Organisation, Management and Control Model in accordance with Italian Legislative Decree no. 231 of 8 June 2001

- GENERAL PART-

CONTENTS	

DEFINITIONS	
At-risk activities	A process, a transaction, an act or a set of transactions and acts that may expose Datalogic to a risk of offences
National Collective Labour Agreement	National Collective Labour Agreements applied by Datalogic
Code of Conduct	Corporate Code of Conduct for listed Companies, in its most recent version approved in 2015, issued by the *Corporate Governance Committee* and promoted by Borsa Italiana, the complete text of which is available on the web site www.borsaitaliana.it
Code of Ethics	The Code of Ethics adopted by the Group and approved by the Datalogic Board of Directors on 4 November 2009, as amended, the complete text of which is available at www.datalogic.com
Consultants	Parties that act in the name and/or on the behalf of Datalogic pursuant to an agency contract or another professional service contract
Datalogic	Datalogic S.p.A., headquartered in Calderara di Reno (Bologna) on Via Marcello Candini no. 2, resolved, subscribed and paid-in share capital EUR 30,392,175.32, Bologna Company Register enrolment number and tax code 01835711209, Administrative and Economic Index no. BO-391717
Decree	Italian Legislative Decree no. 231 of 8 June 2001, as amended
Addressees	Corporate bodies, Employees, Consultants, Partners and Suppliers
Employees	Persons with an employment or coordinated and continuous contractual relationship with Datalogic, including managers
Suppliers	Suppliers of goods and services to Datalogic which are not classified as Partners
Group	Datalogic S.p.A. and its subsidiaries or associates
Offences	Administrative offences consisting of abuse of inside information (art. 187-bis TUF - Consolidated Law on Finance) and market manipulation (art. 187-ter TUF) for which an appreciable risk level was identified as regards the activities carried out by Datalogic

Model	Organisation, Management and Control Model adopted by Datalogic, in accordance with articles 6 and 7 of the Decree
Corporate Bodies	Datalogic's Board of Directors and Board of Statutory Auditors
Supervisory Body	The collective body within Datalogic in charge of supervising the implementation of and compliance with the Model, as well as its updating
Partner	Contractual counterparty (including customers) with which Datalogic has established a contractually governed relationship, and which will work together with Datalogic in the area of at-risk activities
General Part	The section of the Model containing, among other things, the description of the role of the Model and of the Supervisory Body, as well as a description of Datalogic and the Group
Special Parts	The parts of the Model expressly dedicated to each Crime and Offence, which also set forth the relative prevention procedures
Public Administration	The public administration and, for offences related to the public administration, public officials and public service employees
Crimes	The type of crime to which the administrative liability regulations set forth in the Decree apply. The Model considers only the crimes for which an appreciable risk level has been identified within Datalogic's business
Consolidated Law on Finance (TUF)	Italian Legislative Decree no. 58 of 24 February 1998 - "Consolidated Law of financial intermediation provisions"- as subsequently supplemented and amended

1. Italian Legislative Decree no. 231/2001 – *Preamble.*

In execution of the mandate pursuant to Italian Law no. 300 of 29 September 2000, on 8 June 2001[1], the Italian government issued Italian Legislative Decree no. 231/2001 containing the "*Provisions on Administrative Liability of legal persons, companies and associations, also without legal personality*", which updated Italian law in relation to the liability of legal persons on the basis of some International Agreements previously signed by the Italian government[2].

The Delegated Legislator has introduced into the Italian legal system an autonomous liability system applicable to entities, for offences following the committing of crimes (to be added to the liability of the physical person who has materially committed them), characterised by presuppositions and consequences other than those expressly set forth in terms of the criminal liability of the physical person.

Therefore entities may be held responsible if, before a crime is committed by a subject associated therewith (see *infra*), they had not adopted and effectively implemented their own organisational and management model capable of avoiding crimes of the type that was committed.

In particular, the entities may be held liable about the offence if the crime was committed:

(i) by physical persons carrying out representative, administrative or management functions for said entities or for one of their organisational units holding financial and functional autonomy; by physical persons who carry out, de facto or otherwise, the management and the control of said entities (i.e. *subjects in a top corporate position*) as well as by

(ii) by physical persons under the management or supervision of one of the subjects listed at point sub (i) (i.e. *subjects in a subordinate position*).

This liability applies in addition to the liability of the natural person who actually executed the deed.

In order to hold the company liable, it is also necessary that the assumed unlawful conduct of the identified subjects was carried out “in the interest or to the advantage of the Company”[3], whereas said liability is expressly excluded if the crime was committed “in the perpetrator's own or in a third party's exclusive interest”.

---

[1] In force as of 4 July 2001.

[2] OECD (Organisation for Economic Cooperation and Development) convention of 17 December 1997 on the bribery of foreign public officials in international business transactions. OECD and European Union conventions against bribery in international commerce and against fraud to the detriment of the European Community. In particular, art. 11 of the Delegate law (Italian Law no. 300 of 29 September 2000) delegated the government to regulate this type of liability.

[3] As regards the liability for crimes committed by legal entities and by companies, the provisions of the law, based on the assumption that the crime was committed “in the perpetrator's own interest or advantage”, do not contain a hendiadys because the terms refer to two legally different concepts with a distinction made between an upstream interest related to an undue enrichment, envisaged ex ante but possibly never materialised, following the unlawful act, and an advantage that was objectively achieved by committing the

More precisely, the Court of Cassation has stated that the entity is not liable for an administrative offence that depends on a crime since the act was committed by a subject in its own or third party's interest, not even partially connected with the interest of entity, or if it is not possible to configure an identification between the company and its corporate bodies. Except for the above, the entity does not recognise liability for what its employee/representative has committed if it can demonstrate to have adopted the necessary measures to avoid the type of offence that was committed (adoption and effective implementation of the Model).

The case law has also pointed out that the liability attributed to the entity by Italian Legislative Decree 231/2001 results from a "negligent act within the organisation" of the legal entity (ex plurimis, Criminal Court of Cassation, Section VI, 18-02-2010 - 16-07-2010, n. 27735). The non-adoption of the Model, in the presence of the objective and subjective conditions described above (offence committed in the interest and for the advantage of the company, and senior management position of the perpetrator of the offence) is sufficient to constitute that kind of blameworthiness, mentioned in the Ministerial Report transposing the Legislative Decree, and to represent a situation subject to sanctioning due to the omission of the set forth organisational and management precautions for the prevention of some types of crime. The concept of blameworthiness implies a new "regulatory" form of culpability for organisational and management omission, since the legislator has already reasonably deduced from actual facts that have occurred in recent decades, within an economic and management scope, the legitimate and grounded conviction of the necessity that any organisational structure constituting an entity, ex art. 1, paragraph 2 of Italian Legislative Decree 231/01, adopts organisational and management models designed to prevent the commission of certain offences, which experience has demonstrated to be functional to structured and consistent interests[4]. This "organisational culpability" assumes specific relevance within the scope of a group of companies.

1.1 (continues): The adoption of the Model as a possible exemption from liability.

However, in introducing the aforementioned system of administrative liability, art. 6 of the Decree sets forth a specific form of exemption from said liability if the entity can demonstrate that, in the case of an offence committed by subjects in a senior management position:

a) the executive body of the entity had adopted and **effectively implemented**[5], before the act was committed, an organisational and management model designed to prevent the *liable offences* of the type that occurred;

---

crime, although not predicted, so that the interest and the advantage are actually linked. Court of Cassation, Section II, 20.12.2005 no. 3615. The requirement of the interest or advantage of the entity, as a criterion for objective attribution of liability to the entity itself, can also certainly include an indirect advantage, intended as an acquisition for the company of a privileged position in the market resulting from the crime committed by a senior management subject. Nevertheless, the nature of the liability attribution criterion as recognised by the law, requires a concrete, and non-abstract assertion of the existence of such interest or advantage, to be understood respectively as a potential or actual usefulness, although not necessarily of an equity nature, deriving to the entity from the commission of the liable offence. Court of Milan – Order of 28.04.2008.

[4]Criminal Court of Cassation Section VI – 9.07.2009 no. 36083.

[5] Necessary requirement because the adoption of the model exempts the entity from liability if said model is effectively implemented.

b) the task of supervising the functioning of and compliance with the models as well as of ensuring their update has been entrusted to one of the entity's bodies which has independent powers of initiative and control;

c) the persons who have committed the liable offences have acted in fraudulent evasion of the aforementioned models;

d) the body pursuant to letter b) above did not fail to or insufficiently supervise.

In the event of a crime committed by a person in a subordinate position, the adoption and effective implementation of the Model means that the entity shall be liable only if the crime was made possible due to non-compliance with the obligations of direction and supervision.

Furthermore, the Decree sets forth that the models pursuant to letter a) must satisfy the following requirements:

a) identify the activities regarding which it is possible that the offences and crimes may be committed;

b) set out specific protocols which plan the definition and implementation of the entity's decisions in relation to the crimes and offences;

c) identify financial resource management procedures which are suitable for preventing committing those crimes and offences;

d) set out information obligations in relation to the body in charge of supervising the functioning of and compliance with the model;

e) introduce an internal disciplinary system suitable for penalising the failure to comply with the measures set forth in the model.

Finally, art. 7, paragraph 3 and 4, of the Decree, introduces two principles that appear to be significant and decisive for the purpose of the entity's exemption from liability, since it is expressly set forth that:

a) the model must set out measures suitable for guaranteeing that business is carried out in compliance with law, and for discovering at-risk situations in a timely fashion, taking into consideration the type of business carried out as well as the type and size of the organisation;

b) for the model to be effectively implemented, routine controls must be carried out and the model must be amended if significant violations of legal precepts are discovered or if significant changes are made to the organisation or regulations.

It should be noted that, ultimately, from a merely formal perspective, the adoption and effective implementation of a model is not required; rather, it is an option for entities. However, for the companies with shares listed in the Segment of Equities with High Requirements (S.T.A.R.) of the Telematic Stock Exchange (M.T.A.), organised and managed by Borsa Italiana S.p.A. (as are the shares of Datalogic), the adoption and

effective implementation of a model is considered a fundamental prerequisite for a listing in this segment.

1.2 (continues): Liable offences.

Not all offences committed by the parties indicated above involve the administrative liability of the entity, since the Decree considers only specific types of offences (called liable offences) relevant. Furthermore, it must be taken into consideration that the "catalogue" of relevant liable offences pursuant to the Decree is being continuously expanded.

For further details on the liable offences currently in effect, please refer to related regulatory framework, available on the Gazzetta Ufficiale (www.gazzettaufficiale.it).

However, please note that the Special Parts of this Model only consider the *liable offences* for which an appreciable risk level has been detected in relation to the business carried out by Datalogic. The Datalogic Board of Directors shall be responsible for adding Special Parts in relation to other types of liable offences, if such action is found to be necessary on the basis of routine controls.

1.3 (continues): Penalties.

Should the persons pursuant to the introduction commit one of the liable offences, the entity may be subject to the following administrative penalties:

a) financial penalties;

b) interdiction penalties, such as:

   i) the prohibition from carrying on business;

   ii) the suspension or withdrawal of authorisations, licences or concessions which may support committing the crime;

   iii) the prohibition from contracting with the public administration, unless to obtain public services;

   iv) the exclusion from facilitations, loans, contributions or subsidies and the possible withdrawal of those already granted;

   v) the prohibition from advertising goods and services.

c) confiscation;

d) publication of the ruling.

These interdiction penalties may be adopted also as a precaution.

Moreover, the Judicial Authorities may order:

1. the preventive attachment of items permitted to be confiscated;

2. the conservative attachment of the entity's moveable property and real estate if there is a grounded reason to believe that the guarantees for the payment of financial penalties, expenses for the legal proceeding or other amounts due to the government do not exist or are being wasted.

1.4 (continues): Model suitability

For the purpose of drawing up the Model and the subsequent assessment of its suitability, it should be noted that it is important to take into account the case-law (still quite scarce) on that issue and the criteria set out thereby; in particular the Court of Cassation (holding an opposite view from the GUP of Milan on 17.11.2009 and the Court of Appeal of Milan on 21.03.2012) has established, in summary, that "a model is deemed suitable when the procedures supporting it are suitable to avoid the commission of a liable offence".

It is also important to underline what was established by the G.I.P. of Milan (Mr D'Arcangelo) in November 2010. The judgement has set out the principle according to which "*acting in compliance with the law is removed from the discretion of the businessman, and the non-compliance risk cannot be considered by the Directors as an acceptable risk*".

This judgement also states that "*the judge who is called to decide on the suitability of an organisational model must refer to the regulations of a certain sector in terms of the time when the disputed criminal conduct occurred, and must verify which organisational precautions were adopted by the entity to avoid such criminal act and how the same were actually implemented with reference to the best technical expertise available at the time" [...] "the suitable precautionary model is, in fact (as it can be deduced, at a methodological level, also by the mandatory content of art. 30 of Italian Legislative Decreeno. 81 of 9.4.2008) the one built on the best knowledge, proven and accepted at the historical moment when the offence was committed, in terms of the methods applied for neutralising or minimising the typical risk".*

2. GROUP STRUCTURE – *Preamble*.

Datalogic is a global technology leader in the automatic data capture and factory automation markets. In particular, the company is specialized in the designing and production of barcode readers, mobile computers, sensors for detection, measurement and safety, RFID, vision and laser marking systems, with the aim to increase the efficiency and quality of processes in the Retail, Manufacturing, Transportation & Logistics and Healthcare industries, along the entire value chain.

The Organisational Structure of the Group encompasses the following companies, included in the scope of application of Italian Legislative Decree no. 231/2001, directly or indirectly controlled by Datalogic S.p.A.:

- **Datalogic S.r.l.**;
- **Datasensing S.r.l.;**
- **Datalogic IP TECH S.r.l..**

2.1 (continues): Datalogic S.r.l.

The company Datalogic S.r.l. carries out design, manufacturing (also under license agreements), marketing, sale and distribution (including related installation, repair and maintenance services) of the products - services of the Datalogic Group, and in particular:

- Electronic equipment, software and systems for the reading, recognition, acquisition, collection, processing, monitoring, control, transmission and communication of data and voice of any type, including devices (fixed and/or portable) for the scanning of bar codes (and/or other symbols) and mobile computers for the collection, processing and transmission of data and voice, fixed scanning systems for reading bar codes and/or other symbols for any type of application that allows for the generation, collection, processing and transfer of data;

- Data reading, writing and transmission with RFID (Radio Frequency Identification) technology or other technologies;

- Laser-based technology systems for the marking, cleaning and/or welding of products, and for applications in the medical and safety fields;

- Sensors for identification, measurement and safety;

- Vision systems;

- Image-based identification systems;

- Control, management and configuration of equipment network systems and software;

- Software for the management of points of sale.

Datalogic S.r.l. uses different R&D centres (located in different countries such as Italy, the US and China) as well as different production sites (located in Italy, Slovakia, Vietnam and Bulgaria) operating in more than 30 countries through its own subsidiaries and/or companies (Europe, America, Asia and Oceania).

2.2 (continues): Datasensing S.r.l.

The company Datasensing S.r.l. carries out research, design, manufacturing, marketing, sale and distribution of the products - services of the Datalogic Group, and in particular:

- Vision and image-based identification systems;

- Sensors for identification and measurement and safety;

- Optical and laser sensors for applications in safety fields.

Datasensing S.r.l. uses an R&D centre as well as different production sites (located in Italy and China) operating in different countries through its own subsidiaries and/or companies.

2.3 (continues): Datalogic IP TECH S.r.l.

The company IP TECH S.r.l. carries out activities for the development, coordination, organisation and deployment of advanced research works within the Datalogic Group, through:

- the use and exploitation, in all forms, of the results obtained from the research;
- acquisition of and making available technologies and know-how as well as the management of technological products;
- management, in all forms, of the activities related to the protection of patents, licenses, know-how and other intellectual and industrial property rights.

2.4 (continued): Datalogic Group and administrative liability as per Italian Legislative Decree 231/2001

As the Holding company of the Group, Datalogic S.p.A., in order to further improve the application of the provisions of the Decree, has deemed it appropriate to adopt, with this Model, a "231 System" which would represent, through its principles, the reference point for the other companies that are part of the Group. The system can be summarised as follows:

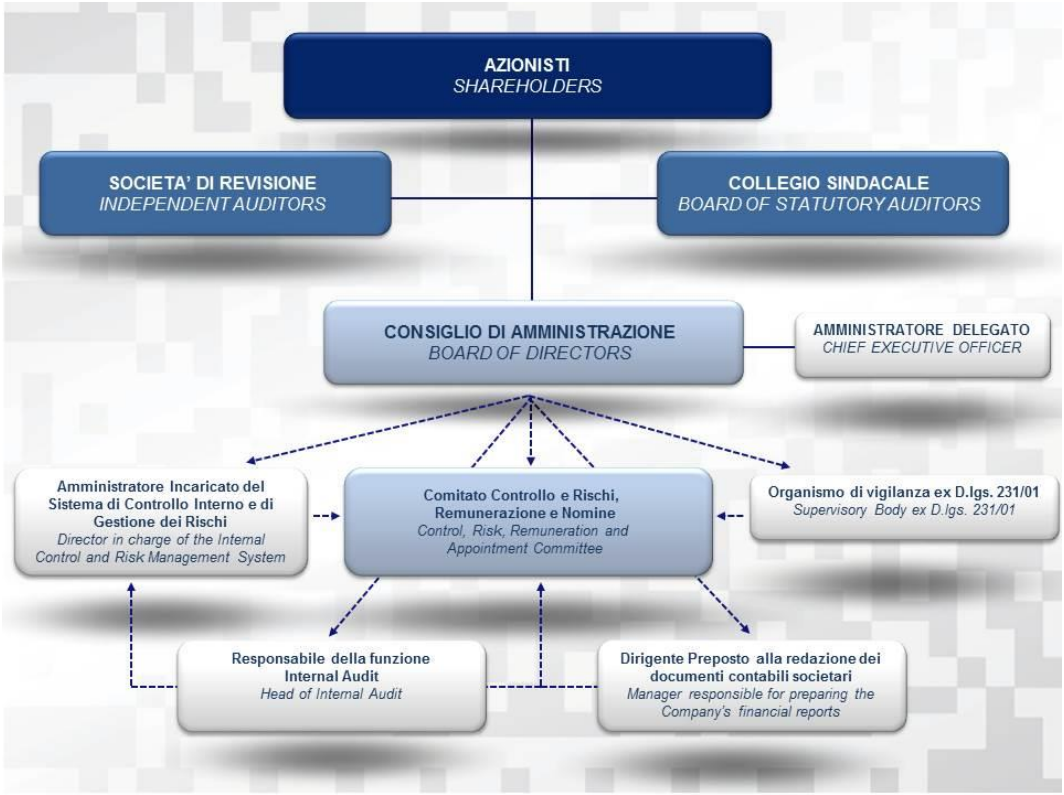
1. all the Italian companies that are part of the Datalogic Group, directly or indirectly controlled, have adopted, autonomously and depending on their own characteristics and structure, as well as of their risk profile, an Organisational Model;
2. this Model, once adopted, is subject to appropriate implementation for the most effective execution;
3. for each company, a Supervisory Body is appointed, in compliance with the provisions of the Decree in terms of composition, expertise and functions;
4. Datalogic S.p.A. sets out, for its own protection, the minimum criteria of the Organisational Model adopted by the several subsidiaries, as well as the operational criteria of the different Supervisory Bodies;
5. The Supervisory Body of Datalogic S.p.A., among its specific tasks, must monitor to ensure, through appropriate information flows, that all the Supervisory Bodies of the Group correctly carry out their control activities, as set forth in the Decree.

3. CORPORATE GOVERNANCE - *Datalogic S.p.A.*

Datalogic continuously places particular focus on the effectiveness and implementation of its corporate governance system, and uses corporate governance domestic and international best practices as a basis for a further development of its decision-making and control structures.

Datalogic S.p.A. traditional corporate governance system, shown in the flowchart below, is inspired by the principles of management and informational fairness and transparency, which it achieves through a process that continuously controls the effective implementation and effectiveness of those principles.

In compliance with the unique features and characteristics of its corporate structure, Datalogic complies with the Code of Conduct in the forms and in compliance with the conditions set forth in its Report on Corporate Governance and Ownership Structure, drawn up pursuant to article 123-bis of the TUF, which may be found at www.datalogic.comin the Governance section. The content of this report is an integral and essential part of the Model.



4. THE DATALOGIC MODEL – *Preamble.*

Datalogic decided to adopt and implement the Model with the conviction that it could be a valid instrument for raising awareness in all parties that work in the name and on behalf of Datalogic, so that they behave correctly and consistently while carrying out their tasks in order to prevent the risk of committing crimes and offences.

The Datalogic Model - representing a "*deed issued by the executive body*" (pursuant to art. 6, paragraph 1, letter a) of the Decree) - was approved for the first time by the Board of Directors of the Company on 12 May 2005, and was subsequently fully adopted by the administrative bodies which, over time, have succeeded the previous ones and have made, at the request of the Supervisory Body, a range of additions to the Model in accordance, on the one hand, with the evolution of the organisational structure of the companies and, on the other hand, with any new provisions applicable to this area over

the years through the introduction of additional types of liability offences[6].

The Organisational Model of the Company, drawn up also in compliance with the Confindustria "Guidelines", is based on a pyramid structure of principles and procedures that can be described as follows:

a) A General Part, where the Model is described in terms of objectives, functioning and corporate bodies in control thereof;

b) A Special Part, where all the operating processes, aimed at preventing the commission of offences within the corporate scope, are defined, in particular:

   i. Crimes against the public administration;

   ii. Corporate crimes;

   iii. *Market abuse*;

   iv. Occupational safety;

   v. Receiving stolen goods and money laundering;

   vi. Cybercrimes and unlawful data processing;

   vii. Tax crimes.

For the definition of the Special Part "Safety at the workplace", the OHSAS 18001:2007 international standards have been adopted as a reference point for the parts regarding safety and hygiene at the workplace.

[6] The Board of Directors carries out the following activities in order to adopt and routinely update the Model:

a) identifying the corporate operating areas to be included in the Model and mapping the at-risk activities to subject to analysis and monitoring;
b) analysing existing protocols on at-risk activities and defining any implementations aimed at ensuring compliance with the precepts of the Decree; in that area, particular attention is paid to:
   (i) the definition of ethics principles in relation to the behaviours that could amount to the crimes and/or offences;
   (ii) the definition of Datalogic processes which, in principle, could provide the conditions, occasions or means for committing crimes and/or offences;
   (iii) the definition of employee training procedures;
   (iv) the definition of information to be provided to Addressees;
   (v) the definition and application of disciplinary provisions which are suitable for penalising lack of compliance with the measures set forth in the Model and are suitable for deterring the commission of crimes;
c) the identification of the Supervisory body and attributing specific tasks to it aimed at supervising the effective and correct functioning of the Model;
d) the definition of information flows to the Supervisory Body.

4.1 (continues): Role of the Model.

The Model is based on a structured and organised system of procedures and control activities (to be carried out also preventively), implemented by Datalogic and aimed at preventing the commission of crimes and offences.

In particular, through the identification of at risk activities, as well as of the control measures to which said activities are subject, the Model intends to:

a) develop awareness in all parties that work in the name and on behalf of Datalogic, especially in those at-risk activities, that if they violate the provisions set forth in the Model, they are committing a crime subject to penalties on both the criminal and administrative levels, which will be charged not only against that party, but also against Datalogic;

b) remind the addressees that Datalogic strongly condemns those unlawful behaviours since (even if Datalogic were apparently in the condition to reap advantages from them) they are in any case against both legal provisions and the ethical-corporate principles that the company adheres to in executing its corporate mission;

c) permit Datalogic to react in a timely manner to prevent or impede the commission of crimes and offences by making use of a system to monitor at-risk activities.

Datalogic has identified the following specific tools that are employed to plan the definition and implementation of company decisions and execute controls on corporate activities, also in relation to the crimes and offences to be prevented:

1. the rules of corporate governance adopted in transposing the Code of Conduct;
2. the Code of Ethics;
3. the internal audit system;
4. the penalty system referred to in the National Collective Labour Agreements.

4.2 (continues): Mapping of at-risk activities.

Through an analysis of the operating structure of Datalogic, the main at risk activities, as well as the related corporate areas[7] and protocols adopted as preventive measures, have been identified. The results of this analysis are summarised in the table below.

[7] The functional aggregation of the At-Risk Areas - Activities is representative of the current Organizational Design – Operational Footprint of the Group (available on the website www.datalogic.com – *Organization* section).

Special parts	At-risk activities	Corporate areas at risk								Preventive protocols			Risk Assessment Highlights	
		AFC	LEG & IP	IT	RU	SG	OP	COM	ST	ORG	PROC	SIS	Main At-risk activities	Main preventive protocols (related to main activities)
A	Crimes against the Public Administration	✓	✓		✓	✓			✓	✓	✓	✓	> Administrative measures instrumental to the performance of corporate activities (authorizations - certifications)	> Governance: AFC – SG – LEG & IP > Processes: vendor selection – indirect procurement – payment management > Systems: accounting – information
B	Corporate Crimes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Representation of corporate events in the Financial Statements	> Governance: AFC – LEG & IP > Processes: financial reporting > Systems: accounting – information > Certifications: accounting – financial
													> Extraordinary transactions	> Governance: AFC – LEG & IP > Processes: inside information – extraordinary transactions > Systems: accounting – information > Certifications: accounting – financial
C	Market Abuse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Inside information - extraordinary transactions	> Governance: Company Direction – AFC – LEG & IP > Processes: inside information – internal dealing > Systems: accounting – information > Certifications: accounting – financial
													> Public reporting	> Governance: AFC – LEG & IP – COM > Processes: corporate events management – external communication > Systems: accounting – information > Certifications: accounting – financial
D	Safety in the workplace	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Facility Management	> Governance: SG – RU – LEG & IP > Processes: safety safeguards management > Systems: accounting – information > Certifications: ISO 45001 – ISO 14001 – SA8000
E	Handling stolen goods and money laundering	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Commercial Transactions	> Governance: OP – VM – AFC – LEG & IP > Processes: procurement – payment – sales – revenues > Systems: accounting – information > Certifications: accounting – financial
													> Financial Transactions	> Governance: AFC – LEG & IP > Processes: financial management > Systems: accounting – information > Certifications: accounting – financial
F	Cybercrimes and unlawful data processing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> IT security – internal infrastructure	> Governance: IT – LEG & IP > Processes: IT security management (software – hardware) > Systems: accounting – information > Certifications: ISO 27001
													> IT security – products and solutions	> Governance: RS – IT – LEG & IP > Processes: IT security management (products – solutions) > Systems: accounting – information > Certifications: ISO 27001
G	Tax crimes	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Tax declarations	> Governance: AFC > Processes: tax calculation – ICTP model > Systems: accounting – information > Certifications: accounting – financial
													> Tax credits	> Governance: AFC – RS – LEG & IP > Processes: calculation of patent box credits – product and solutions development > Systems: accounting – information > Certifications: accounting – financial

Corporate areas at risk:

- **AFC** Administration, finance and control
- **LEG & IP** Legal affairs and intellectual property
- **IT** Computer systems
- **RU** Human resources
- **SG** General services
- **OP** Purchasing, planning, production, logistics, quality, engineering (Operations)
- **VM** Communication
- **ST** Strategy

Preventive protocols:

- **ORG** Organizational structure / System of proxies / Separation of roles
- **PROC** Corporate procedures and processes / Codes of conduct / Operational frameworks
- **SIS** Information and application systems / IT infrastructure

The following preventive protocols guarantee the prevention of offences and/or crimes as well as the monitoring of the corporate areas at risk:

ORG: general configuration of the corporate organizational structure and consequent assignment of powers and responsibilities; segregation of duties aimed at avoiding overlapping or centralization of approval powers;

PROC: existence of corporate procedures and processes that guarantee the protection of company assets, the efficiency and effectiveness of company operations, the reliability of the accounting and financial information and compliance with laws and regulations; adoption of codes governing suitable rules of conduct to guarantee the exercise of business activities;

SIS: presence of an IT system to guarantee the process to prepare accounting and financial reports, as well as to oversee reliability – fairness of information and activities, conveyed through the use of applications and, more in general, of the corporate IT infrastructure.

A Special Part is dedicated to these at risk activities to which reference should be made.

The risk associated with other liable offences[8], as set forth in the Decree, is actually quite remote and difficult to conceive in the interest or advantage of Datalogic.

4.3 (continues): Control principles and preventive control systems.

The Model is based on the internal control system of Datalogic, founded on the attribution of responsibilities, hierarchical structure lines and description of tasks, with a specific set out of control principles, such as, for example a system of checks and balances.

In particular, the manual and electronic procedures implemented by Datalogic (the management computer system and in general the processes managed by the Information Systems function) are such as to regulate the carrying out of activities while setting up the appropriate control points and adequate security levels.

In addition, in designing the processes, where ever possible, a separation of tasks was introduced for those who carry out crucial activities within a process at risk, and transparency and auditability principles were taken into consideration (in particular, it was ensured that each operation, transaction, action would be verifiable, documented, consistent and appropriate).

As regards financial management where the procedural controls use validated tools, different preventive protocols were adopted including joint signature (for amounts exceeding the strict needs of daily operations), frequent reconciliations, supervision and levels of authorisation, separation of responsibilities with the above mentioned system of checks and balances.

The model also provides for a management control system capable of providing timely alerts, as the case may be, regarding the onset or the existence of abnormal situations.

Within the organisational system, specific attention was paid to the system of bonuses that are meant to be incentives but are also achievable, thus avoiding objectives that are obviously unreasonable and unreachable which then might lead to the commission of offences and/or crimes.

In addition, with a special reference to authorisation and signature powers, these have been assigned based on the defined organisational and management responsibilities, thus establishing in advance, when necessary, a precise indication of the thresholds for expense approval.

The limits in authorisation and signature powers are transposed, as blocking protocols, into the general information system.

In all cases, depending on the current Model, nobody is attributed unlimited powers and appropriate measures are adopted so that powers and responsibilities are clearly defined and well known inside the organisation.

[8] For the complete list of offenses, please refer to the full text of Italian Legislative Decree 231/2001, and subsequent amendments and additions.

To this end, no one can manage in total autonomy an entire process, and for each transaction an adequate documentation support (or electronic support for processes under the management information system) is required and can be, at times, audited to verify the characteristics of and motivation for a specific transaction as well as to identify the subjects who have authorised, recorded or verified said transaction.[9]

Therefore, the Model covers all aspects of Datalogic activities also through a clear distinction between the operating tasks and the control tasks, for the purpose of correctly managing activities at risk and avoiding possible conflict of interest situations.

In particular the controls involve, with different roles and at different levels, the Board of Directors (in particular the Control and Risk Committee established within it), the Board of Statutory Auditors, the subject in charge of internal controls (Internal auditor)[10], the Supervisory Body and the Employees.

As regards the aspects of "controls", the Model, besides providing for the establishment of an autonomous and independent Supervisory Body, guarantees the integration and coordination of the activities carried out by the latter with the existing system for internal control, building on the accrued expertise.

The Model does not modify the functions, the tasks and the objectives already existing in the control system, but aims at providing greater guarantees about compliance of the corporate practices and activities with the provisions of the Code of Ethics and the corporate regulations which set forth the principles that govern the at-riskactivities.

Finally, still in the areas of controls, the Models provides for the obligation of documenting (also through the drawing up of reports) any inspection and control activity that is carried out.

5. MODEL AND CODE OF ETHICS

The conduct rules in this Model are complementary to those in the Code of Ethics, although, due to the ends that the Model intends to pursue in the implementation of the provisions set forth in the Decree, its scope is different from that of the Code of Ethics.

In fact, while the Code of Ethics is an instrument adopted independently, and is generally applied by Datalogic in order to express the principles of "corporate ethics" that the Datalogic Group recognises as its own and with which all employees are called

[9]The Model aims at guaranteeing the principle of separation of functions, so that the authorisation for carrying out a transaction must be under the responsibility of a person different from the one in charge of the accounting, or the one who is operatively executing or controlling the transaction.

[10]It must be noted that on 26 June 2007, the Board of Directors of Datalogic approved the regulations issued by the Audit Committee aimed at governing, in a uniform and coordinated fashion, the tasks and the accounting control functions of the Special Accounting Committee, called Audit Committee. More specifically, the Audit Committee ensures the monitoring and the control of the organisation and ensures the efficiency of the internal control procedures and processes for the preparation of the financial statements, while also guaranteeing the uniformity, comparison and coordination of the activities carried out by the existing control bodies (such as the Control and Risk Committee, the Board of Statutory Auditors and the Independent Auditing firm). Currently the *Audit Committee* has been established at Datalogic S.r.l.

to comply, the Model, on the other hand, satisfies specific precepts contained in the Decree and in the TUF, aimed at preventing the commission of crimes and offences.

6. THE SUPERVISORY BODY – *Preamble*.

As a condition for obtaining exemption from administrative liability, art. 6, lett. b) of the Decree requires that the task of supervising the functioning of and compliance with the Model as well as its relative updating be entrusted to a body within the company that has independent powers of initiative and control.

The Board of Directors, considering the size of the Company, its organisational structure and the characteristics of its business, establishes the Supervisory Body by appointing its members after determining the number, in compliance with the requirements stated in this paragraph, or attributing the related functions to the Board of Statutory Auditors appointed by the Shareholders' Meeting.

The Supervisory Body is characterised by the following requirements:

- Autonomy and independence

  The requirements of autonomy and independence are fundamental in ensuring that the Supervisory Body is not directly involved in the management activities that constitute the subject matter of its control activities. These requirements are guaranteed by the indisputability, by the corporate bodies, of the decisions made by the Supervisory Body and provide for the obligation of reporting to the Board of Directors.

- Professionalism

  The Supervisory Body has, internally, the technical-professional skills and expertise adequate to the functions that it is called upon to carry out; these characteristics, together with its independence, guarantee the objectivity of its judgement.

- Business continuity

  The Supervisory Body (i) works constantly on the supervision of the Model, vested with the necessary auditing powers; (ii) it is configured as an internal structure, so as to guarantee the continuity of its supervisory activity; (iii) it ensures the implementation of the Model and its constant update; (iv) it does not carry out operating tasks that may affect its overall corporate vision of the activities performed.

The tasks assigned to the Supervisory Body require, therefore, that, in carrying out its activities: (i) it holds autonomous powers of initiative and control; (ii) it is placed outside of the production processes, as a staff unit reporting directly and exclusively to the Board of Directors and therefore is not bound by any hierarchical relationship with the individual managers of the corporate operating structures.

In carrying out its supervisory and control activities, the Datalogic Supervisory Body (i) is supported by all the corporate functions and may use other external resources, if

necessary, from time to time; (ii) is authorised to freely access all the Company's functions – without any prior consent – in order to obtain information or data that it deems necessary to carry out the tasks as set forth in Italian Legislative Decree 231/2001.

It must be noted that as regards health and safety, the Supervisory Body may use all the resources available for the management of related aspects, including the Manager of the Prevention and Protection Service (Responsabile del Servizio di Prevenzione e Protezione - RSPP), the staff of the Prevention and Protection Service (Addetti al Servizio Prevenzione e Protezione - ASPP), the Workers Safety Representative (Rappresentante dei Lavoratori per la Sicurezza - RLS) and the Occupational Physician (Medico competente - MC) as well as the staff in charge of providing first aid and managing any fire emergency situations.

6.1 (continues): The composition of Datalogic's Supervisory Body.

The Board of Directors, if the functions of the Supervisory Committee are not attributed to the Board of Statutory Auditors, may freely choose the members of the Body itself from among those subjects who meet the following:

- Professional requirements

  The members of the Supervisory Body must be chosen from among those subjects who are specifically qualified and with experience in administrative or control activities, or subjects who have held executive positions in companies, public entities, public administration or who have carried out or are carrying out professional or university teaching activities in judicial, economic and financial subject matters.

  In consideration of the size and related rules of corporate governance, the presence in the Supervisory Body of the following is recommended:

  a. the manager of the Internal Auditing office of Datalogic who must be knowledgeable of the organisational and corporate structures and be therefore able to facilitate the actual and concrete activities to be carried out by the Supervisory Body, as set forth in the Decree;

  b. two professionals, lawyers or economists, who have accrued specific expertise in the criminal law applied to the economy, finance and corporations, so as to consistently support the activities of the Supervisory Body with a "*legal sensitivity*" that is clearly "*specialised*"[11].

- Personal and integrity requirements

[11]For biographical and background information on the members of the Supervisory Body in office, see the Corporate Governance and Shareholding Structure Report, pursuant to art. 123-bis of TUF, to be consulted on the web site www.datalogic.com- section *Governance*.

It is also necessary to guarantee that the members of the Supervisory Body have, in addition to professional qualifications, also personal qualities such as the ability to carry out the tasks assigned to them which they must declare at the time of their acceptance of the appointment. The members of the Supervisory Body must be free from any incompatibilities and conflicts of interest that may affect their independence and freedom of action and judgement.

Those who do not meet the requirements of integrity set forth for the members of the Board of Directors, pursuant to art. 147-quinquies of TUF, as well as unfit, disqualified and incapacitated subjects may not be appointed as members of the Supervisory Body.

At the time of their appointment, the members of the Supervisory Body must issue a specific declaration stating that they meet the set forth requirements and that they undertake to inform the Company in case their eligibility should change in the course of their mandate. The Supervisory Body members shall be appointed by the Board of Directors and generally remain in office until the expiry of the mandate set for that Board of Directors by the shareholders' meeting, or for the entire period established by the Board of Directors at the time of the appointment.

The Board of Directors provides the Supervisory Body with the financial resources necessary to fulfil its duties.

The functions and powers of the Supervisory Body (identical for all Special Parts) as well as the procedures for managing the necessary information flows are summarised in the paragraphs below.

6.2 (continues): Roles and powers of Datalogic's Supervisory Body.

The Supervisory Body is responsible for supervising:

a) Addressees' compliance with the Model;

b) the effectiveness and adequacy of the Model with respect to the corporate structure and its effective ability to prevent the commission of crimes and/or offences;

c) the opportunity to update the Model, if the prerequisites are met, by formulating proposals to the Board of Directors as a consequence of: (i) significant violations of the provisions of the Model, (ii) significant changes in the internal structure of the Company and/or the methods for carrying out company activities, (iii) legislative amendments to Italian Legislative Decree 231/2001 or amendments that hypothesise new direct liabilities of the entity;

In addition, the Supervisory Body, following the assessment of infringements of the Organisational Model, is required to timely report such violations to the Human Resources Dept. and in case of the objective gravity of the infringements involving a disciplinary action (also in consideration of the role held by the subject who committed the infringement) to the Board of Directors and to the Board of Statutory Auditors for the necessary disciplinary actions to be taken.

The above tasks are completed through the execution of the following activities:

(i) preventive inspections and controls on at-risk activities, using specific check lists, or on the effectiveness of company processes and filing of the related documentation;

(ii) Interviews with top managers of Datalogic, holding the main responsibilities for the activities at risk;

(iii) employee training and addressee information disclosure;

(iv) updating and maintenance of the Model in relation to changing corporate and/or regulatory conditions;

(v) analysis of reports received regarding each violation or suspected violation of the Code of Ethics and/or any other preventive protocol envisaged by the Model.

The Supervisory Body makes use of information flows obtained from the managers of each business area, as well of Internal Audit, as Datalogic's head of internal control. The activities carried out and the tools utilised allow for detecting any exceptions and anomalies as well as implementing the necessary corrective actions.

The Supervisory Body formally meets at least once every quarter, except for in emergency situations. Minutes on each meeting must be drawn up in the previously authenticated register of Supervisory Body meetings. The minutes of each meeting shall be signed by all Supervisory Body members in attendance.

6.3 (continues): reporting of Datalogic's Supervisory Body.

The following procedures are used to report on the Supervisory Body's activities:

a) half-yearly, to the Datalogic Audit and Risk Committee and the Board of Statutory Auditors;

b) annually, to the Board of Directors in a report containing results achieved during the year and the action plan for the subsequent year.

The Board of Directors and Board of Statutory Auditors may call a meeting of the Supervisory Body at any time, and the latter in turn has the right to request, through the applicable functions and parties, that the aforementioned bodies meet for urgent reasons.

7. INFORMATION FLOWS TO EMPLOYEES

Since Datalogic is aware that training and information disclosure are part of a preventive protocol of utmost importance, it works to ensure that employees are familiar with the content of the Decree and the obligations generated thereby and the Model.

The activities related to training, awareness raising and information flow for the Employees, as well as for all Corporate Bodies, are managed by the heads of the corporate functions involved in the application of the Model in cooperation with the

Supervisory Body, starting from the hiring time or the beginning of the employment relationship.

The following activities should be noted:

a) delivery, to the newly hired employees, of an information set (in addition to the materials indicated by other policies or corporate procedures, such as privacy and protection of personal information, hygiene and safety at the work place); the National Collective Labour Agreement; a summary of the contents of the Decree and the Model, with which to ensure that they acquire the knowledge that is considered relevant;

b) employees must sign a dedicated form indicating acknowledgement and acceptance;

c) specific training is provided either in classroom courses or through e-learning tools and services (in that case, with a solution whereby it may be verified that the training took place).

There is a specific area of the corporate IT network dedicated to the Decree, which also guarantees that employees are trained and are knowledgeable.

8. INFORMATION FLOWS TO THIRD PARTIES

The corporate functions that have institutional contact with other Addressees, namely Partners, Suppliers and Consultants, shall provide them with dedicated informational documents, in coordination with the Supervisory Body, on Datalogic's policies and procedures based on the Model and the Code of Ethics as well as on the consequences that behaviours contrary to the expectations of the Model or in any case contrary to the Code of Ethics or current regulations may have on contractual relations.

When possible, the contractual terms shall contain specific clauses aimed at enforcing those consequences, such as termination clauses or rights to withdraw in the event of behaviours contrary to the standards of the Code of Ethics and/or protocols of the Model.

9. DISCIPLINARY SYSTEM - *Preamble*.

A system of penalties proportional to the violation of preventive protocols and/or additional rules of the Model or the Code of Ethics is necessary in order to guarantee that the Model is effective and that the Supervisory Body can act efficiently. In fact, in accordance with art. 6, paragraph 1, letter e) of the Decree, this disciplinary system is an essential requirement for Datalogic's exemption from liability.

The disciplinary system of Datalogic provides for penalties applicable to any Addressee, depending on the type of relationships and in compliance with the principles of proportion and litigation, due to which the penalty applied is always commensurate to the gravity of the disputed act, thus guaranteeing to the involved subject the possibility to justify and defend his/her own behaviour.

The application of the disciplinary system and related penalties is separate from the possible establishment of criminal proceedings and the resulting judgement for an unlawful behaviour covered by Italian Legislative Decree 231/2001. The main objective of the disciplinary system of Datalogic, by completing the Model and making it effective, is in fact not so much the repression of offences once they have been committed, but rather the avoidance of the behaviours that typically precede the commission of offences and consequently avoiding the materialisation of such offences, except for fraudulently circumventing the Model itself.

The disciplinary system of Datalogic plays therefore an essentially preventive role and acts as an additional internal control for preventing the application of "external" penalties imposed by the Court.

The disciplinary system of Datalogic is constantly monitored by the Supervisory Body and by the Human Resources Dept.

As regards the assessment of infringements, the disciplinary procedures and the application of penalties are under the responsibility of Human Resources, notwithstanding the necessary involvement of the Supervisory Body in the procedures for the assessment of the infringements and the application of penalties for infringing the Model. Therefore, the storage of a disciplinary provision, or the application of a disciplinary penalty for infringement of the Model, needs the preventive information to and opinion from the Supervisory Body.

It is therefore the right of the Company to have recourse for the damages and/or liabilities deriving to it from the conduct of the employee in violation of the Model.

In order to preventively specify the criteria correlating the workers' offences and the disciplinary measures adopted, the Board of Directors classifies the actions undertaken by Directors, Auditors, Employees and third parties into:

1. behaviours which show that orders imparted in both in written and verbal form by Datalogic were not followed while carrying out at-risk activities, such as, but not limited to:

   - violation of procedures, regulations, or internal written or verbal instructions;
   - negligently violating, avoiding or disabling one or more preventive protocols;

2. behaviours which show that a serious infraction of workplace regulations and/or diligence has occurred, causing the Company to completely lose faith in the Director and/or Employee, such as:

3. adoption, while carrying out activities at risk, of behaviours under previous point 1 unequivocally aiming at the commission of an crime and/or offence or offences appearing as damaging to Datalogic; behaviours which cause serious moral or material damage to Datalogic, such that the relationship cannot be continued, even temporarily; for example acting in a way which constitutes one or more offences and/or unlawful behaviour, or behaviours, under previous point 1, carried out with the intent to cause damage.

4. conduct that prevents or affects the use of communication channels dedicated to reporting any violations of the Model (so-called Whistleblowing), such as:

   - failure to establish reporting channels;
   - failure to establish procedures for making and handling whistleblowing;
   - adoption of procedures for the execution and management of reports that do not comply with the provisions of the law;
   - implementation of acts, or behaviors, retaliatory, or impediments, to the release of the whistleblowing.

The Supervisory Body is continuously monitoring the suitability of the disciplinary system in relation to the precepts of the Decree.

9.1 (continues): Employee penalties.

For employees, the limitations related to disciplinary powers imposed by article 7 of Italian Law no. 300/1970 (called the "Statute of workers' rights") and by National Collective Labour Agreements must be respected, both as regards applicable penalties (which are generally classified based on the connection with undue disciplinary specifications) and as regards the form and exercise of that power.

The disciplinary system currently applied by Datalogic is in line with the provisions of the National Collective Labour Agreements and complies with the requirements of effectiveness and deterrence.

An employee's failure to respect and/or violation of the general principles of the Model, of the conduct rules imposed by the Code of Ethics and of corporate procedures, regulations or instructions is therefore breach of the obligations imposed by the employment relationship and a regulatory offence (such as insubordination, negligent execution of services, or detriment to company regulations or morals, in accordance with article 24 of the National Collective Labour Agreement, letters c), d) and i); infractions of the regulations and/or diligence of the employment relationship more serious than those pursuant to article 24, in accordance with article 25, letters A) and B)).

The applicable penalties shall be adopted and applied with full respect for the procedures set forth by national collective labour regulations applicable to that employment relationship.

Without prejudice to the principle of the link between the applicable disciplinary measures and the cases in which these measures may be implemented, the principle of proportionality between the infraction and the penalty must be respected when applying the disciplinary penalty. There is no prejudice, and reference is hereby made, to all the provisions under above mentioned art. 7 of the Italian law 300/1970 concerning both the exposure of the disciplinary codes “through the display in a place accessible to all” and the obligation of a preventive notification of the charge to the employee, also in order to allow said employee to acquire an appropriate defence and provide any necessary justification.

9.2 (continues): Manager penalties.

If managers violate the general principles of the Model, the conduct rules imposed by the Code of Ethics and the other preventive protocols, Datalogic shall apply the measures deemed suitable for those managers on the basis of the seriousness and significance of the violations committed, also in consideration of the particular trust existing in the relationship between Datalogic and the employee in the role of manager.

In the cases pursuant to point 2. of the introduction, Datalogic may terminate the work contract in advance or apply another penalty deemed suitable in relation to the seriousness of the case. If the manager's behaviour exemplifies the cases set forth in point 3. of the introduction, Datalogic shall enact the advance termination of the work contract without prior notice pursuant to article 2119 of the Italian Civil Code and article 23, paragraph 1, point 1. of the National Collective Labour Agreement. This is because the deed must be deemed to have been implemented against the will of Datalogic in the interest or to the advantage of the manager and/or third parties.

9.3 (continues): Penalties for the Board Directors and the Board Auditors.

If a Datalogic director or auditor commits crimes and/or offences or violates the Code of Ethics, the Model and/or the relative preventive protocols, the Supervisory Body shall inform the entire Board of Directors and the Board of Statutory Auditors, which are responsible for taking suitable action.

In cases of serious violations by the Directors which are unjustified and/or not authorised by the Board of Directors, the deed may be considered just cause for the revocation of the office. Behaviours constituting the crimes and/or offences are considered a serious, unjustified violation.

9.4 (continues): Third party measures.

Except for exceptional situations to be brought to the attention of the Supervisory Body, any type of contract, including supply, outsourcing, agency, commercial agency, business agent, joint venture and consulting contracts, may not be considered validly executed with Datalogic unless the contractor commits to respecting the Code of Ethics and/or the applicable preventive protocols.

These contracts must include termination clauses or rights to withdraw in favour of Datalogic, which shall bear no penalty, if crimes and/or offences are committed, or if rules of the Code of Ethics, the Model and/or the relative preventive protocols are violated.

In any case, Datalogic reserves the right to possibly request indemnification if it undergoes damages as a result of that behaviour, for example if the judge applies measures sets forth by the Decree to Datalogic.

10. REPORTING

Each recipient of the Model has the right to report any violations to the Company, even anonymously, through the following communication channels:

> Whistleblowing Platform available on the Company's website (https://datalogic.integrity.complylog.com/), which guarantees the possibility of issuing written whistleblowing reports or through the recording of voice messages.

Thus, through a face-to-face meeting with the Company's Supervisory Body.

Each whistleblowing is taken over and assessed by the Company according to the corresponding provisions of the law[12], in the relative ways and times, providing:

- acknowledgment of receipt of the report, within 7 days of the same;
- formal response, within 3 months of acknowledgment of receipt;
- consequent document archiving.

In order to ensure an adequate assessment, the contents of the whistleblowing are characterized as:

- based upon facts that are objective, detailed and consistent, as well as free of any personal opinion;
- free of any opportunistic, disparaging, improper or instrumental purpose;
- aimed at protecting the integrity of the Company.

Finally, please note that the Company guarantees adequate protection to the whistleblower from any retaliation and prejudicial consequences, not revealing his identity, without prejudice to legal obligations.

***** OMISSIS *****

[12] Legislative Decree 231/2001 as amended, EU Regulation 2016/679 on Privacy and in the EU Directive 2019/1937 on reporting (so-called "Whistleblowing").