

**ORGANISATION,
MANAGEMENT AND
CONTROL MODEL**

**PURSUANT TO ITALIAN LEGISLATIVE DECREE
D.LGS. 231/2001**

adopted by



Revision history - Model 231

REVISION	DATE	DESCRIPTION
00	June 2020	First Issue

CONTENTS

1.	ITALIAN LEGISLATIVE DECREE NO. 231 OF 8 JUNE 2001	5
2.	GENERAL INFORMATION ABOUT THE COMPANY	11
2.1	The Company	11
2.2	Corporate Governance.....	12
2.3	Corporate organisation.....	13
3.	THE ORGANISATION, MANAGEMENT AND CONTROL MODEL.....	14
3.1	Objectives and purposes pursued in adopting the Model.....	14
3.2	The methodology adopted for the Model's implementation	15
4.	Features and structure of the Internal Control System	17
4.1	General principles of the Internal Control System	17
4.2	The sources of the Internal Control System.....	17
4.3	The Control System's modular structure.....	18
5.	Exposure to risk	19
5.1	Methodology	19
5.2	Sensitive processes	19
5.3	Offences against Public Authorities (Articles 24 and 25 / D.lgs. 231/2001)	21
5.4	Computer crime (Art. 24 bis Legislative Decree D.Lgs. 231/2001) and offences committed in violation of Copyright Law (Art. 25 novies Legislative Decree D.Lgs. 231/2001)	27
5.5	Organised crime (Article 24 ter of Legislative Decree D.Lgs. 231/2001), crimes relating to terrorism and the subversion of democratic order (Article 25 quater of Legislative Decree D.Lgs. 231/2001), transnational offences pursuant to Italian Law 146/2006	29
5.6	Counterfeiting of coins, public credit notes, revenue stamps and identifiers or signs (Art. 25 bis of Legislative Decree 231/2001) crimes against industry and trade (Art. 25 bis.1 of Legislative Decree 231/2001)	33
5.7	Corporate crimes (Art. 25 ter of Legislative Decree D.Lgs. 231/2001)	36
5.8	Crimes of manslaughter and culpable severe or very serious negligent injuries, committed in violation of accident prevention regulations and the protection of hygiene and health at work (Art. 25 septies Legislative Decree D.Lgs. 231/2001)	41
5.9	Crimes of receiving stolen goods, money laundering, self-laundering and use of goods of illicit origin (Art. 25 octies Legislative Decree D.Lgs. 231/2001)	45
5.10	Environmental offences (Art. 25 undecies / Legislative Decree D.Lgs. 231/2001)	49
5.11	Employment of illegal immigrants (Art. 25 duodecies of Legislative Decree D. Lgs. 231/2001)	50
5.12	Tax crimes (Art. 25 quinquiesdecies of Legislative Decree D.lgs. 231/2001)	52
5.13	Other crimes.....	54

6.	The Supervisory and Control Body.....	55
6.1	General points	55
6.2	Appointment and composition.....	55
6.3	Term of office, replacement and removal of members of the Supervisory and Control Body	56
6.4	The requirements of the Supervisory and Control Body	56
6.5	The resources of the Supervisory and Control Body	57
6.6	Convocation of General Meeting	58
6.7	Confidentiality.....	58
6.8	Duties and powers of the Supervisory and Control Body.....	58
6.9	Management of internal monitoring system verifications.....	60
6.10	Reports and communications to the Supervisory and Control Body Reports (Whistleblowing).....	61
6.11	Information flow to the Supervisory and Control Body.....	62
	Actions of the Supervisory Body.....	62
	Other information.....	62
6.12	Reporting and management of documents	63
7.	The Disciplinary System	64
7.1	Purpose of the Disciplinary System	64
7.2	Sanctions for employees	64
7.3	Sanctions for management	66
7.4	Measures for Administrators	66
7.5	Measures for Auditors	67
7.6	Measures for other recipients.....	67
7.7	Measures for the violation of provisions on Whistleblowing	67
7.8	Additional measures.....	68
8.	Training and information.....	69
8.1	Training of personnel	69
9.	Annexes.....	70

1. ITALIAN LEGISLATIVE DECREE NO. 231 OF 8 JUNE 2001

With Legislative Decree No 231 of 8 June 2001, the “administrative liability of legal entities, companies and associations, including those without legal personality” as a result of committing an offence, was introduced into the Italian legislation.

The decree is applicable for the following crimes:

- Art. 24: “Misappropriation of funds, fraud against the State or a public entity or to obtain public funds and computer fraud against the State or a public authority”, which correlates the administrative liability of an entity with committing crimes such as misappropriation of funds against the State (or other public authority, or the European Communities), fraud (to the detriment of the State or another public body or aggravated for accessing public funds), and computer fraud (if committed against the State or other public authority);
- Art. 24-bis: “Computer crimes and unlawful data processing”, which correlates the administrative liability of an entity with committing crimes such as illegal access to a computer or telecommunications system; the offence of possession and unauthorized disclosure of access codes to computer or telecommunications systems; the offence of installing equipment, devices, or programs aimed at damaging or interrupting a computer or telecommunications system; the offence of intercepting, impeding or illegally interrupting computer or electronic communications; the offence of IT forgery; and the offence of damage to information, data and computer programs, used by the State or other public authority, or of public utility;
- Art. 24-ter: “Crimes relating to organized crime”, which in particular correlates liability to cases of mafia facilitation;
- Art. 25: “Extortion, bribery, embezzlement, and corruption”, which correlates the administrative liability of an entity with committing crimes such as bribery, undue inducement to provide or promise services, and corruption to influence an official or for an act against official duties. Law no. 3/2019 (so-called ‘Spazzacorrotti’ [sweeping away corruption] also includes the crime of Trafficking in illicit influences (Article 346 bis of the Criminal Code).
- Art. 25-bis: “Forgery of currency, public credit notes, revenue stamps and identification tools or signs”, which correlates the administrative liability of an entity with committing crimes of accounting fraud, use of counterfeited securities, forgery and use of

distinctive trademarks and patents, as well as the introduction into the country and trade of products bearing false indications;

- Art. 25-bis 1: “Crimes against industry and commerce”, which correlate the liability of the entity to committing crimes such as disturbing freedom of industry or commerce, illicit competition with threats or violence, or offences committed in commercial fraud;
- Art. 25-ter: “Corporate crimes”, which correlate the administrative liability of an entity to committing crimes such as issuing false company documents in the new formulation post Law 69/2015, false reports or communications of auditors, stock manipulation, illegal distribution of profits and reserves, illegal transactions involving stocks or shares of the parent company, transactions to the detriment of creditors, illegal influence on the Shareholders' Meeting, failure to disclose a conflict of interest, hindering the exercise of the functions of public oversight authorities. Law 190/2012 has also added to these crimes that of corruption between private entities, recently reformed by Legislative Decree D. Lgs. 38/2017, in addition to Law no. 3 of 9 January 2019;
- Art. 25 quater: “Crimes related to terrorism or the subversion of democratic order”, which correlate the administrative liability of an entity to committing crimes related to terrorism or subversion of the democratic order, as provided for in both the criminal code and special laws;
- Art. 25-quater-1: “Mutilation of female genital organs”;
- Art. 25 quinquies: “Crimes against the individual”, which correlate the administrative liability of an entity to committing crimes such as obligating or maintaining an individual in slavery or servitude, the possession of pornographic material (produced through the sexual exploitation of minors), child prostitution and tourist initiatives aimed at exploiting child prostitution. Law 199/2016 has also added to these crimes that of illegal employment;
- Art. 25 sexies: “Market abuse offences”, which correlate the administrative liability of an entity to committing crimes of abuse of privileged information and market manipulation;
- Art. 25-septies: “Manslaughter and serious or very serious negligent injuries, committed in violation of accident prevention regulations and the protection of hygiene and health in the workplace”;
- Art. 25-octies: “Receiving stolen goods, money laundering and the use of money, goods or assets of illicit origin, including self-laundering”, which correlate the administrative liability of an entity to the transfer, concealment, substitution or use of illegally obtained

assets (including where the subject has committed or contributed to committing the alleged offence);

- Art. 25-novies: "Crimes relating to violation of copyright", i.e. aimed at the unlawful use of copyrighted material;
- Art. 25-decies: "Inducement not to provide statements, or make false statements to the judicial authorities";
- Art. 25-undecies: "Environmental crimes", pursuant to the new formulation post Law no. 68/2015 which correlates the liability of an entity to committing offences such as environmental pollution, environmental disasters, illegal waste disposal, the dumping of waste on the ground, in the subsoil and in the groundwater, in violation of the Consolidated Environmental Text [T.U.A.];
- Art. 25-duodecies: "Employment of illegal immigrants", aimed at the exploitation of labour under illegal conditions, recently reformed by Law no. 161/2017;
- Art. 25-terdecies: "Xenophobia and racism", as introduced by 2017 European Legislation with express reference to the crime referred to in Art. 3, par. 3-bis, of Law no. 654 of 13 October 1975, currently repealed by Art. 7 of Legislative Decree D. Lgs. 21/2018 which simultaneously introduced the new criminal offence referred to in Art. 604 bis of the Italian Criminal Code;
- Art. 25 quaterdecies: "Fraud in sports competitions, abusive gambling or gambling, betting and games of chance exercised by means of prohibited devices", introduced under Law no. 39 of 3 May 2019, which implemented into our legal system the Council of Europe Convention on the manipulation of sports competitions, passed in Magglingen on 18 September 2014;
- Art. 25 quinquiesdecies: "Tax Offences", introduced with Law no. 157 of 19 December 2019, as a conversion of Legislative Decree D. Lgs. No 124 of 26 October 2019 (so-called tax decree);
- "Transnational crimes" (introduced with Law no. 146 of 16 March 2006) correlating the administrative liability of an entity to offences such as money laundering and criminal association on an international scale.

For a more complete and detailed examination of the so-called predicate offences, express reference is made to the Regulatory Appendix to be understood as an integral part of this Organisation, Management and Control Model.

Pursuant to Art. 5 of Legislative Decree D. Lgs. 231/2001, in order for administrative liability to be contested and attributed to an entity, a natural person functionally connected to the entity must have committed (or attempted to commit) one of the aforementioned crimes (so-called predicate offences) and that the offence be committed "in its (editor's note; the

institution's) interest or to its advantage", providing as an exemption the hypothesis that the perpetrator has "acted in its own exclusive interest or that of third parties".

In order for the administrative liability of the entity to emerge, in parallel with the criminal liability of the perpetrator of the crime (natural person), it is also necessary that the crime be committed by persons in a senior management role within the entity or persons in a subordinate position. More specifically, pursuant to Art. 5, "the entity is liable for crimes committed in its interest or to its advantage:

- a) by persons who are sales representatives, directors or managers of the entity or any of its organisational units with financial and functional independence, or by persons who even de facto exercise the management and control thereof (i.e. senior managers);
- b) by persons subject to the management or supervision of one of the persons referred under subparagraph a) (so-called subordinates).

According to a consolidated jurisprudential orientation, the administrative liability deriving from a crime is also applied in the presence of a Group, albeit with some significant limitations and conditions, when, for instance, a subsidiary commits a crime predicated on the liability (so-called ascent of liability).

In the event of proven liability, the Company would incur one of the following penalties: financial fines, disqualification sanctions, confiscation (as ordered with the entity's sentencing) and publication of the judgment.

With reference to the pecuniary sanction, a system of calculation by units has been established, to be determined by quantity and value, in order to better adapt the amount of the sanction to the reality of the case. Each unit ranges from a minimum value of approximately € 258.00 to a maximum of approximately € 1,550.00; a total number of units of less than one hundred (100) or more than one thousand (1000) cannot be applied. Therefore, the financial penalties range from a minimum of € 25,823.00 to a maximum of approximately € 1,549,360.00.

Based on Art. 11 of the Decree, the judge must firstly determine the number of units taking into account various elements: the gravity of the offence; the entity's degree of responsibility; any actions carried out to eliminate or mitigate the consequences of the offence; any actions aimed at preventing committing further offences. Subsequently, the judge will proceed to determine the overall amount in units, taking into account the entity's economic and financial conditions, in order to ensure the effectiveness of the sanction.

Disqualification sanctions, on the other hand, include: disqualification from exercising the business activity; the suspension or revocation of authorisations, licences or concessions functional to committing the offence; a ban on contracting with Public Administration, with the exception of obtaining public services; exclusion from concessions, loans, contributions or subsidies and the possible revocation of those already granted; and a ban on advertising goods or services.

Unlike the pecuniary sanction, which always applies, disqualification sanctions are applied as expressly provided for by law and provided that at least one of the conditions referred to under Art. 13, i.e., that the entity must have gained a significant profit from the crime and that the offence was committed by persons holding a senior management role or by persons subject to the management of others when the offence was committed, determined or facilitated by serious organisational deficiencies; or in the eventuality of repeated offences.

Disqualification sanctions have a duration of no less than three months and no more than two years.

In determining the type of sanction and the duration, the judge must take into account: the severity of the offence, the entity's liability, any actions aimed at preventing or mitigating the consequences, as well as the suitability of the individual sanctions to prevent offences of the type committed.

Article 6 of the Decree provides that when the offence is committed by persons in senior management positions, the entity shall not respond administratively if it can prove that:

- prior to committing the crime, the governing body adopted and effectively implemented suitable organisation and management models aimed at preventing crimes of the type that occurred;
- the task of supervising the functioning and observance of the models and their updating was entrusted to a body within the entity with independent powers of initiative and control;
- the persons committed the offence by fraudulently eluding the organisation and management models;
- there was no omitted or insufficient supervision by the body referred to under subparagraph b).

In this sense, the deeper purpose of the Legislative Decree D. Lgs. 231/2001 is to encourage businesses to adopt an organisational, management control model which is in tune with establishing a "culture of prevention", aimed at pursuing a "new entrepreneurial culture".

To ensure its exempting effectiveness, the organisation and management model must address the need to:

- identify those activities where offences may be committed;
- provide for specific protocols directed at planning the conception and implementation of the entity's decisions in relation to crimes to be prevented;
- identify ways of managing financial resources suitable to inhibiting offences from being committed;
- provide mandatory information to the body entrusted with supervising the functioning and observance of the models;
- introduce a proper disciplinary system for sanctioning any failure to respect the measures indicated in the model.

Articles 12 and 17 of Legislative Decree D. Lgs. 231/2001 also recognise a remedial efficacy to the organisation and management model, since they provide for a reduction of pecuniary sanctions and exemption from disqualification sanctions when the entity has adopted and made operational, prior to the declaration of opening of the first instance hearing for the crime already committed, an organisation and management model suitable for preventing crimes of the kind that occurred (so-called ex post model).

2. GENERAL INFORMATION ABOUT THE COMPANY

2.1 The Company

IMS TECHNOLOGIES S.p.A. is currently synonymous with excellence on a global scale, in the design, manufacturing and sale of high-tech machinery in the Converting, Packaging and Automotive sectors.

Indeed, IMS TECHNOLOGIES Group specializes in multiple industries, thanks to recently acquired subsidiaries: the acquisition in 2013 of GOEBEL Schneid-und Wickelsysteme GmbH, becoming with the GOEBEL IMS brand a global leader in the construction of primary industry machinery (slitter-rewinders, unwinders, winders, embossers, etc.) and converters in the paper, aluminium and plastic film sectors.

In the Packaging industry, IMS is represented by ROTOMAC, a company founded in 1890 and incorporated in 2008, which manufactures rewinders and auxiliary machinery (cartoning machines, case packers, etc.) for the production of aluminium rolls, plastic film and baking paper for domestic and professional use.

In the Automotive sector, IMS operates under the DELTAMATIC brand, manufacturing automatic and semi-automatic machinery for thermoforming automotive interiors (car bottoms, trunk linings, wheel arches, overhead bins, etc.).

The KASPER brand, a company founded in 1942 and acquired in 2005, produces numerically controlled horizontal and vertical lathes for the machining of complex parts in the automotive sector (differentials, pinions, transmissions, etc.).

The Group's DELTAMOULD brand, acquired in 2009, manufactures moulds for the aluminium casting of complex pieces.

In 2017, the Group was acquired by the Coeclerici Group as part of a business diversification merger.

Headquartered in Calcinate (BG), IMS TECHNOLOGIES S.p.A. currently numbers 400 employees at five production sites – three in Italy, one in Germany and one in the United States – in addition to having established a presence in China with a commercial and after-sales branch, and in the USA and India, respectively, with a branch for sales and support service.

IMS TECHNOLOGIES is especially attentive to establishing a culture of legality, and it is in this regard that it has decided to comply with the provisions of Legislative Decree D. Lgs. 231/2001 and, therefore, to implement a system for preventing the risk of crime.

2.2 Corporate Governance

The corporate governance structure at IMS TECHNOLOGIES S.p.A., under the sole shareholder CoeClerici S.p.A., adopts a traditional administrative system, headed by a Board of Directors. The Board of Statutory Auditors is responsible for monitoring the conformity and correctness of operations and ethics, assuring the clarity, accuracy, truth and fidelity of results, which may make use of a network of internal controls, responding to senior management. Ultimately, the organisational structures respond to the administrative body, to which the control and supervisory body refers.

The functions of the aforementioned corporate bodies are briefly described below:

- Board of Directors: consists of ten Directors, one of which acts as Chairperson and one as Managing Director. The Directors are responsible for managing the company, carrying out the required operations for implementing the corporate purpose, without prejudice to the need for specific authorisation in cases required by law. More specifically, the following powers are attributed to the Board of Directors:
 - merger resolutions in the cases referred to under Articles 2505, 2505-bis, 2506-ter, last paragraph of the Italian Civil Code;
 - indicating of which Directors represent the Company;
 - reducing the share capital in the event of a shareholder withdrawing;
 - adapting the bylaws to regulatory provisions;
 - providing a reduction in capital if more than one third of the share capital is lost and the company has issued shares with no par value; until otherwise resolved by the shareholders' meeting, no Director is bound by the competition prohibition sanctioned by Article 2390 of the Italian Civil Code; the Chairperson on the Board of Directors is responsible for the company's substantive and procedural representation, and for this purpose can delegate a director.
- Board of Auditors: consists of five members, with three regular members, including a Chairperson, and two alternates. All members of the Board of Auditors remain in office for three fiscal years, and may be reappointed. The Board of Auditors is entrusted with the task of monitoring:
 - compliance with the law and company bylaws;
 - compliance with the principles of proper administration;

- the adequacy of the Company's organisational structure, internal monitoring system and administrative accounting system, including with reference to the administrative accounting system's reliability in correctly describing management operations.

IMS TECHNOLOGIES S.p.A. also avails itself of an external auditing firm.

2.3 Corporate organisation

IMS TECHNOLOGIES S.p.A. is structured according to four organisational lines, which report to the Group's CEO:

1. Operations: reports to the Group Operations Director and includes the areas of Project Management, Budgeting, Product & Planning and the various area Managers (Group Supply Chain, Engineering, Deltamould BU, Automotive);
2. Sales: reports to the Sales & Marketing Managing Director and includes the areas of Communications, the Sales Directors and Sales Managers;
3. Services: reports to the Group Service Director and includes the areas of Sales Service and Technical Support;
4. Personnel includes the areas of HR, HSE, ICT and Finance Administration.

For a more detailed explanation of the organisational structure, refer to Organisation Charts contained in Annex 1 of this Model.

3. THE ORGANISATION, MANAGEMENT AND CONTROL MODEL

3.1 Objectives and purposes pursued in adopting the Model

IMS TECHNOLOGIES is sensitive to the need to ensure fairness and transparency in conducting its business and corporate operations, protecting its position and image, the work of its employees and expectations of stakeholders, and is aware of the importance of adopting an internal control system capable of preventing unlawful conduct on the part of its directors, employees, contractors and business partners. The Company has adopted the organisation and management model with the awareness that an efficient and balanced corporate organisation, suitable for preventing the committing of crimes, is pursued by intervening primarily on the processes of conceiving and implementing the Company's decisions, on preventive and subsequent controls, as well as on information flows, both internal and external.

Through the adoption of the Model, IMS TECHNOLOGIES intends to pursue the following main objectives:

- sensitize all those who work in the name and on behalf of the Company to a corporate culture based on legality, making them aware that in the event of a violation of the provisions contained therein, they may incur in the commission of offences subject to criminal penalties that can be imposed against them, and administrative sanctions that can be imposed on the Company;
- reiterate that these forms of unlawful conduct are strictly condemned by the Company, since (even in the event that Company may appear to benefit from them) they are in any case contrary not only to the provisions of the law but also to the ethical principles which the Company intends to adhere to in implementing its corporate mission;
- allow the Company to take prompt action to prevent or oppose the committing of offences through the dissemination of a culture of supervision aimed at governing all decision-making and operational phases of corporate activities, and providing a monitoring action on areas of activity at risk.

The Model and the principles contained therein apply to the Company's corporate bodies, its employees, contractors, consultants, suppliers and business partners, and more generally to all those who, for whatever reason, operate in sensitive activities on behalf or in the interest of IMS TECHNOLOGIES (hereinafter the "Recipients").

3.2 The methodology adopted for the Model's implementation

In compliance with the provisions of Legislative Decree D. Lgs. 231/2001 (in particular under Art.6) and illustrated in the trade association guidelines adopted, as well as defined by consolidated case law, the organisational model is constructed as the ultimate result of a series of complex activities. This is to allow for the adoption of the model to represent an effective and efficient prevention tool through the adoption of a general, complete and suitable internal control system.

The activities for its implementation and/or for its review/update are divided into the following stages:

- Identification of sensitive activities, i.e. those activities or process phases that provide for significant exposure (in abstract) to the risk of committing (or attempting) crimes.
- Conducting interviews with the various process managers on operational management methods aimed at highlighting the existing control system and the reference documentation.
- Based on the results obtained, a comparison was drawn on existing procedures, the level of controls defined, their degree of knowledge and dissemination, and the activities at risk, so as to define and formalise the Company's Gap Analysis, evaluating those areas and/or activities not sufficiently supervised to guarantee the effectiveness of the organisation and management model.
- With the outcome of the above assessment, the level of criticality for each sensitive activity was defined based on the level of control and potential risk. Controls on sensitive activities are determined by verifying the presence and adequacy of the control standards defined by Confindustria. The potential risk for a sensitive activity is determined starting from the severity of the sanctions of the related crime, or the maximum amount of the applicable sanction (administrative and/or disqualifying).
- Following the identification and acceptance of the criticality level for each sensitive activity, actions and countermeasures for the management of the defined risk were identified (mitigation, acceptance, transfer and elimination).
- Adoption of prevention and control measures within the documentation constituting the Model:

- formalisation and/or integration of the Company's existing documentation with the activities and controls defined and/or the production of ex-novo regulatory documentation;
 - updating of the Organisation and Management Model as a document summarising and connecting the principles, rules of conduct, defined protocols, specific prevention and control measures, bodies and persons concerned, and the system of sanctions;
 - definition and updating of the information flow system, specifically highlighting the object of the information flow, the person responsible and sampling frequency.
- Planning of differentiated training sessions and auditing on processes identified as exposed to the risk of offences being committed.

4. Features and structure of the Internal Control System

4.1 General principles of the Internal Control System

The internal control system is defined as the set of tools aimed at providing a reasonable degree of assurance towards achieving the objectives of efficiency and operational effectiveness, reliability of information, compliance with laws and regulations, as well as safeguarding of assets against possible fraud or offences.

As defined by the Confindustria Guidelines, the following elements characterises the control system:

- formalisation of the system of controls in an appropriate corporate documentation aimed at defining and regulating the methods and timing of activities relating to the controls, as well as the implementation of controls, including supervisory controls;
- traceability aimed at rendering the checks certifying the characteristics and reasons of individual operations documentable and verifiable, clearly identifying the persons who authorise, perform, record and verify operations;
- segregation aimed at assuring a separation of functions, thus avoiding that the management of the entire process is carried out independently by a single person;
- attribution of powers of authorisation (proxies and powers of attorney), where it is possible and appropriate to distribute such powers consistently with the corporate organisation in order to avoid the attribution of unlimited powers and, above all, assure a clear awareness both inside and outside the organisation of all powers and responsibilities.

4.2 The sources of the Internal Control System

The sources of the Company's Internal Control System are contained in the:

- Code of Ethics: a document that illustrates the Company's guiding values by recommending, promoting or prohibiting certain behaviours and, if necessary, dictating specific prohibitions and requirements in relation to offences; it should be considered an essential foundation on which the Model is built, since the provisions contained in the latter presuppose compliance with the provisions of the former, together forming a systematic corpus of internal rules aimed at disseminating a culture of ethics and corporate transparency;
- The Organisation and Management Model of IMS TECHNOLOGIES, which describes the prevention and control measures directed at preventing the offences provided for under Legislative Decree D.lgs. 231/01 and its regulatory principles;

- The internal operational documentation, specifically the organisational procedures, as well as the contractual documentation defining the general reference principles in the management of business processes (see Annex 2).

4.3 The Control System's modular structure

The Company has adopted a control system modulated in the following levels:

- Level I controls are represented by the so-called "line controls", executed by department managers or through the use of external professionals; these include audits and controls defined by corporate operating procedures.
- Level II controls normally aimed at monitoring the risk management and control process; these include, for example, audits by the Supervisory Body or verification activities conducted by Certification Bodies.
- Level III controls, possibly aimed at providing assurance and carrying out independent assessments on the design and operation of the overall Internal Control System (including by assigning audits to external consultants).

5. Exposure to risk

5.1 Methodology

The processes defined within IMS TECHNOLOGIES for effective and efficient service delivery may be exposed to the risk of committing the crimes under Legislative Decree D. Lgs. 231/2001 in three distinct ways:

- **Direct Exposure**, if the performance of activities within the process itself provides a risk of committing illicit activities. For example, requests for permits, authorisations and/or qualifications, involving direct contact with the Public Administration, exposes managing personnel directly to the crimes of fraud, corruption or misappropriation of funds;
- **Instrumental Exposure**, if the process in itself is not exposed to a risk of committing an offence, but its result is. For instance, the hiring of employees related to Public Administration officials, which can constitute "bestowal" through which the crime of corruption is confirmed in exercising the function or for an action that is contrary to official duties or, furthermore, in stipulating consultancy contracts which, if executed without particular attention or precautions, can constitute a way to establish funds to be used for purposes of an illicit nature.
- **No Exposure**, if the activity or process does not have a significant degree of exposure to the risk of committing any of the so-called predicate offences.

5.2 Sensitive processes

In light of the risk analysis carried out, for the purpose of preparing this Model, the following identifies the exposure to risk for committing an offence, for each sensitive process / activity.

Offences pursuant to D.Lgs No. 231/01	Section	Corporate processes
Art. 24 Art. 25	(see 5.3)	Sales, Budgeting, Operations, Supply chain, Warehouse management, Production (Seriante site), Administration and Finance, HR, Communications, Services, Legal, Management of relations with P.A.
Art. 24 bis Art. 25 novies	(see 5.4)	Communications, ICT

Art. 24 ter Art. 25 quater Transnational crimes	(see 5.5)	Sales, Budgeting, Operations, Supply chain, Warehouse management, Production (Seriata site), Administration and Finance, HR, Communications, Services
Art. 25 bis Art. 25 bis.1	(see 5.6)	Sales, Engineering, Operations, Production (Seriata site), HR, Legal
Art. 25 ter	(see 5.7)	Sales, Budgeting, Project Management, Operations, Supply chain, Warehouse management, Production (Seriata site), Administration and Finance, HR, Communications, Services, Legal
Art. 25 septies	(see 5.8)	Engineering, Operations, Production (Seriata site), Management of Health and Safety and the Environment
Art. 25 octies	(see 5.9)	Supply chain, Warehouse management, Administration and Finance, HR, Communications
Art. 25 decies	(see 5.3)	Legal
Art. 25 undecies	(see 5.10)	Management of Environmental fulfilments
Art. 25 duodecies	(see 5.11)	HR
Art. 25 quinquiesdecies	(see 5.12)	Administration and Finance, Services

The mapping results allowed for the:

- identification of organisational units within the Company which, in view of assigned tasks and responsibilities, could potentially be involved in crime risk activities;
- identification of primary types of risk/crime;
- outlining of possible ways of committing illegal actions.

The list of the primary documentation (policies, procedures, etc.) containing the main prevention and control measures referred to in this Model, as pertaining to the risks identified for committing offences, is represented in Annex 2.

5.3 Offences against Public Authorities (Articles 24 and 25 / D.lgs. 231/2001)

The definition of Public Administration

Public Administration refers to all public entities, whether territorial or not, members and internal bodies of entities, including public officials.

As regards persons acting in the sphere of and in relation to the Public Administration, for the purpose of integrating the cases of predicate offence pursuant to Legislative Decree D. Lgs. 231/2001, the roles of "Public Officials" and "Public Service Officers" take on particular relevance, governed respectively by Articles 357 paragraph I and 358 of the Italian Criminal Code.

Art. 357 of the Italian Criminal Code defines as a Public Official someone who "*exercises a public legislative, judicial or administrative function*".

Considering that a "public function" encompasses administrative activities that constitute the exercise of decision-making, authoritative or certifying powers, it can be said that the qualification of public official must therefore be recognised to subjects, public employees or private individuals, who can or must, within powers regulated by public law, form and manifest the will of the P.A., or exercise authoritative or certification powers (e.g. an employee of an Administration with powers of certification or attestation).

Art. 358 of the Italian Criminal Code, on the other hand, defines persons in charge of a public service as "*persons who, in whichever capacity, provide a public service*".

Considering that "public service" must be understood as an activity governed in the same forms as a public function, but characterised by a lack of powers typical of the latter, and with the exclusion of the performance of simple tasks relating to order and providing merely material work, the law has identified the category of persons in charge of a public service, placing the accent on the nature of the instrumentality and accessory nature of their activities, as compared to public activities in a strict sense. A series of "revealing indices" of the public nature of an institution have thus been identified. In particular, reference is made to the following indices: the subjecting to administrative and control activities for social purposes as well as the power to appoint and revoke administrators by the State or other public bodies; the presence of an agreement and/or concession with the public

administration; the financial contribution from the state; the immanence of interest in economic activity.

Based on the above, the discriminating element indicating whether a person holds or does not qualify as a "person in charge of a public service" is represented not by the legal nature of the Entity, but by the functions entrusted to the subject, which must consist of upholding the public interest or satisfying needs of a general interest.

Exposure to risk

The results of the risk analysis have led to the identification, within the business processes, of the following activities as those in which IMS TECHNOLOGIES is most exposed to the risk of committing the offences referred to in Articles 24 and 25 of Legislative Decree D. Lgs. 231/2001:

- Management of relations with P.A. for obtaining permits, authorisations o concessions	Relations with P.A.
- Management of relations with P.A. regarding inspections	
- Sales management	Sales
- Pricing and discounts	
- Management of relations with agents and data gatherers	
- Budgeting	Budgeting
- Deltamould	Operations
- Management of supplies	Supply Chain
- Management of credit lines for professional services and assignments	
- Qualification and evaluation	
- Warehouse management	Warehouse management
- Management of liabilities	Administration and Finance
- Management of assets	
- Treasury	
- Administrative control	
- Management of detection, registration and representation in accounting records and determination of tax and fiscal charges	
- Management of intragroup relations	

- Maintenance and services	Production (Seriarte site)
- Selection and hiring - Administrative management of personnel - Management of bonus and incentives system	HR
- Technical and institutional communications - Events and trade fairs - Gifts and sponsorships	Communications
- Services management	Services
- Claims management	Legal

In addition to activities that involve direct contact with the Public Administration (e.g. for obtaining permits, authorisations or concessions or in the case of inspections) and, therefore, physiologically expose the Company to the risk of committing an offence (e.g. bribery towards inspection agents to avoid the imposition of sanctions), processes involving the development of sales activities, procurement, human resources and related administrative processes can also be considered exposed to the risk of committing offences of corruption.

For instance, the stipulation of a contract for a non-existent service can constitute the means, whether directly or indirectly, to obtain the price of a service from a Public Official or Public Service Representative, as well as the issuance of invoices for non-existent operations, i.e. for amounts higher than the value of a given service, can be the means through which "off-book" funds be set up to be used for the purposes of corruption. Furthermore, the qualification and issuance of an order in favour of a supplier who has been proven unsuitable by the Company's established parameters, or the selection of unsuitable personnel may represent a corruptive element of exchange towards provisions favourable to the Company by a public client rather than from a public body that must issue a favourable provision (e.g. authorisation / concession).

The offences that can be applied in relations with the Public Administration also include the crime of inducing persons not to make statements or to provide false statements to the judicial authorities, however, as provided for under Article 25 decies.

Prevention measures

Regarding activities and checks implemented in order to prevent offences against or to the detriment of Public Administration, the Company has adopted the following prevention and control measures:

- **Code Ethics** that expressly prohibits all corruption practices, illegitimate favours, collusive behaviour, direct and/or indirect requests for personal advantages, recalling respect for the principles of honesty, integrity and fairness, as well as defining specific principles of conduct regarding conflicts of interest, relations with suppliers and relations with personnel.
- **System of powers of attorney and delegation** which defines authorisation and control powers and assigns them consistently to operating practice, expressly providing for which subjects have the power to interface with Public Administration in the name and on behalf of the Company.
- **Flow procedure to the Supervisory Body** which defines the type of flows, the company areas involved and frequency of transmission to the Company's Supervisory Body.
- **Policy for managing relations with P.A.** which defines specific prohibitions and rules of conduct in relations with the Public Administration during audits. Specific prevention and control elements are envisaged, such as:
 - the Company's power of representation towards the P. A., as defined by the system of powers of attorney
 - relations with P.A. or authorities are managed in a unitary manner by appointing a specific manager for each operation, delegated to do so (participation in the minutes, delivery and collection of documents, formal responses to P.A., etc.)
 - the documentation must be verified by the appointed delegated manager, and if necessary, signed by a person with specific powers
- **Sales management procedure** which defines roles and responsibilities, and specific control measures in managing relations with sales agents, prospects, clients and pricing:
 - control and monitoring on the pricing system, and definition of specific limits and authorisations for discounts;
 - due diligence on agents and acquisition of a self-declaration on the absence of pending charges;
 - ethical and eco-fin due diligence on clients;

- signing of clauses on knowledge and compliance with the principles defined in the Model and in the Code of Ethics (so-called 231 Clauses).

Specific control measures are also defined in relation to the issuing of active invoices and after-sales activities, which provide for the creation of active invoices and sales and transport documents directly from the management system, as well as specific control measures such as verification of correspondence between order requests, delivery notes and invoices.

The traceability of each and every post-sales operation is guaranteed, both through the management system and through specific operating reports.

- **Budgeting procedure** which defines specific control measures in the management of budgeting activities, such as:
 - definition of a dedicated budget;
 - valuation of estimated contract costs based on specific defined criteria, such as job orders, machine component costs, hourly design costs, historicity, etc.;
 - monitoring of correspondence between price quotes and offers.
- **Procurement procedure** which defines roles, responsibilities and specific control measures in the management of the procurement process, guaranteeing the traceability of operations such as:
 - verification of effective procurement needs;
 - qualification of suppliers through due diligence, ensuring appropriate professional and technical valuation elements, in addition to possessing specific authorisations where applicable (e.g. authorizations for transport and waste disposal) and specific certificates or certifications where necessary; for certain categories of supply, ethical due diligence is also envisaged;
 - specific supply selection criteria;
 - purchasing authorisation and signing of contracts by persons with suitable powers (proxies and/or delegated power of attorney);
 - verification of effective supplies (goods and/or services);
 - signing of clauses on knowledge and compliance with the principles defined in the Model and Code of Ethics (so-called 231 Clauses).
- **Procedure for the active and passive cycle** which defines roles, responsibilities and specific control measures in the management of active and passive invoices, financial flows and treasury, management control and allocation of accounting data, ensuring the traceability of operations such as:

- verification of services effectively provided (active / passive);
- verification of correspondence between invoices / purchasing requests / purchase orders / contracts;
- invoice blocking and management of irregularities;
- authorisation to pay and execute payments by persons with specific powers;
- monitoring and control of incoming and outgoing financial flows through IT support systems (Piteco, JD Edwards);
- periodic bank reconciliations.

Administrative and accounting procedures also ensure specific prevention and control measures for the following activities:

- method of entering accounting data;
 - periodic checks and rectifications;
 - financial statement reclassification;
 - determining and verifying the correctness of tax and fiscal charges;
 - approval of financial statements;
 - accounting audits.
- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;
 - differentiated selection methodology based on key hiring criteria;
 - due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);
 - signing of contracts by persons holding appropriate administrative powers.

Administrative procedures relating to personnel require specific control measures with reference to payroll activities (detection and traceability of attendance, holidays, leaves, overtime; definition of rules for the management of expense reports, traceability of bonuses and incentives system).

- **Procedure for sponsorships, donations and events** which defines roles and responsibilities as well as specific control measures on the following activities:

- with regard to sponsorships, specific control elements are envisaged on the assessment of interest, due diligence on beneficiaries, formalisation and completeness of sponsorship contracts with the signing of clauses on knowledge and compliance with the principles defined in the Model and in the Code of Ethics (so-called 231 Clauses), and the verification of performances;
 - with regard to donations, defining admissibility limit values, as well as specific control elements on due diligence on beneficiaries and attestation of actual use where admissible;
 - with regard to the management of trade fairs and events, specific control elements on costs related to events defined through budget forecasting, as well as the monitoring and redefinition of periodic forecasts.
- **Policy for managing intragroup relations** which defines specific management and control measures in management economic relations, such as shared services or transfer prices.

5.4 Computer crime (Art. 24 bis Legislative Decree D.Lgs. 231/2001) and offences committed in violation of Copyright Law (Art. 25 novies Legislative Decree D.Lgs. 231/2001)

Art. 24 bis of Legislative Decree D.Lgs. 231/2001 extends liability to the near totality of computer related crimes, thereby referring to activities aimed at the manipulation, interception or damage of data and IT systems, regardless of whether their nature or destination is private (e.g. market competitors) or public: indeed, offences include unauthorised access to an IT or telecommunications system , the illegal possession and dissemination of access codes to IT or telecommunications systems, the dissemination of equipment, devices or IT programs aimed at damaging or interrupting an IT or telecommunications system, the interception, impediment or illicit interruption of IT or telecommunications, and damage to IT or telecommunications systems of public utility.

Art. 25 novies of Legislative Decree D.Lgs. 231/2001 regards so-called "crimes relating to copyright infringement" and, considering the MOST recurrent (non-exclusive) method of committing such crimes through the use of company IT systems, a unitary treatment was deemed appropriate, given the fungible nature of prevention measures applied for the management and prevention of the risk of committing both crimes.

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, such as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Articles 24-bis and 25-novies of Legislative Decree D. Lgs. 231/2001:

<ul style="list-style-type: none"> - Management of corporate hardware and software infrastructure for related goods (Art. 24 bis and 25 novies) 	ITC
<ul style="list-style-type: none"> - Management of physical / logical accesses and privileges and management of internal and external networks (Art. 24 bis and 25 novies) 	
<ul style="list-style-type: none"> - Technical and institutional communications (Art. 25 novies) 	Communications

Prevention measures

Regarding control activities implemented with the aim of preventing computer crimes and copyright infringement, the Company has adopted the following prevention and control measures:

- **Code of Ethics and company regulation** which requires all employees to work diligently to protect company assets, prohibits intervening on the IT or telecommunications system, the altering of data, information or programs and also requires compliance with laws relating to copyright infringement and the protection of intellectual property rights.
- **System of proxies** which assigns authorisation and control powers in a coherent manner.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Management of information systems** where, in agreement with the Parent Company, specific control measures are defined on:
 - enabling / disabling of user or profile changes;
 - preparation and updating of a machinery register where the machine code of installed programs, indication of license numbers, expiry dates and authorised user operators are duly inventoried;
 - disaster recovery system;
 - specifications limiting Internet browsing;
 - records (log files) and verifiability;
 - mapping of machinery;

- traceability through the labelling of machinery (site, type, progressive number);
- controls over machine status when conducting routine and extraordinary maintenance;
- profiling and traceability of users via special reports;
- regulation of physical / logical accesses and privileges, and management of internal and external networks

5.5 Organised crime (Article 24 ter of Legislative Decree D.Lgs. 231/2001), crimes relating to terrorism and the subversion of democratic order (Article 25 quater of Legislative Decree D.Lgs. 231/2001), transnational offences pursuant to Italian Law 146/2006

The extension of liability for entities to organised crime offences committed within the territory of the State is aimed at countering the committing of any type of crime, provided that it is in an associated form, or with the stable, ongoing and organised collaboration of at least three subjects: this logic means that even offences formally not included among the classes of offences pursuant to Legislative Decree 231/2001, can determine the administrative responsibility of IMS TECHNOLOGIES, if committed within a logic of association.

The activities within whose scope the types of crime referred to in Art. 25-quater of Legislative Decree No. 231/2001 may abstractly be committed are essentially related to the management of business relationships with natural or legal persons having their headquarters or operating in geographic locations considered at risk, the management of financial transactions, or the execution of transactions to countries deemed at risk.

Failure to provide verification and control of the possible presence of names in the international black list, or the ineffectiveness of controls may favour the risk of hiring persons linked to criminal associations or issuing orders in favour of suppliers who for some reason are connected to criminal associations.

Furthermore, note that Law 146 of 16 March 2006 introduced the concept of "transnationality" for offences into Italian law if an organised criminal group is involved and meets the following conditions: the offence committed is punished with a prison sentence of no less than a maximum of four years; it is committed in MORE than one state or is committed in one state, but a substantial part of its preparation, planning, management or control takes place in another state; it is committed in one state, but an organised criminal group is involved that is implicated in criminal activities in MORE than one state or, ultimately, it is committed in one state but has substantial effects in another state. When these conditions are met, the crimes of:

- mafia-type association Art. 416 bis of the Italian Criminal Code
- criminal association Art. 416 of the Italian Criminal Code
- money laundering Art. 648 bis of the Italian Criminal Code
- use of money, goods or benefits of illicit origin Art. 648 ter of the Italian Criminal Code
- self-laundering Art. 648 ter-1 of the Italian Criminal Code

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Articles 24-ter and 25-quater of Legislative Decree D.Lgs. 231/2001:

- Sales management	Sales
- Pricing and discounts	
- Management of relations with agents and data gatherers	
- Budgeting	Budgeting
- Deltamould	Operations
- Management of supplies	Supply Chain
- Management of credit lines for professional services and assignments	
- Qualification and evaluation	
- Warehouse management	Warehouse management
- Management of liabilities	Administration and Finance
- Management of assets	
- Treasury	
- Administrative control	
- Maintenance and services	Production (Seriante site)
- Selection and hiring	HR
- Technical and institutional communications	Communications
- Gifts and sponsorships	
- Services management	Services

Prevention measures

Regarding activities and checks implemented in order to prevent offences relating to organised crime and the financing of terrorism, the Company has adopted the following prevention and control measures:

- **Code of Ethics** which expressly rejects any form of collaboration and facilitation in full compliance with current legislation and on the basis of general principles of integrity, transparency, correctness, collaboration and loyalty.
- **System of proxies and powers of attorney** which defines authorisation and control powers and assigns them consistently according to operating practice.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Sales management procedure** which defines roles, responsibilities and specific control measures in the management of relations with agents, prospects, clients and pricing:
 - controls and monitoring on the pricing system and the definition of specific limits and authorisations for discounts;
 - due diligence on agents and acquiring self-declarations on the absence of pending charges;
 - ethical and eco-fin due diligence on clients;
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).

Furthermore, specific control measures are defined for the issuing of active invoices and after-sales activities, including the issuance of active invoices and sales and transport documents directly from the management system, as well as specific control measures such as verification of correspondence between order requests, delivery notes and invoices.

The traceability of every post-sales intervention is guaranteed, both through the management system and through specific intervention reports.

- **Prevention procedure** which defines specific control measures in budgeting management, such as:
 - the definition of a dedicated budget;
 - valorisation of estimated contract costs based on specific defined criteria, such as job orders, machine component costs, hourly design costs, history, etc.;
 - monitoring of correspondence between quoted budget costs and actual prices.

- **Procurement procedure** which defines roles, responsibilities and specific control measures in managing the procurement process, ensuring the traceability of operations such as:
 - verification of effective procurement needs;
 - qualification of suppliers through due diligence, guaranteeing technical and professional suitability evaluation elements, as well as the possession of any specific authorisations (e.g. authorisations for transport and waste disposal) and specific certifications where necessary; for certain categories of supply, ethical due diligence is also envisaged;
 - specific supplier selection criteria;
 - purchasing authorisation and signing of contracts by persons holding suitable powers (power of attorney and/or proxies);
 - verification of effective supply (goods and/or services)
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).

- **Procedure for the active and passive cycle** which defines roles, responsibilities and specific control measures in the management of active and passive invoices, financial flows and treasury, management control and allocation of accounting data, ensuring the traceability of operations such as:
 - verification of services effectively provided (active / passive);
 - verification of correspondence between invoices / purchasing requests / purchase orders / contracts;
 - invoice blocking and management of irregularities;
 - authorisation to pay and execute payments by persons with specific powers;
 - monitoring and control of incoming and outgoing financial flows through IT support systems (Piteco, JD Edwards);
 - periodic bank reconciliations.

Administrative and accounting procedures also ensure specific prevention and control measures for the following activities:

- method of entering accounting data;
- periodic checks and rectifications;
- financial statement reclassification;
- determining and verifying the correctness of tax and fiscal charges;
- approval of financial statements;

- accounting audits.
- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;
 - differentiated selection methodology based on key hiring criteria;
 - due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);
 - signing of contracts by persons holding appropriate administrative powers.

Administrative procedures relating to personnel require specific control measures with reference to payroll activities (detection and traceability of attendance, holidays, leaves, overtime; definition of rules for the management of expense reports, traceability of bonuses and incentives system).

- **Procedure for sponsorships, donations and events** which defines roles and responsibilities as well as specific control measures on the following activities:
 - with regard to sponsorships, specific control elements are envisaged on the assessment of interest, due diligence on beneficiaries, formalisation and completeness of sponsorship contracts with the signing of clauses on knowledge and compliance with the principles defined in the Model and in the Code of Ethics (so-called 231 Clauses), and the verification of performances;
 - with regard to donations, defining admissibility limit values, as well as specific control elements on due diligence on beneficiaries and attestation of actual use where admissible;
 - with regard to the management of trade fairs and events, specific control elements on costs related to events defined through budget forecasting, as well as the monitoring and redefinition of periodic forecasts.

5.6 Counterfeiting of coins, public credit notes, revenue stamps and identifiers or signs (Art. 25 bis of Legislative Decree 231/2001) crimes against industry and trade (Art. 25 bis.1 of Legislative Decree 231/2001)

Among the offences cited under Articles 25 bis of Legislative Decree D.Lgs. 231/2001, the greatest exposure for regards crimes for disrupting freedom of industry or trade (Art. 513 of the Italian Criminal Code) and illegal competition with threats or violence (Art. 513 bis of the Italian Criminal Code).

Crimes relating to the counterfeiting of money, the spending and introduction, after agreement, of counterfeit money into the State (Article 453 of the Italian Criminal Code), alteration of money (Article 454 of the Italian Criminal Code), spending and introduction into the State, without agreement, of falsified coins (Article 455 of the Italian Criminal Code).

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Articles 25-bis e 25-bis 1 of Legislative Decree D.Lgs. 231/2001:

- Sales management (Art. 25 bis 1)	Sales
- Converting Technical Department (Art. 25 bis 1)	Engineering
- Packaging Technical Department (Art. 25 bis 1)	
- Production & Planning (Art. 25 bis)	Operations
- Automotive (Art. 25 bis)	
- Deltamould (Art. 25 bis)	
- Production (Art. 25 bis 1)	Production (Seriante site)
- Selection and hiring (Art. 25 bis 1)	HR
- Management of intellectual and industrial property (brands and patents) (Art. 25 bis)	Legal

Prevention measures

As regards the activities and controls implemented in order to prevent crimes of counterfeiting money, public credit notes, revenue stamps and identification instruments or signs, as well as crimes against industry and commerce, the Company has adopted the following prevention and control measures:

- **Code of Ethics** which illustrates the Company's guidelines in relation to relations with competitors, recommending compliance with the legislation to protect the principle of fair competition.
- **System of proxies and power of attorney** which assigns authorisation and control powers in a consistent manner.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.

- **Sales management procedure** which defines roles, responsibilities and specific control measures in the management of relations with agents, prospects, clients and pricing:
 - controls and monitoring on the pricing system and the definition of specific limits and authorisations for discounts;
 - due diligence on agents and acquiring self-declarations on the absence of pending charges;
 - ethical and eco-fin due diligence on clients;
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).

Furthermore, specific control measures are defined for the issuing of active invoices and after-sales activities, including the issuance of active invoices and sales and transport documents directly from the management system, as well as specific control measures such as verification of correspondence between order requests, delivery notes and invoices.

The traceability of every post-sales intervention is guaranteed, both through the management system and through specific intervention reports.

- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;
 - differentiated selection methodology based on key hiring criteria;
 - due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);
 - signing of contacts by persons holding appropriate administrative powers.

Administrative procedures relating to personnel require specific control measures with reference to payroll activities (detection and traceability of attendance, holidays, leaves, overtime; definition of rules for the management of expense reports, traceability of bonuses and incentives system).

- **Policy for managing brands** which defines specific management and control measures in the management of trademark registration operations, with particular reference to the search for novelty / prior art, registration in classes, coexistence agreements etc.

5.7 Corporate crimes (Art. 25 ter of Legislative Decree D.Lgs. 231/2001)

These types of crimes are of particular relevance, both for the large number of activities that potentially expose the Company to the risk of their being committed, and for the multiplicity of legal interests protected by the provisions referred to in Art. 25 ter of Legislative Decree 231/2001 (transparency of corporate information, integrity of company assets, legitimate market performance of financial instruments, etc.).

Recently the law has intervened on Art. 25 ter of Legislative Decree 231/2001, making significant changes: the first intervention dates back to Law 190/2012 through which liability was also extended to the Company for the benefit or in the interest of which money or other benefits were given or promised in favour of the directors, general managers and executives charged with preparing corporate accounting documents, as well as statutory auditors and liquidators, in executing or omitting acts in violation of the obligations inherent to their office, or obligations of loyalty eliciting damage to the Company (active corruption pursuant to Article 2635, paragraph III of the Italian Civil Code; the second intervention, on the other hand, dates back to Law 69/2015, through which the crime of false corporate communications referred to in Articles 2621-2622 of the Italian Civil Code was rewritten with important repercussions on Legislative Decree 231/2001.

More recently, Law 3/2019 has extended the range of predicate offences with the case in point "Incitement to corruption between private individuals", which punishes inductive or instigating acts of private corruption, meaning such acts as the promise or offer, whether direct or indirect, of money or other undue benefits.

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Article 25-ter of Legislative Decree D.Lgs. 231/2001:

- Sales management	
- Pricing and discounts	Sales
- Management of relations with agents and data gatherers	
- Budgeting	Budgeting
- Project Management	Project Management

<ul style="list-style-type: none"> - Production & Planning - Automotive - Deltamould 	Operations
<ul style="list-style-type: none"> - Management of supplies - Management of credit lines for professional services and assignments - Qualification and evaluation 	Supply Chain
<ul style="list-style-type: none"> - Warehouse management 	Warehouse management
<ul style="list-style-type: none"> - Management of liabilities - Management of assets - Treasury - Administrative control - Management of detection, recording and representation in the accounting books, and determination of tax and fiscal charges - Management of intragroup relations 	Administration and Finance
<ul style="list-style-type: none"> - Maintenance and services 	Production (Seriarte site)
<ul style="list-style-type: none"> - Selection and hiring 	HR
<ul style="list-style-type: none"> - Technical and institutional communications - Events and trade fairs - Gifts and sponsorships 	Communications
<ul style="list-style-type: none"> - Management of services 	Services
<ul style="list-style-type: none"> - Claims management - Management of corporate deeds and conflicts of interest 	Legal

The abovementioned activities could see the Company involved in the following criminal offences (provided they occur in its interest or to its advantage): false corporate communications to the detriment of shareholders or creditors, impeded control, hindering the exercise of the functions of public supervisory authorities, unlawful influence on the assembly, fictitious formation of capital, operations to the detriment of creditors, corruption between individuals.

With regard to the latter, it should be noted that although the Strasbourg Convention

intends to punish the behaviour of those who provide or promise undue advantage, as well as those who receive the bestowal or promise of advantage in order to perform an act contrary to their own duties (thus active and passive corruption), Art. 25 ter of Legislative Decree 231/2001, as formulated today with respect to a partial reference to Art. 2635 of the Italian Civil Code (only paragraph III), places liability deriving from the committing of active corruption on the entity. Thus, the conduct of someone who pays or promises to pay money or other benefits (e.g. hiring a person indicated by the corrupt person, or entrusting a consultancy appointment in favour of a professional connected to the corrupt person) to one of the persons indicated in Art. 2635, I of the Italian Civil Code (e.g. executive or general manager) of the client company in order to award the contract to IMS TECHNOLOGIES, even if more disadvantageous compared to the offers of competitors, or to the conduct of someone who pays or promises to pay money or other benefits to a representative of the Supplier under Art. 2635 of the Italian Civil Code, to apply a decisive discount for the awarding of an order and, above all, for preparing a more advantageous offer than that of their competitors.

Prevention measures

As regards the activities and controls implemented in order to prevent crimes of corporate crimes, the Company has adopted the following prevention and control measures:

- **Code of Ethics** which illustrates the Company's guidelines, recommending the truthfulness, completeness, correctness and accuracy of the accounting data and information, and imposing efforts to prepare accurate and complete economic and financial data for a clear, truthful and correct representation of the Company's administrative situation, establishing and using suitable tools to identify, prevent and manage risks of any kind, including fraud and incorrect behaviour. The principles of conduct regarding potential conflicts of interest and the management of confidential and/or privileged information are also expressed.
- **System of proxies and power of attorney** which assigns authorisation and control powers in a consistent manner, appointing persons with the power to represent the Company or the power/duty to fulfil communication requirements.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Procedure for the active and passive cycle** which defines roles, responsibilities and specific control measures in the management of active and passive invoices,

financial flows and treasury, management control and allocation of accounting data, ensuring the traceability of operations such as:

- verification of services effectively provided (active / passive);
- verification of correspondence between invoices / purchasing requests / purchase orders / contracts;
- invoice blocking and management of irregularities;
- authorisation to pay and execute payments by persons with specific powers;
- monitoring and control of incoming and outgoing financial flows through IT support systems (Piteco, JD Edwards);
- periodic bank reconciliations.

Administrative and accounting procedures also ensure specific prevention and control measures for the following activities:

- method of entering accounting data;
 - periodic checks and rectifications;
 - financial statement reclassification;
 - determining and verifying the correctness of tax and fiscal charges;
 - approval of financial statements;
 - accounting audits.
- **Sales management procedure** which defines roles, responsibilities and specific control measures in the management of relations with agents, prospects, clients and pricing:
- controls and monitoring on the pricing system and the definition of specific limits and authorisations for discounts;
 - due diligence on agents and acquiring self-declarations on the absence of pending charges;
 - ethical and eco-fin due diligence on clients;
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).

Furthermore, specific control measures are defined for the issuing of active invoices and after-sales activities, including the issuance of active invoices and sales and transport documents directly from the management system, as well as specific control measures such as verification of correspondence between order requests, delivery notes and invoices.

The traceability of every post-sales intervention is guaranteed, both through the management system and through specific intervention reports.

- **Budgeting procedure** which defines specific control measures in the management of budgeting activities, such as:
 - definition of a dedicated budget;
 - valuation of estimated contract costs based on specific defined criteria, such as job orders, machine component costs, hourly design costs, historicity, etc.;
 - monitoring of correspondence between price quotes and offers.

- **Procurement procedure** which defines roles, responsibilities and specific control measures in managing the procurement process, ensuring the traceability of operations such as:
 - verification of effective need of procurements;
 - qualification of suppliers through due diligence, guaranteeing technical and professional suitability evaluation elements, as well as the possession of any specific authorisations (e.g. authorisations for transport and waste disposal) and specific certifications where necessary; for certain categories of supply, ethical due diligence is also envisaged;
 - specific supplier selection criteria;
 - purchasing authorisation and signing of contracts by persons holding suitable powers (power of attorney and/or proxies);
 - verification of effective supply (goods and/or services)
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).

- **Project Management procedure** which defines specific management and control measures for project management operations, such as:
 - definition of production indicators;
 - management and traceability of FAT and SAT activities;
 - monitoring system for production trends (e.g. periodic meetings, action lists, periodic reports, commission Gantt charts).

- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;
 - differentiated selection methodology based on key hiring criteria;
 - due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);

- signing of contracts by persons holding appropriate administrative powers.

Administrative procedures relating to personnel require specific control measures with reference to payroll activities (detection and traceability of attendance, holidays, leaves, overtime; definition of rules for the management of expense reports, traceability of bonuses and incentives system).

- **Procedure for sponsorships, donations and events** which defines roles and responsibilities as well as specific control measures on the following activities:
 - with regard to sponsorships, specific control elements are envisaged on the assessment of interest, due diligence on beneficiaries, formalisation and completeness of sponsorship contracts with the signing of clauses on knowledge and compliance with the principles defined in the Model and in the Code of Ethics (so-called 231 Clauses), and the verification of performances;
 - with regard to donations, defining admissibility limit values, as well as specific control elements on due diligence on beneficiaries and attestation of actual use where admissible;
 - with regard to the management of trade fairs and events, specific control elements on costs related to events defined through budget forecasting, as well as the monitoring and redefinition of periodic forecasts.
- **Policy for managing intragroup relations** which defines specific management and control measures in management economic relations, such as shared services or transfer prices.

5.8 Crimes of manslaughter and culpable severe or very serious negligent injuries, committed in violation of accident prevention regulations and the protection of hygiene and health at work (Art. 25 septies Legislative Decree D.Lgs. 231/2001)

On 1 April 2008, the Italian Council of Ministers approved the Decree implementing Law 123 of 3 August 2007 relating to safety in the workplace; this Decree refers to the Organisation and Management Models (Article 30), stating that:

- The organisation and management model exempting the administrative liability of legal persons, companies and associations, including those without legal personality, as per Legislative Decree no. 231, must be adopted and effectively implemented, ensuring a corporate system for the fulfilment of all legal obligations relating to:

- observance of the technical and structural standards regarding equipment, facilities, workplaces, chemicals, and physical and biological substances;
 - risk assessment activities and the preparation of related prevention and protection measures;
 - organisational activities, such as emergencies, first aid, contract management, periodic safety meetings, consultations with workers' representatives on safety issues;
 - health monitoring activities;
 - workers' information and training activities;
 - supervisory activities regarding the observance of safety procedures and safe work instructions by workers;
 - the acquisition of legally mandatory documentation and certifications;
 - periodic checks for the implementation and effectiveness of adopted procedures.
- The organisation and management model pursuant to the first point must provide suitable recording systems for the actual implementation of the activities reported above.
 - The organisational model should in any case ensure, as required by the nature and size of the organisation and the type of business activity, an organisation of functions that provides the technical skills and powers required for verification, evaluation, management, and monitoring of risk, as well as a disciplinary system to punish non-compliance with the measures mentioned in the model.

The organisational model should also provide an appropriate monitoring system on the implementation of the model and maintenance over time of the eligibility conditions for the measures adopted. The review and possible amendment of the organisational model must be adopted when significant violations of the rules relating to accident prevention and health and safety at work are found, or in the event of changes in the organisation and activity relating to scientific and technological progress.

In their initial implementation, the business organisation models defined in accordance with UNI-INAIL guidelines for a health and safety management system at work (SGSL) dated 28 September 2001, or the British Standard OHSAS 18001: 2007, are presumed to comply with the requirements set out in the preceding paragraphs for the corresponding sections. For the same purposes, further corporate organisational and management models may be indicated by the Commission under Article 6.

Exposure to risk

The definition of sensitive activities under the Decree was made taking into consideration those activities within which injuries may occur, as well as those within which the Company may commit the offence of culpable violation of prevention rules and measures. In view of this dichotomy, the following can be distinguished:

- activities with a risk of accident and occupational disease as exemplified in the Risk Assessment Document and understood as activities where harmful events may potentially occur;
- activities at risk of offences, considered as activities that may potentially cause crimes pursuant to Art. 25-septies of the Decree, as their omission or ineffective implementation could complement the Company's liability under the Management Liability, as part of resource management and service implementation.

The following processes are exposed to the risk of committing the aforementioned offences:

- SSL	Management of Health and Safety requirements
- Converting Technical Department	Engineering
- Packaging Technical Department	
- Production & Planning	Operations
- Automotive	
- Production	Production (Seriata site)

Prevention measures

In accordance with the provisions of Art. 30 of Legislative Decree. 81/2008, Model 231 constitutes a further control and verification of the existence, effectiveness and adequacy of the management system structure for the protection of health and safety in the workplace, ensuring specific control measures in relation to the following elements:

- Risk assessment
- Management of emergencies (accidents and near misses)
- Health monitoring
- Training and information

- **Code of Ethics** which defines the principles and behaviours that should be observed by Company employees, as well as by all external parties who are lawfully on the Company premises, providing in particular that all persons, within their own sphere, must contribute to maintaining a healthy and safe working environment in which they operate, ensuring the safety of colleagues and collaborators, and that all recipients are also required to manage risks in a preventive manner, following the appropriate procedures and using personal protective equipment. In the event of a hazardous situation, including where it has not led to damage or injury to people or property, the situation must be immediately reported to a senior manager so that it can be made known to the RSPP [Head of the Prevention and Protection Service] in order to assess whether further countermeasures are necessary, or if those already in place are sufficient.
- **System of powers of attorney and proxies** which assign authorisation and control powers in a consistent manner, appointing persons in charge of:
 - implementing the necessary information and training of employees on generic and specific work risks, as well as on safety devices and the means, measures and preventive activities adopted, on the dangers connected with the use of substances and on the obligations that the law also places on workers in terms of prevention;
 - entrusting the tasks to workers, taking into account their abilities and conditions in relation to their health and safety;
 - monitoring the use of individual and collective means of protection and safety devices in general, and their maintenance and efficiency;
 - providing for and implementing emergency measures in the event of first aid, firefighting, evacuation of workers and serious and immediate danger.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Procedure for the management of technical and professional qualifications** which defines the methodology for managing the technical and professional qualifications (pursuant to Article 26 of Legislative Decree 81/08) of suppliers, through a request for specific elements that guarantee the assessment of technical suitability (in health and security), including specific certifications where necessary;
- **Procedure for compliance with the Machinery Directive** which defines the roles and responsibilities of persons involved as well as specific control measures regarding the

analysis of safety risk and certificates of conformity for machinery in all production sectors.

- **Safety policy** which defines roles and responsibilities in the management of health and safety within the workplace, in order to prevent risks and in compliance with current regulations.
- **Manuals, procedures and operating instructions** which define roles, responsibilities and specific control measures in the management of obligations, together and consistently with the risk assessment document, action plan and emergency plan:
 - DVR [Risk Assessment Document]
 - Definition and updating of emergency plans
 - Health monitoring
 - Identification of hazards, assessment of risks and definition of control systems
 - Measurement of performances and monitoring inherent to Safety
 - Personal protective equipment (PPE)
 - Management of emergencies

5.9 Crimes of receiving stolen goods, money laundering, self-laundering and use of goods of illicit origin (Art. 25 octies Legislative Decree D.Lgs. 231/2001)

IMS TECHNOLOGIES could incur liability pursuant to Legislative Decree 231/01 in the event that one of the crimes referred to in Articles 648, 648 bis, 648 ter and 648 ter.1 of the Italian Criminal Code, or in the event that a senior manager or subordinate should purchase, receive or hide money or property deriving from any crime, replace or transfer money, goods or other benefits from a crime, also committed by the same perpetrator (so-called self-laundering), or should in some way employ money, goods or other utilities of criminal origin in economic or financial activities.

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Articles 25-octies of Legislative Decree D.Lgs. 231/2001:

- Management of supplies	Supply chain
--------------------------	--------------

- Management of appointments for services and professional assignments	
- Qualification and evaluation	
- Warehouse management	Warehouse management
- Management of liabilities	
- Management of assets	
- Treasury	
- Administrative control	Administration and Finance
- Management of detection, recording and representation in the accounting books, and determination of tax and fiscal charges	
- Management of intragroup relations	
- Administrative management of personnel	HR
- Management of system of bonuses and incentives	
- Technical and institutional communications	
- Events and trade fairs	Communications
- Gifts and sponsorships	

Prevention measures

Regarding activities and controls implemented in order to prevent the offences of receiving stolen goods, money laundering, self-laundering and the use of goods of illicit origin, the Company has adopted the following prevention and control measures:

- **Code of Ethics** which illustrates the Company's guidelines and explicitly prohibits the substitution or transfer of money, goods or other benefits deriving from illegal activities or carrying out other operations in relation to the latter, such as to hinder the identification of their origin. It also prohibits the use of the aforementioned assets in economic or financial activities and requires the prior verification of available information (including financial information) on commercial, financial counterparties and suppliers, in order to ascertain the respectability and legitimacy of their business operations prior to establishing a business relationship.
- **System of powers of attorney and proxies** which assign authorisation and control powers in a consistent manner.

- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Procedure for the active and passive cycle** which defines roles, responsibilities and specific control measures in the management of active and passive invoices, financial flows and treasury, management control and allocation of accounting data, ensuring the traceability of operations such as:
 - verification of services effectively provided (active / passive);
 - verification of correspondence between invoices / purchasing requests / purchase orders / contracts;
 - invoice blocking and management of irregularities;
 - authorisation to pay and execute payments by persons with specific powers;
 - monitoring and control of incoming and outgoing financial flows through IT support systems (Piteco, JD Edwards);
 - periodic bank reconciliations.

Administrative and accounting procedures also ensure specific prevention and control measures for the following activities:

- method of entering accounting data;
- periodic checks and rectifications;
- financial statement reclassification;
- determining and verifying the correctness of tax and fiscal charges;
- approval of financial statements;
- accounting audits.
- **Procurement procedure** which defines roles, responsibilities and specific control measures in managing the procurement process, ensuring the traceability of operations such as:
 - verification of effective procurement needs;
 - qualification of suppliers through due diligence, guaranteeing technical and professional suitability evaluation elements, as well as the possession of any specific authorisations (e.g. authorisations for transport and waste disposal) and specific certifications where necessary; for certain categories of supply, ethical due diligence is also envisaged;
 - specific supplier selection criteria;

- purchasing authorisation and signing of contracts by persons holding suitable powers (power of attorney and/or proxies);
 - verification of effective supply (goods and/or services)
 - signing clauses on the knowledge of and compliance to the principles defined in the Model and Code of Ethics (so-called 231 Clauses).
- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;
 - differentiated selection methodology based on key hiring criteria;
 - due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);
 - signing of contracts by persons holding appropriate administrative powers.

Administrative procedures relating to personnel require specific control measures with reference to payroll activities (detection and traceability of attendance, holidays, leaves, overtime; definition of rules for the management of expense reports, traceability of bonuses and incentives system).

- **Procedure for sponsorships, donations and events** which defines roles and responsibilities as well as specific control measures on the following activities:
 - with regard to sponsorships, specific control elements are envisaged on the assessment of interest, due diligence on beneficiaries, formalisation and completeness of sponsorship contracts with the signing of clauses on knowledge and compliance with the principles defined in the Model and in the Code of Ethics (so-called 231 Clauses), and the verification of performances;
 - with regard to donations, defining admissibility limit values, as well as specific control elements on due diligence on beneficiaries and attestation of actual use where admissible.
 - with regard to the management of trade fairs and events, specific control elements on costs related to events defined through budget forecasting, as well as the monitoring and redefinition of periodic forecasts.

5.10 Environmental offences (Art. 25 undecies / Legislative Decree D.Lgs. 231/2001)

Article 25- undecies of Legislative Decree D.Lgs. 231/2001 (substantially reformed by Law 68/2015) extends the liability of entities to committing offences aimed at damaging and exploiting flora and fauna (killing, destruction, capture, taking or possession of specimens of protected plant or wild animal species , destruction or deterioration of habitats within a protected site), as well as illegally constituting environmental pollution or environmental damage (unauthorised discharge of industrial wastewater, exceeding limits for air quality, malicious and negligent pollution), and more generally committing offences resulting from the explicit violation of applicable legislation (unauthorised waste management activities, illicit waste trafficking, organised activities for illicit waste trafficking).

More specifically, the cases referred to in Art. 25 undecies of the Decree are: environmental pollution (Art. 452 bis of the Italian Criminal Code), environmental disaster (Art. 452 quater of the Criminal Code), culpable crimes against the environment (Art. 452 quinquies of the Criminal Code), trafficking and abandonment of highly radioactive material (Art. 452 sexes of the Criminal Code), killing, destruction, capture, taking, possession of specimens of protected wild animal or plant species (Art. 727 bis of the Criminal Code), destruction or deterioration of habitats within a protected site (Art. 733 bis of the Criminal Code), environmental regulations - criminal sanctions (Article 137 of Legislative Decree 152/2006), discharges onto the ground (Art. 103 of Leg. Decree 152/2006), discharges into the subsoil and groundwater (Art. 104 of Leg. Decree 152/2006), discharges into sewage networks (Art.107 of Leg. Decree 152/2006), discharges of hazardous substances (Art.108 of Leg. Decree 152/2006), unauthorised waste management activities (Art. 256 of Leg. Decree 152/2006), prohibition of abandonment (Art. 192 of Leg. Decree 152/2006), violation of the remediation of sites (Art. 257 of Leg. Decree 152/2006), violation of obligations of communication, keeping of mandatory records and forms (Art. 258 of Leg. Decree 152/2006), illicit waste trafficking (Art. 259 of Leg. Decree 152/2006), activities organised for the illegal trafficking of waste (Art. 452 quaterdecies of the Criminal Code), violations relating to the traceability of waste (Art. 260-bis of Leg. Decree 152/2006), sanctions (Art. 279 of Leg. Decree 152/2006), offences pursuant to Articles 1, 2, 6, 3bis of Law no. 150 of 7 Feb. 1992, cessation and reduction of the use of harmful substances, malicious pollution and culpable pollution.

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of

committing the offences under Art. 25- undecies of Legislative Decree D.Lgs. 231/2001:

- Environment	Management of environmental obligations
---------------	---

Prevention measures

Regarding the activities and controls implemented in order to prevent environmental crimes, the Company has adopted the following prevention and control measures:

- **Code of Ethics** which provides for an explicit commitment to the use of processes, technologies and materials that allow for a reduction in the consumption of natural resources and have the lowest environmental impact; limiting waste production, where possible, through their reuse; as well as involving and motivating all personnel, through information and training actions, on environmental issues.
- **System of powers of attorney and proxies** which assign authorisation and control powers in a consistent manner in relation to the management of environmental issues.
- **Management of supplier qualifications** through due diligence activities, which ensure evaluation elements for technical and professional suitability, as well as the possession of any specific authorisations (e.g. authorisations for transport and waste disposal) and specific certifications where necessary; for certain categories of supply, ethical due diligence is also envisaged.
- Specific control measures and roles and responsibilities have been defined in order to guarantee checks on required emission abatement plants, as well as maintenance aimed at ensuring compliance with the limits set for atmospheric emissions and air quality.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.

5.11 Employment of illegal immigrants (Art. 25 duodecies of Legislative Decree D. Lgs. 231/2001)

The issuing of a residence permit has a real constitutive effect in terms of a foreigner's legitimacy to work, prior to which it is not at all possible to enter into a lawful relationship (under penalty of committing the crime in question). The law therefore requires a prompt verification of a residency permit to confirm regular immigration status.

The active party of the crime is the employer. However, the law assimilates within the concept of employer any person who "hires and pays one or more persons, for a fixed or indefinite term, with the task of performing an employment activity of any nature".

A prerequisite of the crime is the employment of a foreign citizen in one's employ.

Law 161/2017 reformed the Anti-Mafia Code and has also amended Art. 25 duodecies introducing the crime of transporting illegal aliens in the territory of the State, as well as that of aiding and abetting the stay of irregular aliens in the territory of the State. Both crimes foresee the application of disqualification sanctions pursuant to Art. 9, paragraph 2 of Legislative Decree D. Lgs. 231/2001 for a period of not less than one year.

Exposure to risk

The types of offences referred to in Article 25-duodecies of Legislative Decree D. Lgs. 231/2001 are represented by the management of the recruitment process of employees and non-EU collaborators.

The processes are exposed to the risk of committing the offences in question:

- Selection and hiring	HR
------------------------	----

Prevention measures

Regarding activities and controls implemented in order to prevent the offences of employing illegally landed immigrants receiving stolen goods, money laundering, self-laundering and the use of goods of illicit origin, the Company has adopted the following prevention and control measures:

- **Code of Ethics** illustrating the Company's guidelines in the selection, hiring and protection of personnel.
- **System of powers of attorney and proxies** which assigns authorisation and control powers in a consistent manner.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Procedure for managing Human Resources** which defines specific control measures in personnel selection and hiring, administrative management and training activities, such as:
 - verifying needs in human resources and approval by Management;

- differentiated selection methodology based on key hiring criteria;
- due diligence on candidates (e.g. acquiring statements for executives and middle managers, for pending charges, criminal records and declarations of absence of conflict of interest);
- acquisition of residence permits;
- signing of contacts by persons holding appropriate administrative powers.

5.12 Tax crimes (Art. 25 quinquiesdecies of Legislative Decree D.lgs. 231/2001)

The Law for the reform of Tax Offences, Law no. 157 of 19 December 2019, in conversion of the Legislative Decree no. 124 of 26 October 2019 (so-called Tax Decree), has extended the liability of entities to tax offences, by inserting Art. 25 quinquiesdecies in Legislative Decree D.Lgs. 231/2001.

Tax crimes include the offences of: fraudulent declaration through the use of invoices or other documents for non-existent transactions and/or other artifices; issuing of invoices or other documents for non-existent transactions; concealment or destruction of accounting records and fraudulent evasion of tax payments.

Exposure to risk

The results of the risk analysis have led to identifying the following activities, within company processes, as those in which IMS TECHNOLOGIES is more highly exposed to the risk of committing the offences under Art. 25-quinquiesdecies of Legislative Decree D.lgs. 231/2001:

- Management of liabilities	
- Management of assets	
- Treasury	
- Administrative control	Administration
- Management of detection, recording and representation in the accounting books, and determination of tax and fiscal charges	and Finance
- Management of intragroup relations	
- Management of services (Issuing of active invoices)	Services

Prevention measures

Regarding activities and controls implemented in order to prevent the offences of tax related crimes, the Company has adopted the following prevention and control measures.

- **Code of Ethics** illustrating the Company's guidelines, recommending the truthfulness, completeness, correctness and accuracy of the accounting data and information.
- **System of powers of attorney and proxies** which assigns authorisation and control powers in a consistent manner.
- **Flow procedure to the Supervisory Body** which defines the type of flows and corporate areas involved, and the transmission frequency to the Company's Supervisory Body.
- **Procedure for the active and passive cycle** which defines roles, responsibilities and specific control measures in the management of active and passive invoices, financial flows and treasury, management control and allocation of accounting data, ensuring the traceability of operations such as:
 - verification of services effectively provided (active / passive);
 - verification of correspondence between invoices / purchasing requests / purchase orders / contracts;
 - invoice blocking and management of irregularities;
 - authorisation to pay and execute payments by persons with specific powers;
 - monitoring and control of incoming and outgoing financial flows through IT support systems (Piteco, JD Edwards);
 - periodic bank reconciliations.

Administrative and accounting procedures also ensure specific prevention and control measures for the following activities:

- method of entering accounting data;
- periodic checks and rectifications;
- financial statement reclassification;
- determining and verifying the correctness of tax and fiscal charges;
- approval of financial statements;
- accounting audits.
- Specific control measures are also defined in relation to the issuing of active invoices and post-sales activities, which provide for the creation of active invoices and sales and transport documents directly from the management system, as well as specific control measures such as verification of correspondence between order requests, delivery notes and invoices. The traceability of each post-sales intervention is guaranteed, both through the management system and through specific

intervention reports.

- **Policy for managing intragroup relations** which defines specific management and control measures in management economic relations, such as shared services or transfer prices.

5.13 Other crimes

From the analysis conducted, it can be stated that the Company is not significantly exposed to the risk of committing the offences referred to in the following articles:

- 25 quater-1 "Female genital mutilation practices",
- 25 quinquies "Crimes against the individual's personality",
- 25 sexies "Market abuse offences",
- 25 terdecies "Racism and Xenophobia",
- 25 quaterdecies "Fraud in sports competitions, abusive gambling or betting and gambling exercised by means of prohibited devices".

As the Company is not significantly exposed to these offences, no additional controls are implemented beyond what may be required by the Code of Ethics adopted, by the internal documents, procedures and protocols.

6. The Supervisory and Control Body

6.1 General points

The legislative decree includes Art. 6, among the conditions for which the Entity is not liable for any predicate offences committed internally, having entrusted to a Body appointed by the entity with autonomous powers of initiative and control the task of supervising the functioning and observance of the organisation and management model prepared, as well as its updating¹.

In compliance with this requirement, the Company entrusts this function to a Supervisory Body of a collegial nature, which is appointed directly by the administrative body.

The completion of the Supervisory and Control Body's tasks constitutes an essential element for the exemption provided for by the Decree.

6.2 Appointment and composition

Supervisory and Control Body is an entity of a collegial nature, and is composed of two standing members, one of which acts as its Chairperson.

The members of the Supervisory and Control Body are chosen from among qualified candidates endowed with outstanding professionalism and possessing the integrity requirements to be understood as referred to in Art. 4 of Legislative Decree no. 516 of 30 December 1998.

The following criteria are adopted by the Company in constituting the Supervisory and Control Body:

- Composition of several members,
- Internal and external professional resources,
- Competence of each individual member.

The components of the Supervisory and Control Body are appointed by the administrative body with a resolution indicating the tasks and powers of the SB, the duration of their appointment and the remuneration due to each member, as well as the budget allocated to the appointed Body.

The appointment resolution is promptly communicated through suitable means of communication.

¹ As of 1 Jan. 2012, the task of supervising the functioning and observance of the models and of overseeing their updating (functions previously entrusted to the SB) may, in joint stock companies, also be carried out by the Board of Statutory Auditors, by the Supervisory Board or Management Control Committee. This is established pursuant to Art. 14, paragraph 12 of Law 183/2011 (2012 Stability Law) which in fact introduces paragraph 4-bis to Art. 6 of Legislative Decree D.Lgs. 231/01.

6.3 Term of office, replacement and removal of members of the Supervisory and Control Body

In order to ensure full autonomy and independence, the SB remains in office until its revocation and/or forfeiture, as established at the time of appointment by the BoD.

The absence of the subjective requirements of integrity of a member of the SB shall determine their immediate forfeiture of office. In the event of forfeiture, death, resignation or revocation, the Administrative Body will promptly replace the terminated member.

The possible revocation of the members of the Supervisory Body may only take place for just cause, by resolution of the Board of Directors, where "just cause" means gross negligence in the performance of the tasks related to the assignment such as, among other things:

- failure to draft information reports on the activities carried out by the Board of Administration;
- failure to draw up the Supervisory Board's Audit Plan;
- failure to verify the reports addressed to the Supervisory Body, regarding the commission or alleged commission of crimes referred to in the Decree, as well as the violation or alleged violation of the Model or of the procedures established in its implementation;
- failure to call and hold meetings of the SB during a semester;
- non-participation in meetings by a member without justification;
- failure to conduct routine/ad hoc verification activities on sensitive issues referred to in the Supervisory Board's Audit Plan.

6.4 The requirements of the Supervisory and Control Body

Autonomy and Independence

IMS TECHNOLOGIES is committed to guaranteeing the SB full autonomy of initiative and to protecting it from any form of interference or conditioning. To this end it is provided that:

- its members are free, if possible, from directly operational tasks, taking into account the degree of exposure to the risk of crime in the function in which they operate and have no possibility of interfering in the Company's operations, or that the heterogeneous, multi-subject composition of the SB is capable of ensuring the 'aforementioned non-interference, although there an internal resource is also present;

- In carrying out its function, the SB is not subject to hierarchical and disciplinary power of any corporate body or function;
- the SB reports directly to the administrative body;
- the adoption of its decisions and the determination of its activities are not subject to appeal.

Professionalism

To ensure the proper performance of its duties, it is essential for the SB to ensure adequate professionalism. In this respect, the following is relevant:

- knowledge of legal matters (in particular the structure and mode of committing offences as well as the Decree as a whole);
- an in-depth knowledge of the Company's organisational structure;
- adequate expertise in auditing and control (analysis techniques and risk assessment).

Integrity and absence of conflict of interest

This requirement should be understood as follows:

- the members of the Supervisory Body are chosen from among qualified persons with outstanding professionalism, that also meet the requirements relating to integrity, to be interpreted pursuant to Art. 4, of Leg. Decree no. 516 of 30 December 1998.
- The members of the Supervisory Body must maintain themselves free of any situation which could lead to an actual conflict of interest.

Continuity of action

The continuity of action of the Supervisory Body is ensured through the term in office and the possibility of revocation solely for just cause under the terms described above.

6.5 The resources of the Supervisory and Control Body

The administrative body assigns the Supervisory Body the human and financial resources deemed appropriate for the purpose of carrying out its assignment, at any rate adequate to the size of the Company and the duties of the SB according to the degree of risk exposure.

With regard to financial resources, the Supervisory Body has access to its annual allocated budget, on the proposal of the SB itself.

With regard to human resources, the Supervisory Body may make use of the assigned personnel and external consultants, including the assistance of all corporate structures.

In case of need, the Supervisory Body may request from the Board of Directors, via a written and motivated notification, for the allocation of additional human or financial resources.

6.6 Convocation of General Meeting

The Supervisory Body shall meet whenever it is deemed appropriate by the Chairperson, or as requested by at least one member to the Chairperson. The SB holds a minimum of three meetings a year. After each meeting, a specific report is drawn up, signed by the attendees.

6.7 Confidentiality

The members of the Supervisory Body are bound to secrecy regarding facts and information acquired in the exercise of their functions.

The members of the Supervisory Body shall ensure the confidentiality of any information they receive, particularly if related to reports received concerning alleged violations of the Model. In addition, the members of the Supervisory Body agree to refrain from seeking and using confidential information for purposes other than those under Art. 6, or in any case for purposes not consistent with the Supervisory Body's functions, except as expressly authorised.

In any case, all information held by the members of the Supervisory Body is treated in accordance with current legislation and, in particular, in accordance with the European Regulation for the protection of personal data.

Failure to comply with these obligations shall imply the automatic removal from office of the member of the Supervisory Body at fault.

6.8 Duties and powers of the Supervisory and Control Body

In accordance with Art. 6, paragraph 1 of the Decree, which entrusts the Supervisory Body with the task of supervising the functioning and observance of the Model and its updating, the Company's Supervisory Body has the following tasks:

- check the adequacy of the Model, i.e. its capacity to prevent the occurrence of illegal behaviour, as well as point out any committed or attempted offences;
- monitor the effectiveness of the control of the Model;
 - plan auditing activities, and review the results of previous audits;

- conducting checks on the activities and transactions identified in the risk areas (e.g. updating of procedures, system of proxies in terms of consistency between the powers granted and activities carried out; knowledge of the Model);
- conducting regular meetings with the senior management of IMS TECHNOLOGIES and with the Board of Statutory Auditors, in order to discuss, verify and report on the progress of the Organisation and Management Model;
- promoting meetings with the administrative body, whenever it deems appropriate, in order to make an assessment of or take an action to discuss matters relating to the functioning and effectiveness of the Organisation and Management Model;
- verify the Model's effectiveness, i.e. the correspondence between concrete behaviours and those formally provided for by the Model;
- establish an effective and efficient system of internal communications in order to obtain the reporting of relevant information pursuant to the decree (reporting of possible violations and/or non-compliance with the Model);
- perform complete, timely, accurate, accessible, and continuous training and information activities for the Company's employees and consultants, in particular by promoting and defining initiatives for the dissemination of knowledge pertaining to the decree and the consequences resulting from its implementation (Organisation and Management Model, risk analysis, etc.);
- monitor the updating of the Model:
 - evaluating, with the cooperation of the competent functions, any actions to be undertaken, and required to update the Model;
 - evaluating any changes from an organisational/managerial standpoint, and legislative amendments to mandatory standards, in terms of their impact on Organisation and Management Model;
 - proposing to the administrative body the changes to the model made necessary by significant violations of the provisions, by any changes in the organisation, by legislative interventions that require its adaptation or by the actual committing of offences.
- ensure a flow of information to the Company's senior management.

It should be noted that, in terms of the updating of the Model, the adoption of any changes shall be decided by the administrative body, which is directly responsible for the adoption and effective implementation of the Model.

The supervisory function is also extended to the Code of Ethics on which the Supervisory Body performs monitoring activities.

In carrying out its duties, the Supervisory Body is required to:

- document, including through the completion and keeping of specific registers, all activities carried out and measures adopted;
- document reports and information received, in order to ensure the traceability of all actions;
- record and store all documentation.
- In carrying out the tasks it has been assigned, the Supervisory Body possesses all the powers required to ensure timely and efficient supervision, in particular:
 - execute, without notice, all inspections deemed appropriate;
 - freely access all Company areas and functions, archives and documents;
 - avail itself of, under its direct supervision and responsibility, the assistance of all Company structures or external consultants;
- have access directly to the financial resources specifically allocated.

6.9 Management of internal monitoring system verifications

The Supervisory Body requires that each and every Company process at risk of crime be subject to verification by the internal control system at the intervals established by the Supervisory Body, based on the relevance and risk factor of the processes, and on the basis of the results highlighted by the audit reports of previous years. In addition, the SB may decide to conduct extraordinary checks of the internal control system based on particular reports, or if reasons related to organisational changes or identification of deficiencies render it appropriate.

The checks can also be conducted by personnel who are not part of the SB, as long as they have skills similar to those required for members of the SB.

The audits of the internal control system are conducted on the basis of a programme drawn up by the SB, approved by the Management. The programme is drawn up according to the state of importance of the activities to be subjected to verification.

The audits of the internal control system are conducted using tools such as, for example:

- interviews
- examination of the documentation,
- direct observance of activities,
- checklists (where specifications are required for each process).

The results of the activities of the SB will be shared with the Board of Directors through the annual report.

6.10 Reports and communications to the Supervisory and Control Body

Reports (Whistleblowing)

In accordance with the Whistleblowing legislation (Bill No. C. 3365-B; definitively approved on 15 Nov. 2017) and the newly introduced Art. 6 paragraph 2 bis) of Legislative Decree. D. Lgs. 231/2001, the Company recognises and protects the right of senior management and, likewise, of subordinates, to submit reports of illegal conduct or violations of this Organisation, Management and Control Model, of which they have become aware in light of the functions they perform.

The Company provides for reporting channels reserved for reporting alleged violations of rules of professional conduct and/or principles of ethics referred to by current legislation - internal and external - and/or illicit or fraudulent behaviours referable to employees, members of corporate bodies, group companies and third parties (customers, suppliers, consultants, collaborators), which can directly or indirectly cause economic damage or to assets and/or the Company's image.

All employees, members of corporate bodies or third parties (customers, suppliers, consultants, collaborators) having business relationships with the Company have the right to submit detailed reports of illegal conduct, relevant pursuant to this decree and based on elements of actual facts and agreed upon, or violations of the Organisation, Management and Control Model by directing them to the Supervisory Body.

Reports can be submitted either by ordinary mail to be addressed to IMS TECHNOLOGIES S.p.A., Via Cav. A. Beretta, 25, 24050 Calcinate (BG), confidentially reserved for the attention of the Supervisory Body of IMS TECHNOLOGIES or, alternatively, by electronic transmission to the mailbox managed by the SB. In both cases, the recipient of the report must guarantee the confidentiality of the whistleblower; however, for the latter this is ensured and guaranteed by a series of IT control measures specifically provided for.

The Company ensures the confidentiality and anonymity of whistleblowers in order to exclude the hypothetical risk of retaliation and/or discrimination against persons making reports.

No form of retaliation or discrimination is permitted against whistleblowers, affecting their working conditions for reasons related to complaints, including discriminatory measures, unjustified disciplinary actions, harassment in the workplace and any other form of retaliation that determines intolerable conditions in the workplace.

Likewise, any form of abuse related to reports is prohibited, such as, by way of example, defamation or slander, improper use or intentional exploitation of the institution. In this regard, the Company reserves the right to pursue the distorted use of the instrument itself (abuse of the right) by imposing a disciplinary sanction proportionate to the seriousness of the case.

6.11 Information flow to the Supervisory and Control Body

Pursuant to Art. 6, par. 2, lett. d) of the Decree, the obligation to inform the Supervisory Body is established regarding situations of potential risk of offences, or acts configured as violations of the System.

Actions of the Supervisory Body

The Supervisory Body examines all reports received for its attention, evaluates them and, if deemed necessary, moves to take action by initiating all necessary investigations, such as:

- convening the person responsible for the violation (or presumed such);
- involving the functions in affected by the report;
- accessing whatever source of information within the Company, document or data deemed relevant for the purposes of the investigation.

Other information

The entire organisation (corporate bodies, executives, managers and employees) is obliged to communicate to the Supervisory Body all information identified in the so-called information flow system.

The reporting frequency can be divided into the following:

- By event: whenever an episode occurs, without undue delay;

- Supervisory Body meetings: the SB provides adequate advance notice to the corporate functions of their meeting, allowing them to prepare the specified information flow;
- Specified frequency, established on the basis of potential criticality and related volumes to the information.

6.12 Reporting and management of documents

In order to ensure its full autonomy and independence, the Supervisory Body reports directly to the administrative body.

The Supervisory Body annually compiles a written report to the administrative body which must at the very least contain the following information:

- supervisory activities carried out by the Supervisory Body during the reference period;
- any criticalities that have emerged both in terms of internal behaviours and effectiveness of the Model;
- planned corrective improvement actions and their state of implementation;
- a summary of reports received by persons within and outside of the Company, including that which has been directly found, in relation to alleged violations of the provisions of this Model, of the prevention protocols and related implementation procedures, and the outcome of consequent checks carried out;
- any disciplinary actions and sanctions applied by the Company, with reference to violations of the provisions of this Model, of the prevention protocols and of related implementation procedures;
- reporting of any changes to the regulatory framework and/or significant changes to the Company's internal structure and/or methods of carrying out business operations that require an update of the Model.

The Supervisory Body may be convened at any time by the administrative body to report on particular events or situations relating to the effectiveness and efficiency of the Model; they may also ask to be heard at any time deemed appropriate to examine or intervene regarding the adequacy of the Model.

Meetings with the persons and bodies cited above must be recorded, with copies of the minutes kept by the Supervisory Body.

7. The Disciplinary System

7.1 Purpose of the Disciplinary System

IMS TECHNOLOGIES considers compliance with the Model essential and, therefore, in compliance with Art. 6, par. 2, lett. e), and Art. 7, par. 4, lett. b) of Legislative Decree D. Lgs. 231/01, has adopted an appropriate system of sanctions to be applied in the event of non-compliance with the rules provided for by the Model, since the violation of these rules and measures, imposed by IMS TECHNOLOGIES for the purpose of preventing the crimes envisaged by the Decree 231, damages the relationship of trust established with the Company.

For the purposes of the application by IMS TECHNOLOGIES of the disciplinary sanctions provided, the establishment of any criminal proceedings and their outcome are not necessary, since the rules and measures provided for in the Model are adopted in full autonomy, regardless of the offence that any conduct may have caused.

In no case shall an unlawful, illegitimate or violation of the Model be justified or deemed less serious, even if carried out in the interest or to the advantage of IMS TECHNOLOGIES. Attempts and, in particular, acts or omissions unequivocally aimed at violating the rules and provisions established by IMS TECHNOLOGIES are also sanctioned, even if the action is not carried out or the event does not occur for some reason.

7.2 Sanctions for employees

In compliance with applicable legislation, IMS TECHNOLOGIES must inform its employees of the provisions, principles and rules contained in the Organisation, Management and Control Model, through the information and training activities described in the section below.

The violation by an employee of the provisions, principles and rules contained in the Model prepared by IMS TECHNOLOGIES in order to prevent committing a crime pursuant to Decree 231 constitutes a disciplinary offence, punishable according to the procedures for contesting violations and the imposition of consequent sanctions provided for by the applicable National Collective Labour Agreement, as reported and described in the section "Disciplinary Regulations", and in compliance with the provisions of Art. 7 of the Workers' Statute, as transcribed below.

The disciplinary system relating to the Model has been configured in strict compliance with all provisions of the law on labour matters. No methods and sanctions have been envisaged other than those already codified and reported in collective agreements and trade union agreements. The applicable National Collective Labour Agreement provides for a variety

of sanctions capable of modulating the sanction to be imposed on the basis of the seriousness of the infringement. By way of example and not limited to, the following constitute a disciplinary offence, in relation to the activities identified at risk of crime:

- failure to observe the principles contained in the Code of Ethics or adopting behaviours that are non-compliant with the rules of the Code of Ethics;
- failure to respect the provisions, rules and procedures of the Model;
- missing, incomplete or untrue documentation or incorrect storage of document sources needed to ensure transparency and verifiability of activities in accordance with the rules and procedures contained in the Model;
- infringement and circumvention of the control system, through the removal, destruction or alteration of the documentation provided by the above procedures;
- impeding controls and/or unwarranted hindering of access to information and documentation to persons responsible for providing checks, including the Supervisory and Control Body.

The above disciplinary offences may be punishable, depending on the severity of the deficiencies, with the following measures:

- verbal warning
- written warning
- fines
- suspension
- dismissal

Sanctions should be imposed in consideration of the seriousness of the infringements: in view of the extreme importance of the principles of transparency and traceability, as well as the importance of monitoring and control activities, the Company will be required to apply the measures with the greatest impact on those infringements which by their very nature infringe the very principles on which this Model is based. Likewise, by way of example, the management in total autonomy of an entire process that includes not only authorisations, but also accounting issues, from which a risk among those listed in the special part of this Model arises (or may arise), may lead, following the exhaustion of the disciplinary procedure, to the dismissal for the functions involved.

The type and extent of each of the sanctions must be applied taking into account:

- the intentionality of the behaviour or degree of negligence, imprudence or inexperience, including with regard to the predictability of the event;
- the employee's overall conduct, especially with regard to the existence or otherwise of previous disciplinary measures, within the limits of the law;
- the employee's assigned tasks;
- the functional role and level of responsibility and autonomy of the people involved in the facts constituting the violation;
- any other particular circumstances relating to the disciplinary offence.

The Supervisory Body is entrusted with the task of verifying and assessing the suitability of the disciplinary system in light of Leg. Decree 231. In its periodic annual report, the Supervisory Body must also promptly indicate possible areas for improving and developing this disciplinary system, especially in light of the developments in the relevant legislation.

7.3 Sanctions for management

In the event of a violation of the Model by management personnel, the Supervisory Body will have to inform the IMS TECHNOLOGIES Board of Directors.

The Company will arrange to impose the most appropriate disciplinary measures. Moreover, in the light of the more serious fiduciary bond which, by its very nature, binds the Company to its executives, as well as in consideration of the greater experience of the latter, violations of the provisions of the Model in which executives should incur will above all involve expulsive measures, as they are deemed more appropriate.

7.4 Measures for Administrators

Upon notification of a violation of the principles, provisions and rules referred to in this Model by the members of the Board of Directors, the Supervisory Body is required to promptly inform the Board of Directors and Board of Auditors, for the adoption of appropriate measures and in order to adopt the most suitable measures.

In providing information, the Supervisory Body must not only report on the details regarding the violation, but also indicate and suggest appropriate further investigations to be conducted, if the violation is ascertained, as well as the most appropriate measures to be adopted.

7.5 Measures for Auditors

Upon notification of a violation of the provisions and rules of the Model by the members of the Board of Statutory Auditors, the Supervisory Body is required to promptly inform the entire Board of Statutory Auditors and the Board of Directors, for the adoption of appropriate measures.

In providing information, the Supervisory Body must not only report on the details regarding the violation, but also indicate and suggest appropriate further investigations to be conducted, if the violation is ascertained, as well as the most appropriate measures to be adopted (e.g. revocation of an auditor involved).

7.6 Measures for other recipients

Compliance by those who, in whichever capacity, operate in the name and on behalf of IMS TECHNOLOGIES, and by other recipients of the rules of the Code of Ethics and the Model (the latter limited to aspects that are applicable from time to time) is ensured through the provision of specific contractual clauses concerning applicable sanctions in the event of non-compliance with the Code of Ethics and the Model.

Any violation, or the committing of offences provided for by Leg. Decree 231 by such parties will not only be sanctioned in accordance with the provisions of the contracts stipulated with them, but also through appropriate judicial actions for the Company's protection. By way of example, in the most serious cases these clauses may provide for the right of termination of the contract by IMS TECHNOLOGIES, or the application of penalties for minor violations.

7.7 Measures for the violation of provisions on Whistleblowing

In accordance with Law 179/2017 (Whistleblowing), the Company pursues the improper use and intentional exploitation of reports, providing for the application of the disciplinary system as required by the CCN in relation to this issue.

The abuse of the reporting mechanism, whether through defamation or slander against the reporting party is further prosecuted.

The Company will apply the most suitable disciplinary measures taking into account the seriousness of the conduct.

7.8 Additional measures

IMS TECHNOLOGIES retains the right to avail itself of all other remedies permitted by law, including the possibility of claiming compensation for any damage resulting from a breach of Decree 231 by all of the parties listed above.

8. Training and information

8.1 Training of personnel

For the purposes of the effectiveness of the Model, it is IMS TECHNOLOGIES' objective to ensure correct disclosure and knowledge of the rules of conduct contained therein with regard to the resources already present in the company and those to be included, with different degrees of detail in relation to the various levels of involvement of the resources in activities at risk.

The information and training system is supervised and supplemented by the activity carried out in this field by the Supervisory Body, in collaboration with the heads of the corporate Functions or Areas from time to time involved in the application of the Model.

Initial notification

This Model is communicated to all Company resources at the time of its adoption through appropriate forms of communication. New hires are given an information set, in which they are provided with the knowledge considered of primary importance.

Training

Aimed at spreading knowledge of the legislation referred to in Legislative Decree D. Lgs. 231/2001, training activities are differentiated in their contents and methods of delivery according to the qualifications of recipients, the risk level of the area in which they operate, and whether or not they hold representative functions within the Company. In particular, IMS TECHNOLOGIES provides different levels of information and training through dissemination tools such as, by way of example, periodic targeted seminars, occasional e-mail updates and internal memos.

Information to collaborators and other third parties

Collaborators and outsourced contracting parties who operate, in any capacity, on behalf or in the interest of IMS TECHNOLOGIES and who are involved in carrying out "sensitive" activities pursuant to the Decree, must be informed, for the respective parties, of the contents of the Model and IMS TECHNOLOGIES' requirement that their behaviour comply with the provisions of Legislative Decree D. Lgs. 231/2001.

9. Annexes

In addition to the **Regulatory Appendix** containing an exhaustive illustration of the types of offences as provided for by Italian Legislative Decree 231/2001, the following Annexes should be considered an integral part of this Organisation, Management and Control Model:

- **Annex 1:** Corporate structure
- **Annex 2:** Crime risk exposure matrix



IMS TECHNOLOGIES S.p.A.

Via Cav. A. Beretta, 25

24050 Calcinate (BG)