ORGANISATION AND MANAGEMENT MANUAL FOR THE PREVENTION OF THE REGULATORY, ETHICAL AND CRIMINAL RISKS OF THE COMPANY **"SAMTACK S.L."**

Update approved by the Joint and Several Directors of the company at their meeting on 21/06/19

PURPOSE OF THIS MANUAL

The purpose of this manual is to establish a regulatory compliance programme, as a business organisation and management tool, to set out the regulatory risk control policies that emerge from the company's own organisational structure. It basically consists of a set of rules and procedures that make it possible to identify and prevent regulatory risks properly and to investigate and penalise possible illegal behaviour.

It is therefore a matter of establishing and consolidating a corporate culture of respect for ethical values and legal standards, the latter covering state and community regulatory provisions, international conventions signed and ratified by states, and recommendations, circulars, guides, standards and guidelines issued by national and international bodies.

Thus, as stated in Circular 1/2016 of the Attorney General's Office and the UNE 19601/2017, the organisation and management models are not intended to avoid criminal penalties for the company, to the effect that their mere existence is a kind of insurance against possible criminal actions, but to promote a corporate ethical culture that serves to significantly promote the elimination or, at least, the reduction of the risk of criminal or illicit behaviour. The case law of the Supreme Court also highlights this fact (STS 154/2016 of 29 February, 221/2016 of 16 March, among others).

Without prejudice to the above, there is no doubt that the availability of a good organisational and management model for the control of regulatory risks has unquestionable consequences for the possible criminal liability that a legal entity may face due to the criminal conduct of its directors, managers and employees.

For all these reasons, this updated regulatory compliance manual is being prepared and implemented in the company, replacing the previous versions.

***

1. OBJECTIVE AND SUBJECTIVE SCOPE OF THE MANUAL.

1.1. Objective scope and company identification

The company that carries out the work of implementing this corporate ethical and preventive model regarding the criminal liability of the legal person is "**SAMTACK, S.L.",** with Value Added Tax Identification Number (N.I.F.) **B-60529476**, and registered offices at C/ **Cerámica, nº 3, 08292-ESPARRAGUERA (Barcelona - Spain).**

1.2. Subjective scope

It is expressly established that this Manual shall apply to dependent employees and workers of the company now being studied, as well as to its directors and managers.

It shall also apply to customers, suppliers and business partners, and other entities and individuals who have a relationship with "SAMTACK S.L.", to the extent that it may affect them.

2. INTRODUCTION AND DEFINITION OF THE MODEL OF CORPORATE ETHICAL CULTURE AND CRIME PREVENTION. INTENTIONS OF REGULATORY COMPLIANCE.

The regulatory compliance and crime prevention programme to be implemented by the company has the specific function of establishing and consolidating a model of ethical culture in the company, as well as complying with the legal provisions set out in Article 2 of the Crime Prevention Act. 31a of the current Penal Code (Act 10/1995, of 23 November; hereinafter PC), according to the latest wording included in said Act, following the amendment made by Act 1/2015, of 30 March, modifying the PC, with a view to consolidating and promoting impeccable and excellent business ethics that help to exonerate the legal entity from any criminal liabilities arising from the actions of its staff.

The model to be implemented is therefore intended to comply strictly and formally with this ethical aspect, as well as with current criminal and sectoral legislation, demonstrating the company's express desire to meet these objectives through a specific body responsible for ensuring compliance with this organisational model. It will be defined and explained in the relevant section.

In addition to the irregularities that are contrary to the code of ethics and the regulatory compliance programme established, the organisational model to be implemented considers the offences in the specific part of the PC that may be committed by the individuals referred to in article 31a, identifying all the risks detected in the various departments of the company and in its production processes.

Nevertheless, given the corporate purpose of the company and its factual circumstances, emphasis is placed on the difficulty of predicting crime, since the possible number of situations and interpersonal relations is virtually unlimited. Furthermore, although article 31a. 2. of the PC establishes a more or less detailed breakdown of the actions and elements that exonerate, or where appropriate, attenuate the criminal liability of companies, this breakdown is of an essentially general nature as it introduces major programmatic principles, but without a

specific and individualised classification of the content of these elements, given the absence of implementing or accompanying regulations.

In view of this situation, the continuous development and permanent updating that will be carried out on this organisational model has the purpose of alleviating these shortcomings, as well as adding to it both the natural changes that occur in the company (with special emphasis on the ethical and social aspects involved), and those that are likely to generate new criminal risks. The case law doctrine that the Supreme Court draws up in the development of the institution will also be taken into consideration for updating.

3. PREVENTIVE PART.

3.1. Code of Ethics and company policies

3.1.1. Definition and purpose of this Code of Ethics

The "Code of Ethics" of "SAMTACK, S.L.", identifies and develops the ethical principles on which the company's activity is based, describing the behaviours to be promoted and the behaviours to be avoided.

The code of ethics is the most important regulatory instrument in the regulatory structure of the company. It represents the commitment of "SAMTACK, S.L." to comply with the laws and the ethical values defined. Thus, it aims to consolidate a demanding, high quality corporate ethical culture.

3.1.2. Objective and subjective scope of the Code of Ethics and the regulatory compliance system implemented

The code of ethics will be applicable to all activities carried out by the company regardless of their territorial scope of action.

Thus, it is very important to establish fair and correct guidelines for action in order to provide the company with the prestige and excellence it deserves.

The aim is not only to observe the legal regulations applicable to the company's activity, but also to respect the principles of transparency, correctness, strictness and reliability which are required of any legal entity operating in the market. Among such regulations, we would like to highlight the following: Royal Legislative Decree 1/2010, of 2 July, approving the Revised Text of the Corporate Act; Royal Decree, of 22 August 1885, by which the Commercial Code is published; Act 10/2010, of 28 April, on prevention of money laundering and financing of terrorism; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; General Tax Code 58/2003 of 17 December; Act 10/1995, of 23 November, on Criminal Code.

Although this code of ethics may contain general principles and instructions, it establishes precise rules for action, aimed at implementing the aforementioned corporate ethical culture, as well as preventing the occurrence of specific offences in relation to the activities carried out by the company.

As we have said, and now repeat, it extends to all the company's personnel: employees, members, workers, management positions, and even the company's directors and control bodies (the Supervisory Board of the Crime Prevention Model itself, as will be described later).

If possible, it will be extended to the company's suppliers, distributors, business partners and customers, in any commercial relations they may have, in all matters that may affect them.

3.1.3 General Principles

3.1.3.1. Code Compliance

The joint and several administrators, or where appropriate, the members of the board of directors of the company, undertake to comply with and enforce this code of ethics among all workers, members, employees and business partners of the company, in order to achieve a correct and demanding corporate ethical culture.

3.1.3.2. Objectivity, impartiality and transparency

The actions of the joint and several administrators, or, where appropriate, of the board of directors as an institution, or of each of its members, shall be governed by the principles of objectivity, impartiality, loyalty and transparency in their decisions.

The company is committed to maintaining an accounting, financial and fiscal policy in accordance with the guiding principles established in current legislation and, more specifically, in General Tax Code 58/2003 of 17 December and related regulations.

3.1.3.3. Autonomy and independence

The joint and several administrators, or where appropriate, the members of the board of directors, shall have autonomy and independence. In compliance with this code of ethics, they shall act in accordance with the decision-making formulas set out in the company's bylaws and in the law. In the event of a conflict of interest, whether direct or indirect, they shall refrain from acting and shall inform the other administrators, or the board of directors, of this circumstance before the board takes any decision in this respect.

Like the administrators, all the employees of the company, whatever the administrative or labour regime that links them to the company, are obliged to avoid situations that could generate any commercial or mercantile conflict of interest with the company.

With the intention of avoiding possible conflicts of interest, the company will ask its employees at the time of admission for a sworn statement with the express commitment to behave in a manner that does not harm in any way the expectations of the company, its third party contractors and its other collaborators.

3.1.3.4. Competitive practices on the market

The professional ethical standards and ethical codes that must be observed in each case shall govern the hiring of clients, suppliers and professionals of all kinds. In this way, the relations that arise will be guided by the mercantile standards of correctness, professionalism, transparency and loyalty, and any type of obscurantist and controversial dealings, relations or behaviour that is undesirable from a professional and mercantile point of view shall be prohibited.

The company will be free to choose such clients and suppliers, taking into account their legitimate social and commercial aspirations, but without disregarding the

reliability, competence and quality of the service they may offer, as well as the correctness of the personal, professional and commercial relations that may be established at any given time.

For the contracting of suppliers and the choice of clients, attention will be paid to their correct procedure, good commercial practices and trade and business good faith.

3.1.3.5. Social and environmental commitment

The company will promote specific policies in environmental matters. It will pay special attention to the legislation in force in this area, and more specifically, to the following regulations: Act 11/2014, of 3 July, amending Act 26/2007, of 23 October, on Environmental Responsibility; Royal Decree 1015/2013, of 20 December, amending the Annexes I, II and V of Act 42/2007, of 13 December, on Natural Heritage and Biodiversity, Act 11/2012, of 19 December, on Urgent Environmental Measures; Royal Decree-Law 17/2012, of 4 May, on Urgent Environmental Measures; Royal Decree 815/2013, of 18 October, approving the Regulation on Industrial Emissions and implementation of Act 16/2002, of 1 July, on Integrated Prevention and Control of Pollution; Act 5/2013, of 11 June, amending Act 16/2002, of 1 July, on integrated pollution prevention and control and Act 22/2011, of 28 July, on waste and soil pollution; Royal Decree 97/2014, of 14 February, regulating Transport Operations of Dangerous Goods by Road in Spanish Territory; ADR**:** European agreement on the international transport of dangerous goods by road, concluded in Geneva, on 30 December 1957 and their amended versions.

3.1.3.6. Supervisory and control body of the code of ethics and model established

The company will have an autonomous management body in charge of the control and surveillance of any irregular actions of the company, which will be called "Supervisory Board of the Crime Prevention Model" (hereinafter CSMPD). It will be granted managerial, organisational, supervisory, corrective and disciplinary functions in its field of action. It will enjoy total independence and autonomy in the performance of its functions.

The advisory lawyer is responsible for advising the CSMPD at all times. He or she is responsible for directing the research and analysis of criminal offences. He or she will present the conclusions of this work to the CSMPD and, finally, will propose the relevant actions, both in the legal and disciplinary framework.

3.1.3.7. Confidentiality

All company staff, regardless of their rank and function, shall be governed at all times by the principle of confidentiality in the handling of the classified information obtained in the performance of their functions. Likewise, they shall refrain from using it for any spurious, arbitrary purposes or in their own interest.

In any event, the directors and managers of the company shall guarantee the confidentiality of the personal data of its employees, processing them and maintaining their secrecy in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and using them only for the work and

professional purposes for which they were registered.

In the same way, the reserved information that any worker of the company may become aware of, shall be handled with the utmost discretion and caution, acting at all times in accordance with the stipulations established in the aforementioned regulations.

Such discretion and caution shall also be applied to any dealings and relationships that may be established with competitors; the requirement shall also be extended to the company's customers and suppliers.

Any worker linked to the company and in possession of sensitive data covered by the aforementioned European Regulation shall immediately and reliably inform the company's directors, who shall then inform the Chairman of the CSMPD. In any event, the worker shall abstain from using or transferring such data to third parties.

Following their analysis, the CSMPD shall inform the directors of the correct procedure to be followed, which shall be transferred to the worker concerned.

Any clients and suppliers that may have knowledge of protected data on company workers shall be required to proceed in accordance with the aforementioned (EU) Regulation. The directors shall inform them of this fact immediately and in a reliable manner, requiring them to cancel the corresponding entry in their internal records.

"SAMTACK S.L." shall act in the same way regarding any protected data it may have regarding its clients and suppliers.

3.1.4. Commitments to responsible conduct and practices

3.1.4.1. Competence and capacity

The joint and several administrators, or where appropriate, members of the board of directors, shall at all times possess the knowledge and skills necessary to carry out their management duties competently and appropriately. They shall therefore have the necessary technical training to carry out their duties according to the nature, complexity and importance of the functions to be performed.

3.1.4.2. Immediacy of actions

The joint and several administrators, or where appropriate, the members of the board of directors, shall carry out their functions with the immediacy and speed required by their actions and decisions. They shall therefore take into account factors of urgency, priority and specificity in the performance of their corporate activities.

3.1.4.3. Action in the event of risks

The CSMPD shall identify the risks and critical or controversial points that might arise during the company's operations, with a view to guaranteeing corrective actions and the appropriate responses in the event of the actual occurrence of such contingencies. In this way, it will be responsible for the implementation within the company of the protocols and internal control systems required to allow for the efficiency, functionality and operability of the company.

The directors declare their agreement with the functions assumed by the CSMPD and expressly state their intention to fulfil the tasks of supervision, surveillance

and control contained in this organisational model.

Such internal control systems shall be specific to the different risk fields or sectors that may entail liability for the company in all spheres, and especially in civil and criminal work. In this way, these control systems shall include risk prevention models in the fields susceptible to corporate responsibility, which shall be included in the action protocols for their avoidance, and the company's appropriate response systems in the event of their effective occurrence.

3.1.4.4. Recruitment and promotion

The company's main corporate function is to achieve and maintain a homogeneous and qualified human group that makes it possible to achieve the proposed commercial goals in a correct and satisfactory manner. Therefore, in the process of joining and being promoted in the company, the principles of merit, competence, and equal opportunities shall prevail, without allowing discrimination of any kind for reasons of sex, age, race, ethnicity, religion, ideology, beliefs, nationality, sexual orientation or identity, illness or disability.

The company shall also guarantee a transparent system of rewards, promotions, responsibilities and participation in its corporate activity, which is totally transparent and in no way arbitrary.

3.1.4.5. Training and qualification

The company shall at all times ensure that its staff, whether at the beginning of their working relationships or during the course thereof, receive the information and specific training necessary to carry out their duties safely and correctly. The training system shall be continuous and shall be adapted to any new corporate circumstances and technical innovations that may arise in the company.

The company shall assign the necessary economic resources to the training and information system for the workers in an efficient and productive way.

3.1.4.6. Human relations

The company shall promote at all times a regime of polite, loyal and professional personal relationships, avoiding incorrect and derogatory statements and behaviour among its members. Attitudes and behaviours that undermine the dignity, honour or self-esteem, whether personal or professional, of its employees and other personnel linked to the company will not be tolerated.

3.1.4.7. Company relations; directors, managers and employees with authorities and officials

With regard to recruitment and personal relations maintained by the company's staff with authorities and officials, the principles of respect, transparency, loyalty and excellence, contained in the previous sections, shall be observed.

3.1.4.8. Workplace

The company shall guarantee a safe and healthy physical environment for all workers, taking the appropriate measures according to the circumstances of each of its different departments.

3.1.4.9. Efficient use of the company's assets, services and technologies for exclusively business purposes

All material assets of the company shall be used in a responsible and sustainable manner solely for the purposes they are intended for, always for the fulfilment of the company's corporate purpose.

3.1.4.10. On the acceptance and offer of gifts, donations, benefits and hospitality

All personnel linked to the company, in the exercise of their legal or statutory functions, shall abstain from receiving, requesting or accepting gifts, handouts, benefits or advantages of any kind whose objective is a commercial or trade consideration, all this in the manner stipulated in the specific protocols of the company.

The same control measures shall be applied in the case of payments to facilitate or speed up procedures.

3.1.4.11. Intellectual and Industrial Property Rights Protection

The company undertakes to strictly respect any work, creation or service, of whatever kind, that has generated intellectual property rights, if it does not have the authorisation of the holders of the respective rights, or of their assignees. In its combat protocols, it shall establish the guidelines to be followed by all company personnel in order to respect the rights now being addressed.

This shall also apply to objects, procedures and trademarks that are subject to industrial property protection or are registered with the patent and trademark office.

3.1.4.12. Periodic audits

The company renews its commitment (as it has done historically) to continue with the system of annual audits.

3.1.4.13. Due diligence procedures

In the case of trade relations with third parties involving any kind of economic transactions, the relevant information and tax documentation accrediting the business integrity of the company shall be requested. The preventive protocols shall establish the guidelines and requirements for the observance of such due diligence.

In the transport and handling of the goods (due to their hazardous nature), strict control and monitoring of the conditions referred to in the special legislation mentioned above shall be observed, and these shall be set out in detail in the applicable protocol.

3.1.4.14. Channels for complaints and internal investigations

The company provides a channel for complaints so that any manager, employee, worker or member of the company who has knowledge of any practice contrary to the code of ethics, the system of regulatory compliance or the law, by any member of the company, can proceed to report it, in the manner and form that is set out in point 4.1. of the manual.

It also establishes a protocol for internal investigations, aimed at the investigation

of possible irregularities. This is described in point 4.1.2 of the manual.

3.1.4.15. Ways of disseminating the code of ethics

The joint and several administrators of the company, or where appropriate, the board of directors, shall communicate the existence of this code of ethics to the entire staff through the internal dissemination system that they consider most appropriate. Likewise, they shall inform the Works Council, should there be one at any time, of its existence, for their own knowledge and as an additional information dissemination channel for the rest of the staff.

3.1.4.16. Legal compliance

The joint and several administrators, or where appropriate, the members of the board of directors, shall carry out their functions observing and respecting at all times the principles and duties applicable to directors according to civil, commercial, labour, criminal and tax legislation. In particular, they shall respect and observe the following regulations; especially, the following regulations; Royal Legislative Decree 1/2010, of 2 July, approving the Revised Text of the Corporate Act; Royal Decree, of 22 August 1885, by which the Commercial Code is published; Act 10/2010, of 28 April, on prevention of money laundering and financing of terrorism; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; General Tax Code 58/2003 of 17 December; Act 23/2006, of 7 July, amending the Revised Text of the Copyright Act , approved by Royal Legislative Decree 1/1996, of 12 April; Royal Legislative Decree 2/2015, of 23 October, approving the Revised Text of the Workers' Statute Act; Royal Legislative Decree 8/2015, of 30 October, approving the Revised Text of the General Social Security Act; Act 10/1995, of 23 November, on Criminal Code.

3.2. THE RISK ASSESSMENT

3.2.1. Identification and risk analysis. Organisational structure of the company.

As already stated in point 1.1., the company “SAMTACK, S.L.”, with Value Added Tax Identification Number (N.I.F.) B-60529476, located and registered offices at C/ Cerámica, nº 3, 08292-ESPARRAGUERA, is the company that carries out the implementation of this regulatory system of compliance.

This company was incorporated on 21 March 1994, under the initial name of “SAMTACK, SOCIEDAD LIMITADA”, through a Public Deed executed before the Notary of Barcelona, MODESTO VENTURA BENAGES, under number 1268/94 of his notarial record, its current corporate purpose, as established in its own bylaws, being the manufacture of all kinds of glues, including synthetic glues, hot melts, gelatines, varnishes and all kinds of auxiliary products for the leather and rubber industry.

For the rest of the corporate references, we refer to the aforementioned public deed.

The company has no business partners.

The company currently has a direct workforce of 22 workers, who provide their labour services at the facilities of C/ Cerámica nº 3, 08292-ESPARRAGUERA. The

company is basically divided into five working or professional departments; Direction-Management, Administration, Production, Laboratory and Sales.

The **"Direction-Management Department"** of the company is the Board of Directors, which is included and described in the bylaws contained in the aforementioned notarial deed dated 21 March 1994.

Thus, the general management of the company is entrusted to the Board of Directors, which is made up of four members; a chairman, a secretary and two board members, who carry out their functions according to the specifications of the Bylaws and applicable legal regulations. Such positions are currently held by:

- Chairman: Mr. EUDALD MAS BORSOT
- Secretary: Mr. EUDALD MAS ORTAS
- Board member: Mr. ALBERT MAS ORTAS
- Board member: Ms. GEMMA MAS ORTAS

This body is responsible for taking all the important decisions of "SAMTACK, S.L.". The Board of Directors, as the supreme management body, is responsible for the following tasks:

- Strategic management of the company.
- Planning, organisation, management and corporate control policies of the company.
- Preparation and development of long-term plans
- Command and authority over the rest of the company's departments.

The Board of Directors carries out the functions of management and administration according to the stipulations contained in the Bylaws and as established in all other regulations in force. It meets sporadically, with no set agenda, and deals with all issues of general interest to the company in its various areas of operation.

It should be noted that, both because of its characteristic configuration and because of the real possibilities of action, the risk of occurrence of most of the possible crimes that may occur within the scope of the company is linked to possible actions carried out by its directors.

The **"Administration Department"** is under the direct responsibility of Ms. GEMMA MAS ORTAS, who is in charge of four workers. This department is responsible for the following tasks or specific business processes:

1.- Sales Management Process of the company. Once the clients and suppliers have been acquired by the management of the company, or by its three salespersons (GEMA MARTÍNEZ GAMARRA, JORDI GONZÁLEZ LÓPEZ and JUAN JOSÉ BERNAT COVES), the department is responsible for the following tasks;

- Initial registration of these contracts as clients or suppliers, as the case may be.
- Registration of incoming and outgoing products.
- Communication with clients and suppliers regarding the status of the service.
- Dealing with them for the subsequent hiring of specific services.

These processes and tasks are carried out jointly and individually, under the

supervision of Ms. GEMMA MAS ORTAS, by each of the four members of the department, all of whom are equally qualified to carry out these tasks.

2.- Accounting process, consisting of the handling of all the tasks associated with the recording of entries in the company's cash books;

- Issuing and registering customer and supplier invoices.
- Creation of Excel sheets with all types of accounting entries.
- Preparation of the Journal, General Ledger, Inventory and Balance Sheet Book, and Operations Record Tax Book.

Tax forms, such as those for Corporate Tax, VAT and declarations of withholdings to professionals and workers, are drafted physically by the economic consultancy that will be referred to later.

3.- Bureaucratic and Office Management Process of the company, such as:

- Communication and customer service.
- Management of goods transport
- Logistics.

The company has outsourced certain management services to specialised companies that carry out the following support tasks, related to the general administration of the company:

- The agency "UNIGEST, S.A.L." performs the following labour services: preparation of payroll and social security for the company's staff; processing of dismissals; formalisation of employment contracts; relations with public administrations; management of leave, holidays, overtime and sick leave; absenteeism control; and disciplinary proceedings; payment of salaries; occupational risk prevention;
- Mr. EDUARD QUEIRÓS VILLANUEVA is responsible for economic and financial advice and other related functions.
- The company "NG SOFT, S.L." is responsible for the management and maintenance of the operating systems, networks and servers of the company, and in general, for all the tasks related to the management of Information and Communication Technologies (ICT): installation and updates of software and hardware, computer tools that process, store, summarise, retrieve and present information, etc.
- The company "ISERN PATENTES Y MARCAS, S.L." is responsible for the management and updating of the company's brands and patents.

The "**Production Department**" is under the direct responsibility of Mr. CARLOS PEÑALVER BERNAL, Operation Manager, and Mr. JOSÉ ANTONIO ALBIOL, Warehouse Manager, who are in charge of eight workers. This department is responsible for the following specific business tasks:

- Manufacture of the final product from the materials and products received from the different suppliers.
- Physical reception of these materials and products.
- Storage in the respective company warehouses and stores.
- Internal transport of materials;
- Manufacture of the product from various production lines.

The manufacture of the product is carried out through the following production

lines; a hotmelt line with three product outlets, an aqueous dispersion line with three other presentation outlets, two sealant lines and two UV varnish lines. 60% of the production is made in the aqueous dispersion line.

In the manufacturing processes of some products, certain acrylic dispersions are used which remain adhered to the final product and which consist of disposable plastic bags for dispensing food, such as: crisps, rinds, snacks and other appetisers. They are also manufactured plasticised or laminated on printed paper. These products are subjected to significant chemical migration tests to check for possible contamination or transfer to the foods they contain, given the danger to human health as the chemicals are harmful to the body. These tests analyse the results obtained from such migrations depending on the type of chemical used and the time the food product is packaged.

These tests are carried out periodically or every time there is a change in the chemical bonding material, by a person from the company stationed at the laboratory of the University of Zaragoza. This university issues the relevant certificate of suitability.

The **"Laboratory Department"** is under the direct responsibility of Mr. FERRAN PRATS LLADÓ, who is in charge of six workers; one at the University of Saragossa and five at the Esparraguera centre. This department is responsible for the following specific business tasks:

- Processes of research, testing and analysis of the elements, substances and materials that the company uses in the manufacture of its final products.
- Analysis of the finished product to check whether it meets all the legal requirements and purposes it is intended to achieve. Specifically, it analyses the aforementioned migration or transfer processes of the elements and substances found in the container products to the products finally contained.

The **"Sales Department"** has no specific manager, all its members reporting directly to the management of the company. It is made up of three people; GEMA MARTÍNEZ GAMARRA, JORDI GONZÁLEZ LÓPEZ and
D. JUAN JOSÉ BERNAT COVES, all of them hired under the general social security system.

The functions performed by these workers are the same as those of any salesperson, i.e:

- Searching for, attracting and dealing with the company's customers and suppliers of all kinds.
- Preserving or replacing them, depending on the interests of the company.

Their territorial scope is basically national, but they also carry out some activity in France.

All the company's employment policies depend on the Board of Directors, which establishes the recruitment and selection criteria based on the principles of merit and aptitude according to verified professional CVs and interviews with pre-selected candidates. Training is provided by the heads of the departments of which the recruited worker is a member. This training is also complemented by the specialised training courses given by the professionals of the mutual insurance company and by the occupational risk prevention company.

Wage policy, promotions, economic incentives and environmental working conditions also depend on the company's management body, although so far they have not undergone much development due to the company's great job stability. Salaries are set, upwards, by the tables established in the company's labour agreement referred to below, while the few promotions that may be considered are granted to the personnel of the department affected by the variation, according to criteria of competence and seniority in the job.

From now on, all labour, salary, promotion, and incentive policies, as well as aspects related to environmental conditions, will be governed by the principles established in the Code of Ethics, sections 3.1.4.4 to 3.1.4.8.

The company does not comply with the criteria stated by Royal Decree 1514/2007, of 16 November, approving the General Accounting Plan, and by Royal Legislative Decree 1/2010, of 2 July, approving the revised text of the Corporate Act, for the presentation of the profit and loss statement in its abbreviated form, its presentation being the ordinary or normal one.

The company is a member of the "Petita i Mitjana Empresa de Catalunya" (Small and Medium-Sized Enterprises of Catalonia, PIMEC) and the "Asociación Española de Fabricantes de Colas y Adhesivos" (Spanish Association of Glue and Adhesive Manufacturers, ASEFCA) and the "Convenio Colectivo General de la Industria Química" (General Collective Bargaining Agreement for the Chemical Industry) (hereinafter CCGIQ), whose latest approval was published in the Official State Gazette on 19 August 2015, in accordance with the Resolution of 3 August 2016 of the Directorate General of Employment of the Ministry of Employment and Social Security.

3.2.1.1 Company objectives and business activities.

The company's objective is to achieve maximum economic profitability by optimising its human and material resources, always in compliance with the applicable regulations and the code of ethics established in this document.

3.2.1.2. External and internal context of the company

The business activity of "SAMTACK, S.L." consists basically of the manufacture of all kinds of glues, gelatines, varnishes and other auxiliary products for the leather and rubber industry.

The main applicable regulatory framework are the EU European Regulations 10/2011 and 1935/2004 "On plastic materials and articles intended to come into contact with food".

In the framework of its activity "SAMTACK, S.L." is particularly prone to generate risks to natural persons who consume food contained in packages or bags to which the company has added adhesive substances. The adhesive substances that "SAMTACK, S.L." applies to such product containers are in indirect (but extremely close; separated by microns) contact with the food products that are finally sold by the client companies of "SAMTACK, S.L.". Therefore, although remote, in the checks performed, a certain risk of intoxication or poisoning by ingestion of these substances is observed.

Contractual relations with customers, suppliers, service providers, and other legal and natural persons are carried out by virtue of the appropriate specific contracts,

which stipulate and specify the entire scope of the business relationship between the parties.

In the daily course of business operations, there are usually no interactions of any kind with public authorities and entrepreneurs, and when there are, these are limited to the few technical inspections that may occur, and any licence applications or updates that may be required by the business.

As mentioned above, the company does not have an IT department, but the management and maintenance of the company's operating systems, networks and servers are carried out by the company "NG SOFT, S.L.".

The company uses advanced systems and applications to automatically capture data from its customers and suppliers, in case of voluntary supply thereof. In the performance of their tasks, the different workers of the company use the necessary technical computer means to carry them out; In this way, they make regular use of landline and mobile phones, computers, e-mails, SMS, etc.

The company has never been charged with any crime, nor has it been declared civilly liable for any criminal act.

3.2.1.3. Previously existing controls in the company

Prior to the implementation of this regulatory system, the company did not have any guided or protocolised controls implemented to prevent crimes or irregular situations. It just had a CCTV system installed in the places where the operations tasks were carried out, more for the control of possible intruders than to supervise the correct professional performance of the workers.

Normally, the communications of incidents or anomalies of any type were of a verbal nature, being made between the people involved in them or aware of them, and the heads of department or directors of the company.

In any event, throughout the history of the company, no controversial episode has taken place involving the personnel of the different departments that might be of criminal relevance or typically associated with any of the offences for which legal entities are criminally liable.

3.2.1.4. Risk Analyses. Identification of risks and sources of the regulatory system.

In order to follow a suitable methodology in the handling of the matter, a breakdown is made of the activities or processes undertaken by each department of the company, in order to subsequently establish a risk map according to the activity carried out by these departments with regard to these processes and weighting these criminal risks according to their possible commission with the values high, high-medium, medium, medium-low or low.

The risks analysed relate both to possible administrative or labour irregularities, or those that violate, in any event, the company's code of ethics and this regulatory compliance system, and to possible criminal offences. Possible criminal offences refer to the commission of both specific crimes, due to the business model and the specific activity of the company, and common crimes, which can affect any commercial legal entity due to the simple fact of operating in the market.

Likewise, the risks observed take into account the possible unlawful behaviour of natural persons, from the different forms of criminal participation admitted by the

connecting factor. Taking into account the possible concurrence of "specific offences" and the possible extension to *extraneous* participants, the following points are included and clarified:

i) Natural persons, administrators, directors or employees, who commit a common crime will be the perpetrators of that unlawful behaviour, which will constitute the connecting factor for the legal person, provided that the rest of the requirements established in art. 31a et seq. of the Penal Code are met.

ii) The directors and managers of the legal person will also be the perpetrators of the "special offence" they commit, in accordance with the provisions of Article 31 of the Penal Code, without prejudice to the fact that this unlawful behaviour is the connecting factor for the legal person, provided that the rest of the requirements established in art. 31a et seq. of the Penal Code are met.

iii) Members and employees of the company who are not directors or managers (i.e. de facto or de jure managers or legal or voluntary representatives of the legal person) may not be perpetrators a specific offence. However, they may be liable for inducement or necessary cooperation, but never as accomplices, in the unlawful conduct of the suitable perpetrator, the latter being the connecting factor for the legal person.

iv) Directors and managers who do not fulfil their duties of supervision, monitoring and control of the activities of their employees, art. 31a.1(b), may possibly be liable for unlawful conduct that does not comply with, or even violates, art. 31a.(a), which may constitute the connecting factor for the legal person, without prejudice to any other characteristic conduct.

It should also be made clear that, in general terms, in order for unlawful behaviour or a connecting factor to occur, it will be necessary for the natural person acting to do so on behalf of the company, and for the direct or indirect benefit of the company. Notwithstanding the foregoing, on the understanding that a good regulatory compliance system must be more geared towards ensuring a corporate ethical culture than towards crime prevention, some considerations and obligations are established in cases where the natural person acts substantially for his or her own benefit, or they commit an irregular act that does not constitute a crime.

Purely by way of explanation, the general catalogue of crimes that may be committed by the legal person "SAMTACK, S.L." is established, such crimes being the consequence of previous unlawful acts carried out by the company's natural persons. However, as mentioned above, their handling is systematised in a broken down and analytical way by departments and management processes.

The following is a general catalogue of crimes that may be committed by the different workers of the company's departments in their different characteristic forms and those derived from them that may be attributed to the company itself:

- Crimes against privacy and computer trespassing: Articles 197, 197(a), 197(b) of the PC (natural person), in relation to Article 197(d) of the PC (legal person).
- Swindles and frauds: Articles 248.1, 2.(a) and (c), 249 and 250.1.(2), (3), (4), (5) and (6) of the PC (natural person), in relation to Article 251a of

the PC (legal person).

- Computer damage (Article 264 of the PC): Article 264.1 of the PC (natural person), in relation to Article 264(c) of the PC (legal person).
- Crimes against intellectual and industrial property, the market and consumers: Articles 278.1 and 286(a), (1) and (2) of the PC (natural person), in relation to Article 288 of the PC (legal person).
- Money laundering: Article 301 of the PC (natural person), in relation to Article 302(2) of the PC (legal person).
- Crimes against the Public Treasury and the Social Security: Articles 305, 307 and 307(b) of the PC (natural person), in relation to Article 310(a) of the PC (legal person).
- Crimes against Public Health: Articles 359, 360, 364.1, 365 of the PC (natural person), in relation to Article 366 of the PC (legal person).
- Crimes against Public Health: related to trafficking in toxic drugs, narcotics or psychotropic substances: Articles 368 and 369 of the PC (natural person), in relation to Article 369(a) of the PC (legal person)
- Crime of smuggling in Article 2 of Act 12/1995, of 12 December, on the Prevention of Smuggling.
- Crimes of smuggling of legal goods in its different forms in Article 2.1 (a), (b), (c) and (d) (natural persons), and 2.6 (legal persons) of Act 12/1995, of 12 December, on the Prevention of Smuggling.

Although consideration has been given to the possible commission of certain offences whose execution by any of the natural persons referred to in section 31a may entail liability for legal persons, this is initially ruled out, as it is totally unimaginable that they could be committed.

This is the case of art. 284 of the PC relating to the market and consumers, the commission of which is ruled out in all its forms, given that it is unimaginable that any worker of the company could use violence, threats or deception to try to alter the prices that would result from the free competition of products, merchandise, securities and other financial instruments, services and any other movable or immovable item, given the company's activity as a wholesaler positioned and consolidated in the market.

As for the offence under Article 286 3), it is also impossible to commit it a priori, since the possibility of corrupting a public official by offering, promising or granting any benefit or advantage is inconceivable, given the scant, if not non-existent, relationship with those authorities, since dealings with them are limited to purely administrative formalities.

After assessing the possibilities of commission of the offences referred to in Articles 424 and 429 of the PC, in relation to active bribery and influence peddling, it is concluded that there are no such possibilities, since, as has already been said, the relationship with civil servants or public authorities is virtually non-existent, being limited solely and exclusively to purely administrative procedures.

Nor are there any possibilities of committing the environmental crimes of sections 325 and 326 of the Penal Code, since the company's waste is minimal, and its

transport or disposal is entrusted to specialised companies.

As for the remaining infringements or irregularities affecting the code of ethics or the regulatory compliance system, the following methodology has been used for their handling and presentation, and for ruling out possibilities: the relevant legislation has been analysed and compared with the probabilities of risks in light of the specific circumstances of the case; the company's internal documentation has been analysed; the history of infringements has been reviewed; security inspections have been carried out and any records and background information that may have existed have been taken into account; the audit analysis has been carried out; interviews with directors, senior management and other company personnel have been taken into account; specialised software for data collection and mapping of identified regulatory risks have been taken into account.

Without prejudice to the possible crimes that may be committed and which are included in the risk map provided for this purpose, we now point out the violations of the code and the regulatory compliance system which this manual includes and which may be committed by any of the company's personnel, regardless of the department to which they belong.

Such infringements are typified and penalised in the disciplinary code included in this manual, following the list of offences.

Specifically, the following are prohibited:

a) Any action of any kind that violates the principles of impartiality and transparency.
b) Actions by company personnel that may generate a conflict of interest with the company's corporate purpose.
c) The violation of commercial standards of professional correctness, transparency and loyalty, in the processes of hiring suppliers, other professionals and in relation to customers.
d) The violation of any environmental commitment imposed by the company in compliance with the legislation on the subject, indicated in section 4.1.3.5.
e) The violation of the principles of confidentiality, in the exercise of the functions assigned to the workers who have a relationship with the company.
f) Violation of the duties of promptness in professional and/or business actions.
g) Non-observance of the principles of merit, competence and equal opportunities in the hiring of personnel.
h) Non-observance of transparency criteria when establishing rewards, promotions, responsibilities and participation in corporate activity.
i) Improper use of the company's assets, services and technologies, other than for exclusively business purposes.
j) Internal or external actions aimed at discrediting the company, its managers, workers, customers, suppliers and professionals, and all those third parties who have a relationship with the company.
k) Internal or external actions, aimed at discrediting the company, with regard to its working methods; objectives and structural organisation.

3.2.2. Risk estimation and assessment

Prior to the risk analysis by department, the risk estimation system is established, in accordance with the following parameters:

HIGH

MEDIUM-HIGH

MEDIUM

MEDIUM-LOW

LOW

These parameters are established according to the possibilities the crime actually being committed, the existing historical background, the possible scope and harmful consequences of the offence, and the possibilities of repairing the damage caused.

Once again, it is stressed that the list of crimes covers those considered possible, at this moment, according to the risk assessment carried out, and that other forms of crime cannot be ruled out, even if at this moment they are not seen as probable.

Should they be seen as possible in the future, they would be added to the table with their references of probability and level of commission.

Department	Risk	Probability	Level
Dir/Management	1) Crime of discovery and disclosure of secrets in Articles 197, 197(a) and 197(b) of the PC	Remote	Low
	2) Crime of fraud in Article 248, 249 and 250(1) of the PC	Remote	Low
	3) Crime of computer damage in Article 264.(1), 264a.(1) and 264b of the PC	Small	Medium-Low
	4) Crime of discovery and disclosure of company secrets in Article 278(1) of the PC	Remote	Low
	5) Crime of business corruption in Article 286a (1) and (2) of the PC	Small	Medium-Low
	6) Crime of money laundering in Article 301 of the PC	Remote	Low
	7) Crime against the Public Treasury in Article 305 of the PC	Remote	Low
	8) Crime against the Social Security in Article 307 of the PC	Remote	Low
	9) Crime against the Social Security in Article 307(b) of the PC	Small	Medium-Low
	10) Crime of smuggling of goods	Remote	Low
Administration	1) Crime of discovery and disclosure of company secrets in Article 278(1) of the PC (P. Sales Management)	Remote	Low
	2) Crime of business corruption in Article 286a (1) and (2) of the PC (P. Sales Management)	Remote	Low
	3) Crime of fraud in Article 248, 249 and 250(1) of the PC (P. Accounting)	Remote	Low
	4) Crime against the Public Treasury in Article 305 of the PC (P. Accounting)	Remote	Low
	5) Crime against the Social Security in Article 307 of the PC (P. Accounting)	Remote	Low
	6) Crime of discovery and disclosure of secrets, Articles 197, 197(a) and 197(b) of the PC (P. Bureaucratic and Office Management)	Small	Medium-Low
	7) Crime of computer damage in Article 264.(1), 264a.(1) and 264b of the PC (P. Bureaucratic and Office Management)	Small	Medium-Low
Production	1) Crime against public health by supplying harmful substances in Article 359 of the PC	Remote	Low
	2) Crime against public health by supplying adulterated food in Article 360 of the PC	Remote	Low
	3) Crime against public health by applying adulterating agents in Article 364.(1) of the PC	Remote	Low
	4) Crime against public health by supplying adulterated food in Article 365 of the PC	Remote	Low
	5) Crime against public health by drug trafficking in Articles 368 and 369 of the PC	Remote	Low
Laboratory	1) Crime against public health by supplying harmful substances in Article 359 of the PC	Remote	Low
	2) Crime against public health by supplying adulterated food in Article 360 of the PC	Remote	Low

	3) Crime against public health by applying adulterating agents in Article 364.(1) of the PC	Remote	Low
	4) Crime against public health by supplying adulterated food in Article 365 of the PC	Remote	Low
Trade	1) Crime of discovery and disclosure of company secrets in Article 278(1) of the PC	Small	Low
	2) Crime of business corruption in Article 286a (1) and (2) of the PC	Medium	Significant

A) Management Department (Company's directors)

As indicated above, most of the risks of irregular behaviour, criminal or otherwise, occurring are related to possible actions taken by the company's directors.

Having said this, it is made clear that all the characteristic possibilities referred to in the different subsequent protocols take on special importance when we refer to the directors of the company, since in fact, it is they who undoubtedly have the power to act as perpetrators, in most cases, under the specific premises established in Article 31(a) of the PC. In fact, due to their own characteristic structure, some of the types of criminal offences that make it possible for the legal person to be held liable can only be committed by its own directors and by representatives of the company.

For this reason, there is a risk that each and every one of the crimes reflected in such protocols may undoubtedly be committed by some of the individuals who hold the power of management of the company, either because they may also be directly perpetrated by them, or because they have acted in collusion with the workers responsible for the crimes committed.

Furthermore, it is also possible that the criminal action of the specific worker was possible due to an inexcusable failure to observe the care that the directors should have taken over their actions. Therefore, in one way or another, the director will always be involved in the crime committed, even if his or her specific action or omission in his or her duty to act entails one type of situation or another vis-à-vis the crime, and therefore, the responsibility it entails.

Notwithstanding this, and in order to follow the system used up to now, we will now specifically identify the crimes for which the directors of the company may be directly responsible.

Taking into account the characteristic forms established by the PC, and due to the special situation of privilege in the control and direction of the company that the directors have, we observe the following risks of the commission of crime that must be mitigated.

1) Possibility of commission of **crimes of discovery and disclosure of secrets in Articles 197, 197(a), and 197(b) of the PC**.

Given that the use of ICTs by the directors of the company is commonplace and without any kind of control (use of the Internet, internal company programmes, specialised networks, social media, etc.), there is a risk that they may take possession of papers, letters, e-mails, or any other documents or personal effects, both from the staff of the company "SAMTACK, S.L." itself and from its client companies, suppliers or service providers, in order to discover their secrets or violate their privacy.

The same applies to the risk of interception of telecommunications, or use of technical devices for listening, transmission, recording or reproduction of sound or

image, for the same purposes. The risk also extends to actions of seizure, use and modification, to the detriment of third parties, of another person's reserved data of a personal or family nature (many of which are particularly sensitive, such as workers' medical records) that are recorded in files, computer, electronic or telematic media, or in any other type of public or private file.

Similarly, there is a risk that the directors may, by violating the security measures established to prevent it, or by illegally accessing an information base or system of client or supplier companies, or by using specific technical devices or instruments, intercept non-public transmissions of computer data that are made from, to or within an information system.

However, it is not usually the custom of the company's directors to deal directly with third parties through ICTs, and the data of interest to which they generally have access are usually innocuous, public, and without any intimate component. Therefore, the risk of committing any form of the offence should be considered LOW.

2) Possibility of commission of a **crime of fraud in Articles 248 (1), (2).a, 249 and 250 (1), (2), (3), (4), (5) and (6) of the PC.**

The possibility of fraud being committed by the directors of any entity or company is particularly high, since the cases of possible criminal action are virtually infinite. In that regard, there are many cases and forms in which, for the profit of the company, someone has deceived a third party, whether a natural or legal person, who, as a result of the error caused by such a trick, has performed an act of disposal of assets with evident detriment to him or herself or to another person.

Such illicit actions take on particular relevance and likelihood of occurrence, when the one who acts is the one who holds the power of decision and the management of the economic dealings of the company. For this reason, there is a risk that the directors, when carrying out their tasks of trade interrelation with other natural or legal persons, may commit some illicit act that is not covered by the crime of fraud.

Notwithstanding the foregoing, and despite the fact that the number of actions likely to involve fraud for third parties is enormous, the risk observed is LOW, as it is difficult to imagine a situation of economic interest for the company that would involve such an action, especially considering that the company is in a flourishing economic situation.

3) Possibility of commission of a **crime of computer damage in Article 264(1) of the PC.**

The same applies to the analysis of this criminal possibility. The power of disposal that the directors of the company have over all the technical-computer equipment available, allows us to imagine possible actions of deletion, damage, deterioration, alteration and suppression of other people's computer data or electronic documents to the detriment of third parties; and this, with or without the collaboration of the company workers with computer skills.

Also, in this case, the risk of occurrence of such criminal activities can be considered MEDIUM-LOW, given the multiple possibilities of action offered by ICTs, and the nature of the data that can be attacked, as well as their possible consequences.

4) Possibility of commission of a **crime of discovery and disclosure of company**

secrets in Article 278(1) of the PC.

The board of directors of the company, insofar as it exercises the supreme management of the business, is the group with the highest level of dealings with client companies, suppliers or service providers. As a result of these dealings, there is a risk that the directors, when carrying out their functions, according to the laws and Bylaws, may become aware of all kinds of data and information of vital importance for the client, supplier or service provider company which, because they affect its ability to compete, are considered "company secrets".

The possibilities of access to these secrets observed are numerous, taking into account the possible methods and dynamics of commission of such offences. Thus, the discovery of such secrets may result from the ease of access of the director to data, written or electronic documents, computer media or other objects that contain such secrets, or to the use of any of the means or instruments indicated in section 1 of Article 197 of the PC (seizure of papers, letters, emails or any other documents or personal belongings of the company, interception of telecommunications or use of technical devices for listening, transmission, recording or reproduction of sound or image, or any other communication signal), as a result of the various commercial dealings and personal interrelations of a commercial nature.

Notwithstanding the foregoing, the risk observed must be considered LOW, given that the capacity of the company's directors to interfere is minimal, as they are normally in possession of information that has already been controlled and debugged by the client company itself.

5) Possibility of Commission of a **crime of business corruption in Article 286a (1) and (2) of the PC.**

As has been said, the board of directors of the company, insofar as it exercises the supreme management of the company, is the group that has the highest level of dealings with clients, suppliers or service providers. As a consequence of these dealings, there is a risk that the directors, when carrying out their functions of trade interrelation with the different managers of client companies (such as their directors, executives, sales managers, etc.), may be tempted to accept gifts, benefits or advantages as compensation for offering contracts to these companies or any profit in trade relations.

Undoubtedly, this type of action is commonplace among companies of all types and sectors, as it is considered legally and even morally acceptable, although, as noted, it is prohibited by law.

In the same vein, but conversely, according to the stipulations for this type of criminal offence which seek to reflect the criminal action from the opposite perspective, there is also the risk that the directors of the company are those who in turn offer or promise this type of benefit to their counterparts in client companies, suppliers or service providers, for trade relationships already established or in the process of being established, and with the intention of unduly favouring them under the same budgets or commercial relations as the previous type.

Naturally, as the reverse of the previous action, these behaviours are also very common in business dealings.

The risk observed must be considered MEDIUM-LOW given the frequent dealings between the company's Directors and their counterparts in the client, supplier or service provider companies.

6) Possibility of commission of a **crime of money laundering in Article 301 of the PC.**

A common risk of any company operating in the market is that the individuals who hold the decision-making and strategic management positions may acquire, convert or transfer goods that come from illicit trade with the intention of hiding or covering up this illicit origin, or even helping the offenders to avoid its legal consequences. Although such an offence is often linked to classic previous offences, such as drug or narcotics trafficking, its possible occurrence is feasible in relation to any kind of predicate offence involving the generation of assets or material benefits. Furthermore, the possibility of the crime of money laundering being committed through serious negligence increases the range of possible criminal actions even further.

Therefore, there is a risk that the directors of the company, in trying to help avoid legal consequences for client companies, suppliers or service providers, accept or transfer products whose illicit origin is known, or about whose legality there are serious suspicions.

However, it is not clear what the benefit to the company might be, given that the type of product it handles does not naturally offer possibilities of criminal collusion that would allow for money laundering or assistance in avoiding responsibility. Nor is there any suspicion of criminal activity among the clientele with which the company has to deal, and therefore the risk observed must be considered LOW, even for the possibility of commission through negligence.

7) Possibility of commission of a **crime against the Public Treasury in Article 305 of the PC.**

The crime against the Public Treasury of Article 305 of the PC is a *specific crime*, which means that it can only be committed by whoever has the specific qualities to be the perpetrator. In this case, the crime can only be committed, as far as the perpetrator is concerned, by the taxpayer. According to the case law of the Supreme Court (STS 14/07/03 and 02/03/05, among others), when the obligor is a legal person, responsibility must be borne by the person who acted as a director or body of the legal person or in its legal or voluntary representation.

Therefore, there is a risk that the directors will carry out by themselves, or order, or act in collusion with certain employees of the Administration Department linked to the Accounting Process (or even with the specialised companies responsible for the economic and financial advice of the company), with the aim of presenting tax returns with alterations that cause serious economic damage to the Treasury.

The possibilities of such fraud extend to the state, regional and local tax authorities; by tax evasion; amounts withheld or that should have been withheld or paid on account, or in terms of improperly obtaining rebates or enjoying tax benefits in the same way, provided that the amount of the tax liability that has been defrauded, the amount not paid of the withholdings or payments on account, or the rebates or tax benefits improperly obtained or enjoyed exceed the amount of one hundred and twenty thousand Euro (€120,000).

The risk observed is low, since the company's turnover range and the transparency of its accounting, now controlled and audited by the SII system, make such a high level of fraud very unlikely.

8) Possibility of commission of a **crime against the Social Security in Article 307 of the PC.**

The tasks of data transmission to the legal department are carried out by the employees of the company's administration department. There is a remote risk that the directors could entrust them with the delivery of biased information to third parties (labour consultancy or the General Treasury of Social Security) that would allow fraud in the social security contributions of the company's workers.

The same applies to obtaining undue rebates or enjoying deductions for any reason, provided that they also exceed the amount of fifty thousand Euro (€50,000)

Notwithstanding the foregoing, the risk observed must be considered LOW, given the traditionally non-existent participation of the company's Directors in the aforementioned labour processing procedure.

9) Possibility of commission of a **crime against the Social Security in Article 307(b) of the PC.**

As has already been pointed out, it is a fairly widespread practice within the employment sphere for companies to be willing to negotiate with their workers for simulated dismissals or other situations that require the company's collaboration, so that the latter can enjoy the benefits of the social security system. Since the company's directors are involved in the work of hiring and firing workers, there is a risk that they may unduly facilitate the enjoyment of those benefits by simulating, misrepresenting or concealing facts or situations from the relevant public administration, with the consequent detriment to that body.

The risk observed must be considered to be MEDIUM-LOW, given that the company's policy on hiring and firing is fairly contained, meaning that the workforce usually remains unchanged, at least until the drafting of this document.

10) Possibility of commission of a **crime of smuggling of legal goods in its different forms in Article 2.1 (a), (b), (c) and (d), and 2.6 of Act 12/1995, of 12 December, on the Prevention of Smuggling.**

The possibility of committing this type of crime, which is covered by a special law apart from the Penal Code, is limited to the personnel of the Management Department as they are the only ones who can be involved in the possible criminal acts that may occur, given the nature of this type of crime.

In this way, there is a risk that the directors may import or export legal trade goods without presenting them for clearance in the customs offices or in the places authorised by the customs administration, with such assets, merchandise, goods or items having a value equal to or greater than one hundred and fifty thousand Euro (€150,000).

There is also a risk that the aforementioned persons may carry out operations of trade, possession or circulation of legal trade goods without complying with the legally established requirements for proving their legal import.

The risk also extends to the possibility of goods in transit being used for

consumption in breach of the regulations governing the customs procedure, and specifically of EC Regulation 450/08 of the European Parliament and of the Council, of 23 April 2008, laying down the Community Customs Code, or of goods subject to administrative authorisation being imported or exported after falsifying the supporting documentation for such products.

Notwithstanding the foregoing, the risk of any of the aforementioned offences occurring must be considered LOW both because the operations carried out abroad are currently minimal and subject to all kinds of administrative control, and because it is unthinkable that the company would be interested in encouraging actions of this type. Moreover, the bulky and visible nature of the goods, as well as their administrative control and inspection, are such that it would be extremely difficult to carry out the criminal conduct.

Without prejudice to the generic methodology already mentioned in section 3.2.1.4, the following is a brief description of the methodology used in the analysis of the aforementioned criminal cases:

The background information of the company has been taken into account; this is a family company run by the MAS ORTAS brothers. The personal interviews have been particularly useful. Background information of interest and incidents have been requested; the minutes of the meetings held by the board of directors, between directors and heads of department, as well as annual planning, forecasts, budgets and possible deviations; and incidents in the company in recent years. All the strategic decisions of the group have also been reviewed with the directors.

B) Administration Department.

In accordance with the characteristic forms established by the PC, and the activities that the aforementioned workers carry out, the risks of criminal conduct observed are the following:

1) Possibility of commission of a **crime of discovery and disclosure of company secrets in Article 278(1) of the PC.**

Given that this department is responsible for identifying, relating to and dealing with the client or supplier while the commercial relationship is in progress, there is a risk that the workers of this department, in the sales management process, may become aware of all types of data and information of vital importance for the client, supplier, or service provider company of SAMTACK, S.L. which, by affecting the competitiveness of the company, may be considered “company secrets”.

This possibility of discovery of secrets may result from knowing data, written or electronic documents, computer media or other objects that refer to this specific secret, or to the use of any of the means or instruments indicated in section 1 of Article 197 of the PC (seizure of papers, letters, emails or any other documents or personal belongings of the company, interception of telecommunications or use of technical devices for listening, transmission, recording or reproduction of sound or image, or any other communication signal).

Notwithstanding the foregoing, the risk observed must be considered LOW, given that the capacity of the company's workers to interfere is minimal, as they are normally in possession of information that has already been controlled and debugged by the client, supplier or service provider company itself.

2) Possibility of Commission of a **crime of business corruption in Article 286a**

(1) and (2) of the PC.

Since this department is responsible for carrying out the day-to-day business with the company's clients, and for monitoring and preserving such clients, there is a risk that the employees who are involved in the sales management process may request, receive or accept unjustified benefits or advantages of some kind, in return for unduly favouring the companies concerned, when contracting new services or in trade relations in general.

Notwithstanding the foregoing, the risk observed must be considered LOW, given that the manoeuvring capacity of these workers is very low, as the features of these commercial relations have already been defined by the company's management.

3) Possibility of commission of a **crime of fraud in Articles 248(1), (2)a and c, 249 and 250(1), (2), (3), (4), (5) and (6) of the PC.**

This department is responsible for carrying out all the procedures related to the entries in the company's official tax books, as well as handling the registration of invoices issued to clients and received from suppliers, and there are many risks associated with these tasks.

Thus, by means of considerable deception, it is feasible to the client companies to make errors, inducing them to carry out an act of disposal of assets to their detriment. This can be done by issuing incorrect invoices by duplication with machinations that exceed the possibilities of self-protection of the client companies; issuing improper invoices for excess amounts to client companies; or other machinations to convince them of the performance of services that have not actually been carried out, provided that in all cases the use of tricks has meant that the possibilities of self-protection of such companies have been exceeded.

Notwithstanding the foregoing, the risk observed must be considered LOW, given the possibilities of verification of the client companies, which are at all times aware of the operations actually carried out and the services actually provided.

Notwithstanding the foregoing, the risk observed should be considered LOW, given the high degree of computer knowledge required to carry out such manipulations and due to the lack of the necessary media to carry out such transfers.

4) Possibility of commission of a **crime against the Public Treasury in Article 305 of the PC.**

As already indicated, the crime against the Public Treasury of Article 305 of the PC is a *specific crime*, which means that it can only be committed by whoever has the specific qualities to be the perpetrator of the crime. In this case, the crime can only be committed, as far as the perpetrator is concerned, by the taxpayer.

However, the *extraneus* (that is, the person who does not have these specific qualities; in this case, the company's worker), can be responsible as the necessary inducer of or co-operator in the act committed by the *intraneus*, so his action is not exempt from criminal liability.

Therefore, given that this department is responsible for physically carrying out all the procedures related to the company's fiscal and tax operations, there is a risk that the employees, workers or members of this department could interfere in the preparation of the tax forms concerned by providing false information.

The possibilities of such fraud extend to the state, regional and local tax authorities, both in terms of tax evasion, amounts withheld or that should have been withheld or paid on account, or in terms of improperly obtaining rebates or enjoying tax benefits in the same way, provided that the amount of the tax liability that has been defrauded, the amount not paid of the withholdings or payments on account, or the rebates or tax benefits improperly obtained or enjoyed exceeds one hundred and twenty thousand Euro.

Notwithstanding the foregoing, the risk observed must be considered LOW, given that the manoeuvring capacity of such workers is very low, the tax returns being submitted directly for collection by the Administrator, Ms. GEMMA MAS ORTAS, who is the head of this department and who, after checking that they are correct, is responsible for paying them to the Tax Office by means of an automated telematic system.

5) Possibility of commission of a **crime against the Social Security in Article 307 of the PC.**

Given that this department is responsible for sending the labour agency all the elements and data of a corporate nature so that it can send the Social Security the necessary information for the purpose of preparing the appropriate contribution forms, there is a risk that the company employees in charge of this information transfer process may provide false or misleading data to the agency in order to alter the final preparation of the contribution forms.

Notwithstanding the foregoing, the risk observed must be considered LOW, given the control filter that the agency's participation in the process entails, as well as the low monthly variation of the data transferred and the supervision of these by the head of the department, the Administrator Ms. GEMMA MAS ORTAS, who, after checking that they are correct, is responsible for making the payment by means of an automated telematic system.

6) Possibility of commission of a **crime of discovery and disclosure of secrets in Articles 197, 197(a), and 197(b) of the PC.**

Given the widespread use in companies of ICT equipment, software and application possibilities (use of Internet, internal company programmes, specialised networks, social media, etc.), there is a risk that workers in the administration department of the company may take possession of papers, letters, emails or any other documents or personal effects, both of the staff of the company itself “SAMTACK, SL” and of its customers, suppliers or service providers in order to discover their secrets or violate their privacy.

Likewise, there is a risk of interception of telecommunications, or use of technical devices for listening, transmission, recording or reproduction of sound or image, for the same purposes.

Given the aforementioned use of these ICTs, the innumerable communication processes between the company's own personnel, and even between external companies due to circumstances of all kinds, there is also a risk that the employees of the company's Administration department may take possession of, use and modify, to the detriment of third parties, other people's confidential personal or family data (many of which are particularly sensitive, such as workers' medical records) that are recorded in files, computer, electronic or telematic media, or in

any other type of public or private file.

Similarly, there is a risk that these workers may, by violating the security measures established to prevent it, or by illegally accessing an information base or system of client or supplier companies, or by using specific technical devices or instruments, intercept non-public transmissions of computer data that are made from, to or within an information system.

This is feasible when the worker accesses databases and computer programmes of client and supplier companies in order to carry out procedures for which he or she is in principle authorised.

The numerous variants of the crime mean the risk of committing any of them must be considered as MEDIUM-LOW, especially if we consider the consequences that could result from the disclosure of these secrets and details, due to the extreme sensitivity of certain data and information.

7) Possibility of commission of a **crime of computer damage in Article 264(1) of the PC.**

Once again, the use of ICTs and the processes of interrelation and communication they entail, make the risk swing towards the field of software alteration. Thus, there is a risk that the personnel of the Administration Department may delete, damage, impair, alter or block access to other people's computer data, computer programmes or electronic documents, thus causing serious damage to the companies concerned.

The feasibility of such conduct results from the possibility of access to other people's computer systems by the company's workers who are involved in the bureaucratic and office management process.

Given the enormous possibilities offered by the use of these ICTs, the risk of such criminal conduct occurring can be considered MEDIUM-LOW, since in all cases, the action must comply with the parameters and elements established in the participatory form of Article 31a of the PC (that is, the action must be “on behalf of the company”, and for the “benefit of the company”).

Without prejudice to the generic methodology already mentioned in section 3.2.1.4, the following is a brief description of the methodology used in the analysis of the crimes of this department:

Personal interview with the heads of the department. Background information of interest and incidents. Analysis of work systems; relationships with customers and suppliers; attracting systems; forms of payment. Data protection.

C) Production Department.

According to the characteristic forms established by the PC, and following the list of processes carried out by the department, the following risks linked to its activity are observed and must be mitigated:

1) Possibility of commission of a **crime against public health involving the manufacture and dispatch of substances harmful to health or hazardous chemicals that may wreak havoc in Article 359 of the PC.**

The possibility of this crime being committed is determined by the fact that, as long as the company “SAMTACK, S.L.” adds to its products adhesive substances in

indirect (but extremely close; separated by microns) contact with the food products that are finally sold by client companies in the market, there is a risk that the personnel of this operating department, for whatever reasons, with the intention of favouring the company or even following its instructions, may end up introducing into the market products for packaging (flexible packaging complexes for food or blister packs for medicines), preservation and in general, containing goods, which contain substances that are harmful to health or chemicals that may wreak havoc among the population due to mass contamination. This possibility is encouraged by the fact that the employees of this department are responsible for physically handling all types of adhesion, printing and embossing of the company's container products.

Nevertheless, the risk of this crime being committed must be considered LOW, given the strict safety systems established by the specialised regulations implemented by the company, the internal migration tests carried out by the company, and the lack of interest in intervening in any process of this nature by means of a fraudulent action.

2) Possibility of commission of a **crime against public health by supplying adulterated food in Article 360 of the PC.**

The possibility of this crime being committed results from the existence of a risk that the workers of this department could add harmful substances or chemicals to the aforementioned "container products" manufactured by the company, without fulfilling the formalities established by the Laws and Regulations that regulate, respectively, the use of such substances and products. Specifically, in EU Regulations 10/2011 and 1935/2004 "On plastic materials and articles intended to come into contact with food".

Notwithstanding the foregoing, the risk of such an offence being committed must be considered LOW, given the absence of any specific interest on the part of the company in carrying out fraudulent actions of that nature.

3) Possibility of commission of a **crime against public health by applying adulterating agents in food and beverages in Article 364(1) of the PC.**

The possibility of this crime results from the existence of a risk that the workers of this department could add unauthorised agents to the aforementioned container products manufactured by the company, which by migrating from such containers to the contained products (food of different kinds), could cause harm to human health.

Nevertheless, the risk of this crime being committed must be considered LOW, among other things, because the possible harmful actions indicated would be difficult to classify technically or subsume legally in the aforementioned crime. Thus, the aforementioned crime, to judge by its typical exposure, seems to be aimed at the direct adulteration of the dispatched food or drink product by the manufacturers of that product, rather than by third party providers of other services linked to the finishing of the product, but unconnected with the direct process of food manufacture.

Notwithstanding the foregoing, the possibility of such an offence being committed is included, given the endless and boundless deviousness of human nature.

However, there is a clear lack of specific interest in the workers of this department

in carrying out such fraudulent actions.

4) Possibility of commission of a **crime against public health by supplying adulterated food in Article 365 of the PC.**

There is also a risk that these workers could poison the food intended for human consumption with substances that are harmful to human health, through the same processes of adhesion or coupling of such substances to the food containers and their lethal migration to the foodstuffs finally contained.

Notwithstanding the foregoing, the possibilities of such offences being committed may be considered LOW, since this offence merits the same technical and legal reservations as those referred to in the previous case. It should not be forgotten that, in any event, the action must be in accordance with the parameters and elements established in the participatory form of art. 31a of the PC (that is, the action must be "on behalf of the company" and for the "benefit of the company"), and this is only conceivable in cases of "laboratory" criminal actions of this nature that might favour the company. Such actions seem more akin to cases of sabotage, in which the company would also be harmed, than to anything else.

5) Possibility of commission of a **crime against public health by trafficking in drugs, narcotics and psychotropic substances in Articles 368 and 369 of the PC.**

The possibility of this crime being committed by the personnel of the department results from the existence of a risk that the workers of this department, due to their daily contact with goods transport vehicles (typical means used for the introduction of drugs and narcotic substances), could carry out some of the characteristic forms established by these legal norms. Thus, activities of trafficking or aiding in the transport of toxic drugs, narcotics or psychotropic substances to or from the company for the consumption of third parties cannot be ruled out.

Notwithstanding the foregoing, the risk of such criminal activities occurring can be considered LOW, since in any event, as has already been said, the action should comply with the parameters and elements established in the participatory form of art. 31a of the PC, making it very difficult to conceive of cases of drug trafficking in which the company makes some kind of direct or indirect profit, and in which the person responsible has acted "on behalf of the company".

Without prejudice to the generic methodology already mentioned in section 3.2.1.4, the following is a brief description of the methodology used in the analysis of the crimes of this department:

Personal interview with the heads of the department. Background information of interest and incidents. Analysis of work systems. Direct observation of the operation of the production plant and the workshop.

D) Laboratory Department

According to the characteristic forms established by the PC, and following the list of processes carried out by the department, the following risks linked to its activity are observed and must be mitigated:

1) Possibility of commission of a **crime against public health involving the manufacture and dispatch of substances harmful to health or hazardous chemicals that may wreak havoc in Article 359 of the PC.**

2) Possibility of commission of a **crime against public health by supplying adulterated food in Article 360 of the PC.**

3) Possibility of commission of a **crime against public health by applying adulterating agents in food and beverages in Article 364(1) of the PC.**

4) Possibility of commission of a **crime against public health by supplying adulterated food in Article 365 of the PC.**

Given the attributions and competencies that the workers of the laboratory department have, everything stated for the Production department is also applicable to them, the same risks and arguments used when analysing the latter department being used to substantiate them. Therefore, the risk of such offences being committed must also be considered LOW, for the same reasons as those given for the Production Department.

Without prejudice to the generic methodology already mentioned in section 3.2.1.4, the following is a brief description of the methodology used in the analysis of the crimes of this department:

Personal interview with the head of the department. Background information of interest and incidents. Analysis of work methods. Direct observation of the operation of the laboratory.

E) Sales Department

According to the characteristic forms established by the PC, and following the list of processes carried out by the department, the following risks linked to its activity are observed and must be mitigated:

1) Possibility of commission of a **crime of discovery and disclosure of company secrets in Article 278(1) of the PC.**

Insofar as this department is responsible, at all times, for attracting and dealing with the personnel of the companies that are clients or suppliers of "SAMTACK, S.L.", there is a risk that both employees of the sales department may become aware of all types of data and information of vital importance for the client, supplier, or service provider company of "SAMTACK, S.L." which, by affecting the competitiveness of the company, may be considered "company secrets".

This possibility of discovery of secrets may result from (as in the other cases) knowing data, written or electronic documents, computer media or other objects that refer to this secret, or to the use of any of the means or instruments indicated in section 1 of Article 197 of the PC (seizure of papers, letters, emails or any other documents or personal belongings of the company, interception of telecommunications or use of technical devices for listening, transmission, recording or reproduction of sound or image, or any other communication signal).

Notwithstanding the foregoing, the risk observed must be considered LOW, given that the capacity of the company's workers to interfere is minimal, as they are normally in possession of information that has already been controlled and debugged by the client or supplier company itself.

2) Possibility of Commission of a **crime of business corruption in Article 286a (1) and (2) of the PC.**

Insofar as these workers are, as noted, the employees of the company that

maintain a constant, direct and personalised relationship with their counterparts or members of the aforementioned client companies or suppliers of "SAMTACK, S.L.", there is a risk that they may receive, request or accept unjustified benefits or advantages of some kind in return for unduly favouring the company concerned in the contracting of new services or in commercial relations in general.

The risk observed must be considered MEDIUM, since although the manoeuvring capacity of these workers in their commercial relations may be considerable, the main features of these commercial relations are drawn up by the company's management.

Without prejudice to the generic methodology already mentioned in section 3.2.1.4, the following is a brief description of the methodology used in the analysis of the crimes of this department:

Personal interview with the sales staff. Background information of interest and incidents. Analysis of work methods.

3.3. RISK PREVENTION, MANAGEMENT AND MONITORING SYSTEM

Through the regulatory risk management and monitoring system, the company establishes the set of bodies, functions, rules, measures, procedures and activities aimed at identifying, assessing, preventing and managing the regulatory risks linked to the exercise of the business activity at an early stage.

3.3.1. Regulatory risk and control bodies

The company's regulatory control system will consist of the following risk management and control bodies

a) The company's directors

The company's directors shall be responsible for ensuring the design and implementation of the entire supervision, monitoring and control model. The directors shall exercise leadership of the entire management and monitoring system of the regulatory compliance programme, undertaking to ensure its effective deployment. To this end, they shall operate according to the following guidelines:

- They shall take the necessary decisions to reinforce the ethical values of the corporate culture.
- They shall adopt, implement, maintain and continuously improve a regulatory risk system suitable for identifying and preventing illicit activities or for drastically reducing the risk of their occurrence.
- They shall provide the risk management and monitoring system and, in particular, the regulatory compliance body, with adequate and sufficient financial, material and human resources for its effective operation.

b) The company's senior management and heads of department

Senior management and heads of department shall be directly involved in the effective operation of the legal person's compliance system. To this end, in the exercise of their executive senior management and departmental responsibility functions they must, among other measures:

- Ensure that the regulatory compliance programme approved by the

governing bodies is properly implemented.
- Ensure that the requirements arising from this programme are incorporated into the company's operational processes and procedures.
- Ensure the availability of adequate and sufficient resources for the effective implementation of the programme.
- Direct and support the staff in order to achieve compliance with the requirements and effectiveness of the legal person's risk prevention, management and monitoring system.

c) The Supervisory Board of the Crime Prevention Model (CSMPD).

As already mentioned, the company is required to create this body, as it cannot carry out by itself the functions entrusted to it by law, since the only requirement established in article 31a (3) of the PC to do so (the submission of the profit and loss statements in an abbreviated form) is not met.

The aforementioned body has already been functioning since the company first adopted the present regulatory compliance model, in a different presentation format. However, as this manual is going to replace the previous one, the criteria and guidelines that will govern the actions of the aforementioned control and supervision body of the aforementioned regulatory compliance model are once again reiterated.

The CSMPD is an independent and autonomous body in terms of initiative and control, which demonstrates the company's commitment to maintaining a corporate ethical culture.

The CSMPD is the body responsible for effective compliance with the regulatory system of the organisational model and performs the ordinary functions of supervision, monitoring and control thereof. As an independent body with its own prerogative over its tasks and functions, it will not obey the instructions and guidelines of any of the company's higher powers of command, maintaining operational independence from the company's directors. Although there is currently a company director present in this body, this does not imply any reduction in its autonomy and independence, since all issues arising in relation to the present system of regulatory compliance will be assessed by the CSMPD lawyer, the director acting on the basis of his advice and not on that of the Board of Directors. Consequently, the relationship between the Board of Directors and the CSMPD is one of competence and is in no way hierarchical.

The CSMPD shall also be responsible for drawing up the organisational and risk management models it considers appropriate in light of the business circumstances that arise, ensuring their correct operation at all times. It shall also have the power to establish the audit services it considers most appropriate at all times, as well as the surveillance and control services for compliance with the requirements established by law in article 31a, sections 2, 3, 4 and 5 of the Penal Code. It shall ensure that the company's actions in the pursuit of any irregular or criminal acts that may occur cover the self-imposed standards in its code of ethics and regulatory compliance system, as well as in the laws themselves. To this end, its personnel shall: have sufficient knowledge and professional experience to carry out their duties; have the appropriate technical means; have access to internal processes; as well as the existing information necessary to be able to carry out their functions. The knowledge of the position may be provided by the CSMPD's

external advisory lawyer who, in the event of any event occurring or important decision to be taken, will always be the first source of advice.

The CSMPD will therefore be the body responsible for ensuring compliance with the controls and protocols contained in this manual, with a view to preventing irregular actions against the code of ethics and the regulatory risk system, as well as crimes, or significantly reducing the risk of their commission, by providing an appropriate response in the manner established in these protocols. This body is also covered by the code of ethics set out in the last section of this manual.

The aforementioned CSMPD is currently made up of the following persons and positions:

- Mr. EUDALD MAS ORTAS, who shall be the Chairman

- Mr. IGNACIO PASTOR SANTIAGO, as external advisor, and specialist in criminal law, member of the Bar Association of Barcelona, who shall act as secretary.

Although this body has autonomous powers of decision and control in this area, as prescribed in Article 31a. (2.2), it shall periodically inform the Board of Directors of any incidents that may occur in a timely manner.

The CSMPD shall hold an Ordinary Meeting twice a year, at the end of June and December, to discuss and verify the effective operation of the system; take whatever decisions are deemed appropriate in relation to the deviations or omissions observed in the model implemented; to the organisational changes that occur in the company, or to the legislative or jurisprudential variations that may affect the CPM implemented.

Notwithstanding the foregoing, any circumstance or event occurring within the company that might make a meeting of the CSMPD advisable shall imply the calling of an Extraordinary Meeting to deal with the situation and adopt whatever measures are deemed appropriate.

The meeting shall be convened by the external advisor, by means of an e-mail sent to the Chairman of the CSMPD, which shall include the agenda to be dealt with and other legal requirements.

Both members must be present at the meetings of the CSMPD, and no delegations or substitutions of any kind shall be allowed. All decisions must be approved by both members; in the event of a disagreement, the issue addressed shall remain unchanged with regard to the previous natural situation.

The meetings shall be held at the company's headquarters.

The external advisor of the CSMPD shall act as secretary in the ordinary and extraordinary meetings, taking the appropriate minutes, which shall be included in a “CSMPD Minutes Book” created for this purpose. The book may be electronic.

The management of the company does not, at this time, establish any specific budget item to provide the CSMPD with economic funds for the exercise and performance of its functions. Nevertheless, it is willing, and expressly and formally declares this, to cover any expense that might arise from the maintenance of the regulatory compliance system and organisational model it implements, as long as this is acceptable and reasonable in terms of the amount involved and the company's cash flow.

The following decision protocol is established to decide whether or not the expense incurred is justified:

- When both members of the CSMPD agree on the expenditure to be made, they shall submit the proposal to the Board of Directors, through the Chairman of the CSMPD, for its endorsement.

- The Secretary of the CSMPD shall take the appropriate minutes of the decision of the company's Board of Directors, which shall include, in all cases, the initial proposals-decisions taken by this body and submitted to the management of the company, as well as the final decision taken by the latter.

Notwithstanding the foregoing, the company may at any time decide to allocate, or budget for the item it deems appropriate in the field of criminal risk prevention on an annual basis.

As regards the provision of human resources, although the management of the company does not assign any specific person to assist the CSMPD, it expressly accepts that this body may count on the collaboration of any member of the company whose intervention is required for the performance of its tasks.

3.3.2. Measures and procedures

For the purposes of preventing the risks of regulatory and auxiliary non-compliance, the following regulatory risk management and monitoring system is established during the process of formation, adoption and execution of business decisions:

- The hiring of senior executives and specialised personnel (including petrol station managers) shall be carried out directly by the Board of Directors, taking into account the curriculum vitae; verified external references; Tax Agency (AEAT) certifications of being up to date with tax obligations; criminal record certificate and, if necessary, training tests to carry out the proposed job, as well as any personal interviews deemed necessary.

- For the hiring of suppliers; distributors; business partners; intermediaries, etc., other than the current ones, complete “due diligence” will be required, which must be reviewed by the directors and heads of department who may be involved with any of these agents.

- Controls in the financial resource management processes. The company shall adapt its ordinary expenses and investments to the annual budget prepared for this purpose. For anything that exceeds the aforementioned budget and, consequently, generates an unforeseen and non-additional expense, the approval of the Board of Directors must be obtained, following a risk and opportunity assessment.

- For all non-financial processes, such as commercial operations, advertising and any other of a similar nature that exceeds the annual budget, the Board of Directors must also give its approval.

- In the contracting of services with suppliers; distributors; contractors; business partners; intermediaries; consultants, etc., the penal clauses deemed most appropriate shall be stipulated, in order to prevent regulatory

risk and, in the event of non-compliance with the risk prevention policy, to set out the consequences, namely: decreeing the nullity and/or suspension of contracts signed with third parties; request of damages; disclaimer; clauses on restitution and compensation for damage caused; indemnities, etc.

- The company, through the CSMPD, reserves the right to carry out internal and/or external audits to assess the regulatory compliance system, as the model is developed and as required by the company's internal and external circumstances.

- The periodic review of the risk prevention, management and monitoring system shall be performed by the CSMPD, at the initiative of the external advisor or of the members of this body. Always taking into account the opinion of senior management and the company's administrative bodies. This periodic review shall be carried out by the external advisor, in accordance with the provisions set out in the section on the review of the model.

- Follow-up activities; measurement; analysis; assessment and review of the regulatory compliance programme shall be performed by the CSMPD, in accordance with the needs discussed in each case and in response to the details provided in the section on the operation of this body.

- The reports required for the correct operation of the prevention and response mechanisms implemented shall be drawn up by the CSMPD. They shall be submitted to the meetings scheduled periodically for discussion and approval, where appropriate.

- For the filing of documentation; traceability and control of communications and relevant information, in order to verify the existence and efficiency of the entire regulatory compliance system, an electronic recording system is established, with the following basic characteristics:

    - The access system shall be restricted to directors, heads of department and positions of trust, to be decided at any time by the managers of the company.
    - Any relevant information on anomalies that may be detected by employees or personnel outside the company shall be referred to the heads of department, who shall record it in the programme to be created for this purpose. Preferably, employees will use the e-mail system for their communications, although they may also communicate verbally. Minutes shall be taken of the conversation and recorded in the system. All of this shall be done independently of the prerogatives established in the reporting channel set out in point 4.1. of this manual.

- Documents; communications; Any complaints and relevant information shall be brought to the attention of the periodic meetings of the SBCPM for

the adoption of whatever measures may be appropriate in order to comply with this regulatory compliance system.

3.3.3. Protocols to prevent irregularities and crimes that may be committed in the different departments of the company.

3.3.3.1. Avoidance of the commission of the crimes of discovery and disclosure of secrets in Article 197(d) of the PC, in relation to Article 197, 197(a) and 197(b) of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Management and Administration.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- It is totally forbidden for the directors, managers and workers of the company to take possession of papers, letters, emails or any other documents or personal effects, either of the staff of the company "SAMTACK, S.L." itself or of any other company, which, by its nature and content, is of a secret, confidential or intimate nature.

2.- It is strictly forbidden for the directors, managers and employees of the company to access other people's e-mails, and the possibility of corporate communication is limited to the mere sending of e-mails related to the performance of the functions inherent to the specific position.

3.- For its professional communications, the management of the company shall establish a corporate communication system of an open and non-secret type, which allows the business power of surveillance and control of compliance with the obligations relating to the use of email given its business ownership and exclusive use for communications of a professional nature.

4.- When any director, manager or worker suspects that some other employee of the company is illegally interfering with the company through the use of ICTs, he or she shall immediately inform the Chairman of the CSMPD, who shall immediately remove the worker from his or her computer terminal, assigning him or her other professional tasks in accordance with his or her professional category, and shall report the matter to the CSMPD's legal advisor, who shall take whatever legal action he or she deems appropriate on behalf of the company. The Chairman of the CSMPD shall also intervene in the proceedings as a representative of the company.

5.- It is expressly forbidden for the directors, managers or employees of the company, to carry out any form of interception of telecommunications, use of technical devices for listening, transmission, recording or reproduction of sound or image, to find out any confidential matter or content of a third party, either of the company "SAMTACK, S.L." or of any other company.

6.- It is expressly forbidden for the directors, managers or employees of the company to obtain, use or modify any third-party confidential personal or family data which are recorded in files, computer, electronic or telematic media, or any other type of public or private file, whether it belongs to staff of the company "SAMTACK, SL" or of any other company.

7.- It is expressly forbidden for the directors, managers or employees of the

company to obtain illegal access, violating the established security measures, to a database or information system of companies of any kind.

8.- It is expressly forbidden for directors, managers or employees of the company to intercept non-public transmissions of computer data from, to or within an information system of any type of public or private enterprise or legal person by using technical devices or instruments.

9.- Directors, managers and workers who, as a result of their activity, may have access to data of a confidential nature, must at all times have sufficient training and information about the basic aspects stated by Act 15/1999, of 13 December, on Personal Data Protection and the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This training shall be given by personnel specialised in the subject.

10.- The management of the company shall hire a company specialised in this legislative field, which shall be responsible for the necessary management and updating of services and the carrying out of a biannual audit.

11.- The management of the company shall implement a computer system by which each employee, worker or member can carry out the tasks entrusted to them by means of a system of restrictive authorisations for the performance of such work or specific functions, as well as a system of personalised user codes and passwords.

12.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another director, manager or employee of the company, whether from the aforementioned departments or any other, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.2. Avoidance of the commission of the crime of fraud in Article 251(a) of the PC, in relation to Articles 248(1), (2)a and c, 249 and 250(1), (2), (3), (4), (5) and (6) of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments; Management and Administration.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- All directors of the company are strictly forbidden to prepare invoices, delivery notes or equivalent documents of any kind. Invoices, and their associated documentation, shall always be prepared by the company's administration department and under the authentic invoicing items and amounts.

2.- It is strictly forbidden for the personnel of the administration department in charge of invoicing to prepare any invoice, delivery note or equivalent commercial document that does not reflect the reality of the situation that has occurred and been contracted by the client company, and which, in any event, represents a financial loss for the company that can be clearly identified and assessed.

3.- Notwithstanding the foregoing, any of the directors may, at any time, request all types of information from the employees of the administration department

regarding the operations that are taking place.

4.- All invoices received and issued by the company (from all types of customers and suppliers) shall be subject to periodic checking and marking by the personnel of the department assigned to these invoicing management functions, and in the event of anomalies being observed, a brief written note shall be sent to the head of the department, who shall subsequently inform the CSMPD. Such checks and the associated communications shall be carried out monthly.

5.- The head of the administration department shall personally carry out a monthly sample check of two billing days for that month, selected at random (one day of the first fortnight and one day of the second fortnight), checking and marking the invoices (issued and received) for those two days to verify the existence of possible anomalies. In the event of the existence of anomalies, the Chairman of the CSMPD must be informed.

6.- Any data or specification the department has about the bank accounts or any present or future institution that houses financial assets of a client company, supplier or service provider of "SAMTACK, S.L." is confidential, and its knowledge is reserved solely and exclusively to those members of the department who are directly involved in the actual invoicing processes.

7.- The actual processes of payment by transfer and by any other method commonly used in commerce and used by the company shall also be subject to periodic verification and marking by the staff assigned that specific function within the department. Likewise, these employees shall also send a brief written note referring to the anomalies observed to their immediate superior, who shall inform the Chairman of the CSMPD. Such checks and the associated communications shall be carried out monthly.

8.- Each month the head of the administration department shall personally carry out a two-day sample check of the list of transfers and of the other commercial means of collection and payment for that month (selected at random: one day of the first fortnight and one day of the second fortnight), checking and marking the transfer orders and other means of collection and payment used by the company and their effective performance in order to verify the correctness or anomalies reported to him by his subordinates. In the event of anomalies being observed by the head of the department, these shall be reported by way of a suitable note to the Chairman of the CSMPD.

9.- Once the head of the administration department has paid the applicable VAT, he shall block the period settled, such that no subsequent expenditure may be allocated or recognised during that period. Sales shall also be affected by the same allocation criterion.

10.- The head of the administration department shall also carry out the administrative control of the so-called "IMMEDIATE VAT INFORMATION SYSTEM" (SII), according to the instructions given by the Tax Office itself. In this way, he must check monthly that both the Tax Bases and the amounts of the purchase and sales invoices are declared within a period of less than four days with respect to their dates of issue, and settled at the end of the month, all of which is in line with the company's general accounts.

In any event, before proceeding to settle any VAT period, the head of the

administration department shall once again check that the settlement to be submitted perfectly matches the input and output VAT entered in the company's accounting records.

11.- The staff of the administration department shall check all the company's bank transactions on a daily basis. At the end of the day, they shall provide the head of the department with a summary of all the balances of the banking positions and forecasts for the following day. At the end of the day, the head of the department shall check by computer that the balances recorded are indeed those of each of the banks.

12.- The head of the administration department shall check that the transfers to be made as a result of the payment of the company's employees' withholdings, for which the official forms are physically filled in by the company's tax advisors (forms 111 and 190), match up perfectly with the data in the payroll tables that the company has set up as its internal accounting control system.

13.- The results of the checks, as well as the communications referred to in this section related to control functions, shall be carried out by e-mail and shall be entered in an electronic file to be created and integrated into the company's management programme.

14.- Any data or specification the department has about the bank accounts or any present or future institution that houses financial assets of a client company, supplier or service provider is confidential, and its knowledge is reserved solely and exclusively to those members who are directly involved in the actual invoicing processes.

15.- The company's collection and payment system shall be verified by bank transfer, or by the use of cheques, bills of exchange or promissory notes, or any other type of credit or payment commonly used in commercial practice within the sector.

16.- Payment in cash for an amount greater than 1,000 Euro is expressly prohibited. Thus, no credit or payment in bank notes, coins (national or foreign), bank cheques made out to the bearer, or any other physical means, including electronic ones, designed to be used as a means of payment to the bearer, shall be permitted.

17.- Any director of the company shall behave in accordance with the provisions of Act 7/2012, of 29 October, amending the tax and budgetary regulations and adapting the financial regulations for the intensification of actions in the prevention and fight against fraud.

18.- Any director of the company shall behave in accordance with the provisions of Act 10/2010, of 28 April, on prevention of money laundering and financing of terrorism.

The guidelines for action in accordance with these regulations are set out in the section on the prevention of the crime of money laundering. In any event, they shall be observed in all matters that might be appreciable from the standpoint of the hypothetical commission of a fraud.

19.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another manager or employee of the company, whether from the aforementioned departments or any

other, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.3. Avoidance of the commission of a crime of computer damage in Article 264(c) of the PC, in relation to Article 264(1) of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Management and Administration.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- It is expressly forbidden for the directors, managers and employees of the company to carry out any unauthorised form of deletion, damage, impairment, alteration or any other action that blocks access to computer data, software or electronic documents of any type of company or natural person with whom "SAMTACK, S.L." has any kind of business or professional relationship.

2.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another manager or employee of the company, whether from the aforementioned departments or any other, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.4. Avoidance of the commission of the crime of discovery and disclosure of company secrets in Article 288 of the PC, in relation to Article 278(1) of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Management, Administration and Sales.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- Any director, manager or employee of the company who as a result of their work comes into possession of a business secret of a client company, supplier or service provider of "SAMTACK, SL", is expressly required to maintain the confidentiality of such material.

2.- Among other data and information, this confidentiality or obligation to remain silent shall apply to: lists of customers and suppliers of the company; unpublished turnover; accounting items; organizational charts; plans; internal memoranda; product cataloguing; graphic descriptions, and purchase and retail prices that can be found in letters; emails, written or electronic documents; documents or personal effects of the company, computer media and objects relating to them, insofar as they may affect the company's competitive capacity. The lists are purely by way of example and are not exhaustive.

3.- Obtaining or holding the elements and, consequently, secrets listed in section 2.- will only be admissible with the express authorisation of the client, supplier or service provider, and they shall be used exclusively for the purposes for which they were effectively provided.

4.- The unauthorised obtaining or possession of the elements and, consequently, secrets listed in section 2. for the express purpose of obtaining said business

secrets is strictly prohibited.

5.- Any employee in possession of such knowledge and media of controversial information shall immediately cease the activity that has given rise to such knowledge, and shall immediately report it to the head of the department in question, who shall pass it on to any of the company's directors, pending receipt of instructions on how to continue with his or her activity in an uncontroversial manner.

6.- The unauthorised obtaining or possession of the information and, consequently, secrets listed in section 2.- by chance, shall be immediately reported to the company that owns them by the director, manager or worker who has had access to such material, who shall refrain from making any use of it. If it is held by a manager or employee, it shall also be reported to any of the directors of "SAMTACK, S.L.".

7.- The communications referred to in this section shall be made by email and must be entered in an electronic file to be created and integrated into the company's management programme.

8.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another manager or employee of the company, whether from the aforementioned departments or any other, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.5. Avoidance of the commission of the crime of business corruption in Article 288 of the PC, in relation to Article 286a (1) and (2) of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Management, Administration and Sales.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- The directors, managers and employees of the company, in the exercise of their duties, are strictly forbidden to receive, request, or accept gifts, donations, benefits or advantages of any kind that are intended to obtain a commercial or trade consideration, whatever it may be, in favour of a client, supplier, or service provider company. The only gifts and gratuities that may be received must be completely free of charge and without any kind of consideration.

2.- Such permissible gifts, donations, benefits or advantages must be of reasonably moderate value and, by their nature, must be consistent with normal customs of courtesy and gratitude.

3.- The directors, managers or employees of the company, in the exercise of their duties, are also strictly forbidden to request or receive any kind of gifts or items that are totally unacceptable due to their high price or value, and that clearly depart from the normal customs of courtesy and gratitude.

4.- The directors, executives or employees of the company, when they find themselves in any of the prohibited situations described above, shall abstain from accepting any such gift, donation, benefit or advantage. If it has been given, it shall immediately be handed over to the CSMPD for return to the issuer.

The communications shall be verified by means of an e-mail which shall be entered in the file created for this purpose.

5.- The directors, managers and employees of the company in the exercise of their duties are strictly forbidden to promise, offer or grant to the directors, managers, employees or collaborators of any company that is a client, supplier or service provider with which they have commercial dealings, or which they are in the process of attracting, gifts, benefits or advantages of any kind that are intended as consideration for unduly favouring the company "SAMTACK, S.L." over others in the acquisition or sale of goods, contracting of services or in business relations. The only gifts and gratuities that can be offered must be completely free of charge and without any kind of consideration.

6.- Such gifts, donations, benefits or advantages which may be offered must be of reasonably moderate value and, by their nature, must be consistent with normal customs of courtesy and gratitude.

7.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another manager or employee of the company, whether from the aforementioned departments or any other, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.6. Avoidance of the commission of the crime of money laundering in Article 302(2) of the PC, in relation to Article 301 of the PC.

The risk of commission of the aforementioned offence has been identified only in the company's management department. However, it is mandatory for all personnel in general.

1.- Any Director acting on behalf of the company, is strictly forbidden to acquire, possess, use, convert, or transmit goods, knowing or suspecting that they have their origin in a criminal activity of a client company, supplier, or service provider of "SAMTACK, SL". Likewise, it is forbidden to carry out any act that entails the concealment or cover-up of said unlawful origin, whether by means of the aforementioned activities or by any other imaginable means.

A director will be considered to have a "suspicion" when the different departments of the company, after carrying out the relevant investigations or consultations, inform him or her that there are reasons to believe that the company with which he or she intends to contract, may maintain shady or presumably criminal dealings with respect to its assets, business activity, equity or finances.

2.- Any Director of the company acting on behalf of the company must behave in accordance with the provisions of Act 10/2010 of 28 April on the prevention of money laundering and financing of terrorism (hereinafter LPBCFT). To this end, the CSMPD and any worker with financial responsibility functions that so requests will have at their disposal a copy of the aforementioned Act to learn and inform themselves about its contents. Likewise, the regulations for the monitoring of said Act, contained in Royal Decree 304/2014 of 5 May on the Prevention of Money Laundering and the Financing of Terrorism, shall also be available to them.

Such copies may be kept in a computer file and need not be printed out.

3.- In the case of new contracts, the directors, managers or workers, operating on behalf of the company, shall formally identify the companies and professionals with whom they intend to enter into a contract. Specifically, they will identify any natural or legal persons who intend to establish business relationships or intervene in any operations in the manner established by the LPBCFT.

4.- When there are indications that the identity of the beneficial owner declared by the client is not accurate or truthful or there are circumstances that determine special examination in accordance with Article 17 of Act 10/2010 of 28 April, or communication by indication, in accordance with Article 18 of Act 10/2010 of 28 April, the accreditation of the beneficial owner shall be carried out by obtaining information from documents or reliable independent sources.

5.- When the company is faced with a situation in which the circumstances of the previous point occur, prior to contracting, the management will seek the advice and assistance of the external advisor of the CSMPD, who will issue a report establishing the guidelines for action to be followed by the company in order to be able to contract with absolute assurance with the company or individual in question.

6.- Only after such consultation shall the company management take the appropriate decision regarding the aforementioned contracting.

7.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another manager or employee of the company, whether from the aforementioned departments, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.7. Avoidance of the commission of the crime against the Public Treasury in Article 310(a) of the PC, in relation to Article 305 of the PC.

The risk of commission of the aforementioned offence has been identified in the company's management department.

This protocol is especially aimed at the Administrator in charge of the administration department, although it is compulsory for all company personnel in general.

1.- The only person authorised to physically complete the periodic tax returns and self-assessment forms of the state, regional and local tax authorities is Ms. GEMMA MAS ORTAS, who will pay them using the CRN (Complete Reference Number) system, with the exception of VAT, which will be paid directly by the labour consultancy from the company's account.

2.- Other workers of the company may only take part in the process of calculating and paying taxes if there is a specific order to do so from the administrator, Ms. GEMMA MAS ORTAS, limiting their actions to the specific content of the order received.

3.- The administrator, Ms. GEMMA MAS ORTAS, shall always include in the tax forms the authentic amounts or financial positions of the company. She will not allow any alteration of financial data that distorts the payment of what is actually due.

4.- The administrator, Ms. GEMMA MAS ORTAS, before submitting the tax returns, shall send a photocopy of them to the Chairman of the CSMPD for his information two days before their submission and payment to the official body. If no counter order is received within 24 hours, she shall proceed to make said submission and payment.

5.- The aforementioned obligation also extends to any form or way of declaration that refers to the payment of amounts withheld or that should have been withheld or paid on account, or in terms of improperly obtaining rebates or enjoying tax benefits.

6.- The payment shall always be made electronically to the Government Tax Office using the NRC system. Any changes to this payment mechanism must be approved by the Board of Directors of the company.

7.- The Board of Directors is required to hire an approved and reputable company or institution to carry out an annual audit of the company in order to assess and verify the correctness of the company's financial and tax situation and legal transactions in general.

8.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by the aforementioned administrator or another manager or employee of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.8. Avoidance of the commission of the crime against the Social Security in Article 310(a) of the PC, in relation to Article 307 of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Management and Administration.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- All the labour information that the workers of the department send to the legal consultancy to be forwarded to the Social Security so that it can prepare the appropriate contribution forms, must be supervised directly by the administrator Ms. GEMMA MAS ORTAS.

2.- The submission and payment of such contribution forms and documents shall always be made electronically to the General Treasury of Social Security through the NRC system. Any change in this payment mechanism must be approved by the Board of Directors of the company.

3.- Under no circumstances shall it be permitted to provide the legal department with biased data relating to workers' social security contributions.

4.- In the event of significant changes in the employment situations of workers, the administrator, Ms. GEMMA MAS ORTAS, shall report this situation to the Chairman of the Board of Directors of the company.

5.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by the aforementioned administrator or another manager or employee of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel

set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.9. Avoidance of the commission of the crime against the Social Security in Article 310(a) of the PC, in relation to Article 307(b) of the PC.

The risk of commission of the aforementioned offence has been identified only in the company's management department.

This protocol is especially aimed at the directors of the company, although it is compulsory for all company personnel in general.

1.- It is strictly forbidden for the Directors of the company to aid any employee of the company to receive any benefit from the social security system in an unlawful manner, by simulating fictitious situations, misrepresenting facts, or consciously concealing aspects which they had a duty to report.

2.- In the letters of dismissal or in the supporting documents that enable the Public Administrations to collect from third parties, the events that have actually taken place shall always be stated, without any alterations, omissions or vagueness of any kind that might lead to confusion on the part of the Administration with economic damage to the latter.

3.- All the documents referred to in the previous point must be signed by two of the company's Directors, and the situation must be reported to the Board of Directors at the next periodic meeting.

4.- Either of the two Directors shall deliver a copy of the aforementioned documents to the Chairman of the CSMPD for the records of said body. The dismissal of the worker shall be dealt with at the following ordinary meeting of the CSMPD, which may decide as appropriate in the event of any factual inaccuracy of economic significance for the public administration being observed.

5.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by the directors or another manager or employee of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.10. Avoidance of the commission of the crime against public health involving the manufacture and dispatch of substances harmful to health or hazardous chemicals that may wreak havoc in Articles 359 and 360 of the PC, in relation to Articles 366 and 367 of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Production and Laboratory.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- It is expressly forbidden at all times for company personnel handling “container products”, or packaging products, of client companies to introduce or add to them substances, chemicals or products of any other kind that are harmful to human health and that may cause nutritional problems among the population. These workers may only introduce or mix products which have been expressly tested by the company's laboratory and which have the approval of that department, and

which must also be compatible and comply with the specific legislation governing such products, if such legislation exists.

2.- It is therefore expressly forbidden for any worker, employee or member of the company that intervenes in the production process to apply substances or chemicals to the "container products" or packaging of food that is to be shipped, without it being expressly stated that the formalities foreseen in the Laws and Regulations that regulate the processing and use of such substances and products have been complied with. Compliance with such formalities must be verified in the manner set out in the following points.

3.- In order to be able to carry out such additions or mixing, the company's laboratory, each time a new product is introduced, must have the certificate of suitability of the product issued by the Faculty of Chemistry of the University of Zaragoza.

The company's laboratory shall prepare a document to which a copy of the aforementioned certificate is attached, which shall be sent to the Production Department.

Once the Production Department has received this document, it can start the addition or mixing process.

If this document is not provided by the company's laboratory, the head of the Production Department must request it from the head of the laboratory, and under no circumstances may an addition or mixing process be commenced without the Production Department being in possession of the aforementioned document and the copy of the attached certificate.

In the event that this document is not available after having been duly requested, the head of production shall inform the Chairman of the CSMPD of this fact and await his orders in order to proceed.

4.- In the aforementioned document issued by the laboratory, express mention shall also be made of the fact that the products to be added comply with the conditions to which the specific regulations governing the use of such products may refer.

5.- The production department shall have a "Register of Documents of Technical Accreditation of Products" in which all the documents and certificates referred to in the two previous points shall be kept.

6.- The company shall direct the CCTV cameras it currently possesses towards the manufacturing processes where such product addition and mixing tasks are performed.

7.- Any incident occurring during the addition and mixing processes shall be reported by the production manager to both the laboratory manager and the Chairman of the CSMPD, a written note being taken by the latter, who shall take the appropriate measures, following advice from the laboratory department. For this purpose, a "Production Process Incidents Register" shall be opened.

8.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another member of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may

result in the liabilities established in section 4.2.2.2.

3.3.3.11. Avoidance of the commission of the crimes against public health involving adulteration with additives or agents, and poisoning or adulteration with infectious substances, of foodstuffs and food substances, in Articles 364(1) and 365, in relation to Articles 366 and 367 of the PC.

The risk of commission of the aforementioned offence has been identified in the following company departments: Production and Laboratory.

This protocol is especially aimed at the managers and workers of these departments, although it is compulsory for all company personnel in general.

1.- It is expressly forbidden, at all times, for company personnel handling "container products", or packaging products, of client companies, to introduce or add to these products any kind of unauthorised agent that is harmful to human health.

2.- It is expressly forbidden, at all times, for company personnel handling "container products", or packaging products, of client companies, to apply to them any kind of poison, toxic substance, virus, bacteria or parasite that may be seriously harmful to human health.

3.- The aforementioned prohibitions apply to all those involved in the production process, and shall be maintained at all times, even when receiving orders to the contrary from the company's senior management.

4.- To avoid the above issues, and given that the notions of "unauthorised agent", or "poison", or "toxic substance" may be unknown to all those involved in the production process, when given any order to apply products or substances, the worker involved in the production process shall always first demand the documents and formalities established in point 3.- of the above protocol.

5.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of the aforementioned illegal practices by another member of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.3.3.12. Avoidance of the commission of the crimes against public health by trafficking in drugs, narcotics and psychotropic substances in Article 368 of the PC, in relation to Article 369(a) of the PC.

The risk of commission of the aforementioned offence has been identified only in the production department.

This protocol is especially aimed at the managers and workers of this department, although it is compulsory for all company personnel in general.

1.- It is expressly forbidden at all times, and regardless of their intentions, for the personnel involved in the reception, transport and storage of products from client or supplier companies, to bring any kind of toxic drugs, narcotic substances and psychotropic products onto the premises of the company.

2.- When anyone in the company, and in particular the workers referred to in the previous point, has reasonable suspicion of the present or future presence of any of these products in the vehicles arriving at the company, they are required to

immediately and directly report this event to the Chairman of the CSMPD.

3.- The Chairman of the CSMPD shall take note in writing of the communication received, and shall immediately contact the management of the client company, supplier or service provider carrying out the transport in question to request explanations and, where appropriate, authorisation to open the aforementioned vehicles in the presence of one of their legal representatives or delegates.

4.- Likewise, and in parallel, the Chairman of the CSMPD shall inform the police, requesting their presence in order to proceed with the opening of the suspect packages or containers, making himself available for whatever is required by the police or judicial authorities.

5.- The Chairman of the CSMPD shall draw up a written note on the matter and shall inform the CSMPD at the next periodic meeting, and the agenda thereof shall include the discussion of the matter and adoption of any other measures deemed appropriate.

3.3.3.13. Avoidance of the commission of a crime of smuggling of legal goods in Article 2 (a), (b), (c) and (d), and 2.6 of Act 12/1995, of 12 December, on the Prevention of Smuggling.

1.- At all times, all the goods, merchandise or items to be imported or exported by the company "SAMTACK, S.L." shall be presented for clearance at the customs offices or places authorised by the customs authorities, in accordance with the provisions of customs legislation; the concealment or removal of any merchandise being inadmissible.

2.- Any batch of goods, merchandise or items to be imported or exported by the company "SAMTACK, S.L." whose value is equal to or greater than one hundred and fifty thousand Euro (€150,000) must be approved by the Board of Directors, who shall establish, if necessary, the conditions of the shipment in accordance with customs legislation.

3.- For this purpose, the company will have a copy of the applicable provisions of the "REGULATION (EC) No. 450/2008 of the EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 23 April 2008, laying down the COMMUNITY CUSTOMS CODE (MODERNISED CUSTOMS CODE)" as well as a copy of the "TIR CONVENTION of 14 November 1975" available for the management and senior executives of the company. This copy may be kept in a computer file and need not be printed out.

4.- Any operation involving a consignment of goods, merchandise or items to be imported or exported by the company "SAMTACK, S.L." whose value is less than one hundred and fifty thousand Euro (€150,000) shall only need to be approved by one of the company's directors, although the CSMPD must also be informed.

5.- All operations of import or export of goods, merchandise or items carried out with countries outside the European Union must have material documentary support which expressly and truthfully states the country of origin of the import, the specific type of goods and merchandise of the shipment, and the strict compliance with the legal requirements established in the customs regulations.

6.- Such accreditation operations shall be carried out by the company's administration department, under the supervision of the administrator responsible for that department and the Chairman of the Board of Directors, and

must be properly documented before the actual implementation of the shipment. Once these verification and supervision operations have been performed, the administration department shall provide a copy of the operation to the CSMPD for its information and for verification of compliance with all the legal requirements.

7.- If the CSMPD observes that any of the requirements necessary for the operation to be considered legal have not been met, it shall inform the Chairman of the Board of Directors, providing him with the most appropriate proposal for amendment, depending on each case.

8.- All operations involving the import or export of goods, merchandise or items subject to prior administrative authorisation shall require that the mandatory documentation be examined by the CSMPD prior to its submission for approval.

9.- Any director, manager or employee of the staff who becomes aware of the carrying out of any of illegal practices by another member of the company, is obliged to report them in accordance with the stipulations contained in the reporting channel set out in section 4.1. Failure to do so may result in the liabilities established in section 4.2.2.2.

3.4. STAFF TRAINING PROGRAMS

In order to disseminate the code of ethics, its principles, the controls implemented, the internal investigation protocols and the preventive and disciplinary policies adopted by the company, a training program will be carried out for all the company's personnel.

The course will be given by the CSMPD's external adviser and shall be based both on a general explanation of the model and on the analysis and solution of specific cases, providing an opportunity for the participants in the training programmes to identify the ethical problems that might arise in the course of their professional activities.

They will also be informed of the existence and functioning of the reporting channels and internal investigation processes, as well as of the disciplinary code and personal and corporate responsibilities arising from possible irregular actions, i.e. those that contravene the code of ethics, the regulatory compliance system and the applicable laws.

4. REACTIVE PART

4.1. REPORTING CHANNEL

The company shall set up a reporting channel so that eligible persons linked to the company can, in good faith and confidentially, report all weaknesses of the compliance system or violations thereof committed by members of the company. All conducts contrary to the commercial code of ethics, the regulatory compliance system or the laws, which represent a significant irregularity for smooth business operation, shall be prosecuted, whether they are criminal conducts (with or without criminal liability for the legal person) or irregularities of an administrative, labour or any other nature.

The reporting channel shall be governed by the following criteria and guidelines:

Any director, employee, worker or member of the company's staff who becomes aware of any practice contrary to the code of ethics, the regulatory compliance system or the law carried out by any member of the company must report it

directly through the CSMPD's legal advisor. For this purpose, all members of the company will have the email address and telephone number of the aforementioned legal advisor.

The manager of the department to which the accused worker belongs may inform any of the members of the board of directors about the irregularities detected, so that they may take the corrective actions they deem appropriate, without prejudice to the decisions that may be taken by the body responsible for processing the reports. In this case, the information regarding the irregularity committed will be given, but without disclosing the name of the informant, in order to safeguard, as far as possible, his/her anonymity.

Disclosure of the identity of the informant shall be made with the utmost discretion and shall always be made in a restrictive manner. In any event, and in the interests of confidentiality, the identity of the informer shall be disclosed only to the extent necessary to enable the successful outcome of the investigation, or to allow any bodies of the legal person that may intervene to be in a position to address the issue. Total anonymity of the informer is allowed in extreme cases where disclosure could lead to possible reprisals and harm to the informer or frustrate the investigation in whole or in part.

When the report involves any of the company's directors or managers, the identity of the informer will never be revealed.

The CSMPD shall take all the measures it deems appropriate to avoid possible reprisals from those affected by the report, or from any other person in the company who considers him or herself to be harmed by the report. To this end, not only will a restrictive identity disclosure system be used (as mentioned above), but when the circumstances relating to the report so advise, the CSMPD may make the following measures available to the informant: the company medical services for possible psychological support; change of their physical location in the company; and even, in extreme cases, encouraging them to request the assistance of the police authority, giving them support in all the procedures of public accusation to be carried out.

The company (by decision of the board of directors), depending on the nature of the report and the risks that the irregular action entails for the company, may reward the informant with a single monetary payment in their next paycheck. It may also promote them to the position considered to be most in line with the actions of unmasking or reporting.

The processing of the reports, and the follow-up of the infringement, shall be carried out by the external lawyer of the CSMPD, in order to preserve its privilege of professional secrecy vis-à-vis possible authorities or public investigations. This professional will initially review and classify the reports submitted, and may discard those he considers irrelevant, harmless or superfluous, or which have been filed in bad faith. As regards the relevant or appropriate reports, he shall carry out an investigation of the offending conduct, requesting the collaboration and support of the CSMPD whenever he considers necessary.

Of all the reports received, he shall send the CSMPD an “acknowledgement of receipt”, expressly stating those for which he has decided to initiate the investigation procedure and guaranteeing, as far as possible, the confidentiality of the matter.

All employees, members, workers, directors, managers and business partners of the company shall be entitled to report. Reports by clients, suppliers and contractors, which come to the attention of the CSMPD by whatever means, shall only follow the course indicated above when the Chairman of the CSMPD considers that this should be the case. Otherwise, depending on the nature of the report, it may be reported to the Board of Directors so that it can take the measures it deems appropriate.

Clients, suppliers and business partners entitled to report may file their report, at their discretion; through their private or corporate e-mail, addressing the message to the Chairman of the CSMPD; verbally, by going to see him in person; or by telephone, by calling his personal corporate number.

When the legal advisor considers that a report has been filed in bad faith, he will not only reject it outright, but will also consider the possibility of instituting appropriate proceedings against the informant, depending on the seriousness of the falsely or improperly reported facts, informing the President of the CSMPD of both the irregular report and the initiation of the proceedings, if any.

The reporting of irregular actions that violate the company's code of ethics, whether they are criminal or not (i.e. whether they are labour, administrative or of any other nature), is always obligatory for the person in question, who is required to report them in accordance with the established guidelines.

The CSMPD will create a restricted computer register, where all the reports filed and all the documentary details related to them will be recorded, apart from any details that the legal advisor may have.

In the event of any criminal act committed by any director, employee, worker or member of the company, which leads to criminal proceedings (whether or not they are of criminal relevance for the legal person), the company shall appear in the legal proceedings as a private prosecutor, provided that its procedural situation allows it.

If the matter is not brought to court, the Chairman of the CSMPD, or any of the members of the Board of Directors, shall proceed to report the alleged commission of the crime to the authorities. This decision shall be agreed upon at an extraordinary meeting of the board of directors.

4.2. PROTOCOLS FOR RESPONSE TO ILLICIT CONDUCT AND EXTERNAL INVESTIGATIONS

4.2.1. Integrated protocol for internal investigations

Through this protocol, the company establishes the internal investigation mechanism as the main tool of the whole response system. The purpose of this protocol is to identify and manage possible violations of the regulatory compliance system, the code of ethics and legal regulations, whether or not they constitute criminal behaviour.

This protocol will take into account all the information obtained, regardless of its origin, in order to get a full picture of what happened and to enable appropriate response measures. Thus, it will take into account: the information received through the reporting channel, the information contained in the media, judicial notifications, consumer complaints, and any other information derived from internal and/or external reports of any kind.

The initiation of an internal investigation will necessarily require the existence of founded and reasonable evidence of a violation of any aspect of the regulatory compliance system. The evidence, or suspicion, may be of any nature (documentary, testimonial, expert, etc.), being limited only by the obvious reasonableness or relevance of the information it contains.

As soon as the company becomes aware of the violation of any aspect of the regulatory compliance system, and the viability, reasonableness and relevance of the evidence is verified, the body of the company responsible for the supervision of the system, will prevent, using any means, the continuance of the illicit or irregular conduct, taking the measures it deems appropriate. Such measures may include, but are not limited to, the following: removing the worker, employee or manager from his or her job, entrusting him or her with other functions in accordance with his or her training and professional category; requesting the administration of the company to take those measures which, by their nature, can only be taken by the board of directors; the adoption any kind of technical, labour and human measures which serve to mitigate or annul the violation that has occurred; and direct action on the violation committed to minimise the damages, or the perpetuation or continuation of the damage.

When the authenticity of the violation of the regulatory system has been established, or when it is considered rationally justifiable, the applicable disciplinary procedures contained in the manual will be activated.

When the aforementioned violation serves as a basis for the formulation of ideas, measures or procedures that are appropriate or desirable for the future mitigation of the same irregular conduct, the supervisory body will convene an extraordinary meeting (within one month of becoming aware of the possibilities for mitigation) to approve, and if necessary, introduce such ideas, measures or procedures for mitigation into the preventive system. The contribution of such ideas may be carried out by any person linked to the company, (worker, member, manager, director, client, supplier, independent professional, etc.), and in any admissible form that clearly states the idea, procedure or measures to be introduced into the regulatory compliance system.

The Secretary of the Supervisory Body shall take the minutes of the meeting, which must be signed by all those attending, and their conclusions or agreements shall be included in the regulatory compliance system in the appropriate manner.

The purpose of the internal investigations will be to gather evidence for the clarification of the facts in question, establishing the following regulatory framework, with the intention of enabling such investigations and avoiding the possible infringement of the fundamental rights of the persons under investigation:

- In the file that may be opened on these internal investigations, the specific purpose of the internal investigation shall be determined in each case. It shall specify whether the purpose is to monitor or change any aspect of the regulatory system, to exercise disciplinary law, or to cooperate with the public authorities in gathering evidence that may substantiate the liability of the natural persons under internal investigation.
- The CSMPD's legal advisor will be responsible for carrying out the internal investigations, and the company must provide him at all times with the

appropriate resources to carry out his tasks. He will always act independently and autonomously, and the company will provide him with all the collaboration he requires.

- The company shall strictly comply with the labour principles and basic rules governed by the Revised Text of the Workers' Statute (hereinafter TRET). In particular: the principle of regulatory hierarchy, referred to in articles 3.1 and 3.2 of said statute; the principle of the most beneficial rule for the worker (pro-employee principle); the principle of absorption and compensation in relation to staff salaries, set out in Article 26.5 of the TRET; the principle of the most beneficial condition; and the principle of inalienable rights, established in Article 3.5 of the TRET.
- With regard to senior management personnel, labour relations will be governed by the will of the parties, taking into account the general system of rights and obligations established in Royal Decree 1382/1985, of 1 August.
- The directors of the company, individually and as a collegiate body, shall observe the principles and rules of the mercantile legal system, established in the following basic regulations:
    - Royal Decree, of 22 August 1885, by which the Commercial Code is published.
    - Royal Legislative Decree 1/2010, of 2 July, approving the Revised Text of the Corporate Act.
    - Act 22/2003, of 9 July, on Insolvency Proceedings
    - Royal Decree 1784/1996, of 19 July, approving the Regulations of the Companies Register.

  All commercial relations shall be governed by the general principles of good faith, known truth, presumption of the onerous nature of the services provided, intention of profit and public order.
- The board of directors and the general management of the company shall ensure that the general principles of criminal procedure are observed in any proceedings initiated in pursuit of possible offences, in particular: the right to a fair trial, the right to defence, and the right not to testify or produce evidence against oneself, as well as those set out in Article 24 EC, in the Judiciary Act and the Criminal Procedure Act.
- The company shall strictly respect, within the scope of the investigation process, the right to the secrecy of communications and the protection of privacy and personal data, and any other fundamental right established directly or indirectly in articles 18 and 24 of the Spanish Constitution.
- Investigative measures shall be governed by the principles of suitability and proportionality. Therefore, the measures to be adopted in the event of breaches or irregularities will vary according to the severity of the case, and may include the adoption of the disciplinary measures referred to in its specific section; providing feedback to the staff involved; communication to the authorities; as well as improving and updating the model controls to prevent similar situations from occurring.

The investigation procedure will include the following phases: preliminary, investigation and decision-making.

The purpose of the preliminary phase will involve all the previous work of assessment about the plausibility of the initial information that questions the conduct of the individual.

The objective of the investigation phase will be to carry out the investigative actions to verify the veracity of the presumed illicit or irregular conduct.

The decision-making phase will determine the concrete reality of the facts in question. Once this has been done, the legal advisor will forward the result to the disciplinary procedure, so that the measures deemed appropriate can be adopted. In addition, internal investigations should be aimed at taking decisions that will prevent the emergence of illicit and irregular conduct in the future, as well as at improving the content and functioning of the regulatory compliance system and the code of ethics.

The body responsible for promoting the internal investigation procedure and the manner in which it is done will respond to the same criteria as those observed in regulating the reporting channel. Therefore, it will be carried out by the legal advisor to the Supervisory Board, who will have already received the reports and will direct the preliminary and investigation phases, not only on the basis of the reports received, but also on the basis of the information gathered by him or sent to him by the CSMPD. In order to carry out the investigation in a satisfactory manner, he must request and obtain from the CSMPD all the resources necessary to conduct the investigation within the company (interviews, access to documentation, etc.); The managers and directors shall provide him with all the information obtained. He will also be responsible for the safekeeping of all the documentation produced during the investigation phase.

The CSMPD will be responsible for the decision-making phase based on the materials contained in the file prepared by the legal advisor, who will present his conclusions and recommendations to the aforementioned Board. The decisions of the CSMPD shall be forwarded immediately to the Board of Directors for the final decisions to be taken. During this decision-making phase, the criteria, guidelines and observations made by the State Public Prosecutor's Office in its circular dated 1/2016 must be adhered to.

4.2.2. Disciplinary Proceedings

The management of the company shall be governed by this disciplinary system in the event of non-compliance with the regulatory system being observed, whether it be any kind of irregular actions, or criminal actions, which infringe the system, its code of ethics, or the law. The system is intended to be a body of rules and regulations, including the conditions, guidelines and penalties considered most useful and appropriate to respond to any kind of irregularities that may be committed.

In order to give it a homogeneous, consistent and unitary character, the disciplinary system will be adapted to the form and structure of the Disciplinary Proceedings stated in the CCGIQ, according to Resolution of 26 July 2018, of the Directorate General of Labour, Agreement Code, No. 99004235011981.

In this way, this disciplinary code adds the illegal actions included in this

regulatory system to those established in the Disciplinary Proceedings of the aforementioned agreement, modulating the penalties according to the level of seriousness established therein.

Therefore, this disciplinary system is complementary to, and not exclusive of, the disciplinary proceedings included in the CCGIQ, and any interpretation made must be in accordance with the fundamental principles and philosophy that govern the aforementioned agreement.

Therefore, any interpretation to be made of the irregularities perpetrated against this regulatory system, its code of ethics, and other legislation, shall be in accordance with the fundamental principles and philosophy governing the aforementioned agreement.

The disciplinary actions established shall be of a labour nature and independent of the criminal penalty that might apply to the guilty party if the offence committed were also a crime. Furthermore, it is intended to respect, at all times, the *non bis in idem* guarantee system that forms part of criminal law.

4.2.2.1. Personal scope of application of the disciplinary proceedings

According to Article 1.1 of the CCGIQ itself, the agreement regulates working conditions between companies and workers in various subsectors of the chemical industry; including those engaged in the production of adhesives, rubbers, dyes and varnishes and other activities related to the chemical industry. It therefore refers to "workers" linked to these companies and activities. In fact, Article 3(1) of the CCGIQ itself is concerned with establishing the express exclusion of those persons, relationships, services or activities that are not affected by the CCGIQ, in accordance with the stipulations set out in Article 1.3 and 2 of the Revised Text of the Workers' Statute Act (hereinafter TRET).

Therefore, "worker" is construed as any person who provides paid labour services as an employee within the scope of the organisation and management of a company. This concept therefore excludes all those persons who hold administrative positions in the decision-making bodies of companies, provided that their activity only involves the performance of tasks inherent to such positions (Article 1.3(a) of the Revised Text of the Workers' Statute Act, hereinafter TRET).

Special labour relations, such as those relating to senior management personnel referred to in Article 2.1(a) of the TRET and Article 3 of the CCCIQ itself, will also be excluded from the aforementioned agreement.

Having said all the above, and in accordance with the provisions of the aforementioned regulations, the list of penalties to be imposed will only apply to those employees, workers and members of staff who, due to their condition or employment relationship with the company, are considered for legal purposes as "employees of the company" and to whom the TRET applies.

Temporary competence is fixed for an indefinite period and is automatically extended when the agreement governing the company is extended.

For the rest of the personnel included in a special labour relations regime, and therefore governed by different regulatory bodies, a specific section is established with the guidelines for action to be observed, in accordance with the possibilities offered by the legislation in force.

The infringements and penalties set out in this disciplinary code shall always be communicated in writing, with a request for acknowledgement of receipt. They must be mandatorily be recorded in the electronic file to be created for this purpose. The refusal to acknowledge receipt by the offender shall be specified in the communication document itself.

4.2.2.2. Infringements that may be considered criminal

The management of the company shall be empowered to penalise employees, workers, members and managers of the company, whose contractual regime allows it, for the actions referred to in the respective section of the manual, in accordance with their seriousness, importance or intention, and in accordance with the classification set out in art. 62 of the CCCIQ.

In this way, misconducts will be classified as: minor, serious or very serious.

The following are considered minor misconducts:

a) Failure to report any of the activities related to the "crimes of discovery and disclosure of company secrets".

b) Failure to report any of the activities related to the "crimes of business corruption".

c) Failure to report any of the activities related to the "crimes of frauds".

d) Failure to report any of the activities related to the "crimes against the Public Treasury".

e) Failure to report any of the activities related to the "crimes against the Social Security".

f) Failure to report any of the activities related to the "crimes of discovery and disclosure of secrets".

g) Failure to report any of the activities related to the "crimes of computer damage".

h) Failure to report well-founded suspicions regarding the introduction into the company of toxic drugs, narcotics and psychotropic substances as referred to in point 2(d) of Annex 2.

The following are considered serious misconducts:

a) Failure to report any of the activities related to the "crimes involving the manufacture and dispatch of substances harmful to health or hazardous chemicals that may wreak havoc".

b) Failure to report any of the activities related to the "crimes involving the adulteration with additives or agents, and poisoning or adulteration with infectious substances".

c) Failure to report having come into contact with a business secret.

d) Requesting or receiving any kind of excessive gift or value item from any client company, supplier or service provider of "SAMTACK, SL."

e) Failure to report having received gifts or effects from third parties.

f) Failure to have placed such gifts and effects at the disposal of the CSMPD.

g) Failure to comply with the duty to check invoices and payments and to notify the supervisor.

h) Failure to comply with the duty to sample invoices and payments.

i) Failure to comply with any of the obligations to complete and submit tax statements.

j) Failure to comply with any of the obligations to complete and submit contribution documents.

k) Failure to notify the management of the CSMPD of the introduction into the company of toxic drugs, narcotics or psychotropic substances by any person.

l) Failure to submit quarterly product migration tests to the Chairman of the CSMPD.

The following are considered very serious misconducts:

a) Carrying out activities that imply unauthorised access to a company secret of any client, supplier or service provider of "SAMTACK, S.L.".

b) Failure to exercise due care regarding business secrets accessed in an authorised or fortuitous manner by using or publicly disclosing them.

c) Making any kind of interception of telecommunications, or using any technical devices for listening, transmitting, recording or reproducing sound or image, or any other communication signal, of any client company, supplier or service provider of "SAMTACK, SL", or any natural person, to discover any aspect or confidential content thereof.

d) Receiving, requesting or accepting any kind of gift, advantage or benefit resulting from a trade consideration for any client company, supplier or service provider of "SAMTACK, S.L."

e) The preparation of duplicate invoices with altered amounts or items.

f) The preparation of invoices, delivery notes or any other similar document that reflects an unrealistic and irregular situation with economic damage to the client company of "SAMTACK, SL".

g) Gaining access to or taking possession of papers, letters, e-mails or any other documents or personal effects, either of the staff of the company or that of any other company, which by their very nature and content, are of a secret, confidential or intimate nature.

h) Taking possession of, using or modifying third-party reserved data of a personal or family nature that is registered in folders, computer, electronic or telematic media, or files, either of the staff of the company or that of any other company.

i) Illegal access, in violation of established security measures, to a database or information system of any company.

j) The interception of non-public transmissions, by means of technical devices or instruments, of computer data from, to or within an information system belonging to any public or private undertaking or legal person.

k) The deletion, damage, impairment, alteration or other similar action that makes third-party data, computer programmes or electronic documents inaccessible.

l) Virtual access to a document, programme or computer application of a third party, without their prior authorisation.

ll) Introduction into the market, through the "container products" or packaging products of client companies, of substances, chemicals or any other type of product that is harmful to human health and that may cause nutritional damage among the population.

m) Introduction into the market, through the "container products" or packaging products of client companies, of non-authorised agents, poisons, toxic substances, viruses, bacteria or parasites that are harmful to human health.

n) Introduction into the market, through the "container products" or packaging of client companies, of chemical substances or products that do not comply with the formalities provided for in the laws and regulations governing the processing and use of such substances and products.

ñ) Applying, adding or mixing new additives, agents or substances to the "container products" or packaging of client companies without the "approval" of the company's laboratory.

o) Introducing toxic drugs, narcotic substances and psychotropic products into the company.

p) Failure to draw up the document establishing the chemical suitability of new products or substances to be added to "container products" or packaging.

q) Defective execution of the document referred to in Misconduct p) because the new products or substances have not been properly checked or tested, or because untruthful statements have been deliberately included regarding the properties, characteristics or legal formalities to be complied with by such substances or products.

4.2.2.3. Violations of the code of ethics and regulatory compliance system

The disciplinary proceedings for violations of the code of ethics and regulatory system is governed by the same principles and criteria established for crimes; and therefore, also the penalty system.

The following are considered minor infringements:

a) The violation of the duties of promptness in professional and/or business actions.

b) The improper use of the company's assets, services and technologies, other than for exclusively business purposes.

c) Internal or external actions aimed at discrediting the company, with regard to its working methods; objectives and structural organisation.

The following are considered serious infringements:

a) Any action of any kind that violates the principles of impartiality and transparency.

b) The violation of commercial standards of professional correctness, transparency and loyalty, in the processes of hiring suppliers, other professionals and in relation to customers.

c) The violation of the principles of confidentiality, in the exercise of the functions assigned to the workers who have a relationship with the company.

d) Non-observance of the principles of merit, competence and equal opportunities in the hiring of personnel.

e) Non-observance of transparency criteria when establishing rewards, promotions, responsibilities and participation in corporate activity.

f) Internal or external actions aimed at discrediting the company, its managers, workers, customers, suppliers and professionals who have a relationship with the company.

The following are considered very serious infringements:
a) Actions by company personnel that may generate a conflict of interest with the company's corporate purpose.

b) The violation of any environmental commitment imposed by the company in compliance with the legislation on the subject, indicated in section 3.1.3.5.

4.2.2.4. Penalties

The management of the company has the power to impose penalties under the terms of this disciplinary code.

For the application of the penalties, the degree of responsibility of the offender will be taken into account, as well as their professional category and the impact of the misconduct on the other workers and on the company.

The management of the company shall inform the workers' legal representatives of any serious or very serious misconduct. In these cases, the person concerned shall have four working days to respond to the communication made by the company regarding the offences of which he or she is accused. Once this period has elapsed, the company shall communicate the penalty imposed, if any.

It will be necessary to file a statement of defence in cases of imposition of penalties on workers holding elected trade union positions, and in those cases established in the legislation in force or determined by the company. The person concerned, as well as the Works Committee or the personnel and/or union delegates, shall be notified of the proceedings and shall be submitted to a hearing before any penalty can be imposed.

4.2.2.5. Types of penalty

In accordance with Article 67 of the CCGIQ, the penalties that may be imposed in each case, depending on the seriousness of the misconduct committed, are as follows:

a) For minor misconducts: Verbal reprimand. Written reprimand. Suspension of the employee and their salary for up to two days.

b) For serious misconducts: Suspension without pay for three to fifteen days.

c) For very serious misconducts: Suspension of the employee and their salary for sixteen to sixty days. Until the termination of the employment contract, in the event that the misconduct is classified as very serious.

In any event, the company, taking into account the circumstances, may apply any of the penalties stipulated for less serious types of misconducts, without such a

reduction in the penalty implying any variation in the classification of the misconduct.

4.2.2.6. Statute of limitations

The statute of limitations for misconduct shall be in accordance with the provisions of articles 68 of the CCGIQ.

The statute of limitations shall lapse after ten days for minor misconducts, twenty days for serious offences and sixty days for very serious offences, from the date on which it became aware of their commission, and in any case six months after the misconduct is committed.

4.2.2.7. Internal procedure for the attribution of responsibilities

Any penalties to be imposed shall be carried out by the management of the company, after observing the following procedural steps; all information obtained through the reporting channel, the conclusions reached by the external advisor and the decisions reached by the CSMPD shall be submitted to the general manager (or, for the most serious cases or matters within its sphere of competence, to the Board of Directors), for the purposes of implementing the appropriate penalty in accordance with the decisions of the general manager or the Board.

If these management bodies refuse to take such a decision, the CSMPD may take whatever actions it deems appropriate to report the situation to the labour, administrative, civil or criminal authorities.

If the decisions relate to the general manager, when the procedure against him is followed, the CSMPD shall report whatever it deems appropriate to the labour, administrative, civil or criminal authorities.

4.2.2.8. Reporting actions among directors

As mentioned above, the TRET establishes a series of requirements and conditions in labour relations that define its scope of application. Thus, due to their positions or special recruitment schemes, certain persons who provide their services for the company are not covered by the legislation contained in CCGIQ.

This is the case of the members of the Board of Directors who are not affiliated to the General Social Security System.

There is no legislation in our law that regulates the labour liability of the directors of a company. However, from a civil, commercial, tax and criminal point of view, their actions and possible responsibilities are legally regulated according to the different legislations.

Thus, for illegal and irregular actions against the system of regulatory compliance, code of ethics, or legal regulations, the company will take the actions stated in art. 236 of Royal Legislative Decree 1/2010 of 2 July, approving the revised text of the Corporate Act (hereinafter TRLSC), against its directors.

Therefore, the company establishes the following guidelines for action:

a) The directors shall be liable to the company, to the shareholders and to any third parties involved, for any damage caused by acts or omissions contrary to the law, the bylaws, the regulatory compliance system or the code of ethics, provided that some kind of fraud or negligence has occurred.

Thus, they shall be liable for all the acts referred to in the section of this manual on non-compliance.

b) Non-compliance by the directors shall be reported by the Supervisory Board to the relevant public authorities.

c) The legal actions or proceedings to be taken shall only be directed against the director who has actually performed the harmful action or omission indicated in the law, the bylaws, the regulatory compliance system or the code of ethics, the rest of the directors of the collegiate body being exempt from such irregularities.

d) The remaining directors shall file directly against the director responsible for any of the offences and irregularities indicated in the section in question, the "corporate liability action" referred to in article 238 of the TRLSC.

e) When the seriousness and importance of the illegal action carried out by the director so warrants and said action constitutes a crime, the company shall initiate criminal proceedings, filing the appropriate criminal charge with the relevant judicial body, subject to the agreement of the General Meeting.

f) If criminal proceedings have already been initiated against the director in question, the company shall appear in the proceedings as a private prosecution when its procedural situation permits, subject to the agreement of the General Meeting.

g) Even if the remaining administrators choose not to file the complaint, they shall proceed to report the activity carried out by the director concerned at the police or judicial headquarters, if it should constitute a crime, and the court has no record of the commission of the crime.

h) For the purposes of mitigating the effects of the action of the director concerned as soon as possible, the other directors shall take all the actions established by the TRLSC in order to ensure the suspension or removal of the director concerned.

i) The actions for compensation that may apply to shareholders and third parties due to the actions of directors that directly harm the interests of the former are excluded.

j) Liability actions against directors, whether corporate or individual, shall be statute-barred after four years from the day on which they could have been filed, as stated in Article 241 of the TRLSC.

k) The criminal actions that may be taken shall be subject to the statute of limitations set out in article 131 of the PC.

4.2.3. Damage repair policies

Any damages that the personnel linked to the company may cause as a consequence of the infringement of the regulatory compliance system, code of ethics, or violation of laws or regulatory provisions of any kind, shall be covered by the company, to the extent that the nature of the damage caused allows it.

When the damage is of an economic nature and can be objectively quantified, the company shall cover it directly, or through the appropriate civil liability insurance, which it is obliged to take out.

The company may take the actions for recovery it deems appropriate against the natural person who has caused the economic damage, in claim of its legitimate

interests.

In any event, the company undertakes to compensate any damages caused to third parties by staff working for the company, whatever their employment status, that are not covered by the company's civil liability insurance, in order to mitigate any negative consequences of the action taken.

4.2.4. Protocol for response to external investigations

By means of this protocol, the company establishes the guidelines for action and measures to be observed by the company's personnel in the event of police/judicial entries and searches in its establishments.

To this end, the company, through the legal advisor of the supervisory board, shall give an information course to the personnel of the CSMPD and the department heads, to teach them how they should behave in the event of entries and searches in the company's premises by police and judicial authorities. Thus, the company's personnel shall be instructed on the following issues: document giving the right to enter and search; where exactly the authorities can enter; what kind of documentation they can examine; whether they can access employees' computers and mobile phones, and whether they can seize them or their contents; and whether or not the presence of the lawyer is necessary in the proceedings. It will also leave in paper format a compilation of the supporting legislation regulating this type of action to be taken by the authorities.

Both the CSMPD and each of the company's heads of department shall have a copy of this document in order to know how they should behave at all times in the event of such action.

For these purposes, the compilation-explanation document shall include all the provisions stated in Chapters I, II, III and IV of Title VIII of Book II of the current Criminal Procedure Act, Royal Decree of 14 September 1882 relating to the entry and search procedure and to the events or incidents that may occur during the procedure.

In any event, one of the members of the CSMPD and the head of the department concerned must always be present in these searches, their mission being to verify the correctness of the actions performed by the members of the police teams and judicial commissions in accordance with the legal provisions established. To this end, they shall check the appropriate entry and search orders and accompany the judicial commission throughout the entire period of the proceedings. The actions of the aforementioned persons shall never hinder or obstruct the actions of the authorities, but shall always be aimed at facilitating their work and demonstrating the company's commitment to an appropriate corporate ethical culture.

4.2.5. Collaboration with the authorities

Once a possible criminal act committed by one of its employees, managers or directors comes to light, depending on the specific circumstances of the case and its legal expectations and defence strategies, the company will decide whether to confess the facts before the authorities and collaborate with them in the investigation, or whether to exercise its constitutional right not to plead guilty and not to produce evidence or to testify against itself.

This decision shall be adopted at an extraordinary meeting of the Board of

Directors and shall be taken after being in possession of a copy of all the background information available to the company on the event (initial report, file open, investigative actions conducted, conclusions of the external advisor of the CSMPD, recommendation of the CSMPD, etc.). Before taking a decision on this matter, the board of directors may take direct advice from the aforementioned lawyer, so that he may inform the board of the various consequences of proceeding in one way or another.

If the person who allegedly committed the criminal act is the general manager or one of the directors, the remaining members of the board of directors shall take the measures they deem appropriate, following the above guidelines.

5. MODEL REVISION

As already indicated in the final paragraph of point 2. this preventive organisational model and regulatory compliance system will be of a dynamic nature as they are subject to permanent updating, with a view to adapting them to the circumstances and business situation existing at any given time. Updates shall take into account natural structural changes in the company (whether they affect its profile or the structure of its activities), as well as any other changes in the profile of criminal risk, adapting them, in any event, to the legislative changes and the jurisprudential doctrine that the Supreme Court defines in the development of the institution.

The entire organisational model and regulatory compliance system of the company shall be reviewed two years after each update. The company shall delete, add or modify any aspects of the model it considers obsolete, outdated or eligible to be updated or modernised.

During the intermediate period between modifications to the model, the CSMPD shall hold the ordinary maintenance meetings referred to in the specific section regulating the functions of the CSMPD. In the event of a crime or act of particular importance, the CSMPD shall hold an extraordinary meeting and shall approve the specific mitigating measures and/or model revisions deemed most appropriate, submitting them to the Board of Directors, for implementation, .

The company currently reserves the right to carry out the periodic internal audits recommended by UNE 19601/17, as well as the other guidelines established in its articles 9.2 to 9.5 and 10, until the effective operation and implementation of the model is verified.

***

IMPLEMENTATION OF THE MANUAL. COMPLIANCE OFFICER

This manual containing the "Compliance" programme for the control and supervision of possible regulatory risks that may be committed by the company "SAMTACK, S.L.", has been prepared by the undersigned, Mr. IGNACIO PASTOR SANTIAGO, assoc. No. 16,743 of the Bar Association of Barcelona, Doctor of Criminal Law from the University of Barcelona, and a graduate in Criminology from the Autonomous University of Barcelona.

In witness whereof, the aforementioned Compliance Officer signs this Manual on 20 June 2019.

Signed: Ignacio Pastor Santiago,

Assoc. No.: 16743 ICAB

TABLE OF CONTENTS

***