ORGANISATION, MANAGEMENT AND CONTROL MODEL

pursuant to Legislative Decree no. 231 of June 8, 2001

"On Administrative liability of legal entities"

This Kardia S.r.l. ("**Kardia"** or the "**Company**")'s "Organization, Management and Control Model" (the "**Model**") is in line with the provisions of articles 6 and 7 of the Legislative Decree no. 231 of 2001. This version of the Model represents an amendment of the Model that had been put in place since years ago. The Italian version of this updated text was approved by the Board of Directors of October 28, 2021.

The "Model" constitutes the proper management tool in order to prevent crimes subject to the above-mentioned Decree, according to the Company's ethical policies.

Contents

DEFINITIONS

Areas exposed to crime-risk: these are the business activities areas where crimes subject to the Decree can potentially be committed;

Activities exposed to crime-risk or sensitive areas: these are processes whose people in charge in the entity can potentially commit crimes subject to the Decrees while carrying them out;

Decree: this is the Legislative Decree no. 231 of June 8, 2001, as subsequently amended and integrated;

Addresses: these are the parties that shall respect this Model;

Guidelines: this term indicates the "Guidelines for the construction of Organization, Management and Control Models pursuant to Legislative Decree 231/01" drawn up by Confindustria on March 31, 2008;

Model: this indicates the present Organization, Management and Control Model, together with its attachments;

Supervisory Board or SB: this is the Supervisory Board pursuant to article 6 of the Decree, as mentioned in Chapter 11 of this Model;

Crimes: these are the crimes mentioned in the Decree;

Company: this is Kardia S.r.l., with registered office in Milan, via Privata Cormons no. 18;

Senior Managers: parties with power of independent decision-making on behalf of the Company;

Subordinate Persons: parties subjected to Senior Managers.

GENERAL PART

1. THE LEGISLATIVE DECREE NO. 231 OF 2001

"Administrative liability of legal entities, companies and associations, including those without legal status, pursuant to article 11 of Law no. 300 of 29 September".

1.1 INTRODUCTION

The Legislative Decree no. 231 of June 8, 2001 (hereafter the Legislative Decree 231/01 or the Decree), implementing article 11 of Law no. 300 of September 29, 2000, introduced in our laws, besides criminal liability of the single person who materially commits the crime, also the criminal liability of the legal entity that took advantage from the crime itself.

Pursuant to international and European Union duties, the above-mentioned Decree introduced in our laws a direct and independent liability of legal entities, linked to specific crimes: so-called "administrative" liability, but substantially a true criminal liability.

The parties

The parties whose crimes are linked to the entity's liability by the Decree shall be linked to the Company by a dependency relationship. In particular, article 5 of the Decree identifies:

- Representatives, directors or managers of the entity or one of its organizational units with financial and functional autonomy, as well as those who exercise, de facto too, management and control over the entity itself (so-called "senior managers");
- Parties subject to management or supervision of others, and execute the decisions made by senior managers on behalf of the entity (so-called "subordinate persons").

The legislator considered relevant also "de facto" situations, where the power to independently act is not immediately recognizable from the organizational role or from official documents (delegations, powers of attorney and so on).

Article 6 of the Decree states that, if senior managers commit crimes, the Company is not liable if it demonstrates that:

a) The management body has adopted and effectively implemented, before the crime was committed, an organization, management and control model suitable for preventing the crimes subject to the Decree;
b) A "body" of the entity, with autonomous powers of initiative and control has been assigned the task of supervising the functioning of and compliance with the models and their updating;
c) The perpetrators committed the crime by fraudulently eluding the organization and management model;
d) There has been no omitted or insufficient supervision by the control body in letter b).

Article 7 states that the entity is liable if the commission of a crime by a subordinate person was made possible by failure to comply with the managerial and supervisory obligations, that can be accomplished, except for opposite proof by Public Accusation, with an effective adoption of the prevention model.

The interest or the advantage of the Company

In order to consider the Company as liable, the crime should be potentially committed "in the interest or to the advantage of the Company", while the Company is not liable when the crime was committed "in the specific interest of the criminal or third parties".

Law then specified that the liability mentioned in the Decree shall come from an "organizational blame" of the legal entity (ex plurimis, criminal Court of Last Resort Sect. VI, 18-02-2010 - 16-07-2010, no. 27735). This blame is constituted by not adopting an organizational and control model in order to monitor the critical processes of the entity effectively and efficiently and, as a consequence, prevent crimes.

Sanctions

Sanctions imposed by the Decree can be divided into different categories:

- monetary: after assessing the entity as liable, they are computed in percentages related to the severity of the crime and to the economic and financial conditions of the Company with the aim of "insuring the effectiveness of the sanction";
- disqualification: they refer to the prohibition of the activities carried out with the suspension of withdrawal of authorizations, permissions, grants, used to commit the crime; prohibition of negotiating with the Public Administration; exclusion from benefits, financing, aids and withdrawal of the obtained ones; prohibition from advertising goods and services).

The sanctions themselves, where allowed (especially from the most severe and relevant crimes, or when a repetition is possible), can be imposed as a precautionary measure for 6 months maximum.

Sanctions imposed substantially change depending on crimes committed and their severity, measured on the (de)merit of the administrative crimes and on the danger of the entity that did not demonstrate improvement after imposing monetary sanctions on a number of crimes.

- The judgment release, imposed only for judgements involving disqualification sanctions;
- Seizure of the crime price or profit, or its equivalent, that is always imposed when negative judgments are issued.

1.2 THE GUIDELINES

Article 6 of the Decree states that organization and management models can be adopted on rules of conduct issued by associations that represent entities and communicated to the Ministry of Justice. Therefore, in drawing this Model the Company considered the "Guidelines for the construction of Organization, Management and Control Models pursuant to Legislative Decree 231/01" drawn up by Confindustria.

Any variance from the above-mentioned Guidelines has been decided by the Company in order to personalize and better adapt the legislator principles to the Company's specificities.

2. THE ORGANISATION, MANAGEMENT AND CONTROL MODEL

2.1 THE MODEL IMPLEMENTED: STRUCTURE

This Model is composed of a general part and a special part.

The general part, after a short law background, describes the actual organizational structure of Kardia and its organizational chart; the reporting lines, functions and related duties; Areas and Activities exposed to crime-risk; the activities carried out for employees' training and communications; the disciplinary system guidelines; the criteria for naming the Supervisory Board and the crimes subject to the Decree.

The Special Part, divided into various sub-parts, describes the various crimes, identifies the business areas particularly exposed to the crime-risk and the procedures adopted in order to prevent or at least reduce the possibility of crimes.

The identification of principles and procedures apt to prevent or reduce the potential of identified crimes is particularly important.

In the special sub-parts will be examined the following crimes:

i) Crimes against the Public Administration, including the ones introduced by Law no. 69 of 2015 (Special Part "A");
ii) All categories of corruption as integrated by Law no. 69 of 2015 (Special Part "A bis");
iii) So-called corporate crimes, including the new ones introduced by Law 69 of 2015 (Special Part "B");
iv) Manslaughter and culpable serious or very serious bodily harm, committed in violation of safety regulations and occupational hygiene and health (Special Part "C");
v) Receiving, laundering and using money, goods or benefits of illegal origin (Special Part "D");
vi) So-called cybercrimes (Special Part "E");
vii) Crimes against judiciary (Special Part "F");
viii) Tax crimes (Special Part "G").

After completing the risk assessment, Kardia did not deem relevant for this Model the following crimes: organized crime, crimes against industry and commerce, crimes of terrorism or subversion of the democratic order, mutilation of female genitalia, crimes against personality, market abuses, crimes concerning breach of copyright, environmental crimes, false statements to the Privacy Guarantor – for which the entities are held administratively liable – since no risk of committing these crimes was identified, considering the specific activities carried out by the Company.

3. KARDIA S.R.L.

3.1 KARDIA S.R.L. AT A GLANCE

Kardia operates at national level in the medical devices business since 1995, with a managerial staff that has a consolidated multi-year experience gained at leading multinational companies.

Initially operating as an importer and distributor of medical devices for Interventional Cardiology, Kardia then broadened its scope to other industries, such as Interventional Radiology, Vascular Surgery and Neuroradiology.

Kardia offers the following services:

- Sale and specialist support for high technology medical devices;
- Sale and specialist and technical support for both consolidated and innovative medical technologies;
- Global management: Kardia was the first company to realize and manage a hemodynamics operating room with this formula.

Kardia is constantly evolving in order to be aligned with the new market needs.

The precise respect of contracts and customer satisfaction are the main Kardia's references.

3.2 THE KARDIA S.R.L. ORGANIZATION

Kardia S.r.l. was formed on September 22, 1993, with initial expiration date on December 31, 2050, as in the deed of September 22, 1993, drawn by notary Mr. Maurizio Olivares.

Subsequently, as in the deed drawn by notary Mr. Oreste Cirillo from Parabiago (MI), repertoire no. 32.840 – collection no. 23.324 dated December 2, 2019, the Quotaholders amended the Company's Bylaws to article 16 of Law no. 2 of January 28, 2009, as well as to new article 2477 of the Civil Code.

The Company's registered office is located in Milan, Via Privata Cormons n. 18.

The Company is managed by a Board of Directors composed of:

KAZUAKI INUKAI	PRESIDENT
ROBERTO RIVA	MANAGING DIRECTOR
DAVIDE LONGONI	MANAGING DIRECTOR
ELENA GIUBBINI FERRONI	DIRECTOR
SHIGENOBU INAGUMA	DIRECTOR

Both the Chief Executive Officers and the President are in charge of the Company's management, with equal powers.

At the moment, the Company structure is as follows:

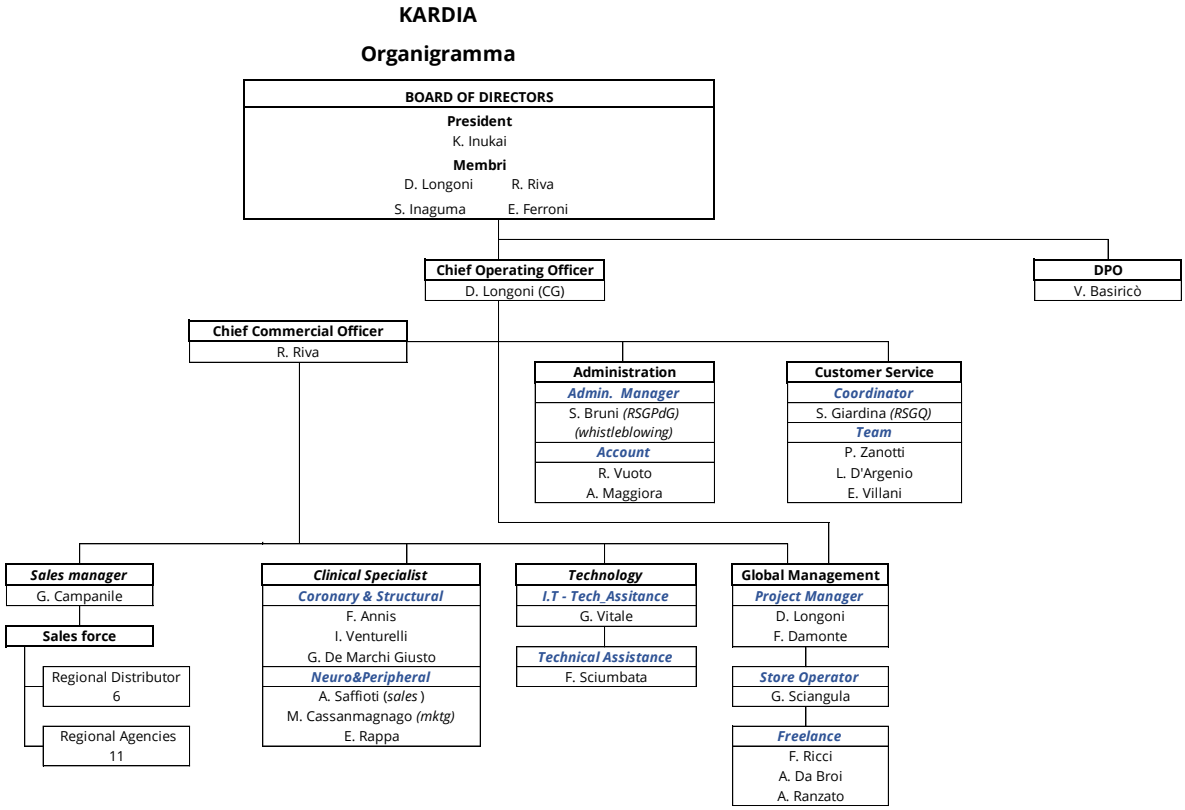
QUOTAHOLDERS	%	NOMINAL VALUE
ASAHI INTECC CO. Ltd	90.00%	90,000.00
DAVIDE LONGONI	10.00%	10,000.00
Total	**100,00%**	**100,000.00**

As of December 4, 2024, there are 19 employees in total, as in the following organizational chart.

Commerce National Collective Bargaining Agreement (CCNL) applies to employees.

Please note that Kardia carries out its activities with the support of internal biomedical engineers, commercial personnel and technicians for support to final clients, hired on their professional skills, as required by the business.

The final aim of the Company, indeed, is the supply of high-quality goods and services, that can meet Interventional Cardiology, Radiology and Electrophysiology health workers' needs.



4. CORPORATE GOVERNANCE

4.1 BOARD OF DIRECTORS

The Company is managed by a Board of Directors, whose composition is described in paragraph 3.2 of this Model.

Directors have full powers related to the ordinary management of the Company.

As regards extraordinary acts, the Directors shall be authorized in advance by an ordinary Shareholders' Meeting decision.

The Board of Directors can name General Directors, Managers and attorneys for specific acts or acts' categories.

4.2 THE INTERNAL CONTROL SYSTEM

The internal control system consists of the rules, procedures and organizational structures that allow the Company to be managed correctly and coherently with the goals set, through the identification, measurement, management and monitoring of the main risks. Goals can be divided into the following categories:

1) Operating goals: they refer to the economic performance of the Company, its financial balance and the protection and development of its assets, in order to protect the Net Equity in the medium and long term;
2) Information goals: they refer to the reliability of the informative system mainly related to the draft and release of reliable economic and financial documents such as annual financial statements, mid-year financial statements, financial ratios, other management indicators and so on;
3) Compliance goals: they grant that parties with powers of attorney and decision-making act in compliance with laws and regulations in force;
4) Legitimation goals: they refer to the Company ability to establish a positive reputation at the main stakeholders.

5. ORGANIZATIONAL PROCESSES

The Company implemented an organization model that formalizes responsibilities, reporting lines and duties.

The main organizational and operating responsibilities are formalized in the Integrated Quality and Environmental Management System Manual, drafted in 2003 pursuant to Rule UNI EN ISO 9001:2015, updated on January 4, 2010, and integrated pursuant to Rule UNI EN ISO 14001:2015, on April 30, 2018.

The Quality System is composed of the Quality Manual and the Procedures Manual and is under direct responsibility of Ms. Giardina Sonia, Head of the RSGQ Quality Management System Area.

The Integrated Quality and Environmental Management System is composed of the following:

1) Introduction;
2) Aim and scope of application;

3) Normative requirements;
4) Terms and definitions;
5) Organization environment;
6) Leadership;
7) Support;
8) Operating activities;
9) Performance evaluation;
10) Areas of improvement.

The Procedures Manual is composed of the following processes management:

1) Catalog Sales;
2) Global Management services Sale;
3) Global Management;
4) Direct technical support;
5) Global Management technical support;
6) Installation and testing;
7) Claims;
8) Purchases;
9) Employees hiring and training;
10) Global Management employees training;
11) Inventories.

For each of the above-mentioned processes a standardized procedure exists in the Procedures Manual, as follows:

1) Cod. P 4.02 001: Documents
2) Cod. P 6.02 001: Hiring and training
3) Cod. P 6.02 002: Global Management hiring and training
4) Cod. P 7.04 001: Purchases
5) Cod. P 7.04 002: Import and distribution
6) Cod. P 7.05 001: Catalog Sales
7) Cod. P 7.05 002: Inventories
8) Cod. P 7.05 003: Direct technical support
9) Cod. P 7.05 004: Global Management technical support
10) Cod. P 7.05 005: Installation and testing
11) Cod. P 7.06 006: Global Management
12) Cod. P 7.05 007: Global Management process
13) Cod. P 7.05 008: Recalls process
14) Cod. P 7.05 009: Tenders process
15) Cod. P 8.02 001: Internal inspections
16) Cod. P 8.02 002: Indicators
17) Cod. P 8.03 001: Non-compliance
18) Cod. P 8.02 003: Customer satisfaction
19) Cod. P. 8.03 002: Customer claims
20) Cod. P. 8.05 001: Corrective and preventive actions

The Company’s Organizational guidelines with related functions and duties refer to the following:

- President and Chief Executive Officers;
- RSGQ Quality Management System Director;
- Technical Support (RAF) Director;
- Commercial Area Director;
- Administration, Finance, Purchases and Human Resources.

The Company documents' management is generally ruled by the Procedures Manual.

Standardizing, approving, issuing, distributing, and archiving Company documents' processes are summarized in procedure P 4.02 001 of the Procedures Manual. This procedure includes also modifying and updating Company documents' rules.

Further procedures relevant for Company's planning are included in the results of the inspection and in the indicators' management in order to continuously improve internal Quality.

6. AREAS AND ACTIVITIES POTENTIALLY EXPOSED TO CRIME-RISK: SCOPE OF INVESTIGATION AND RESULTS OF THE MAPPING PROCESS

According to article 6, paragraph 3, of the Decree (and pursuant to the above-mentioned Guidelines), the General Part of the Model shall have three main purposes:

I) Identify the Business Areas potentially exposed to crime-risk: Risks identification

Article 6, paragraph 2, letter a) of the Decree requires the Model to identify risks as a first step: therefore, it is necessary to carefully analyze the whole activities carried out by Kardia and identify the operating of decision-making phases exposed to crime-risk.

Given the progressive expansion of the relevant crimes to the Decree by law, and the possible changes to the Kardia structure and activities performed, risks identification can never be considered as final and unchangeable but shall be monitored and updated continuously.

Therefore, Kardia and the Supervisory Board will integrate the risks identified, whenever new laws or Kardia changes in organization and activities methods would require it.

II) Implementation of a preventive controls system

Pursuant to article 6, paragraph 2, letter b) of the Decree, after identifying risks, specific protocols should be enacted in order to plan the implementation of the Company's decisions in the areas exposed to crime-risks as identified.

For this specific purpose, in the Special Part of this Model, specific measures and procedure to prevent or massively reduce the crime-risks are detailed.

Moreover, together with these preventive procedures, the Supervisory Board has the explicit power/obligation of carrying out detective inspections on single Company operations or behaviors.

As the risks identification process, also procedures cannot be considered as final: their effectiveness and completeness shall be continuously evaluated by the Supervisory Board, that has also the specific duty of suggesting the Board of Directors areas of improvements, integrations and modifications needed.

III) Supervisory Board identification

The third purpose of the General Part is the identification of the Supervisory Board, with the following duties according to the Decree:

- Continuous control of the respect to the Model and to the specific enacting obligations and procedures herein stated, by all the Addressees;
- Continuous evaluation of the risks identified and of the procedures described in point I) and II);
- Suggestion to the Board of Directors of all the necessary modifications.

In this context, the areas and activities identified as exposed to crime-risk after analyzing business operations are the following:

a) INBOUND LOGISTICS
   - Receiving, storage and distribution of products
   - Inventory control
   - Carriers planning
   - Suppliers returns management

b) OUTGOING LOGISTICS
   - Gathering, storage and warehousing of the products
   - Delivery carriers' management
   - Orders processing
   - Delivery planning

c) MARKETING AND SALES
   - Offer definition
   - Product characteristics definition
   - Price definition
   - Sale channels choice
   - Customers management

d) PURCHASES
   - Suppliers' selection and characteristics
   - Tenders' management
   - Suppliers' orders management
   - Goods inspections
   - Contracts management
   - Suppliers' evaluation

e) HUMAN RESOURCES
   - Human Resources management
   - Selection and hiring of employees
   - Role definition
   - Employees' training
   - Administrative and accounting aspects related to payroll

f) FINANCE MANAGEMENT
   - Cash flow budget
   - Funding sources

- Investments return
- Collection
- Respect of deadlines
- Securities protection
- Securities management
- Appropriate accounting entries

g) INFRASTRUCTURES MANAGEMENT
- Equipment maintenance
- Machinery and premises maintenances

h) IT SYSTEM
- Data gathering - management – processing

i) TAX CRIMES
- Goods suppliers' selection and management and purchases management
- Sale activities management
- Management of accounting, tax and tax payment obligations
- Accounting documentation storage
- Inventory management
- Employees' management
- Intercompany transactions management

7. SENSITIVE PROCESSES: GENERAL CONTROL PRINCIPLES

The identification of business areas and activities "exposed to crime-risk" allowed the Company to define some sensitive processes, during whose phases, sub-phases or activities crimes relevant to the Decree can happen.

Given the above, the Board of Directors enhanced the importance of the procedures that rule the sensitive business processes, so that they comply with the following general principles:

- Segregation of duties. Duties' allocation and related authorization grants shall aim to keep separated all authorization, execution and control functions or to avoid the concentration on one single party of more "primary" phases of the same business Activity;
- Formalization of signatory and authorization powers. The allocation of these powers shall be coherent to duties allocated and formalized through a delegation and procedures system identifying the operating scope and related responsibilities;
- Control formalization. The sensitive business processes shall be formalized (through documents or, preferably, IT systems) and provide for some specific controls;
- Process coding. The sensitive business processes are standardized as much as possible, that means ruled according to specific procedures that aim to define their timing, modes and, if this is possible and/or needed, the objective criteria basing the decision-making processes and anomaly indicators;
- Secrecy protection. IT procedures enacted in sensitive business processes are protected from both internal and external non-authorized accesses through appropriate physical or IT measures.

The Board of Directors and the Supervisory Board are in charge of verify the effectiveness of the procedures.

8. EMPLOYEES' TRAINING AND COMMUNICATION

Kardia knows the relevance of training and communication, therefore is acts are aimed to grant the employees' knowledge of the Decree and the related obligations and of the Model.

The activities aimed at training, awareness raising and communication involve all the employees, including senior managers.

Communication and training activities are planned and implemented during both hiring or at the beginning of the work relationship and in case of changes in employees' function, in the Model or of any other circumstance requiring them in order to grant the correct implementation of the Decree.

9. COMMUNICATION TO THIRD PARTIES

Other Addresses, in particular suppliers and consultants, are informed by the business functions interfacing with them on the specific policies and procedures enacted by Kardia pursuant to the Model and on the consequences of misbehaviors according to the Model or to the law in place in the scope of the contracts.

If possible, this communication is included in specific clauses of the contracts themselves.

10. THE DISCIPLINARY SYSTEM

10.1 INTRODUCTION

In order to grant the effectiveness of this Organization, Management and Control Model, the Company implemented this Disciplinary System, that aims at sanctioning any breach of the rules contained in the Model and related Ethics Code by employees, third party contributors and partners, besides Directors and members of the Supervisory Board.

As regards Company's employees, this Disciplinary System integrates the disciplinary system enacted pursuant to current law, in particular articles 2103, 2106, 2118 and 2119 of the Civil Code, article 7 of the Statute of Workers (Law no. 300 of May 30, 1970), laws on individual layoffs (Law no. 604 of July 15, 1966) and Collective Bargaining Agreements applicable.

As far as concerns the topics not included in this Disciplinary System, laws and rules in act, Collective Bargaining Agreements and any Company by-law are applicable.

The implementation of the Disciplinary System is independent from any criminal proceeding.

10.2 CONDUCTS SUBJECT TO SANCTIONS: MAIN CATEGORIES

This Disciplinary System fines the actions and/or behaviors in violation of the Organization Model and related Ethics Code, and any mis-respect of suggestions and prescription of the Supervisory Board.

Relevant violations can be divided into four main categories, more and more severe:

a) Violations not related to sensitive areas;
b) Violations related to sensitive areas;
c) Violations that integrate only the fact (objective element) of a crime for which the administrative liability of entities is provided;
d) Violations aimed at committing crimes relevant to the Decree or that can attribute the administrative liability to the entities.

For example, some of the sanctionable behaviors are the following:

a) Mis-respect of the procedures described or recalled in the Model;
b) Mis-respect of the information duties included in the control system;
c) Missing or false documentation of operations according to the transparency principle;
d) Missing controls by related in-charge parties;
e) Non-justified mis-respect of training obligations;
f) Missing control on the Ethics Code distribution by in-charge parties;
g) Any elusive behavior of the control systems;
h) Behaviors exposing the Company to be fined pursuant to the Decree.

10.3 GENERAL PRINCIPLES OF SANCTIONS' COMMENSURATION

In choosing and commensurating sanctions, the following criteria shall be used:

a) Responsibility and autonomy of the party committing the violation;
b) Intention of the behavior or degree of negligence, imprudence and inexperience;
c) Other sanctions in the previous twenty-four months;
d) Severity of the misbehavior, considering the actual risk borne by the Company pursuant to the Decree.

10.4 MEASURES AGAINST EMPLOYEES

Sanctions which may be imposed against employees are the following:

- Verbal reprimand;
- Written reprimand;
- Fine with an upper limit of two hours of the minimum pay according to the contract
- Disciplinary dismissal.

The Company cannot enact any disciplinary sanction against the employee without preventively disputing the charge and allowing him to defend himself. Except from the verbal reprimand, the sanction shall be communicated in writing, explicitly indicating the facts.

Disciplinary sanctions cannot be enacted before five days from formal notification of the violation, while the employee can submit his justifications, that are considered accepted in case the sanction is not enacted after six days from submission.

Justifications can be submitted by the employee also verbally, with the possibility to be assisted by a RSA member: in this case, the Company will attend to the verbalization for archival purposes.

The sanction shall be motivated and communicated in writing.

The employee can challenge all disciplinary sanctions different from dismissal before the Trade Unions, according to relevant contract rules. Dismissal, with or without notice, can be challenged according to the relevant rules.

As regards crimes in violation of safety regulations and occupational hygiene and health, sanctions can be imposed to employees breaching article 20 of the Legislative Decree no. 81 of 2008, that is the Unique Text of Occupational Hygiene and Health, also in line with the Ethics Code.

Any sanction against employees pursuant to Legislative Decree 81 of 2008 (and subsequent enacting decrees) do not exclude disciplinary sanctions.

Verbal and written reprimands, fines and suspensions

Verbal and written reprimands, fines and suspensions can be enacted against employees who commit:

a) Violations of the Model or the Ethics Code in non-sensitive areas;
b) Minor violations in sensitive areas not included in violations of point 10.2, letters c) e d);
c) Unjustified non-fulfilment of training obligations;
d) Any violation of obligations stated in the Model and Ethics Code biasing discipline, morale, hygiene and safety of the Company.

These sanctions are enacted proportionally in relation to the violations arisen.

In particular, verbal reprimands are enacted for violations not related to the specific intention of failing in their duties.

Written reprimands are enacted for repeated violations, also minor, when stricter sanctions shall be forewarned.

When verbal and written reprimands did not have the wished result, or in case of more sever violations, the following sanctions can be enacted:

a) A fine, with a maximum amount equal to two hours quantified according to the contractual minimum wage;
b) In the worst cases, or in case of repeated violation, the suspension from duty for up to three days.

Disciplinary dismissal

Disciplinary dismissal is enacted in the following cases:

1. Insubordination and mis-respect of higher management orders;
2. Subtraction, destruction, forgery of documents pursuant to the Decree;
3. Repeated violations that require written reprimands, fines and suspensions, after two suspensions already enacted in the previous two years;
4. Res judicata conviction judgment for crimes where administrative liability of entities is involved.

10.5 MEASURES AGAINST THE BOARD OF DIRECTORS AND SUPERVISORY BOARD'S MEMBERS

When Directors or Supervisory Board's members violate the Model of the Ethics Code, the following sanctions can be enacted:

a) Written reprimand;
b) Warning of complete compliance to the Model and the Ethics Code;
c) Reduction in fees up to 50%;
d) Revocation from the assignment.

10.6 MEASURES AGAINST THIRD PARTIES

Any violation against the Model or the Ethics Code by third parties can lead to the contract termination, through specific clauses, except for the right to the refund for any damage incurred.

The Supervisory Board is in charge for the draft and update of these clauses and for inserting them in agreements and contracts.

11 SUPERVISORY BOARD

11.1 NOMINATION AND TERM'S LENGTH

In order to properly implement the Model, a specific body with independent initiative and inspection powers should monitor its functioning and its respect and be in charge of its update.

Therefore, Kardia's Board of Directors shall nominate a Supervisory Board.

The term of this body will last three years. Its member can be re-elected, can be revoked only with just cause and are terminated when the independence requirement as detailed below fails or when they miss without justification the Supervisory Board's meetings.

11.2 DUTIES

The Supervisory Board is in charge with the following duties:

a. Monitor the effective implementation of the Model through a coherence verification between the actual behaviors in the Company and the cases included in the Model and through the monitoring of the areas exposed to crime-risk identified in chapter 6 above. In order to comply with these duties, the Supervisory Board can implement control activities at very business level, acquiring the proper instruments to timely report Model's anomalies and misfunctioning, through control procedures. Every operation deemed exposed to crime-risk shall be reported to the Board by the internal in-charges in order to enact, in any moment, all the controls to describe the characteristics and purposes of the operation itself and identify the parties who have authorized, accounted for and controlled the operation.
b. Enact the control procedures considering the business operations needs and the fact that the primary in-charges of business activities are the Head of the functions according to the Company organizational chart;
c. Periodically monitor the adequacy of the Model, that is its ability to prevent the behaviors it aims to exclude and contrast, its strength and functioning through time, through a constant monitoring of the control system, of protocols and in general of governance;
d. Update the Model when enacted controls make it necessary.

In particular, the Supervisory Board shall:

- Ascertain the updating of the Model, according to law, internal organization and business activities changes;
- Support the draft and integration of the internal by-laws (deontological codes, operating instructions, protocols, control procedures, and so on) apt to risk prevention;
- Enhance activities aimed at raising awareness among Kardia's employees of the Model, by giving proper instructions and clarifications and organizing training courses;
- Coordinate with other business functions for a better activities' control and for all concerning the concrete implementation of the Model;
- Organize extraordinary controls and/or specific verification, with the power to access directly to the relevant documents in case of detected misfunctioning of the Model or committed crimes relevant for the prevention activities.

11.3 COMPOSITION

The Decree does not explicitly rule the composition of the Supervisory Board, shortly defining it as an "entity body with independent initiative and control powers".

According to article 6, paragraph 4-bis of the Decree, also corporates' Boards of Statutory Auditors can carry out the activities assigned to the Supervisory Board.

The Legislator allows the single entities to freely decide on the Supervisory Board's composition, coherently to the specific entity environment.

Doctrine and practice elaborate different options regarding structure and composition of the Supervisory Board, also considering the entities' dimensions, Corporate Governance rules, and the need for balance between costs and benefits.

At the moment, the Supervisory Board is composed of Ms. Simona Bruni e Mr. Roberto Vagaggini (external member), the latter named by the Board of Directors of October 25, 2024.

11.4 PROFESSIONAL REQUIREMENTS

The respect of this requirements shall be granted by the personal experience of the single Board's members, with technical and specific skills that grant the timely and correct performance of functions established by law.

In particular, the above-mentioned skills are the following:

- Criminal law skills: ability to correctly interpret laws with specific skills on the analysis of the crime cases that could emerge during the business activities and on the possible violations;
- Organizational skills: specific skills on analyzing business organizational processes and procedures; general law principles in compliance and related controls;
- Analysis and control skills: internal control systems experience in business environment;
- Cash flows control skills.

11.5 INDEPENDECE REQUIREMENTS

Although the Legislator does not explicitly require it, the independence is necessary in order to not be subject to any other Company body. Actually, the autonomy of the Supervisory Board would be worthless if its members were personally dependent from Company's top management.

This requirement is granted by the fact that the Kardia Supervisory Board members are not dependent from any other Kardia employees.

11.6 EFFECTIVENESS AND CONTINUITY OF ACTIONS

This is required to grant the Supervisory Board full knowledge of business activities, operating processes in place and changes that could happen during the business cycle.

The Supervisory Board shall meet at least every two months to carry out proper control activities.

One of the members missing without justification two meetings in the same fiscal year, can be considered just cause of revocation from the assignment.

11.7 REPORTING LINES

The Supervisory Board, except for specific needs, shall draft at least annually a report on the Model, including:

- Its observations on the Model effectiveness, with the related suggestions for integrations and updates deemed as necessary;
- Any recommendation to update the Model following law or business and organization changes;
- A summary of the activities carried out and of any correction/preventive action to enact.

11.8 MANDATORY COMMUNICATIONS TO THE SUPERVISORY BOARD

Legislative Decree no. 24 of 2023, "implementation of UE Directive no. 1937 of 2019 of the European Parliament and of the Council dated October 23rd, 2019 about the protection of people reporting Union laws' violations", as well as Law no. 179 of 2019 introduced the so-called whistleblowing law.

Article 6, paragraph 2-bis of the Legislative Decree no. 231 of 2001, as amended by the above-mentioned Decree, states that the Organization, Management and Control Model implemented shall include some internal reporting channels pursuant to Legislative Decree no. 24 of 2023, as well as some information obligations to the Supervisory Board.

Following the European Law, Legislative Decree no. 24 of 2023 aims at improving legal protection of people reporting violations of national and European laws, harming public and private entities' interests and/or integrity, and that emerged during their job. In general, the Decree aims at promoting law and compliance culture in the workplace, through the harmonization of whistleblowing law with European institutions and international best practices.

Therefore, Kardia implemented some internal reporting channels able to grant, also through encryption, the privacy of whistleblowers' identity, of the person involved or mentioned, as well as of the report itself and the related documentation.

Reports can be submitted in writing, also through IT means, or verbally (through phone, vocal messages or, upon whistleblowers' request, through a direct personal meeting by a reasonable term).

Heads of business functions exposed to crime-risk are in charge for these obligations, that will be enacted in case of anomalies emerged in their functions in order to facilitate the monitoring activities.

Pursuant to this aim and to the new enacted law, first of all the Company created a mail address (in particular odv@kardia.it) to allow senior managers and other employees to report specific Model violations based on precise evidence. Moreover, they implemented a specific external platform accessible from the Company website (Whistleblowing - Kardia EN), so that all the interested parties, both internal and external, can submit violations of national and international laws harming public or Company's interests that emerged during their duties, unless the violation is not tied to a personal interest exclusively related to their personal relationship with the Company.

Failure in meeting the reporting obligations shall be considered as a specific disciplinary violation.

11.9 FINANCIAL AUTONOMY

The Board of Directors annually approves the expenses budget.

The budget shall be higher enough to cover the proper Model monitoring and update activities, including consulting expenses, if needed.

The Board of Directors shall authorize and justify the expenses higher than the budget and the non-recurring ones, in writing.

11.10 SUPERVISORY BOARD'S BYLAWS

The Supervisory Board implemented a bylaws ruling the functioning of the body (Attachment no. 1), updated on January 8, 2019.

12. LIST OF CRIMES SUBJECT TO LEGISLATIVE DECREE NO. 231 OF 2001 AND SUBSEQUENT AMENDMENTS

The initial Decree identified as crimes involving the administrative liability of the entities only a short list of crimes against the Public Administration or fraud (articles 24 and 25).

Subsequent amendments widened the list of relevant crimes involving the administrative liability of entities, to the following cases:

- "*Forgery of money, public credit documents and stamps"* (article 25-*bis*);
- So-called corporate crimes pursuant to articles 2621 and subsequent of the Civil Code, as updated by Legislative Decree no. 61 of November 23, 2002 (article 25-*ter*);
- Crimes of terrorism or subversion of the democratic order, besides mutilation of female genitalia (article 25-*quater*);
- Crimes against individual personality (article 25-*quinquies*);
- Crimes of insider trading and market manipulation (article 25-*sexies*);
- "*Failure to disclose a conflict of interest*" (article 2629-bis Civil Code) (as updated by article 25-*ter*);
- Crimes of manslaughter and culpable serious or very serious bodily harm, committed in violation of safety regulations and occupational hygiene and health (article 25-*septies*);
- Crimes of receiving, laundering, and using money, goods or benefits of illegal origin (article 25–*octies*);
- So-called cybercrimes (article 24-*bis*);
- Organized crime (article 24-*ter*);

- Crimes against industry and commerce (article 25 *bis*);
- Crimes concerning breach of copyright (article 25 *novies*);
- Crimes against judiciary (article 25 *decies*);
- Environmental crimes (article 25 *undecies*);
- Employment of third-country nationals staying illegally (article 25 *duodecies*).

Afterwards, article 9 of the recent Law Decree no. 93 of 2013 added the crimes included in article 24-bis, paragraph 1, of the Decree: cyber fraud against digital identity; crimes included in article 55, paragraph 9 of the Legislative Decree no. 231 of November 21, 2007, i.e., crimes of improper use, forgery, modification of credit or payment cards, or any other document allowing withdrawals of money or purchase of goods and services, their possession, transfer or purchase; crimes included in Part III, Chapter III, Paragraph II of the Legislative Decree no. 196 of June 30, 2003 i.e., crimes against personal data (improper data processing, false statements and reports to the Guarantor). Therefore, these crimes are now fully included in the list of cyber and data processing crimes involving the administrative liability of entities.

Law no. 68 of 2015 introduced among the relevant crimes the following environmental crimes: environmental pollution, environmental disaster, unintentional crimes against the environment, abandonment of highly radioactive material.

Law no. 69 of 2015 amended the crimes of false corporate statements and introduced the crime of false corporate statements in listed companies and incitement to corruption between private individuals.

In 2015 the crime of self-laundering was introduced.

Finally, Law no. 161 of 2017 introduced paragraphs 1-bis, 1-ter and 1-quater of article 25-duodecies of the Decree, updating the crimes of employment of third-country nationals staying illegally.

Legislative Decree no. 124 of October 26, 2019, converted with modifications into Law no. 157 of December 19, 2019, introduced new article 25-quinquiesdecies, that states the entities' liability pursuant to the Decree when tax crimes are committed.

Finally, the Legislative Decree no. 75 of July 14, 2020, widened the tax crimes relevant to the Decree.

The last amendments and add-ins were introduced in 2023 and 2024.

In particular, Law Decree no. 105 of 2023, together with the conversion Law no. 137 of 2023, introduced new relevant crimes, such as Disturb of tenders (art. 353 penal code), Disturb of the process of choosing the supplier (art. 353-bis p.c.), Waste abandonment (art. 255 Legislative Decree no. 152 of 2006), Environmental pollution (art. 452-bis p.c.), Environmental disaster (art. 452-quarter p.c.), Fraud value transfer (art. 512-bis p.c.).

Law no. 93 of 2023 introduced some measures to prevent and punish the unlawful distribution of contents protected by copyright through networks of electronic communications (Official Gazette no. 171 of 2023), as well as "Crimes related to copyright violation".

Decree dated February 3rd, 2023 introduced crimes such as "Use of third-country citizen with staying irregularly". Also, art. 25-ter of Legislative Decree no. 231 of 2001, related to company crimes, and art. 25-octies, related to fraud use of values, were modified.

Finally, Law no. 114 of 2024 further modified the relevant crimes. In particular, it:

- revoked the crime of abuse of authority pursuant to art. 323 p.c. (punishing the public official or the person in charge of public service that, during their activities, violated specific conduct laws, intentionally getting for themselves of for third parties an unfair monetary advantage or causing an unfair damage);
- amended the crime of illicit influences transactions pursuant to art. 346-bis p.c.;
- introduced the crime of unlawful use of money or movable things pursuant to art. 314-bis p.c.

Such amendments do not substantially change procedures already in place (however revised and updated) related to crimes concerning transactions with Public Administration, as they were already aimed at preventing any risk and actions violating Kardia's values.

Not all the new crimes introduced in the responsibilities of Legislative Decree no. 231 of 2001 are relevant to Kardia, therefore, referring specifically to the relevant cases, the Board of Directors of Kardia, also upon request by the Supervisory Board, will have to issue proper resolutions to update the Model with new *Special Parts* related to new crimes involving the administrative liability of entities.

SPECIAL PART

1. SPECIAL PART "A": RELATIONSHIPS WITH PUBLIC ADMINISTRATIONS

1.1 CATEGORIES OF CRIMES IN RELATIONSHIPS WITH PUBLIC ADMINISTRATIONS (ARTICLES 24 AND 25 OF THE DECREE)

With regards to the first Special Part, here follows a short description of crimes included in articles 24 and 25 of the Decree:

Embezzlement against the State or the European Union (article 316-bis Criminal Code)
This crime applies when loans or grants from the State or the European Union are not used for the intended purpose (the crime is the stealing, even partial, of the amount without carrying out the planned activity).

Given that the crime is considered as consummated just when executed, the crime is relevant also relating to past amounts received and only subsequently used for improper purposes.

Misappropriation of funds from the State or the European Union (article 316-ter Criminal Code)
This crime applies when loans, grants or other similar benefits are granted by the State or the European Union to parties with no actual right to obtain them, thanks to false statements or documents or with missing information.

In this case, differently to the previous crime (article 316-bis), the purpose for which the amounts are used is not relevant, because the crime is committed when obtaining the grant.

Finally, please note that this crime applies only when the crime of fraud against the State, as detailed below, is not applicable.

Illicit use of money or movable goods (article 314-bis Criminal Code)
Such law punishes, in cases excluded from art. 314, with imprisonment between six months and three years, "the public official or person in charge of public service who have some money or other movable goods because of their duties and use them differently from the specific use stated by law, intentionally obtaining an unfair monetary advantage for themselves or third parties or causing an unfair damage to others.

This new article introduced a specific crime of embezzlement through distraction, merging aspects of embezzlement (article 314) and of the abolished abuse of authority (article 323). On the one hand, it is similar to embezzlement in the (legal) action assumptions: the criminal, public official or person in charge of the public service, already possess money or other movable goods thanks to their duty, and only subsequently they will use such goods unlawfully. On the other hand, it is similar to abuse of authority, first on the objective aspect because:

a) the action (illicit use) shall go against specific laws leaving no margins of choice, as in article 323;
b) the outcome of the crime is the same: an unfair monetary advantage for themselves of third parties, or an unfair damage to third parties.

Secondly, on the subjective aspect:

c) intentional malice is required.

The crime is characterized by the different use of money or other movable goods belonging to others: such crimes that in the past were in the scope of embezzlement cannot be classified otherwise, therefore are still punished according to article 314 of the Criminal Code. Put differently, where goods are permanently stolen from pursuing public interests to have proper of others' benefits, article 314 still is in place, and therefore also sanctions are in line.

The new law amended the punishment of embezzlement that in the past were regulated by abuse of authority, that is the use of goods without permanently stealing it, so that the owner entity does not suffer from any monetary damage, as well as use of public money against accounting principles, aiming at pursuing, together with illicit private interests, also objective public interests.

As per current art. 314-bis, the object of the "different use", that is embezzlement, is money and movable goods only. That means that embezzlement of properties, in the scope of abuse of authority in the past, are not relevant anymore.

The relevant issue to Kardia is any aid from employees to the criminal public official.

Illicit influences' transactions (art. 346-bis Criminal Code)

The above-mentioned law punishes actions usually happening before the crimes of corruption for performing public duties (art. 318), proper corruption (art. 319), corruption in judicial acts (art. 319-ter) and international corruption (art. 322-bis).

Before it was amended, the law punished the case when the criminal claimed credit from a public official or public employee, after an amendment in 2019 abolished arti. 346 of the Criminal Code.

Law no. 114 of 2024 strongly updated the crime underlying give and/or promise, since new art. 346-bis, at the first paragraph, states "intentionally use of existing relationships with the public official or person in charge of public services or another person as per art. 322-bis". Therefore, "relationships between the criminal and the public official shall be actually used and existing (not claimed only)". Hence, such update "partially abolished the crimes underlying, relating to claimed only relationships with public officials and person in charge of public services". In case the criminal claimed such relationships, he could be punished for fraud, if all the elements are present.

Moreover, intentional malice is now requested when using relationships.

The crime involves giving or promising money or any other monetary goods.

Paragraph 2 of article 346-bis, as amended by Law no. 114 of 2024, defines illicit mediation as a mediation to convince public officials or people in charge of public service or one of another person as per art. 322-bis to act against their duties, that could cause an unfair benefit.

Disturbed tenders (article 353 Criminal Code)

This article aims to protect both Public Administrations and private parties from various crimes damaging the free market during tenders organized by public entities, as well as private parties participating such tenders.

The main goal is ensuring that tenders where Public Administration are involved are performed freely and regularly, allowing a correct competition between potential suppliers, so that the outcomes are

the fairest and most convenient for the public interests. Therefore, to be relevant, crimes should not happen only when tenders happen, but in any moment of the procedures, as well as before or after.

Criminal actions are relevant if implemented on behalf of any of the Public Administration involved in the tender or private parties.

Disturbed choice of supplier (article 353-bis Criminal Code)
This "new" crime refers to who "disturbs the administrative procedure aimed at drafting the tenders' contents or any other similar act, in order to influence the Public Administration's choice of the supplier".

Therefore, this law is related to the phase prior to the announcement of the tender, specifically its approval, in order to discourage who try, with the help of the Public Administration, to draft so-called "picture-tenders", that is tenders with requirements that are so specific to tighten the number of potential suppliers.

The necessary objective prerequisite is the start of an administrative process aimed at drafting the tender's content or any similar act. Such crime can be related to any act starting the process of choosing the supplier, since "similar act" can include contract resolutions when no tender is required.

Fraud in public supplies (article 356 Criminal Code)
This law protects the good and regular functioning of Public Administrations against suppliers' frauds in providing goods and services necessary for their public duties.

Such crime involves a fraud non-compliance while carrying out the supply overall. The law requires contractual bad faith, that is using malicious or deceptive expedient to show that the supply is compliant with the contact in place.

Extortion (article 317 Criminal Code)
This crime applies when a public official or a public service officer oblige third parties to obtain undue money or other benefits, by abusing his position.

This crime applies in residual cases with respect to the other crimes considered in the Decree; in particular, this crime could apply when an entity's employee or agent take part in this the public officer's crime (if the entity can take advantage from this crime).

Corruption for an official act or against official duties (articles 318-319 Criminal Code)
This crime applies when a public official receives, for himself or for third parties, money or other benefits to do, miss or delay some acts in his office (with consequent benefits for the paying party).

The public official illicit can be both a due act (for example to speed up the completion of an act among his duties), and an illicit act (for example a public official accepting money to grant a tender).

This crime is different from extortion because in this case there is an agreement between the corrupted public official and the corruptor, while in the previous case the private third party suffers the criminal conduct by the public official.

Corruption in judicial acts (article 319-ter Criminal Code)
This crime applies when the Company participates a process and corrupts a public official (not only the judge, but also another clerk or a witness) to get a benefit during the process itself.

Incitement to corruption (art. 322 Criminal Code)
This crime applies when the public official declines the corruption offered or the private party refuses the extortion proposed. However, when the refusal is not immediate and some negotiations had happened before, a crime of attempted corruption applies and both parties will be liable.

In passive incitement to corruption, the illicit behavior is the offer or the promise of money or other undue benefit to the public official. The offer or promise shall be serious and concrete and able to meet the goal, that is persuading the public official to do or delay a due act or to fail in a due act.

The ability of the offer to meet its goal shall be evaluated ex ante by considering the compensation's amount, the addressee personal qualities and economic situation and any other aspect of the case. Therefore, the crime does not apply if the offer or promise is not able to meet the goal, due to the evident and absolute impossibility of the public official to act illicitly as required.

There is not any need for the offer or promise to be addressed to the public official immediately and directly, as also any middleman is liable.

Fraud against the State or any other Public Entity or the European Union (article 640, paragraph 2, no. 1, Criminal Code)
This crime applies when scams are organized in order to take an illicit benefit, so that the State (or another Public Body or the European Union) is damaged and obliged to provide for a determined financial performance.

For example, this crime applies when a private party provides for unfair information to Public Administrations (for example information based on altered documents), in order to be win a tender.

Aggravated fraud to obtain grants (article 640-bis Criminal Code)
This crime applies when the fraud aims at obtaining public grants, for example when unfair information or false documentation is provided in order to obtain public financings.

Cyber fraud against the State or any other Public Entity (article 640-ter Criminal Code)
This crime applies when a third party alters an IT system or data herein and obtains an illicit profit from the State or any other Public Entity and damages other third parties.

For example, this crime applies when, after fairly obtaining a public grant, the grantee violates the public IT system to increase the amount to obtain.

As already mentioned, all the crimes above are related to relationships with the Public Administration (considered broadly and including also foreign Public Administration, or private entities officials carrying out activities ruled by public Law or, in general, of public interest).

1.2 RISK ASSESSMENT

The risk of committing crimes against Public Administrations is inherent in every business activity: any company has to deal with many Public Entities during ordinary activities for various reasons (even for the mere establishment of the company, various formal registration and communication requirements shall be met).

Moreover, the risk of committing crimes against Public Administration is high due to their specific nature: they are based on a relationship between different public and private parties (corruption is one of the main examples). In this context, even legal but equivocal behaviors (for example relationships

with local public clerk overly close, confident and informal) can generate suspects, determine the start of investigations, and however be misunderstood, by both the public official involved and third parties.

Another sensitive aspect is that law includes a very wide definition of public officials and public service officials (that are the subjects who these crimes apply to), therefore these crimes can apply also to parties employed in formally private entities, due to the "public" service they render.

In particular, Kardia daily joins various public tenders for the supply of its goods and services (please see paragraph 3.1 of this Model for details).

Therefore, Kardia is actually exposed to the risk of committing crimes against Public Administrations.

Considering Kardia's business, the following areas exposed to crime-risk have been identified:

- COMMERCIAL AREA/SALES
- PURCHASES
- HUMAN RESOURCES
- FINANCE

1.3 IDENTIFICATION OF AREAS AND ACTIVITIES EXPOSED TO CRIME-RISK

All the business activities involving a direct contact with the Public Administration are exposed to crime-risk (direct risk activities).

Direct risk activities are the following:

- Pre-contractual relationships with Public Administrations and similar;
- Contractual relationships with Public Administrations and similar;
- Participation in national and international law committees;
- Extra-contractual relationships with Public Administrations, local entities and similar.

Activities related to risk management include:

- Activities aimed at obtaining and/or renewing authorizations, certifications, licenses, permits and grants;
- Management of relationships with auditors;
- Management of relationships with Public Administrations;
- Choice of suppliers and external consultants;
- Management of participating tenders;
- Organization and/or participation to public tenders or private contracting;
- Public supplies.

Moreover, activities involving financial instruments and payments management and all the activities allowing the Company to grant benefits to public officials (or their connected parties) are exposed ti crime-risk (indirect risk activities), even though no direct relationship with Public Administration is involved.

In particular, indirect risk activities that can be used to form hidden money funds or to hide illicit actions are the following

- Administration, finance and tax activities;
- Purchases and payments.

1.4 GENERAL BEHAVIORAL RULES

In case of direct relationships between the Company's directors and employees and Public Administrations, the following behavioral rules shall be respected.

Every party that has relationships with Public Administrations while acting on behalf of the Company shall behave transparently and correctly.

Moreover, Kardia highlights the following very important rules to follow in any case when a Company exponent has any relationship or contact with Public Administrations:

- Any relationship with Public Administrations' physical deputies or with parties that carry out public interest activities broadly considered, shall be considered as exposed to crime-risk by definition;
- All phases and negotiations with Public Administration shall be formally documented, and related documents shall be always available;
- Supervisory Board shall be informed of any litigation with Public Administrations.

As in processes at risk all safety rules shall be precisely respected, in these relationships with Public Administrations the respect of all the internal protocols and behavioral rules contained in this Special Part is essential and shall be strictly respected.

1.5 SPECIFIC BEHAVIORAL RULES

In order to prevent crimes against Public Administrations, all Addressees shall not:

- Implement acts which crimes included in this Special Part could apply to;
- Create conflicts of interest with Public Administrations, Public entities or similar;
- Make any promises (hiring, internship, and so on) to public officials or public service officials belonging to Public Administrations, Public entities or similar;
- Give or promise money or any other monetary goods to public officials or person in charge of public services, as well as compensate their duties;
- Implement actions or behaviors aimed at obliging, persuading or pressing public officials or people in charge of public office to act against their office duties;
- Implement manipulative behaviors influencing tenders, or implement pre-emptive agreements among tenders' participants;
- Sign or endorse agreements aimed at getting secret information about the tenders' requirements, in order to influence the correct performance of the process;
- Document and monitor the supply contracts of goods and services necessary for the correct public functioning;
- Supply goods and services to third parties without any formalized contract;
- Draft and submit public officials inaccurate, misstated, incomplete or false statements, data or any other documents in order to obtain product and/or process certifications, public grants or subsidies;
- Agree and pay to third-party contributors sums of money other than contractual compensations, or distribute gifts that are not explicitly included in the business protocols;
- Use sums of money or other contributions granted by national, international or European bodies for other aims than intended or fail in using those amounts by any deadline included in the granting act;

- Pay in kind or pay in cash when not authorized by business protocols.

2. SPECIAL PART "A BIS": CORRUPTION BETWEEN PRIVATE INDIVIDUALS

2.1 THE CRIME CATEGORY

Law no. 190 of November 6, 2012, introduced some novelties in preventing and suppressing corruption and illicit in Public Administration. Among these, amended article 2635 of Civil Code, title "Corruption between private individuals" is relevant for this Model.

This law punishes directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors, and liquidators who, after granting or even just promising money or other benefits to third parties, commit or omit acts in violation to their duties or to loyalty obligations, consequently harming the Company.

One of the most important amendments to article 2635 of the Civil Code is the introduction of the same punishment also for the so-called "corruptor", that is the party who gives or promises money or other benefits, as introduced by letter s *bis*) to article 25-*ter* of the Decree, that in turn recalls paragraph 3 of amended article 2365 of the Civil Code. Therefore, the only new case when administrative liability of entities applies is the corruptor company, whose directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors, liquidators, or other parties subjected to their leadership or supervision, act corruption.

Legislative Decree no. 38 of 2017 introduced the crime of "Incitement to corruption between private individuals".

This law punishes who offers or promises money or other undue benefits to directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors, and liquidators of companies or private entities, or to any other party with managerial duties, so that they commit or omit an act in violation of their duties or of loyalty obligations.

This law applies also to directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors, and liquidators of companies or private entities, and to other parties with managerial duties who solicit an offer or promise of money or any other benefit for themselves or other parties, also indirectly, so that they commit or omit an act in violation of their duties or of loyalty obligations, when the solicitation is not accepted.

2.2. RISK ASSESSMENT

After identifying the areas exposed to crime-risk related to this crime category, please note that article 2635 of the Civil Code, although being titled *"Corruption between private individuals"*, applies only to relationships between corporates. Indeed, this law punishes corruption only when harming companies' equity, not corruption per se.

Therefore, areas exposed to crime-risk are where Kardia interfaces other third-party companies during its business activities, such as suppliers, consultants, agents, and so on. During these relationships, indeed, Kardia's employees could promise some benefits for unduly favorable supply of goods and services.

This risk is inherent in any kind of Company activities.

As regards this kind of activities carried out by Kardia, the following areas exposed to crime-risk have been identified:

- PURCHASES AND SALES
- RELATIONSHIPS WITH SUPPLIERS
- INVENTORIES

2.3 IDENTIFICATION OF ACTIVITIES EXPOSED TO CRIME RISK

In theory, all activities involving a commercial relationship, also indirect, between the Company and other third-party companies, are exposed to crime-risk.

Moreover, on the one hand all activities able to lead to the ultimate benefit, that is the corruption purpose, can be considered as exposed to crime-risk. These are all activities related to the sales cycle, such as the definition of the sale price of a product or a service, payment terms and conditions, any discount policy, transactions on any litigation.

On the other hand, all activities aimed at gathering the funds needed to the illicit money offers or promises are exposed to crime-risk. These are all activities related to the purchase cycle, such as purchase of goods and services, assignment of consultancies and other professional services, inventory management.

2.4 THE ADDRESSEES OF THIS SPECIAL PART

The potential criminals pursuant to article 2635 of the Civil Code are not only the directors, general managers, and, in general the senior managers identified inside the Company, but also their subordinate persons.

Therefore, this Special Part is addressed to all the Company's employees and to those third parties who act on behalf of Kardia and are subordinate to a Senior Manager.

2.5 GENERAL BEHAVIORAL RULES

The general rule that all the Addressees of this Special Part, as detailed above, shall respect, is as follows:

"None of the employees or of the third parties acting on behalf of Kardia can offer, promise or give money to any other party, as they cannot ask, consent or accept any amount of money from any other party."

This general rule is summarized in the Ethics Code, and specifically where it requires all employees, agents, and all third parties acting on behalf of the Company to respect the laws in place. Market fairness is, indeed, an essential rule of the Kardia business policy: Kardia aims at dominating its competitors thanks to the high quality of the products sold and services provided. It is not allowed to reach the same goal by other ways, especially against law.

3. SPECIAL PART "B": CORPORATE CRIMES

3.1 INTRODUCTION

Legislative Decree no. 61 of 2002 amended the so-called corporate crimes law, updating the Civil Code from article 2621 on. Also, this decree introduced article 25-ter in the Decree, expanding the application of administrative liability of entities also to ‘‘corporate crimes pursuant to the Civil Code, committed on behalf of the Company by directors, general managers, or liquidators and by their subordinated when the crime would have not been committed with their proper supervision”.

As also in the Guidelines, although article 25-*ter* does not explicit the two elements of the Decree (Organization, Management and Control Model and the Supervisory Board), it is implicit that they shall be amended to prevent also corporate crimes.

3.2 CATEGORIES OF CORPORATE CRIMES AS FROM ARTICLE 2621 ON OF THE CIVIL CODE (ARTICLE 25-TER OF THE DECREE)

Here follows a short description of the main crimes relevant to this second Special Part

3.2.1 Forgery hypothesis

False corporate communications and False corporate communications in listed companies (articles 2621 and 2622 of the Civil Code)

Law no. 69 of May 27, 2015 reviewed the criminal liability structure as regards corporate crimes. In particular, articles 9, 10 and 11 amended the Civil Code rules on false accounting

Differently from the past, Law 69 of 2015 differentiates between false accounting in listed and non-listed entities, punishing both crimes. Moreover, for non-listed entities there is an attenuated case and a specific non-punishment clause for minor cases.

False accounting in non-listed entities, previously punished with a monetary fine, is considered again a crime, punished with prison from 1 to 5 years. The liable parties did not change (directors, general managers, managers in charge of drafting corporate accounting documents, statutory auditors and liquidators).

According to amended article 2621 of the Civil Code, the crime is defined as the conscious communication of false material facts or omit to issue mandatory communications of material facts on the economic, financial and cash situation of the company itself or of the group where the company belongs, so that third parties can be actually misled; the crime is prosecutable ex officio.

Moreover, other elements introduced by amended article 2621 of the Civil Code on false accounting are the following:

- Unpunishment thresholds disappeared;
- Fraud matter was modified (in particular, the final aim of taking an unfair advantage remains, but the intention to fraud shareholders or third parties was removed, while the law now explicit the actual awareness of the false data communicated);
- The term “information” was removed and the term “material facts” (on the economic, financial and cash situation of the company or its group whose communication is mandatory by law) was introduced;

- The aspect of the illicit "being actually able to mislead third parties" was introduced.

Article 10 introduced two new rules after article 2621: articles 2621-bis (Minor facts) and 2621-ter (non-punishable facts for specific minor facts).

Article 11 amended article 2622 of the Civil Code too, now titled "false corporate communications in listed entities", that are companies with securities traded on an Italian or other European Union member State regulated market.

Article 12 amended the subjective criteria for the application of liability and sanctions to companies. While the original law limited this application to specific corporate roles (directors, general managers, liquidators or their subordinates), the amended law removed the terms of the above-mentioned Senior Managers.

3.2.2 Share capital protection

Unlawful return of capital contributions (article 2626 Civil Code)
This crime applies when capital contributions are returned or shareholders are released from their contribution obligations, when this return or release is pretended too, in cases external from the law provision.

Only Directors can be liable, as in crimes stated below pursuant to articles 2627-2629 of the Civil Code.

Illegal distribution of profits and reserves (article 2627 Civil Code)
This crime applies when distribution of profits or advances on profits is related to unearned profits or amounts intended to increase reserves by law, or when a non-distributable reserve by law is distributed.

However, this crime does not apply if profits and reserves unduly distributed are returned by the deadline set for the financial statements' approval.

Operations to the detriment of creditors (article 2629 Civil Code)
The introduction of this crime protects creditors and forbid companies to enact actions such as share capital reduction, mergers with other companies or spin-offs, when these harm the company's creditors.

However, the crime does not apply if they receive a compensation for their harm before the judgment is issued.

Improper distribution of corporate assets by liquidators (article 2633 Civil Code)
This crime applies when, during liquidation of the Company, liquidators distribute corporate assets to shareholders before paying company creditors or accruing enough money to their payment, with consequent harm for them.

However, the crime does not apply if they receive a compensation for their harm before the judgment is issued.

Only liquidators can be considered liable for this crime.

3.2.3 Company's well-functioning protection

Impeded control (article 2625 Civil Code)
This crime applies when Directors, only party that can be deemed liable, impede or interfere with other parties – shareholders or other company bodies - controls granted to them by law.

If they actually succeed in causing harm, sanctions will be higher.

Unlawful influence on the shareholders' meeting (article 2636 Civil Code)
This crime applies when third parties influence the majority of shareholders with simulated acts or fraud, in order to get an unduly advantage for themselves or other parties.

3.2.4 Public supervision functions protection

Obstruction in exercising the functions of public supervisory authorities (article 2638 Civil Code)
This crime applies in two cases, different in mode and timing.

The first one is when the Company communicates false material facts on its own financial, economic and cash flow situation, when communication to Public Supervisory Authorities is mandatory by law, or when these material facts are omitted in communication.

The second one consists of any other form of intentional obstruction to Public Supervisory Authorities' activities.

Companies' directors, general managers, managers in charge of drafting accounting documents, statutory auditors and liquidators can be liable for this crime.

3.7 RISK ASSESSMENT AND IDENTIFICATION OF ACTIVITIES EXPOSED TO CRIME-RISK

As regards the relevant crimes above-mentioned, the following areas exposed to crime-risk have been identified:

- Drafting of the financial statements, explanatory notes, corporate communications, in particular related to the economic, financial and cash situation of the Company;
- Corporate operations able to affect share capital and corporate governance system;
- Board of Directors supervisory activities;
- Communications to Supervisory Authorities;
- Management of relationships with Quotaholders, Statutory Auditors and Audit Firm;
- Management of operations on share capital, such as contributions, dividends' distribution, shares' subscription or any other extraordinary operations, like mergers or splits;
- Communication, performing and minutes of quotaholders' meetings;
- commercial negotiations;
- Management of gifts, donations and sponsorships;
- Supply of goods and services;
- Management of consultancies and professional services.

Kardia has long since implemented various internal procedures aimed at ruling the above-mentioned activities, and consequently grant:

- true and fair corporate communications, as well as their agreement to accounting data,

- well-functioning of corporate bodies and the controls system put in place, also on illicit share capital operations,
- true and fair information issued externally the Company.

However, the list of areas exposed to crime-risk can be updated in the future; it is possible, then, to identify further areas, with the consequent drafting of new specific behavioral rules and procedures.

If this happens, the Supervisory Board will be able to suggest any amendment on this Special Part, as deemed appropriate.

Besides these specific suggestions and behavioral rules, as detailed below, it is always essential to follow the basic principles adopted by Kardia and included in the General Part of this Model.

3.8 GENERAL BEHAVIORAL RULES

The Addressees shall:

- Behave correctly, transparently, and collaboratively, respecting all laws and business procedures in force, during all the activities related to the draft of the financial statements and other corporate communications, with the aim of always providing shareholders and third parties a true and fair view of the economic, financial and cash situation of the whole Company;
- Pay high attention to protect the integrity of the share capital and net equity, respecting all laws and procedures in force, in order to fully protect creditors and other third parties;
- Protect the well-functioning of Kardia corporate bodies, granting and helping any form of control over corporate management and granting the free-will of the shareholders;
- Issue all the communications to Public Authorities mandatory by law, in a true, fair and timely manner, without obstructing their control and supervision activities;
- Share news on commercial partners' initiatives and choices (agreements or partnerships with Kardia and so on) only when strictly needed by the partnership itself.

3.9 MANAGEMENT OF THE RELATIONSHIPS WITH AUDIT COMPANIES AND OTHER CONTROLS ON THE COMPANY'S MANAGEMENT

In choosing the Audit Company, the following precautions shall be followed:

- The Supervisory Board shall be immediately informed on the Audit Company chosen, as well as the reasons and considerations for the choice;
- The Supervisory Board shall be promptly informed of any other specific assignment to the Audit Company, or of any relevant news on the relationship between Kardia and the Audit Company;
- In general, any consultancy relationship with the Audit Company shall be prohibited.

Moreover, it is also prohibited to sign self-employed or subordinate employment contracts with the subsidiaries Audit Company's employees after a proper amount of time from the contract between Kardia and the Audit Company or between the employee and the Audit Company.

3.10 SHARE CAPITAL PROTECTION

All the operations that can influence, also indirectly, the Kardia share capital, as the profit and reserves distribution, purchase and sale of shares or branches, mergers, spin-offs, shall involve:

- The specific assignment of decision-making and operative responsibilities in the single projects, as well as the coordination mechanisms between the various functions;
- The involvement of the Supervisory Board in the whole process, including making available all the project-related documentation;
- The possibility of exchanging information between the Supervisory Board and the Audit Company in order to share any critical issues on the projects in progress.

As regards any conflict of interest, Directors shall communicate any role covered, or shares owned in other companies, directly and indirectly, and related modifications, that could reasonably create conflicts of interest pursuant to article 2391 of the Civil Code.

3.11 RELATIONSHIPS WITH PROPER AUTHORITIES

As regards any relationship with proper Authorities, the potential activities exposed to crime-risk are the following three:

- Draft and communication of information, recurring or not, as provided by law and rules;
- Draft and communication of any other information required by proper Authorities;
- Behaviors to have during these Authorities' inspections.

In these cases, the following principles shall be respected:

- Communication's terms and conditions of information required by proper Authorities shall grant the highest fairness and completeness;
- Parties in charge of the relationship with the Authorities shall be identified, so that they verify fairness and completeness of the information gathered and drafted;
- During inspections, all parties involved shall be highly collaborative, and a specific part in-charge of the activities required, able to coordinate all the business functions involved and to make available required documentation to inspectors as soon as possible;
- All the assigned in-charges shall be able to communicate with the Supervisory Board on the activities carried out during the Authorities inspections;
- The party in-charge of the inspections will have to draft a formal report to the Supervisory Board, regularly updated with the inspections developments and results.

4 SPECIAL PART "C": CRIMES IN VIOLATION OF SAFETY REGULATIONS AND OCCUPATIONAL HYGIENE AND HEALTH

4.1 Manslaughter and culpable serious or very serious bodily harm, committed in violation of safety regulations and occupational hygiene and health (article 25-septies of the Decree)

Article 25-septies of the Decree, introduced by Law no. 123 of August 23, 2007, and replaced by article 300 of the Consolidated Act on Safety Regulations and Occupational Hygiene and Health, extended the administrative liability of entities also to crimes of manslaughter and culpable serious

or very serious bodily harm, committed in violation of safety regulations and occupational hygiene and health.

Please consider that the above-mentioned Consolidated Act amended and reorganized the wide existing law on safety and occupational hygiene and health; moreover, it extended the administrative liability of entities also to the above-mentioned crime and introduced some specific rules on the Model drafting.

Manslaughter (article 589 of the Criminal Code)

Any party causing a person's death is punished with imprisonment from six months to five years.

If this happens in violation of traffic rules or of work prevention, imprisonment is extended from two to seven years.

Imprisonment is extended from three to ten years if the crime in violation of traffic rules is committed by:

a) A party in a state of alcoholic intoxication pursuant to article 186, paragraph 2, letter c) of the Legislative Decree no. 285 of April 30, 1992, as subsequently amended;
b) A party under the influence of drugs.

In case of multiple people's death or injuries, the punishment involves three times the punishment provided for the most severe violation, up to fifteen years.

Grievous bodily harm (article 590 Criminal Code)

Any party grievously harming other people's body is punished with imprisonment up to three months or with a Euro 309 fine.

In case of serious bodily harms, the imprisonment can last from one to six months and the fine could amount from Euro 123 to Euro 619; in case of very serious bodily harm, the imprisonment can last from three months to two years and the fine can amount from Euro 309 to Euro 1.239.

If crimes mentioned in paragraph 2 are committed in violation of traffic rules or work accident prevention rules, serious harm punishment is imprisonment from three months to one year or a fine from Euro 500 to Euro 2.000, while very serious harm punishment is imprisonment from one to three years. In case of violation of traffic rules, is the criminal is in a state of alcoholic intoxication pursuant to article 186, paragraph 2, letter c) of the Legislative Decree no. 285 of April 30, 1992, as subsequently amended, or is under the influence of drugs, serious harm punishment is imprisonment from six months to two years, while very serious harm punishment is imprisonment from one and half year to four years.

In case of multiple people's harmed, the punishment involves up to three times the punishment provided for the most sever violation, up to five years.

The crime is prosecutable if the offended party sues the criminal, except for cases as in the first and second paragraph, for violations of work safety or occupational hygiene and health regulations determining any work disease.

Please note that not any case of manslaughter or serious and very serious grievous bodily harm involve administrative liability of entities; pursuant to article 27-septies of the Decree, indeed, only

unintentional actions provoking an injury violating safety regulations and occupational hygiene and health are relevant to the Decree.

Moreover, please note that bodily harm is "serious" pursuant to article 583 paragraph 1 of the Criminal Code if: (i) from the harm derives a life-threatening disease, or a disease that prevent the harmed party to attend his ordinary duties for more than 40 days; (ii) the harm provokes the permanent weakness of a sense or an organ.

Bodily harm is "very serious" pursuant to article 583 paragraph 2 of the Criminal Code if the harm provokes: (i) a surely or probably incurable disease; (ii) the loss of a sense; (iii) the loss of a limb, or a mutilation making the limb useless, or the loss of an organ or the procreation ability, or a permanent and very severe difficulty in speaking; (iv) face deformation or permanent scars.

Three different punishments are provided by the Decree to the entities, depending on the severity level of the crimes. In particular:

a) In the most severe cases of manslaughter pursuant to article 55 paragraph 2 of the Consolidated Act (briefly, omitted or insufficient draft of the risk assessment report provided by law for particularly dangerous activities businesses), penalties are a monetary fine of 1.000 shares and disqualifications lasting from three months up to one year;
b) In case of manslaughter in violation of safety regulations and occupational hygiene and health, monetary fines amount from 250 to 500 shares, while disqualifications last from three months up to one year;
c) In case of serious or very serious bodily harm, monetary fines amount up to 250 shares, while disqualifications last up to six months.

4.2 ADRESSEES OF THIS SPECIAL PART

Given the aim of the analyzed crimes, it is evident that every business activity is exposed to crime-risk, under the safety and occupational hygiene and health protection point of view, for both the employees and the public in general.

Therefore, together with the Addressees of this Model, this Part is addressed also to the following parties:

- All parties covering a role related to safety and occupational health and hygiene (for example, employer's attorneys, work doctors, emergency workers, and so on);
- Third-party service providers working inside the business areas (including temporary or cooperatives workers working inside the business areas only occasionally);
- Contractors' employees working inside the business areas;
- Other occasional contributors;
- Office and any other place when business activities take place visitors.

4.3 AIMS OF THIS SPECIAL PART

Please note that the crimes considered in this Special Part, differently from the others relevant to the Decree, are unintentional acts.

In particular, grievous bodily harm is not intentional, but it is caused by the lack of respect of safety regulations, determined by negligence, imprudence, or inexperience.

Therefore, this Special Part aims at describing the activities carried out by Kardia in order to prevent these crimes, included the internal organizational measures adopted to fulfil all the obligations provided by occupational safety regulations and reduce risk of deficiencies in this field.

Therefore, this Special Parts has six different goals, prone to protect occupational safety:

1) To organize and define the organizational structure of business parties in-charge of occupational hygiene and health;
2) Define the basic rules for the Company, for all the Adressees of this Special Part, and for the parties actively in-charge of occupational hygiene and health;
3) Organize and rule all the business activities required by the Consolidated Act;
4) Organize and rule a correct and regularly updated risk assessment;
5) Organize the regular update and amendment of measures and instruments adopted by the Company to assure occupational safety and health and hygiene, considering both new laws and technical and scientific progresses;
6) Organize and rule regular training courses to employees on safety and occupational hygiene and health.

Specifically, in order to reach the above-mentioned goals, Kardia aims at rule and fulfil the obligations set by the Consolidated Act in relation to:

a) the respect of technical and structural standards set by law regarding equipment, machinery, workplace, chemical, physical and biological agents, and personal protective equipment;
b) the risk-assessment activities and the implementation of consequent prevention and protection measures;
c) organization activities, such as emergencies, first aid, tenders' management, regular safety meetings, communications with the employees' safety deputy;
d) health surveillance;
e) employees' information and training;
f) controls over the respect of procedures and instructions so that employees work safely;
g) acquisition of documentation and certifications required by law;
h) regular controls over the implementation and effectiveness of procedures adopted.

Moreover, this Model explicitly aims at:

- adopting measures and methods able to monitor: (i) overall situation of Kardia's safety protection system; (ii) the effectiveness of the measures adopted; (iii) the rise of new protection needs;
- applying the existing disciplinary system to safety deficiencies, omissions, and violations.

Therefore, by adopting this Special Part, Kardia aims not only at preventing injuries and accidents, given than the Company already has set proper procedures, but also highlighting the essential rules of the organization system to manage safety during its activities. This requires not only rules, but also execution and dynamics, considering the constant organizational, technical and law evolution, and a regular monitoring of the actual effectiveness of the measures implemented.

4.4 SUBJECTS IN CHARGE OF SAFETY MATTERS

Subjects in charge of safety matters are the following:

1. Employer, for duties that cannot be delegated;
2. Head of Prevention and Protection Service (RSPP);
3. Competent Doctor;
4. Employees.

The Company's organizational structure of the prevention system is as follows.

The Employer (identified as the Chief Executive Officer by proper resolution) fulfil the obligations that cannot delegate, related to risk assessment and nomination of the RSPP.

Then, the Company identified the Head if the Prevention and Protection System (RSPP), pursuant to the Consolidated Act, with the proper skills and powers to fulfil his obligations.

Moreover, the Company identified among the employees the people in-charge of firefighting, emergency and business first aid management.

Similarly, the Company identified a Competent Doctor.

4.5 COMPANY'S SAFETY POLICY

The Company considers safety and health protection not only a law obligation, but also a moral duty.

The Company has always followed essential rules like work environment safety protection, refusal to let employees undergo stressful work conditions, and warranty for a safe work environment.

Accordingly, the Company aims at the following goals in its business activities:

- Reduction in the frequency and severity of work injuries and diseases, to the minimum level possible;
- Adoption of any prevention and protection measure apt to eliminate risks, or however reduce them to acceptable levels, in any technical and organization choice;
- Maintenance over time of the desired safety levels, according to the maintenance of an optimal management of safety costs, also thanks to the effective and planned use of the human, technological and material resources available.

In order to do that, Kardia has always put efforts in the continuous update of instruments and technologies made available to its employees during business activities.

To reach the goals proper of its safety and health business policy, Kardia engages in:

- Respecting the law in force and adapt to future updates, amendments, and integrations;
- Grant information, implementation, and support of its policies at every business level so that the system can be fully participated in depending on the various skills and responsibilities, since meeting the above-mentioned goals requires all the employees' efforts;
- Enhance training and activities of the people actively in charge of employees' safety and health, since meeting the above-mentioned goals requires proper technical and management skills;
- Enhance all employees' specific skills on safety and health, by providing them with proper information and training courses on risks and on their prevention or reduction measures, since the best improvements derive from the employees themselves;

- Claim that both internal and external Company's contributors respect the work safety and health law in force, as well as all the internal rules set by the Company, aiming at improving and maintaining the safety levels;
- Grant its employees the continuous update of equipment, machinery, personal protective equipment they use during business activities, since this contributes to the safety and health goals of the Company;
- Enhance the application of safety and health protection rules by asking employees any deficiencies or anomalies in machinery and equipment well-functioning, able to create employees' health and safety damages or to breach any law or internal policy.

4.6 GENERAL PRINCIPLES AND BEHAVIORAL RULES

The Company has already implemented for a long time some general behavioral rules that shall be followed by all the parties involved in the business activities.

First of all, Kardia respects – and requires that all the Addressees of this Special Part to respect, as applicable – the following general principles:

- Strict respect of all the law in force, and implementation of an effective and proper system for managing, executing, and updating the activities carried out and related measurement;
- Draft and communication of internal by-laws and reports, including information and instructions on behaviors and cautions that employees shall follow;
- Availability to employees of proper protective equipment, granting that they will always be adequate to the state of the art and knowledge on the matter;
- Monitoring by proper in-charge parties of the actual effective and constant use of all the protective equipment required by the instructions' manuals mentioned above and any other direction, provided that deficiencies in their use constitute a disciplinary illicit;
- Identification and isolation of the business areas particularly dangerous for safety and health;
- Setting of adequate internal procedures on the regular update of risk assessment, in case of material changes in internal organization or laws enforced;
- Implementation of adequate internal protocols for emergencies, evacuations and fires;
- Written and detailed delegations to the safety in-charge, with any sub-delegations to other parties inside the organization chart;
- Grant the RSPP all the powers and financial autonomy to carry out the proper monitoring and prevention activities;
- Fulfilment of all the training and information obligations set in the Consolidated Act;
- Continuous control on the respect of the safety regulations by suppliers, lenders and any other third parties while providing services to the Company;
- Identification of chemical, noise, vibration risks, as well as all new and further risks as in the Consolidated Act (for example, the work-related stress).

Moreover, all the Addressees of the Model shall implement the following behaviors:

- Strictly respect all the safety, occupational hygiene and health regulations in force;
- Strictly respect all the internal by-laws and instructions on the matter;
- Strictly respect any indication and prohibition on signs and internal reports;
- Use all the protective equipment as intended in the instructions' manual, manufacturer' instructions, and so on;

- Respect the boundaries set for dangerous work areas, and access there only if authorized;
- Attend the training coursed organized by the Company and follow the instructions set in the safety reports provided by chiefs and in-charges;
- Do not use equipment and protection devices different from the one provided by the Company;
- For lenders and services providers, do not use Kardia equipment and protection devices;
- For temporary and cooperatives workers, follow the instructions given by the employer, based on Kardia instructions and pursuant to the Consolidated Act.

The following are RSPP and Employer's duties, as applicable:

- Grant a regular monitoring of the risks identified, so that their assessment is updated and amended based on the new Company's profile;
- Make of the monitoring results a) new proper safety measures and improvement in the existing ones; b) if needed, proper internal communication reports to the parties involved; c) new instructions issued and communicated to the parties involved;
- Base the risk assessment activities on objective criteria, in line with the scientific knowledge on the matter;
- Always consider hypothetical emergency situations, besides ordinary working conditions, in risk assessment activities and drafting of guidelines, regulations and internal information reports;
- Follow up on any safety report received by employees;
- Immediately inform the Supervisory Board, if very serious situations, on anomalies, risk situations, important reports received by single employees;
- Regularly meet, also with external safety consultants, to coordinate their activities;
- Suggest disciplinary sanctions in case of deficiencies in respecting work safety laws or internal regulations by Company's parties.

4.7 SPECIFIC BEHAVIORAL RULES

The above-mentioned laws are completed by instructions given by any of the parties in charge of safety matters, as in formal documents containing instructions for specific activities or for the use of specific equipment.

First of all, pursuant to the Consolidated Act, Kardia identified the risks inherent its business activities. The results of this assessment, together with the procedures aimed at the risks prevention, or at least reduction, were included in the Risk Assessment report, pursuant to the Consolidated Act.

Moreover, the Company has all a series of safety-related documents, for example equipment certificates, ordinary and extra-ordinary maintenance contracts of Company's areas, personal protection devices' instructions manuals.

Among the above-mentioned documents, please note the Emergency Plan, ruling the activities and the measures to implement in case of emergency, such as fires, evacuation and first aid, and the employees' training files, that include and certify the training courses attended by new hires and when employees change their duties, as well as general training courses for all employees.

All the above-mentioned documents are filed in the Safety File, at the RSPP premises, nominated by the Board of Directors on January 8, 2019.

However, all documents are available for consultation from any party entitled to do that.

4.8 RISK ASSESSMENT

In order to effectively prevent work-safety risks, it is essential an effective, detailed and regular organizational risk assessment.

Kardia always acknowledged the problem and dealt with it pursuant to Law 626 of 1994 and subsequent laws, regulations and communications on safety and occupational health and hygiene, lastly reorganizing and updating the risks and procedures assessment pursuant to the amended Consolidated Act.

In its premises, Kardia carries out mostly administrative activities, therefore the risk of committing one of the crimes this Special Part deals with is pretty low.

However, this did not imply that Kardia limited its risk assessment activities only to this kind of activities; in the Risk Assessment Document and related documents, indeed, Kardia analyzed, verified, and implemented adequate measures to prevent or at least reduce any safety risk that could hypothetically in its business areas. Obviously, most attention was given to the main activities carried out, given the Kardia core business, since it constitutes the main source of work accidents and injuries.

The most important document is the Risk Assessment Document pursuant to the Consolidated Act. It was drafted, updated, and refined by the Employer, with the technical support and direct involvement of RSPP and the Competent Doctor.

According to the amended Consolidated Act, the Risk Assessment Document includes also newly introduced risks, such as electromagnetic fields, artificial optical radiations, ionizing radiations, mutagenic carcinogens, asbestos, biological agents, fires, explosive atmospheres, work-related stress, together with the most traditional ones (chemical, manual handling of loads, vibrations, noise).

Moreover, the Company is aware that its duties do not include document drafting (or previous risk assessment) only: it is essential that the risk assessment activities are regular and constant, in order to be able to detect new risk areas arisen from new technical-scientific knowledge or following business activity changes (new work procedures or methods, new equipment, new premises and so on), as well as to detect deficiency and improve existing risk areas. Under this point of view, the Risk Assessment Document provides for, among the other things, a general update whenever modified or new risk factors arise, following activities' updates and/or changes and technical progress. The Document itself, its update and improvement, however, are always on the agenda of work safety and occupational health and hygiene meetings.

Health risks assessment is essential too. The Competent Doctor and health documentation's filing play a fundamental role. Health documentation is filed at the RSPP premises, pursuant to privacy laws.

The Competent Doctor writes a report of the activities he carries out once every two years, including diseases or injuries with particular statistical frequency in the period covered.

Obviously, in the most severe cases, or when deemed as appropriate, the Competent Doctor can (and shall) report immediately data and information known during his activities.

The health documentation includes the meeting between the Competent Doctor and RSPP minutes too.

Kardia files all the reports submitted in the safety files at the RSPP premises.

4.9 DOCUMENTATION AND ACTIVITIES' MINUTES

The documentation and activities' minutes are other vital aspects of the internal safety management system, so that the parties involved and the activities carried out can be traceable. Activities' traceability is a form of self-control and allows all parties involved to easily have a wholesome picture of the business safety and occupational health protection activities.

Therefore, all the parties with a relevant role shall formalize, also briefly, the most important activities carried out (meetings, new instructions and reports issued, as so on).

Kardia already formalizes its internal procedures aimed at training and informing both expert employees and new hires or workers whose duties changed recently.

Moreover, Kardia already detailed in proper documents all the procedures adopted in relation with work safety and health, including both ordinary activities' conditions and exceptional and emergency cases (fires, first aid, and so on.)

These procedures are properly communicated to employees through the information and training procedures addressed to them and the distribution of appropriate brochures.

A Safety File, including all the related documentation, is in place at the RSPP premises, with (paper or electronic) documents filed in chronological order. The Safety File at the RSPP premises includes also all the internal documents, instructions, by-laws and behavioral rules communicated to employees, as an essential method to manage work safety effectively and efficiently.

This part of the File too is accessible to all entitled parties requiring it.

4.10 COMMUNICATION AND TRAINING

In order to effectively protect safety and occupational health and hygiene, every activity carried out to train and inform employees and any other interested party so that they have the appropriate knowledge to always behave as better as possible is essential

As already mentioned, all the relevant parties shall be involved for effective and efficient safety risks prevention.

Regular information and communication between business parties in charge of safety and occupational health and hygiene is very important.

Kardia, together with RSPP, if possible, enacted the proper methods to grant:

- An effective training and communication of employees and all the parties involved in the business activities;
- Adequate technical and experience skills by employees in their day-to-day business activities.

On the one hand, as far as concerns the first bullet point, the Company already carried out and regularly schedule the following activities:

- *una tantum* or regular common training (regular meetings for activities already in place);
- individual training, to new hires and in case of duties change.

On the other hand, as far as concern the second bullet point, Kardia regularly meets with the employees.

All employees' communication and training activities shall be formalized in writing, and proper documentation shall be signed by the employee.

The Safety File at the RSPP premises includes the documentation on both training and reports submitted too.

5. SPECIAL PART "D": FRAUD CRIMES ON ASSETS

5.1 RECEIVING, LAUNDERING AND USING MONEY, GOODS OR BENEFITS OF ILLEGAL ORIGIN (ARTICLE 25-OCTIES OF THE DECREE)

This Special Part relates to crimes of receiving, laundering and using money, goods or benefits of illegal origin, as in article 25-octies of the Decree.

This law, introduced by the Legislative Decree no. 231 of November 21, 2007, titled "Implementation of the European Directive no. 2005/60/CE on the prevention in use profits from criminal activities in the financial system and terrorism financing, as well as of the European Directive no. 2007/70/CE on its implementation measures", provides that: "For crimes pursuant to articles 648, 648-bis e 648-ter of the Criminal Code, a monetary sanction amounting from 200 to 800 quotas applies to the entities. When money, goods or other benefit come from crimes that can be punished with more than five-year imprisonment, the monetary sanction applied amounts from 400 to 1000 quotas. If the entity is sentenced as guilty of one of the crimes included in paragraph 1, interdiction sanctions pursuant to article 9, paragraph 2 apply, for up to two years".

Please see below a detail of the crimes included in article 25-octies of the Decree:

Receiving stolen goods (article 648 Criminal Code)
This crime applies when a party purchases, receives or conceal money or other goods stemming from any illicit activity, or helps in purchase, receive or conceal them, in order to benefit himself or other parties.

The crime applies only if this party did not commit the previous illicit activity.

By purchase we here mean every transaction, with payment or for free, able to transfer the goods to the buyer.

By receiving we here mean every achievement of possession of the goods stemming from illicit activities, even though temporarily or for mere complacency.

Finally, concealing apply with the mere hiding of the goods stemming from illicit activities.

Moreover, this crime applies whenever the party interferes with purchasing, receiving or concealing of goods.

In this latter case, the crime applies just for the intervention in purchasing, receiving or concealing goods stemming from illicit activities happened, even though the final purpose is not reached by the parties.

According to article 648, paragraph 3, Criminal Code, this crime applies also when the party committing the crime money or goods stemmed from cannot be punished.

Laundering (article 648-bis)

This crime applies when any party, not committing the previous illicit activity, replaces or transfers money or other goods stemming from intentional crimes, or operates on them to hide their illegal origin.

Pursuant to paragraph 2 of article 648-bis Criminal Code, the punishment increases if the crime is committing during professional activities.

This crime can be committed in two ways:

a) replacing or transfer of money, goods and other profit stemming from intentional crimes (for example, exporting money or values and exchanging them with foreign currencies);
b) operating on money, goods and other profit, when this is aimed at hiding their illegal origin.

Use of money, goods or benefits of illegal origin (article 648-ter Criminal Code)

This crime applies when any party, not committing the previous illicit activity, intentionally use in financial or economic activities, goods or other benefits stemming from illicit activity, when the previous crimes do not apply.

Punishing this crime has two purposes: avoid the laundering of money stemming from illicit activities and avoid that the "clean" money is legitimately used.

The illegal action here is "use", that is not technically specific, so that it includes a broad variety of activities, any form of employment of money, goods or other profits stemming from illicit activities, regardless of the results reached by the agent.

Self-laundering (article 648-ter Criminal Code)

This crime was introduced to fill a gap in our regulation. The crime of laundering pursuant to article 648-bis of the Criminal Code, indeed, applies only for laundering money, goods or other profits stemming from an illicit activity committed by other parties, while not any sanction is applied for laundering, that means replacing or transferring, money, goods or other profits stemming from an intentional crime committed (or participated in committing) by the same person, or operating differently on them, to hide their illicit origin.

Moreover, the crime of self-laundering involves different punishments based on the severity of the original crime, and is not punished at all if money, goods or other profit stemming from the illicit activity are used personally by the criminal.

Illicit use and forgery of means of payment other than cash (article 493-ter)

Such crime was already included in article 55 of the Legislative Decree no. 231 of 2007, simultaneously abolished with the introduction of article 493-ter of the Criminal Code, although the two laws are in line

Legislative Decree no. 184 of 2021, implementing Directive no. 2019/713/UE of April 17, 2019 of the European Parliament and the Council, related to fight against fraud and forgery or means of payment other than cash, amended art. 493-ter of Criminal Code, now titled "Illicit use and forgery of means of payment other than cash" expanding the scope to all means of payment other than cash, including non-material means of payment, as defined in article 1 of the above-mentioned Decree.

Two crimes are included. On the one hand, the illicit use, by not the entitled person and with the goal to get a benefit, of credit or debit cards, as well as any other similar means of payment enabling to withdraw money or to purchase goods and services. On the other hand, the benefit to themselves or others is got through forgery of instruments or documents enabling to withdraw money or to purchase goods and services, as well as through acquisitions or sale of such instruments or documents with illegal source or however forged, and payment orders with such instruments and documents.

Those two crimes can coexist: who forges the instruments and uses them will be punished for both.

Fraud values transfers (article 512-bis Criminal Code)

Article 4 of Legislative Decree no. 21 of 2018, implementing the delegation included in article 1, paragraph 85, letter q) of Law no. 103 of 2017 on criminal matters' trend reserve, added article 512-bis to the Criminal Code, that punishes the crime of fraud values transfers, already included in article 12-quinquies of the Law Decree no. 306 of 1992, converted into Law no. 356 of 2019, that was simultaneously abolished.

Such crime involves the fraud attribution to other parties of the title to use or the availability of money, goods or other benefits in order to avoid laws in place related to smuggling prevention or to aid receiving stolen goods (art. 648 Criminal Code), money-laundering (art. 648-bis Criminal Code) or use of money, goods or other benefits from illicit origins (art. 648-ter Criminal Code).

Therefore, the specific intention of such crime is to avoid laws in place or aid the other three crimes mentioned in article 512-bis Criminal Code.

The crime involves general danger and requires a prior partial evaluation about the danger of avoidance of laws, therefore referring to the known circumstances at the moment of action, or that can be known by an average person in such situation.

5.2. GENERAL BEHAVIORAL AND DECISION-MAKING RULES IN AREAS EXPOSED TO CRIME-RISK

While carrying out every business activity, especially the activities deemed as exposed to crime-risk, the Addressees shall respect the following rules:

- Avoid any behavior involving law's violations, including the crimes detailed above;
- Avoid any behavior that, although do not involving law's violations per se or the crimes detailed above, could potentially result in them;
- Avoid any transaction or operation on money or goods, when some aspects of the operation or of the counterparty suggest the illegal origin of money or goods (for example, price much higher than average);
- Behave correctly, transparently, respecting law and internal business procedures, in all the activities related to suppliers' and clients' registry management;
- Choose counterparties already included in the suppliers' registry to purchase goods and services;
- Regularly evaluate clients' performance and characteristics, reporting to the Supervisory Board any anomaly;
- Do not have business relationships with suppliers/clients/partners not included in the suppliers'/clients' registers, and with any party certainly or probably belonging to criminal organizations or acting illegally;

- Record any bank transaction in Kardia's IT system, to allow management to daily monitor them;
- Regularly monitor the business financial flows, respecting the business internal procedures that shall always include the reconciliation between the payee/payer and the related accounting documents, with the support of at least two business functions (suppliers/analytic accounting and banks accounting) and the authorization by the Administration of the total payment.

More specifically, it is forbidden to:

- Purchase goods and services at a price much lower than market average, without controlling their origins first;
- Purchase goods and services from suppliers not included in the Company's register;
- Transfer money, goods, or other benefits when they suspiciously stem from an illicit activity, in order to hide or disguise their illegal origin;
- Collect or pay in cash, except for amounts below law limits, amounting however to law value; carry out operation that can appear aimed at hiding the illegal origin of money, goods or other benefits;
- Carry out operations that can appear aimed at reinvesting laundered resources.

5.3 BEHAVIORAL RULES SPECIFIC FOR SINGLE RISK AREAS

In order to the respect the rules mentioned in the previous chapter, besides the principles included in the General Part of this Model, the Addressees shall also respect the following rules:

- Identify the new business counterparties (business partners), through verifying their data from reliable sources, gathering relevant information (such as public prejudicial data, bad bills of exchange, bankruptcy procedures), involving specialized companies in gathering information on companies, its partners, its directors, and so on;
- Include in controls carried out on the inbound financial flows' aspects like the registered office's Country of the business partner (such as tax heavens, countries exposed to terrorism-risk), the banks it used (registered office's Country of the banks involved in the operations), and of any corporate shields and trusts used for extraordinary transactions and operations;
- Proper verification aimed at excluding the risk of committing crimes of laundering, receiving and using money, goods or benefits of illegal origin shall always precedes any commercial or financial operation with third parties, through a clear identification of the business partner and the nature of the transaction;
- All suppliers and partners contracts' terms and conditions shall be defined in writing;
- When entering into new contracts, suppliers and partners shall communicate:
  (i) The acknowledgment of the Decree's law;
  (ii) The commitment to the Decree's respect;
  (iii) Any previous involvement in processes related to crimes included in the Decree.
- Identify and, if possible, reduce the employees enabled to pay suppliers and employees, therefore owning the access codes;
- Plan and implement an internal control system with double signature, other than the one already in place at the company bank level;

- Limit payments and instant payments, or implement some specific authorization measures in case of exceeding specific thresholds;
- Verify periodically the bank accounts in order to submit claims promptly;
- Implement and discipline any company credit/debit cards, or company online means of payments (i.e. PayPal);
- Implement and manage an IT department to monitor company software.

6. SPECIAL PART "D": CYBER AND PRIVACY CRIMES

6.1. CATEGORIES OF CYBER AND PRIVACY CRIMES (ARTICLE 24-BIS OF THE DECREE)

Law no. 48 of 2008 approved and implemented the European Commission Convention on cybercrimes, signed in Budapest on November 23, 2001.

Law no. 48 introduces in the Criminal Code some new crimes and also introduced new article 24-bis of the Decree, providing the administrative liability of entities when committing cybercrimes to take advantage from.

In particular, the law states the following:

"(Cybercrimes and illegal data processing).

1. When crimes pursuant to articles 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies of the Criminal Code apply, the entity is punished with a monetary sanction amounting from one hundred to five hundred quotas.

2. When crimes pursuant to articles 615-quater and 615-quinquies of the Criminal Code apply, the entity is punished with a monetary sanction amounting up to three hundred quotas.

3. When crimes pursuant to articles 491-bis and 640-quinquies of the Criminal Code apply, the entity is punished with a monetary sanction amounting up to four hundred quotas, except for the cases of cyber fraud against the State or other public entities included in article 24 of this Decree.

4. Disqualification sanctions pursuant to article 9, paragraph 2, letters b) and e) apply to parties sentenced guilty for crimes included in paragraph 1. Disqualification sanctions pursuant to article 9, paragraph 2, letters a), b) and e) apply to parties sentenced guilty for crimes included in paragraph 2. Disqualification sanctions pursuant to article 9, paragraph 2, letters c), d) and e) apply to parties sentenced guilty for crimes included in paragraph 3."

Please see below a brief description of the crimes included in this law.

Illicit access to an IT system (article 615-ter Criminal Code)

Similar to physical housebreaking, this crime applies when someone illicitly accesses or remains in a protected IT system against the will of the entitled parties.

Illicit interception, prevention, or interruption of IT or telematic communication (article 617-quater Criminal Code)
This crime applies when someone illicitly intercepts telematic communications, or intentionally interrupts or prevents them.

Installation of equipment aimed at intercepting, preventing or interrupting telematic communications (article 617-quinquies)
This crime applies at the mere installation of intercepting equipment, even though not any actual interception, interruption or prevention activity was enacted.

Damage (635-bis – 635-quinquies Criminal Code)
Articles 635-bis and subsequent apply in a wide range of cases, all having in common the intentional damage of IT data and systems.

First of all, article 635-bis punishes the intentional damage of IT software or data. This law punishes third parties' IT information, data or software destruction, damage, deletion, or alteration with imprisonment from six months to three years.

Article 635-ter punishes more severely IT information, data or software destruction, damage, deletion, or alteration when they belong to the State or to any other public entity, related to public parties or having public utility.

Article 635-quater punishes IT or telematic systems' damage, in particular the parties who, committing some of the crimes pursuant to article 635-bis aimed at data and software's damage, damages the whole IT system's functioning.

Article 635-quinquies punishes more severely crimes pursuant to the above-mentioned article, if related to public utility systems.

Illicit detention and distribution of access codes to IT or telematic systems (article 615-quater Criminal Code)
This crime applies to parties who communicates, distributes, copies, or obtains codes, password or any other means able to grant access to a protected IT system, in order to take advantage or damage other parties.

Distribution of software able to damage or stop an IT system (article 615-quinquies Criminal Code)
This crime applies to parties spreading so-called IT viruses, that are software aimed at entering IT systems and preventing or damaging their correct functioning or deleting data herein.

IT documents fraud (article 491-bis Criminal Code)
This law extends the crime of deeds fraud also for IT documents.

Cyber fraud by electronic signature certifier (article 640-quinquies Criminal Code)
This law punishes the electronic signature certifier violating law requirements to release a certification in order to take an illicit profit for himself or other parties.

Cyber fraud with legal identity replacement (article 640-ter Criminal Code)
This law punishes parties altering an IT system's correct functioning or illicitly acting on data, information or software herein included or related, in order to take an illicit advantage for himself or other third parties or to damage others, through digital identity's replacement.

The Court of Last Resort specified in its Resolution no. III/01/2013 of August 22, 2013, that article 9 of Law Decree no 93 introduced a new special effect aggravating situation of cyber fraud pursuant to article 640-ter Criminal Code, that is when the digital identity's replacement damages one or more parties. According to the Court of Last Resort, the final purpose of the law amendment in digital identity's protection is increasing the citizens' trust in on-line services and reduce frauds enacted through identity thefts (especially in consumer credit). Therefore, punishments are stricter when frauds are committed through illicit accesses to IT systems and the illicit use of others' digital identity, with imprisonment from two to six years (instead of from six months to three years) and from 600 to 3.000 Euro fines.

Illicit data processing (article 167 Privacy Code)
This crime applies when a party processes personal data in order to take advantage for himself or others or damage other parties, violating the Privacy Code.

By "personal data processing" we mean every transaction or set of transactions, carried out also without any electronic instruments, aimed at gathering, recording, organization, keeping, consultation, processing, modifying, selecting, extracting, comparing, using, connecting, blocking, communicating, distributing, deleting and destroying data, even though not recorded in a database.

6.2 AREAS EXPOSED TO CRIME-RISK

All activities performed by parties whose business duties include accessing or using the Company's IT network or employees' and third parties' personal data.

Given the above-mentioned crimes, we can limit the hypothetical Kardia's activities exposed to crime-risk to the following:

- Alter and falsify public or private electronic or paper documents;
- IT Espionage or sabotage to the detriment of public or private competitors (third parties' data creation, modification, alteration; illicit access in third parties' systems; third parties' software non-authorized modifications and damage; illicit possession of passwords to access third parties' IT systems; illicit interception of third parties' IT communications; installation of equipment aimed at these illicit activities; spread of viruses…).

6.3 BEHAVIORAL RULES TO AVOID CYBERCRIMES

In general, all Addressees shall:

- Use the Company's IT network for strictly professional purposes, transactions, and communications;
- Access, connect and exchange data with third parties' IT network only for professional reasons, in the cases and for the time strictly necessary;
- Communicate to the Supervisory Board any fact, event, or anomaly able to create a well-founded suspicion of a cybercrime being committed.

Actual prevention of the crimes included in this Special Part can and shall be based on two aspects:

- The certain identification of every user accessing and operating in the IT network;
- Prevention measures to non-entitled parties' access to the network, so that no one could operate anonymously on the Company's IT network.

All Addressees that use business computers or, in general, access Kardia's IT network, shall use the following password system:

- To access workstation (computer);
- To access e-mail box and download e-mails;
- To any access Administrator workstation;
- To access the Company's IT network and on-line services;
- Screensavers.

The use and correct management of passwords is essential to the certain identification of every user accessing and operating in the IT network.

Therefore, please see below the following behavioral rules:

- Change at the first access the default password assigned by the IT Management;
- Mandatorily and immediately change password when compromised;
- Include in the password at least 8 alpha-numeric characters or, if this is not allowed by the electronic instrument, with the maximum number of characters allowed;
- Do not use easily deducible information for passwords (for example, your name or your family's names, and so on);
- Do not allow other users to operate with your profile (for example colleagues);
- Do not write the password down on easily accessible supports (for example post-its on the monitor).

As regards the second essential aspect, that is the prevention of anonymous or not correctly identified accesses to the Company's computers and network, Addressees shall carefully preserve their workstation (especially if this is a laptop).

Moreover, external visitors shall use the Company's infrastructure only exceptionally. They shall, indeed:

- Always be explicitly allowed to connect to the Company's network by their internal contact person and according to the IT Management rules. Their access is allowed only temporarily until the end of their continuative presence at the Company's premises;
- Comply with this Model rules, law and recommendations.

Finally, all Addressees of this Special Part shall mandatorily report to the Police any loss or theft of laptop workstations, and forward the report to the Administration, reporting sensitive Company's data herein included.

From an IT point of view, Kardia prevent third parties' intrusions (so-call spyware) thanks to a proper software (Firewall) too.

Kardia monitors the respect of the above-mentioned rules, with random controls and regular controls on the regular keeping and updating of passwords.

6.4 BAHVIORAL RULES FOR PERSONAL DATA PROCESSING

Kardia is the personal data holder for its employees and other parties interfacing with it (for example, suppliers); Mr. Giovanni Longoni is the person in-charge, who named ASM CONSULTING S.A.S. by Mr. Maggiora Aldo & C. and other external parties as main contacts.

Kardia, as personal data processing holder, informs in writing the involved parties of the data processing in place, by signing the privacy disclaimer pursuant to the new GDPR no. 679 of 2016.

Therefore, the Holder communicates to the involved parties:

1. *Data processing purposes and methods;*
2. *Whether the data provision is compulsory or optional;*
3. *Any consequence of denying data provision;*
4. *Scope of data communication and distribution;*
5. *Any data communication abroad;*
6. *The involved parties' rights;*
7. *The Holder;*
8. *The in-charge person;*
9. *The authorized parties to process data.*

All the information mentioned above is included in the disclaimer Kardia hands out to the involved parties, that sign it, at the moment of data gathering and, if the data gathering is outside the Company's premises, by the moment of data registration or communication to other third parties. Kardia keeps the signed disclaimers properly, in databases that can accessed only by the in-charge and main contact people for purposes, transactions and communications strictly related to Kardia business activities.

7. SPECIAL PART "E": CRIMES AGAINST JUDICIARY

7.1. Crime category (article 25 - decies of the Decree)

Law no. 116 of August 3, 2009, introduced article 25-decies of the Decree, stating that *"the entity is punished with a monetary sanction up to five hundred quotas for committing crimes pursuant to article 377-bis of the Criminal Code*".

Article 377-bis of the Criminal Code punishes parties not making statements or making false statements to judiciary.

This crime applies when the convened person is induced with violence or threats, or with money or other benefit's offer or promise to make or not make statements or make false statements to the judiciary (useless statements in a special proceeding).

7.2 AREAS EXPOSED TO CRIME-RISK

Every entrepreneurial, commercial, or industrial activity can be inspected by judiciary authorities, especially since the introduction of administrative liability of entities.

Therefore, any entity could hypothetically commit the above-mentioned crime, if one or more representatives are call by the proceeding authority to give information or make clarifications on the entity and on aspects relevant for the accusation.

7.3 GENERAL BEHAVIORAL RULES

Kardia has always carried out its business activity following some general behavioral rules aimed at respecting ethical and legal principles in its relationship with suppliers, customers, commercial partners, and employees.

Kardia explicitly forbids threats, requests, illicit pressures, recommendations, or reports aimed ai persuading any person to commit crimes.

If Kardia or its representative are involved in judiciary investigations, all the Addresses convened to make statements to the judiciary itself shall be completely free to answer truly.

Kardia, indeed, ensures that all Addressees' collaboration with the authorities shall not be source of prejudice, discrimination, or negative evaluation by the Company. As a matter of fact, Kardia considers as essential duty of all Addressees to answer correctly, truly and transparently to all judiciary requirements.

Kardia protects the Addressees' privacy: none of them shall be considered as obliged to communicate to the Company any summon or hearing happened, as well as the Company shall no judge negatively the employees not disclosing such situations.

In general, in case of an inspection on the Company or its representative, Kardia will identify, among its directors, a specific person, in-charge for opening and keeping a dossier with all the official deeds (any warranty, search or seizure report, and so on), and all the main developments of the proceeding.

Basically, if an inspection arises, Kardia will name a trusted lawyer immediately, to support it from the beginning of the proceedings.

The Supervisory Board will be properly informed on the proceedings, the person in-charge for the dossier keeping and the trusted lawyer. All Addressees shall report any attempted influence (or any other suspicious circumstance) to the Supervisory Board, that will act accordingly.

8. SPECIAL PART "G": TAX CRIMES

8.1 CRIME CATEGORIES (article 25-quinquiesdecies of the Decree)

Legislative Decree no. 124 of October 26, 2019, converted with modifications into Law no. 157 of December 19, 2019 (so-called "Urgent tax provisions for uncrastinable needs") and Legislative Decree no. 75 of July 14, 2020 (so-called "Implementation of European Union Directive no. 2017/1371 related to the fight against fraud damaging Union's financial interests though criminal law") introduced these relevant crimes.

In particular, they introduced in the Legislative Decree no. 231 of 2001 the article 25-quinquiesdecies, providing for the following tax crimes:

Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000

This crime applies when parties insert false negative items in their tax declarations in order to evade income or added value taxes, using non-existent transactions' invoices or other documents. The crime

is deemed as committed when these false invoices or documents are posted in mandatory accounting entries or kept as a proof to the tax authorities.

Fraud statements through other mechanisms pursuant to article 3 of Legislative Decree no. 74 of 2000

This crime applies in other cases with respect to article 2, when parties (a) carry out objectively or subjectively false operations or (b) use false documents or other fraud means apt at preventing the tax authorities' inspections or misleading them in order to evade income or value added taxes and therefore insert in tax declarations (i) positive elements lower than actual or (ii) false negative elements or (iii) false receivables and withholdings, when the following two conditions happen at the same time:

1) When each of the taxes evaded is higher than thirty thousand Euro;
2) When the net taxable income (resulting from both lower positive items and higher or false negative items) hidden (i) is higher than 5% of the total positive items included in the tax declarations or (ii) higher than 1.5 million Euro, or (iii) when total false receivables and withholdings subtracted to the tax due is higher than 5% of the tax itself or thirty thousand Euro.

The crime is deemed as committed when the above-mentioned documents are posted in mandatory accounting entries or kept as a proof to the tax authorities. In order for the law to apply, it is not considered as fraud the mere violation of invoicing and positive items accounting obligations or accounting positive items for lower amount than actual.

Unfair declaration pursuant to article 4 of Legislative Decree no. 74 of 2000

This crime applies when the evaded tax is higher than 100 thousand Euro and the total amount of hidden net taxable income (resulting from both lower positive items and higher or false negative items) is higher than 10% of the total positive items included in the declaration or higher than Euro 2 million.

However, pursuant to article 2 of the Legislative Decree no. 75 of 2000 and as explicated by article 2 paragraph 2 of the EU Directive 2017/1371, the above-mentioned tax crime is relevant to the Decree only when the following punishable pre-conditions exist:

- The entity took advantage or had interest in the crime committed;
- The crime was committed within a transborder fraud system (that is involving at least two member States);
- The crime was committed in order to evade VAT for at least Euro 10 million.

In general, please note that not all the hidden items are counted for the punishable threshold pursuant to article 4 of the Legislative Decree no. 74 of 2000. Legislative Decree no. 158 of 2015, indeed, updated the crime of unfair declaration, stating that it applies only to "non-existent" positive/negative items and not "false" anymore.

Therefore, this tax crime does not apply to: (i) the incorrect classification of "objectively existent" positive and negative items, provided that the applied criteria were mentioned in the financial statements or in any other tax relevant documentation; (ii) the violation of accrual-basis, inherence, and real negative items' deductibility principles pursuant to article 4, paragraph 1-bis of the Legislative Decree no. 74 of 2000.

The crime of unfair declaration pursuant to article 4 of the Legislative Decree no. 74 of 2000 constitutes an instant crime, committed when the unfair declaration is submitted.

Omitted declaration pursuant to article 5 of Legislative Decree no. 74 of 2000

This crime applies, in general, when the entity omits to submit income or value added tax declarations, when each evaded tax is higher than Euro 50 thousand. Similarly, sanctions apply also to omitted withholding tax declaration (so-called 770 model), when withholding taxes unpaid amount more than Euro 50 thousand.

Omitted declaration is a proper omission crime (as it can be committed only by parties obliged to submit tax declarations) and is an instant crime, that is considered committed after 90 days from the deadline for submission of the declaration, in line with article 5 paragraph 2 of the Legislative Decree no. 74 of 2000. It is not deemed as "omitted" unsigned declarations or declarations drawn up on an unregular model.

Moreover, this crime requires the explicit intention to evade taxes to apply.

However, the same punishable pre-conditions pursuant to article 4 of the Legislative Decree, mentioned above, are required for this crime to be relevant to the Decree.

Issue of non-existent transactions' invoices or other documents pursuant to article 8, paragraphs 1 and 2-bis of Legislative Decree no. 74 of 2000

This crime applies when parties issue invoices or other documents related to non-existent transactions, in order to allow third parties to evade income or value added taxes. Multiple issue of invoices or other documents in the same fiscal year is considered as one crime only.

Hiding or destruction of accounting documents pursuant to article 10 of Legislative Decree no. 74 of 2000

This crime applies when parties hide or destroy accounting entries or mandatorily kept documents, so to conceal the computation of taxable income or turnover in order to (i) evade income or value added taxes or (ii) allow third parties to evade them.

Undue compensation pursuant to article 10-quater of Legislative Decree 74 of 2000

This crime applies when parties do not pay due amounts, through compensating not due or non-existing receivables higher than Euro 50 thousand, pursuant to article 17 of the Legislative Decree no. 241 of July 9, 1997.

This crime too is relevant to the Decree only if committed within a transborder fraud system and in order to evade value added tax for at least 10 million Euro.

"Not due" or "non-existing" receivables can relate to any kind, also to social security institutions.

This crime is committed over time, as it applies when the punishable threshold is cumulatively overcome, resulting in a series of undue compensations.

Fraud subtraction of due tax payments pursuant to article 11 of Legislative Decree no. 74 of 2000

This crime applies when parties:

a) Fake sales or other fraud transactions on his own or others' goods so that the compulsory collection procedure is fully or partly ineffective, in order to evade payment of (i) income or value added taxes or (ii) interests and administrative sanctions;
b) Include in the documentation submitted within a tax transaction (i) positive elements for lower amounts than actual, or (ii) false negative elements for amounts higher than actual for Euro 50 thousand, in order to obtain for themselves or other parties a reduction in payments due for taxes and related accessory charges.

8.2 RELEVANT DEFINITIONS

Pursuant to Legislative Decree no. 74 of 2000, please note the following definitions:

a) "**Non-existent transactions' invoices or other documents**" refer to invoices or other documents with similar proof relevance to the tax law (i) related to transactions that do not fully of partly exist, or (ii) showing a compensation or value added taxes higher than actual, or (iii) refer the transaction to different parties than actual;
b) "**Positive or negative items**" refer to (i) items, expressed in numbers, concurring positively or negatively to the computation of income or value-added taxable income and (ii) items concurring to the computation of the tax due;
c) "**Declarations**" refer to declarations submitted by companies, entities or physical people's directors, liquidators, representatives or withholding agents too, in cases provided for by law;
d) "**Aim of evading taxes**" and "**Aim of allowing others to evade taxes**" include also (i) aim of obtaining an undue tax refund or a non-existent tax receivable and (ii) allowing others to obtain them, respectively;
e) When committed by companies, entities or physical people's directors, liquidators or representative, "**aim of evading taxes**" and "**aim of allowing others to evade taxes**" refer to the company, entity or physical person on behalf of whom they operate;
f) "**Evaded tax**" refers to the difference between the properly due tax and the amount submitted in the declaration, or the whole tax amount in case of omitted declaration, net of sums paid by the taxpayer or other third parties as advances, withholdings or any other payment made before submitting the declaration or before the deadline; it is not included in this definition the "theoretical" tax not actually linked to a reduction in the current or previous fiscal years' losses;
g) "**Objectively or subjectively false operations**" refer to (i) apparent operations, different from the ones where article 10-bis of Law no. 212 of July 27, 2000 applies, implemented with the aim of not carrying them out completely or (ii) operations related to fictitiously interposed parties;
h) "**Fraud means**" refer to active factitious activities, as well as omitting activities violating specific law obligations, that determine a false reality representation;
i) "**Undue receivable**" refers to receivables whose consistency and amount are certain, but that cannot be compensated yet or any more for any law reason in transactions between taxpayers and Treasury through F24 models, pursuant to article 17 of Legislative Decree no. 241 of 1997;
j) "**Non-existent receivable**" refers to receivables (i) fictitiously computed or declared that, as such, cannot be found in the legal world, or (ii) although hypothetically existing, they refer to other parties or depend on conditions not realized yet.

All these crimes can be intentionally committed by "anyone" (although in some cases while carrying out specific activities), covering specific roles with respect to the entities, as in article 5 of the Legislative Decree no. 231 of 2001:

a) Entity or one of its organizational units with financial and functional autonomy's representatives, directors or managers, as well as parties managing and controlling them de-facto;
b) Subordinate peoples or parties included in letter a) above.

The entity is not liable is the parties mentioned above operate in their own or third parties' interest.

8.3 AREAS EXPOSED TO CRIME-RISK

The Company identified the following sensitive activities, during which tax crimes pursuant to article 25-quinquiesdecies of the Decree could be hypothetically committed:

1) Suppliers' selection and management (technical devices and other goods supply and general services, consultants, etc.…) and supplies' management.
2) Sale activities management.
3) Tax and accounting obligations fulfilment and tax payment.
4) Accounting documents archival.
5) Inventory management;
6) Human Resources.
7) Intercompany transactions.
8) Relationships with Judicial and Financial Authorities.

8.4 GENERAL BEHAVIORAL RULES

With reference to the above-mentioned crimes, the Company implemented specific protocols including, among others, the following controls:

Suppliers' selection and management (technical devices and other goods supply and general services, consultants, etc…) and supplies' management

In carrying out the activities included in this process, the following crimes could be committed:

- Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000
- Fraud statements through other mechanisms pursuant to article 3 of Legislative Decree no. 74 of 2000

As pertains suppliers' management activities, Kardia's internal control system provides for a specific procedure for purchases' management with a clear identification and segregation of duties and responsibilities in the purchase process.

In selecting suppliers, specific ethical and subjective (for example reliability, professional skills, suppliers' behaviors during the process) and objective (for example suppliers' geographical location, non-recurring transactions, shareholders' structure changes, irregular work, work safety and health sentences, and so on) criteria were established.

Goods and services purchases involve specific purchase orders by the individual functions allowed by their in-charge person and controlled by Directors.

Relationships with the goods and services suppliers are rules through specific contracts/agreements/orders or engagement letters (for professionals and consultants), according to the Company's policies, and authorized according to the reporting lines in force.

The Administration Office checks the correct match of data from purchase orders and invoices with specific management and approval procedures, including updates and changes to the orders.

The Administration Office preventively verifies the match between the supplier's name and the bank account owner, so that the Company's payments and cash flows can be always transparent and documented.

Another control is performed between goods and services received and agreed and the related payments are sent only upon Directors' approval.

The above-mentioned processes are implemented also with sales agents, intermediaries and distributors.

Sale activities management

In carrying out the activities included in this process, the following crimes can be committed:

- Issue of non-existent transactions' invoices or other documents pursuant to article 8, paragraphs 1 and 2-bis of Legislative Decree no. 74 of 2000

With reference to the sales' related activities, Kardia implemented specific controls over the correct keeping of clients' data, payment conditions' monitoring, the correct match between orders, contracts, delivery notes, invoices and collections.

Relationships with the clients (mainly hospitals) are managed mainly through specific contracts (after tenders winning)/agreements/orders, according to the Company's policies, and authorized according to the reporting lines in force.

All orders and contracts are uploaded on the IT system with the specific price, payment, delivery terms; any deviance from the inserted conditions shall be motivated and authorized by the Directors, uploading this information on the system too.

The invoice process includes the correct reporting of invoices data, the identification of parties involved and the related contract, the verification for adequate documentation supporting the transaction (proved by the goods' delivery or the services' supply) and the Directors' authorization.

Tax and accounting obligations fulfilment and tax payment

In carrying out the activities included in this process, the following crimes can be committed:

- Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000
- Fraud statements through other mechanisms pursuant to article 3 of Legislative Decree no. 74 of 2000;
- Fraud subtraction of due tax payments pursuant to article 11 of Legislative Decree no. 74 of 2000

With reference to this process, the Administration Office grants proper controls over the formal and substantial correctness of accounting and administrative transactions, ensures the fulfilment of law obligations related to the Company's administration and the financial statements draft, grants and

guards the correct accounting services management, ensuring their correctness and compliance to the law in force, as well as manages any problem related to the Company's employees.

Kardia is supported by an external chartered accountants' professional studio for tax management, as well as by an external payroll consultants' studio for employees' related problems.

Among others, the Company shall fulfil the following obligations:

- Drafting and communicating a tax timetable and monitoring the deadlines to respect for communications, declarations and other obligations with the Tax Authority;
- Regular controls over the correct keeping and updating of accounting statutory and tax books;
- Regular controls over the match between positive/negative transactions and the related accounting entries;
- Respect and share any amended tax laws;
- Involve proper internal functions to evaluate tax effects and respect law in force, when carrying out the typical business activities;
- Ensure that the people in-charge of the various internal functions promptly communicate the information required, giving assurance over the correctness and truthfulness of the information provided, or pointing the parties that could provide the above-mentioned assurance;
- If useful to the information comprehension, ensure that the people in-charge of the various internal functions provide the documentation or other sources supporting them;
- Management and coordination of tax matters with the external chartered accountants' professional studio (in-charge for the draft of the annual financial statements, tax computation and related declarations, as well as VAT declarations), as well as management of the relevant tax documentation provided to the above-mentioned studio;
- Support and help the Sole Statutory Auditor in-charge with financial statements' audit;
- Tax payments upon Directors' approval.

Accounting documents archival

In carrying out the activities included in this process, the following crimes can be committed:

- *Hiding or destruction of accounting documents pursuant to article 10 of Legislative Decree no. 74 of 2000*

Kardia implements specific operating protocols for data and information management in order to grant the correct and complete execution of activities and that not any activity different or further from the authorized ones is carried out, including regular back-ups to reduce the risk of data loss.

A specific procedure is adopted to use IT systems, including the assignment and management of access credentials, and the access to the Company's IT systems, allowed only to authorized employees according to their duties.

As pertains accounting documents archival, Kardia implemented specific procedures for the regular archival and storage of accounting documentation for statutory and tax purposes, in order to prevent their hiding or destruction and to grant the process transparency.

Inventory's management

In carrying out the activities included in this process, the following crimes can be committed:

- Fraud subtraction of due tax payments pursuant to article 11 of Legislative Decree no. 74 of 2000

Kardia implemented specific operating procedure to manage inventory accounting, including, among other aspects, the following:

- Use of IT systems to manage the inbound and outgoing logistics flows traceability;
- Regular inventory counts to verify the match between accounting and physical quantities in stock, as well as analysis of any variance;
- Documentation and authorization of inventory variances adjustments;
- Setting of criteria to identify stocks to sell or dispose;
- Setting of criteria for inventory evaluation and related accounting entries;
- Regular control of the correct posting and update of supporting inventory entries imposed by tax law;
- Regular monitoring of communications imposed by statutory and tax law related to the places where activities take place.

Human Resources

In carrying out the activities included in this process, the following crimes can be committed:

- Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000

As pertains the management of human resources, Kardia implements specific operating procedures, including, among other aspects, the following:

- Creation and management of employees' data registry;
- Authorization to holidays and overtime requests;
- Authorization to wages payment, as well as the match control between payments made and payslips;
- Assignment and communication of reasonable performance goals, balanced according to a previously established authorization process;
- Nature and amounts limit of expenses allowed to be reimbursed;
- Reporting rules for expenses incurred, with indication of the aim of the expenses;
- Controls over the expenses incurred by employees and Directors and over the related supporting documentation;
- Approval methods of expenses reports and consequent reimbursement.

Intercompany transactions

Kardia is subject to Asahi Intecc Co. Ltd's (listed company on the Tokyo Stock Exchange which implemented its own Ethics Code) management and coordination activities.

Crimes pertaining this process that could be committed are the following:

- Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000;
- Fraud statements through other mechanisms pursuant to article 3 of Legislative Decree no. 74 of 2000;

- Issue of non-existent transactions' invoices or other documents pursuant to article 8, paragraphs 1 and 2-bis of Legislative Decree no. 74 of 2000.

As pertains intercompany transactions, Kardia implemented specific operating procedures, including, among other aspects, the following:

- Ruling the intercompany transactions through specific formal agreements (contracts or e-mails) and detailed definition of processes related to accounting transactions among the Group companies;
- Involving the external chartered accountants' studio when needed during the operations definition and during the execution stages, in order to grant that the operations comply with the tax law in force;
- Keeping the documentation supporting the different transactions and, in particular, the documentation proving the transactions' effectiveness;
- Regular controls over economic and financial balances.

Relationships with Judicial and Financial Authorities

Crimes pertaining this process that could be committed are the following:

- Fraud statement through non-existent transactions invoices or other documents pursuant to article 2, paragraphs 1 and 2.bis of Legislative Decree no. 74 of 2000;
- Fraud statements through other mechanisms pursuant to article 3 of Legislative Decree no. 74 of 2000;
- Hiding or destruction of accounting documents pursuant to article 10 of Legislative Decree no. 74 of 2000;
- Fraud subtraction of due tax payments pursuant to article 11 of Legislative Decree no. 74 of 2000.

As pertains relationships with Judicial and Financial Authorities, Kardia implemented specific operating procedures, including, among other aspects, the following:

- Identification of parties authorized to have relationships with Public Administrations;
- Identification of parties in-charge of activities and controls related to the management of relationships with Public Officials during their inspections and to sending documents;
- Establish criteria to equip Public Officials with adequate structures (segregated offices, network accesses, hardware) and to provide them with Company's documentation;
- Formalize through information reports the subject of Tax Authorities' inspections;
- Identification of a lawyer/consultant/professional supporting the Company, if needed.
- Definition of actions to perform, given the nature, matter and value of the legal action, and the related authorization and communication levels.

9. COMMUNICATION FLOWS TO THE SUPERVISORY BOARD

Following Legislative Decree no. 24 of 2023, Kardia implemented some specific internal reporting channels able to ensure, also through encryption, privacy for the identity of the whistleblower, and the people involved or mentioned in the report, as well as what the report is about and the related documents.

Therefore, we state in this Model:

- That we protect the whistleblower from any form or retaliation or discrimination;
- Disciplinary sanctions will be imposed to everyone who violates whistleblowers' protection measures or who submits clearly false reports.

Reports can be submitted in writing, also through IT instruments, or verbally (through phone, vocal messages, or, upon whistleblowers' request, through a personal meeting scheduled by a reasonable timing).

In particular, reports can be submitted by employees, freelance, contributors, professionals and consultants, volunteers and interns, paid and not paid, shareholders and people with administrative, managing, control, monitoring and (merely) representing roles.

It is forbidden to enact retaliation or discrimination measures, both direct and indirect, to the whistleblower for reasons directly or indirectly related to the report, in compliance with Legislative Decree no. 24 of 2023.

All retaliation or discrimination measures to the whistleblowers are null, including dismissal and change in duties. In case of legal causes related to sanctions imposed, demotions, dismissals, transfers, or any other organizational measure with negative effects, direct and indirect, on work conditions, happened after submitting a report, it is the Employer's responsibility to demonstrate that those measure are non-related to the report itself.

In order to ensure the correct management of reports submitted in compliance with Legislative Decree no. 24 of 2023, Kardia:

- Implemented the communication channels required;
- Identified who or which department will manage those channels, with proper training sessions for the employees involved;
- Adopted a specific procedure to manage the various steps of the process and the people involved duties;
- Took communication and awareness-raising initiatives through training sessions to all the employees about the goals of the whistleblowing system and the related use.

Information and the related documentation are kept according to art. 14 of the Legislative Decree no. 24 of 2023, that is for the time strictly necessary to manage the report for 5 years to the utmost since the communication of the final outcome of the report procedure, complying with all the secrecy provisions.

In case reports, information and/or news arise related to the relevant crimes to the Legislative Decree no. 231 of 2001 or any other topic related to violations of the Model and Ethics Code, the person in charge of managing the communication channel will have to immediately inform the Supervisory Board.

People in-charge or Directors inform in writing the Supervisory Board about the data included in the procedures or in the other instruments used to implement the Model, according to the timing and methods herein included.