The manner in which this documentation is stored is left to the discretion of the Board, provided, however, that its confidentiality, integrity and ready availability are guaranteed.

Copies of the documentation required for verification activities are kept in special archives with restricted access.

Article 11

Reference

For anything not expressly covered in these regulations, reference is made to the contents of the Model.

In the event of a conflict between these regulations and the Model, the latter shall prevail.

SECTION 4

STAFF TRAINING AND INTERNAL AND EXTERNAL DISSEMINATION OF THE MODEL

4.1 Personnel Training

CY4GATE promotes knowledge of the Model and its updates amongst all employees, who are required to be familiar with and implement the Model.

The Human Resources Organisational Unit manages communication to personnel as well as training on the contents of the Decree and the implementation of the Model, reporting to the Supervisory Board.

In this context, communicative actions include:

- Communication of the Model and the Code of Ethics to all employees;
- The provision of the Code of Ethics to all existing staff, as well as the distribution of these documents to new employees when they join the Company, with a signature attesting to their receipt and commitment to knowledge of and compliance with its provisions;
- An update on any changes made to the Model and the Code of Ethics.

The training course is divided into the following levels:

- Managerial and representative staff – meetings with first-level managers and class-room style workshops with the managers;
- Other personnel – information at the time of recruitment, any training course carried out by means of meetings or e-learning through IT support on the Company intranet.

Any refresher sessions will be held in the event of significant changes to the Model, where the Supervisory Board does not deem it sufficient to simply disseminate the change in the manner described above, due to the complexity of the issue.

In addition, CY4GATE organises specific courses for personnel working in sensitive areas with the aim of clarifying in detail the critical issues, the warning signs of anomalies or irregularities, and the corrective actions to be implemented for anomalous or at-risk operations.

4.2 Information to External Collaborators, Consultants and Partners

CY4GATE also promotes awareness of and compliance with the Model and the Code of Ethics amongst the Company's business and financial partners, consultants and associates in various capacities as well as its suppliers.

SECTION 5

DISCIPLINARY SYSTEM

5.1 Sanctions for Employees

In relation to employees, the Company complies with the requirements of Article 7 of Law no. 300/1970 (Workers' Statute) and the provisions contained in the applicable National Collective Labour Agreement (Metal-Mechanical Industry Sector), both with regard to the sanctions that can be imposed and to the manner of exercising disciplinary power.

Any employee's failure to comply with the provisions of the Model and/or the Code of Ethics, as well as all the documentation that forms part thereof, constitutes a breach of the obligations arising from the employment relationship pursuant to Article 2104 of the Italian Civil Code and is a disciplinary offence.

More specifically, any Company employee's adoption of conduct that can be qualified, on the basis of the previous paragraph, as a disciplinary offence also constitutes a breach of the employee's obligation to perform the tasks entrusted to them with the utmost diligence, complying with the Company's directives, as set out in the applicable National Collective Labour Agreement.

Upon notification of a breach of the Model, disciplinary action will be taken to ascertain said breach. In particular, at the assessment stage, the employee shall be notified in advance regarding the allegation and will be granted a reasonable period of time to reply. Once the breach has been established, a disciplinary sanction proportionate to the gravity of the breach committed shall be imposed on the perpetrator.

Employees may be subject to the sanctions set in the applicable metalworking industry National Collective Labour Agreement, which, by way of example, are set out below:

- Verbal reprimand for minor offences;

- Written reprimand in the event of repeated infringements of the offences referred to in the previous point;
- Fine to an amount not exceeding 3 hours of normal pay calculated on the minimum wage;
- Suspension from pay and service for up to a maximum of 3 days;
- Disciplinary dismissal without prior notice and with other consequences of reason and law.

In order to highlight the correlation criteria between violations and disciplinary measures, it is specified that:

- Any employee who violates the provisions contained in the Model and in all the documents forming part thereof, or in the performance of activities at risk, adopts conduct that does not comply with the prescriptions contained in the Model itself, and any such conduct that fails to comply with the orders given by the Company shall incur disciplinary sanctions;
  On the other hand, disciplinary termination measures are imposed on any employee who:

- In the performance of the activities at risk, adopts conduct that does not comply with the provisions contained in the Model, and in the documentation that forms part thereof, such conduct being a lack of discipline and diligence in the performance of their contractual obligations that is so serious as to damage the Company's trust in the employee;
- In conducting at-risk activities, adopts conduct that is clearly in conflict with the provisions contained in the Model and in the documentation that forms part of the Model, such as to determine the concrete application against the Company of the measures set out in the Legislative Decree 231/2001, such conduct constituting an act that causes serious moral and material harm to the Company and that does not permit the continuation of the relationship, even temporarily.

The Company may not take any disciplinary measures against the employee without complying with the procedures laid out in the applicable National Collective Labour Agreement for individual cases.

The principles of correlation and proportionality between the violation committed and the sanction imposed are guaranteed by compliance with the criteria of:

- Seriousness of the violation committed;
- The employee's task, role, responsibility and autonomy;
- Predictability of the event;
- Intentionality of the conduct or degree of negligence, recklessness or inexperience;
- Overall conduct of the offender, with regard to the existence or otherwise of disciplinary precedents under the terms of the applicable National Collective Labour Agreement;
- The concurrence of several workers in agreement with each other involving the infringement committed;
- Other special circumstances characterising the infringement.

It is understood that all the provisions and guarantees cited in the National Collective Labour Agreement concerning disciplinary proceedings will be followed.

In particular, to be observed is:

- The obligation to give advance notification of the charge to the employee with an indication of the facts constituting the infringement and of the time limit, from receipt of the notification, within which the employee may present their justifications, and of the hearing of the latter in order to defend themselves;
- The obligation not to adopt the disciplinary measure, if more serious than a verbal reprimand, before the minimum period established under Article 7 of the Workers' Statute from the written notification of the charge, during which the employee may present their justifications;
- The obligation to communicate the adoption of the disciplinary measure in writing, within and no later than the maximum time limits provided for in the applicable National Collective Labour Agreement, from the expiry of the time limit set for the employee to submit their justifications, or else the disciplinary proceedings are concluded with archiving.

The existence of a system of sanctions connected with non-compliance with the provisions contained in the Model and in the documentation that forms part of it must, as a necessity,

be brought to the attention of employees by the means deemed most appropriate by the Company.

5.2 Sanctions Against Managers

In the event of a breach by Managers of the internal procedures provided for in this Model or conduct in the performance of activities at risk that does not comply with the prescriptions of the Model, the appropriate measures will be applied against those responsible in accordance with the provisions of the applicable National Collective Labour Agreement for Managers. Where the breach is such as to break the relationship of trust, the sanction will be dismissal for just cause.

5.3 Measures Against Directors and Auditors

The Supervisory Board informs the Chair of the Board of Directors and the Chair of the Board of Statutory Auditors of reports of violations of the Model or the Code of Ethics by Directors and Statutory Auditors that are not considered manifestly unfounded, so that they may refer the matter to the bodies they preside over. Articles 2392 and 2407 of the Italian Civil Code apply.

5.4 Measures Against Members of the Supervisory Board

In the event of violations of this Model by one or more members of the Supervisory Board, the other members of the Supervisory Board or any of the Auditors or Directors shall immediately inform the Company's Board of Statutory Auditors and the Board of Directors. These bodies, subject to any contest of the breach and taking note of any defensive arguments put forward, shall take the appropriate measures, including, for example, revocation of the assignment.

5.5 Measures Concerning Suppliers, Collaborators, Partners and Consultants

Any violation by Collaborators outside the Company, Shareholders in companies and Entities in which the Company has an interest, Suppliers of goods and services and Partners

of the rules laid down in Decree 231 and/or the Code of Ethics may be grounds for contract termination. The breach must be reported without delay to the Board of Directors or the Managing Director by the person to have detecting the violation. If the Board of Directors or the Chief Executive Officer considers the complaint to be well-founded, it may order the immediate termination of the contract and inform the Supervisory Board. It shall also inform the Supervisory Board of cases in which it does not proceed to terminate the contract due to considering the complaint to be unfounded or because termination would be seriously detrimental to the Company.

Termination of the contract entails the ascertainment of the damages that the Company may have suffered and the consequent action for compensation.

SECTION 6

REPORTING VIOLATIONS (WHISTLEBLOWING)

6.1 Applicable Legislation

CY4GATE implements the discipline of whistleblowing, pursuant to Legislative Decree no. 24/2023, also towards Group companies, through the management of dedicated channels.

The new rules on whistleblowing, acting on Article 6(2-bis), stipulate that organisational models must provide for internal reporting channels, a prohibition of retaliation and a disciplinary system.

6.2 The Whistleblower

Pursuant to Legislative Decree 24/2023, the whistleblower is the person who reports, discloses or denounces to the judicial or accounting authorities, any violations of national or European Union law that harm the public interest or the integrity of the Public Administration or private Entity, of which they have become aware in a public or private employment context.

Persons working in the occupational context of a public or private sector Entity are eligible to report, whereby they are:

- Civil servants;
- Employees of private sector Entities;
- Self-employed persons working for Entities in the public or private sector;
- Collaborators, freelancers or consultants working for Entities in the public or private sector;
- Volunteers and trainees, paid or unpaid;

- Shareholders and persons with administrative, management, control, supervisory or representative functions, even where such functions are exercised on a de facto basis, in public sector or private sector Entities.

6.3 When and What to Report

Reports can be made:

- Whilst the legal relationship is ongoing;
- During the probationary period;
- When the legal relationship has not yet begun, if information on violations was acquired during the selection process or at other pre-contractual stages;
- After the dissolution of the legal relationship if the information on violations was acquired before the dissolution of the relationship (retirees).

What can be reported:

Conduct, acts or omissions detrimental to the public interest or the integrity of the Public Administration or the private Entity and consisting of the below.

Violations of national regulations:

- Administrative, accounting, civil or criminal offences;
- Unlawful conduct pursuant to Legislative Decree no. 231 dated 8th June 2001 (predicate offences) or violations of the organisation and management models provided for therein.

Violations of European regulatory provisions:

- Offences falling within the scope of European Union relative to the following areas:
    - Public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; nuclear safety and security; food and feed safety and animal health and welfare; public health; consumer protection; privacy and data protection and the security of networks and information systems;
- Acts or omissions affecting the financial interests of the Union;

- Acts or omissions concerning the internal market (such as competition and state aid violations);
- Acts or conduct that frustrate the object or purpose of the provisions of EU acts.

6.4 Reporting Channels

Reports must be transmitted through one of the following specially-designated channels:

- Internal channel;
- External channel (A.N.AC);
- Public disclosures;
- Report to the judicial authority.

It is worth pointing out that the choice of reporting channel is no longer left to the discretion of the reporter as the use of the internal channel is favoured as a matter of priority and, only if one of the conditions set out in Article 6 of Legislative Decree 24/2023, is external reporting possible.

CY4GATE has set up **two internal channels** for the transmission and handling of reports that guarantee the confidentiality of the reporting person, the facilitator, the person involved or otherwise the persons mentioned in the report as well as the content of the report and relative documentation.

The reporting channels are described in Article 7 of the SB Regulation (Section III).

6.5 Whistleblower Protection and Handling of 231 Reports

The principles of reference guiding the handling of reports are those laid out in Legislative Decree no. 24/2023 as well as the ANAC Guidelines and subsequent updates, as better listed and described in Article 7 of the SB Regulation (Section III). Also to be noted is:

- Prohibition of retaliation – under no circumstances may the Company apply to the whistleblower acting in good faith any form of retaliation or threat as a result of the report, such as but not limited to dismissal, non-promotion, demotion, reduction in salary, discrimination or non-renewal of the employment contract.