CRIMINAL RISKS MANAGEMENT MANUAL

of

CEDINSA CONCESSIONARIA, S.A.

March 2020

CONTENTS

I.- INTRODUCTION

1.- CEDINSA's commitment to compliance with the law.

CEDINSA CONCESSIONARIA, S.A. and its investee companies are the leading business group in the tollbooth concession system in Catalonia and the second in number of motorway kilometres under the concession regime.

Our technical capacity and economic solvency are guaranteed by the efficiency of the group and of our partners, among which are top builders.

Since CEDINSA CONCESSIONARIA, S.A. was founded, we have kept a clear and firm commitment to compliance with the law, especially in those matters that, as a business group and for our sector of activity, are particularly sensitive. We have been scrupulously complying with and respecting the various obligations that have been generated in recent years as a result of increased legislation on environmental protection, prevention of occupational risks and protection of personal data, among other areas.

As it must, that business policy of complying with the current law extends to criminal law. To minimise the risk of committing unlawful practices, we have designed a criminal risk prevention model within our structure in accordance with the requirements of Organic Law 5/2010, of 22 June, and 1/2015, of 30 March, amending the Spanish Criminal Code [*Código Penal*].

To do so, we assessed the criminal risks that the entity may incur in carrying out its activity and have designed a model to prevent those risks.

2.- Brief reference to the applicable legislation.

Criminal liability of legal entities was regulated for the first time under Spanish criminal law by Organic Law 5/2010, which established the cases in which legal entities may be penalised, establishing a fixed list of offences that may result in the imposition of a penalty. Organic Law 1/2015, of 30 March, was subsequently passed, amending the Criminal Code in this regard, which entered into force on 1 July 2015. In accordance with the new wording of section 31(a), legal entities may be criminally liable in two cases, if they benefit directly or indirectly:

A) From offences committed by their legal representatives or persons who may make decisions on behalf of the company.

B) And from offences committed by other employees if they were able to commit the deeds due to a breach of the duties of supervision, surveillance and control.

In accordance with this new regulation, the legal entity will be exempt from criminal liability provided that its governing body has adopted and implemented surveillance and control measures suitable for preventing offences and that the supervision of the functioning and compliance with the prevention model implemented has been entrusted to a body of the legal entity with autonomous powers of initiative and control.

Criminal law establishes a series of requirements that a prevention model must meet, which can be systematised as follows:

- Identifying the activities in which the offences to be prevented may be committed.

- Establishing the protocols or procedures that specify the process of shaping the intention of the legal entity and the implementation of the decisions adopted.

- Determining the appropriate financial resources management models to prevent offences from being committed.

- Employees must be required to inform the body responsible for supervising the operation and observance of the prevention model of possible risks and breaches.

- Establishing a disciplinary system that adequately penalises breaches of the measures established in the model.

- The model must be periodically verified and amended when there are significant infringements of its provisions, or when there are changes to the organisation, the control structure or the activity carried out that make them necessary.

The penalties that may be imposed on legal entities for committing offences by their employees or executives are fines, disqualification to obtain certain types of public aid, temporary suspension of activities, closure of premises and establishments, court intervention and winding up of the legal entity.

It should be emphasised that the law envisages four mitigating circumstances for the liability of the legal entity, i.e. four practices that could entail a reduction of the liability that corresponds to the company for the commission of the offence in its structure, and that are the following:

- If the legal entity, before finding out that the legal proceedings are being brought against it, confesses the infringement to the authorities.

- Collaborating in the investigation of the incident by providing evidence, at any time in the proceedings, that is new and decisive to clarify the criminal liability arising from the facts.

- Proceeding to repair or decrease the harm caused, at any time during the proceedings, provided that it is before the hearing.

- Establishing, before the start of the oral proceedings, effective measures to prevent and discover any future offences committed under the aegis of the legal entity.

3.- Scope of application.

The criminal risk prevention model and, in particular, the considerations in this Manual apply to CEDINSA CONCESSIONARIA S.A., as well as all companies belonging to the group: CEDINSA EIX DEL LLOBREGAT CONCESSIONARIA DE LA GENERALITAT DE CATALUNYA, S.A.; CEDINSA D'ARO CONCESSIONARIA DE LA GENERALITAT DE CATALUNYA, S.A.; CEDINSA TER CONCESSIONARIA DE LA GENERALITAT DE CATALUNYA, S.A.; and CEDINSA EIX TRANSVERSAL CONCESSIONARIA DE LA GENERALITAT DE CATALUNYA, S.A. , CEDINSA CONSERVACIÓ, S.L.

The references to 'CEDINSA' are understood to refer to all entities comprising the business group.

II.- ELEMENTS OF THE PREVENTION MODEL

1.- Assessment of criminal risks.

CEDINSA's prevention model forms part of the assessment of the criminal risks incurred by the entity based on its activity and the processes comprising it. These risks were assessed using the following parameters:

- Risk exposure of the entity: assessment of the possibility that the various deeds considered to be criminal may be committed.

- Severity of the consequences: assessment of the criminal sanction envisaged by the Code and the reputational harm to the company.

Based on the values resulting from the combination of both variables, the risks are classified as HIGH/MEDIUM/LOW/MINIMUM.[1]

In accordance with these same parameters, the criminal risk assessment should be kept up to date, periodically reviewing the assessment, and making any corresponding changes if the circumstances change.

2.- General and specific prevention measures.

In view of the criminal risks incurred by the entity, a series of general measures aimed at preventing any criminal risk has been designed, which, in short, may take the form of:

- the CEDINSA Code of Ethics
- Design of the responsibilities in the organisational structure.
- Communication channel
- Training

There are also multiple specific prevention measures for the prevention of specific criminal risks, i.e. risks of committing certain offences. These are detailed in the specific risk/measures matrix table that systematises the following elements:

- Area or process of the company in which the criminal risk is generated
- Section of the Criminal Code
- Criminal risk incurred by the entity
- Situation in which the risk can materialise, i.e., action that could result in a criminal conduct.
- Existing specific measures.

[1] It is attached as ANNEX NO. 1 CRIMINAL RISK ASSESSMENT TABLE.

This table should also be updated to take into account any changes that may be made to the criminal risk map, and to take into account the result of the measures already envisaged or the incidents that occurred, which may determine the need to amend those measures or to supplement them with additional ones.

3.- The CEDINSA Code of Ethics.

On 17/03/2016, the Board of Directors approved the Company's Code of Ethics, a document that sets out the rules and principles that should govern the behaviour of all employees forming part of CEDINSA. They are therefore internal mandatory regulations that affect all employees and executives of the entity, and that are also mandatory for the BOARD.

On 5 March 2020, the Board of Directors approved the Ethics Channel Regulations, expanding the possibility of anonymous reporting through the whistle-blowing channel.[2]

4.- The Procedures Manual.

We also have an essential instrument to carry out the various processes comprising the activity of the company, which guarantees its efficient organisation and development. The Procedures Manual contains the activities of each department in an orderly and sequential manner, establishes the working methods and techniques to be followed, and defines the different responsibilities.

All the Company's employees are obliged to perform the activity characteristic of their post in accordance with the Manual.

5.- Organisational structure. Responsibilities.

[2] Attached as ANNEX NO. 2 is the final version of the Code of Ethics complemented by the Ethics Channel Regulations.

The criminal risk prevention model should be present in all processes of the entity, and it is therefore essential to determine the new responsibilities it generates for all employees of the entity.

A) Board of Directors

First, it should be stressed that the design and implementation of a criminal risk prevention model is an obligation of the governing body of the entities, and is a duty that may not be delegated.

CEDINSA's BOARD has assumed and incorporated that duty, and the resources necessary for the design and implementation of the prevention model have been and will be used. It has also been agreed to appoint the *SUPERVISORY AND OVERSIGHT BODY* as the body supervising the performance and proper functioning of the model.

B) The compliance oversight body.

Within the organisational structure of the company, therefore, *SUPERVISORY AND OVERSIGHT BODY*) assumes the functions of supervising the operation and compliance with the criminal risk prevention model. To perform this function, it has autonomous powers of initiative and control, so that it will report directly to the BOARD on the matters it considers appropriate, and is granted the following functions:

a) Verification that the risks map is correct and up-to-date.

b) Verification of the adequacy of the mechanisms envisaged for the prevention of offences

c) Supervision of the proper functioning of the prevention model.

d) Supervision of compliance with the prevention model by the entity's employees, and any other third party subject to its authority.

e) Advising and reporting on decisions relating to the organisation and operation of the company that may affect criminal risks

f) Providing information to the Company's executives, workers and employees about the existence of the model, its content and its duties.

g) Receipt of communications made by employees with regard to criminal risks.

h) Management of communications received with regard to the prevention model and possible breaches.

i) Reviewing and updating the model

j) Submission of information and proposals to the Board of Directors on the functioning of the various aspects of the prevention model.

The *SUPERVISORY AND OVERSIGHT BODY* will meet at least once every 6 months, and minutes of each meeting are kept. Likewise, each year a report will be issued on compliance with the prevention model, incidents occurring during this period, the modification of the entity's criminal risks and the need to adopt new measures or amend existing ones. This report will be submitted to the Board of Directors and will be included in the corresponding minutes.

C) Heads of Department and executives.

The Heads of each area should, within the scope of the prevention model, be the instrument of the supervisory body so that the measures adopted are filtered in all processes of the entity, giving the appropriate instructions to those working under them and carrying out the actions necessary for their knowledge and resolution of doubts. Therefore, fluid and continuous communication between *SUPERVISORY AND OVERSIGHT BODY* and the Heads of Department is crucial.

Any head of department or executive who has knowledge of an incident with regard to the criminal risk prevention model or breach of the Code of Ethics should immediately notify the *SUPERVISORY AND OVERSIGHT BODY*. In addition, before issuing its annual report, the *SUPERVISORY AND OVERSIGHT BODY* will hold a meeting with all the Heads of Department to assess the implementation of the model and any possible incidents, which will be duly recorded.

D) Employees

To meet the common objective of preventing criminal risks, it is essential for CEDINSA to work together with all employees of the companies in the group, since they are the essential element of the organisational structure and the ones who are in daily contact with the different processes in the company's activity.

Clearly, as indicated above, all employees, without exception, are subject to the principles and rules of the Code of Ethics and, therefore, must act in accordance with them. Furthermore, in

order to achieve the common objective of the effective functioning of the criminal risk prevention model, CEDINSA employees must:

- Provide information on the risks and operation of the measures implemented, which may contribute to improving and updating the prevention model.

- Denounce possible breaches of the Code of Ethics and the commission of practices that may entail the commission of an offence or its future materialisation, of which they are aware.

6.- Communication channels.

In order to comply with the obligation to report on aspects that could contribute to improving the risk prevention model or on practices contrary to the Code of Ethics or constituting a criminal risk, employees have different channels:

- COMMUNICATION VIA SENIOR EXECUTIVES.

Employees may contact their senior executives, who must transfer the content of the information to the various higher levels, until they reach the supervisory body of the model.

- SPECIFIC CHANNEL OF COMMUNICATION.

Likewise, if, due to the nature of the information, due to the possibility of a conflict of interest of the person receiving the information, or for any other reason, employees consider this channel safer or more effective, they can contact the SUPERVISION AND OVERSIGHT BODY directly through the following mechanisms:

- email: organsupervisio@cedinsa.cat
- telephone: 932291060
- post: Av. Josep Tarradellas, 38, planta 6, 08029 Barcelona

The communication must contain

- Full name
- National Identification Number
- and Signature

Communications received by any of the channels will be filed and processed in accordance with their content:

- Proposals relating to the operation of the prevention model will be assessed by the SUPERVISION AND OVERSIGHT BODY which will propose to the governing body the adoption of the appropriate measures, informing the employee of the decision taken.

Allegations of breaches of the code or practices that pose a criminal risk, where applicable, will give rise to the initiation of an investigation by the SUPERVISION AND OVERSIGHT BODY that will be processed in accordance with the procedure detailed below.

The communicator's right to confidentiality is guaranteed, whose identity may not be disclosed to third parties, as well as the guarantee of not suffering any type of negative consequence for submitting the communication.

As an exception, and if - despite the confidentiality commitment - claimants believe they may be harmed by having their identity revealed, anonymous complaints will be admitted if they meet minimum standards of credibility given the information provided.

7.- Training.

It is essential to train workers in the new legal reality and in the measures adopted by CEDINSA to prevent criminal risks, whereby the BOARD, through *SUPERVISORY AND OVERSIGHT BODY*, provides training to all employees of the entity in this regard, in the most appropriate manner in keeping with the position performed.

8.- Disciplinary system.

Any gross breach of the Code of Ethics or of the other elements comprising the criminal risk management model will be considered a breach of contractual good faith, the basic duty of employees in accordance with the Spanish Workers Statute [*Estatuto de los Trabajadores*] and, therefore, where applicable, the corresponding disciplinary measures may be adopted.

It should be remembered that various sections of the Workers Statute establish that good faith must govern the relationship between the company and employees, and is a basic duty of the latter, given that employees must comply with the specific obligations of their post, in accordance with the rules of good faith and diligence (sections 5, 20 [2] and 54. [2]).

II.- RESPONSE PROCEDURE.

In addition to the risk detection and prevention measures, CEDINSA has set up a procedure for the entity's response to communications or knowledge of behaviour that entails a breach of the Code of Ethics or behaviour that entails or may entail the commission of a criminal action in the future. To correct the response to these situations

A specific procedure regulated in the Company's Ethics Channel Regulations is envisaged.

IV.- SUPERVISION AND UPDATING OF THE MODEL.

The BOARD adopts a firm commitment - through the mechanisms described above - to ensure the effective and proper functioning of the criminal prevention model, adopting the decisions and allocating the resources that are necessary.

Likewise, the actions necessary to update the model will be performed in order to adapt it to the new risks that may be detected in the operation of the entity, and when there are changes in the organisation, the control structure or the activity carried out that make them necessary.

This version was approved by the Board of Directors of CEDINSA CONCESSIONARIA, S.A. on 5 March 2020

ANNEX NO. 1

CRIMINAL RISK MAP

Based on the sector of activity in which the companies operate and their organisational structure, we have proceeded to make a risk assessment.
The following formula was used to assess the RISK:

CRIMINAL RISK = (RISK FROM ACTIVITY * 70% + RISK FROM BACKGROUND * 30%) * 75% + (IMPACT OF THE PENALTY * 40% + REPUTATIONAL IMPACT * 60%) * 25%

The RISK of committing a criminal conduct is calculated by weighting the PROBABILITY that it will happen by 75% and, by 25%, the IMPACT that the risk occurring would have on the entity.

Based on our experience, more weight must be given in the calculation to the probability that the risk may occur, in view of the possible impact if it happens. The probability is therefore assigned a value of 75%, compared to the impact which is assigned 25%.

Lastly, the following calculation method is used to calculate each of the parameters:

- PROBABILITY

- A value of 30% has been assigned to the possibility that the risk may occur based on the activity carried out by the company. A value of 0 to 4 was used for each item, where 0 is a risk that cannot materialise in view of the activity and 4 is high probability.

- And a value of 30% is assigned to the occurrence of risk materializations before the company. A value of 0 to 4 has been used for each element, where 0 is the absence of a history of the risk materialising and 4 is the existence of very considerable history.

- IMPACT

- A value of 40% has been allocated to the impact of the penalty for committing an offence in the event of a risk occurring. A value of 0 to 4 was used for each element, where 0 is the absence of a penalty and 4 is the expectation of a very serious penalty.

- And a value of 60% has been assigned to the reputational impact, where 0 is the absence of impact and 4 a great affect on the company's reputation.

The application of the aforementioned formula yields the following result, which was then rounded down, and the risks are classified as follows:

0 to 0.99: MINIMUM
1 to 1.99: LOW
2 to 2.99: MODERATE
3 to 4: HIGH

The calculation table is attached as an appendix, the final result of which is the following valuation:

TYPES OF CRIMES	RISK			
	MINIMUM	LOW	MODERATE	HIGH
Organ trafficking (section 156 bis. [3] of the Criminal Code)	X			
Crimes relating to genetic manipulation (section 162).	X			
Workplace harassment (section 173[1])			X	
Human trafficking (section 177[a][7])		X		
Offences involving prostitution and corruption of minors (section 189 bis)		X		
Against privacy and unlawful access to computer data and programs (section 197 *quinquies*)			X	
Scams (section 251 bis)		X		
Fraudulent conveyance (section 258[b])		X		
Negligent insolvency (section 261 bis)		X		
Alteration of petitions in public tenders and auctions (section 262[2])		X		
Criminal misuse of computer systems (section 264 *quater*)	X			
Against intellectual property (section 270)			X	
Against industrial property (section 273)	X			
Against the market and consumers (section 288)			X	
Corporate corruption (section 288)				X
Refusal of inspection actions (section 294[2])		X		
Money Laundering (section 302[2])	X			
Unlawful political funding (section 304 bis. [5])				X
Against Public treasury and Social Security (section 310 bis)			X	

TYPES OF CRIMES	RISK			
	MINIMUM	LOW	MODERATE	HIGH
Offences against workers' rights (section 318)			X	
Offences against the rights of foreign citizens (section 318. Bis [5])		X		
Against land planning (section 319[4])	X			
Against natural resources and the environment (section 328)		X		
Crimes against collective security (section 343[3])	X			
Risk offences caused by explosives and other agents (section 348[3])	X			
Offences against public health relating to medicines (section 366)	X			
Public health offences relating to narcotic substances (section 369 bis)	X			
Counterfeiting (section 386[5])		X		
Forgery of bank cards and travellers cheques (section 399 bis)		X		
Bribery and influence peddling (sections 427 bis, 430)				X
Embezzlement (section 435[5])		X		
Crimes of incitement to hatred and violence (section 510 bis)			X	
Organisation and criminal enterprises and unlawful association (section 570 quater)	X			
Terrorism (section 576[5])		X		
Smuggling (section 2[6] of Organic Law 12/1995)	X			

cedinsa

ANNEX NO. 2

CODE OF ETHICS OF CEDINSA AND ETHICS CHANNEL

CEDINSA CODE OF ETHICS

I.- PURPOSE

CEDINSA's Code of Ethics is the document that establishes the rules and principles that must regulate the behaviour of all employees who form part of the entity in the performance of their employment activity and in their relations with suppliers, customers, public institutions and the company in general.

The Code reflects the commitment of the Company's shareholders and directors to complying with the current law, but also the ethical values that supplement that regulation and that are included in this document. The Board of Directors' firm intention is to develop the mechanisms necessary for all CEDINSA members to know and act in accordance with those principles and values.

This Code of Ethics is also intended to be the focus of the company's management and organisational model for the prevention of criminal risks, in accordance with the specific Manual approved by the Board of Directors.

II.- SCOPE OF APPLICATION

This Code affects CEDINSA CONCESSIONARIA, S.A. and the other undertakings owned by it, therefore any references to "*CEDINSA*", "*the company*" or "*the entity*" must be understood as made to all of them.

The principles and rules of action are aimed at the Company's own directors, executives and other employees, regardless of their position in the Company's structure. Therefore, any references made to "*employees*" should be understood to be addressed to all of them, without exception.

Likewise, employees must ensure that persons or entities that provide services to CEDINSA are aware of this Code and act in accordance with it. Where it is considered appropriate, express and formal acceptance of it by those persons and entities may be requested.

III.- ACCEPTANCE AND COMPLIANCE

CEDINSA will publish the content of this Code so that it has the widest possible dissemination and may be consulted by any person. In particular it will ensure it is understood by all its employees and provide the training and resources that may be necessary for its strict compliance.

In the event of doubts as to the content or interpretation of the code, employees may contact their superior to request any clarifications they consider appropriate.

The Code of Ethics is mandatory for all employees of the entity, as well as for those persons or entities that formally adhere to it. No member of the entity - regardless of their hierarchical position - is authorised to give instructions to an employee that infringes the principles and values indicated.

The Company's employees must state in writing their reception, understanding, acceptance and commitment to comply with the Code. Breaches of the Code will entail the investigation of the behaviour of the employee and may give rise to appropriate penalties in accordance with internal rules, employment agreements and current legislation.

Employees are obliged to notify CEDINSA of any breach of the Code of which they are aware, with a guarantee of the confidentiality of the identity of the communicator and the absence of negative consequences for it. To this end, the Company will make appropriate communication channels available to employees.

IV.- PRINCIPLES AND RULES OF ACTION

The actions of CEDINSA employees should always be based on the integrity and responsibility of performing their professional activity, and should be governed by the principles of rectitude, ethics, honesty and honour.

Without prejudice to this general principle, specific principles and rules are determined in the following fields:

1.- Respect for the law, human rights and ethical values.

CEDINSA agrees to act in accordance with the law in force, with regard to the Universal Declaration of Human Rights and in accordance with the ethical values contained in this Code.

2.- Respect for individuals. Equal opportunities and non-discrimination.

CEDINSA states its commitment to respect and comply with labour legislation and workers' rights. Employees should also be treated with respect, fostering cordial relationships and a pleasant, healthy and safe working environment.

All employees are obliged to treat their peers, their superiors and their subordinates fairly and respectfully. Similarly, the relationships between the Company's employees and those of external collaborating companies or entities must be based on professional respect and mutual collaboration.

CEDINSA considers it important to fully develop the individual and, therefore, will facilitate the necessary balance between professional and personal life.

CEDINSA will actively promote equal opportunities in the professional development of all its employees. The selection and promotion of employees will be based on the competences and performance of the professional functions, and on the criteria of merit and capacity defined in the job requirements.

Any type of discrimination is expressly prohibited against other employees and third persons for reasons of ideology, religion or belief, belonging to an ethnic group, race or nation, sex, sexual orientation, family situation, illness or disability, due to being a legal or union representative of employees, because of their kinship with other workers in the company, due to the use of any of the official languages within the Spanish State, or for any other personal circumstance.
CEDINSA particularly rejects any type of harassment in the workplace, be it physical, psychological, moral or abuse of authority, as well as any other conduct that may generate an offensive environment to the rights of persons, regardless of the grounds or origins of such behaviour.

The entity agrees to investigate and pursue any complaint of the commission of these practices, without prejudice to any actions that may correspond to the directly injured party.

3.- Compliance with tax, financial and Social Security obligations.

CEDINSA expresses its firm intention to strictly comply with all applicable tax, financial and Social Security obligations, and the actions of all its employees should always be aimed at achieving that end.

Employees may not engage in or facilitate the carrying out of practices that involve scams against the Public Treasury of the European Union, or state, regional, foreign or local governments, by avoiding the payment of taxes or other amounts.

Employees should comply with and promote compliance with Social Security regulations, refraining from performing any conduct that entails avoiding the payment of contributions and other due items. Likewise, they must refrain from enjoying or facilitating the enjoyment of Social Security System benefits or the undue extension of them, by means of errors caused by simulation, misrepresentation or concealment of facts.

If grants or any other aid of economic content are requested or received, the data required to grant them must be provided with veracity and accuracy at all times, and the amounts obtained will be used for the purposes on which they are based.

4.- Company loyalty and conflicts of interest.

When performing their professional duties, employees should act loyally and take into account the interests of CEDINSA, which considers that the relationship with its employees should be based on the loyalty arising from common interests.

Employees should avoid situations that could give rise to a conflict of personal and business interests. Conflicts of interest arise in those circumstances where the personal interests of employees, either directly or indirectly, are contrary to or conflict with the interests of the entity, interfere with the correct performance of their professional duties and responsibilities or involve them personally in any transaction or economic operation of the company. Employees should refrain from representing the company and intervening or influencing decision-making in any situation in which they have a personal interest, either directly or indirectly.

5.- Company information and accounting.

CEDINSA declares that veracity of information is a basic principle in all its actions, and its employees must ensure the truthful transmission of all information that they must communicate internally or externally, and in no case may they intentionally provide incorrect or inaccurate information that could lead those who receive it to err.

The various instruments comprising the accounting records of CEDINSA must reflect at all times the true and fair view of the situation of the entity, scrupulously subject to applicable legislation in this area, and with scrupulous recording of all economic transactions that take place.

Employees must always act in accordance with these principles and must refrain from performing any action that breaches the commitment to reflect the movements existing clearly and accurately in the corresponding registries.

6.- Workplace health and safety.

CEDINSA promotes the adoption of occupational health and safety policies and adopts the preventive measures established in current legislation, and ensures regulatory compliance in this regard at all times, adopting the necessary actions. It will also encourage and encourage the application of its occupational health and safety rules and policies by the collaborating companies and suppliers with which it operates.

CEDINSA will provide its employees with the necessary training and resources to enable them to work in a safe and healthy environment, in strict compliance with the legislation on the matter. In turn, employees will be obliged at all times to use the individual or collective occupational risk prevention equipment, equipment for themselves or for third parties, as well as to follow the oral or written rules provided by the company in this regard.

7.- Environmental protection and land management.

Preservation of the environment is one of CEDINSA's basic principles of action. The group's employees must assume that policy and act at all times in accordance with the criteria of respect and sustainability, adopt habits and behaviour related to good environmental practices and contribute positively and effectively to achieving the objectives set forth.

Employees must refrain from carrying out practices contrary to the regulations governing the territory. Likewise, any action contrary to laws or other general provisions protecting the environment is expressly prohibited, which, by itself or jointly with others, causes or may cause substantial harm to the quality of air, soil, water, animals, plants or the balance of natural systems.

8.- Protection of intellectual and industrial property.

Intellectual and industrial property are individual rights expressly envisaged in the Universal Declaration of Human Rights and are essential values for economic, social and cultural development.

CEDINSA employees must protect and promote the protection of these rights, and may not engage in behaviour that entails reproduction, plagiarism or any other conduct that affects literary, artistic or scientific works or services, without the authorisation of the holders of the corresponding intellectual property rights or their assignees. They must also refrain from using and promoting the use of patents and utility models and objects protected by those rights.

9.- Data processing.

CEDINSA fully assumes the value of personal data and information as a good deserving of protection and will ensure, in particular, the confidentiality and security of the data provided by employees and third parties, adequately preserving them from any illegitimate interference, in strict compliance with data protection regulations.

All employees of the company who access or know personal data when performing their duties will be obliged to maintain professional secrecy and confidentiality regarding that information. Those involved at any stage of processing the data are bound to the professional secrecy and confidentiality of that information. Those involved at any stage of processing the data are bound to professional secrecy with regard to them and to the duty to keep them correctly, obligations that will replace even after the employment relationship with the Data Controller has ended.
Likewise, all personnel will be obliged to facilitate the rights of Access, Rectification, Cancellation and Opposition to the data subjects who wish to exercise them, in accordance with the indications made

by the company in this regard. In any case, the Data Controller or the Security Officer must be informed immediately, obtaining the request submitted by the affected data subject.

Likewise, employees themselves may exercise, at all times, the rights of access, rectification, erasure and objection with regard to their personal data, by notifying the Human Resources Department.

Employees may not use the data owned by CEDINSA of which they are aware in accordance with their professional activity for their own benefit or transfer them to third parties. This obligation will remain operational following the termination, where applicable, of the employment relationship. Likewise, any persons who, as a result of their previous employment activity or for other professional reasons, have access to secret information from other undertakings, may not disclose and use it in the interest of CEDINSA.

10.- Use of the Company's resources.

The resources that the company makes available to employees for the performance of their duties must be used appropriately and responsibly, respecting the principle of good faith.

With regard to electronic means, information systems, including electronic communications, made available to users by CEDINSA, they should be used basically for professional purposes, with sporadic and responsible personal use allowed.

11.- Anti-corruption policy.

Corruption occurs when employees use unethical practices to obtain any benefit for the company, whether in the field of relations with private or public entities.

CEDINSA does not tolerate practices that aim to influence the intention of persons outside the company to obtain any benefit through the use of unethical practices and will not allow other persons or entities to use such practices with their employees.

A gift is understood as any gift, advantage or favour for free, as well as any other physical present or pecuniary gift. In general, no type of gift may be sought or accepted, the purpose of which is to ensure that the recipient improperly favours, either directly or indirectly, the person or entity that grants it in the contracting of goods or services. Gifts that are not for that purpose will only be accepted in cases admitted by corporate practices and in accordance with customary commercial practices.

Any type of gift, the purpose of which is for the recipient to favour, the entity or the person granting it in the procurement of goods or services or in the resolution, management or processing of files or decisions of any nature, may not be offered or granted. Therefore, gifts that, in accordance with

social practices, can be considered to be of moderate value are only permitted, assessing proportionality, intention, frequency and relevance, and that cannot be considered a means to influence the decision of the recipient of the gift.

Invitations to meals and entertainment may be accepted provided that the main purpose is to discuss a business of the entity, is in accordance with customary social or commercial practices, and their economic value is moderate.

No gifts may be offered to public authorities or officials in consideration of their position or function. Any act intended to influence a public official or authority, taking advantage of any situation arising from a personal relationship with it or with another public official or authority, to obtain a resolution that could directly or indirectly generate an economic benefit for the Entity, is prohibited.

Donations to political parties, federations, coalitions and groups of voters and their related foundations, either directly or by person or entity brought, are expressly prohibited.

Any participation of the Entity in influence groups that interact with political institutions must be within the framework of the principles of action established in this Code of Ethics, and in strict compliance with the legally enforceable obligations.

12.- Relations with suppliers.

All group employees involved in selection processes for external suppliers and collaborators are obliged to act impartially and objectively, applying transparent criteria and taking into account quality and cost, and avoiding in any case the collision of their personal interests with those of the company.

V.- DISCIPLINARY SYSTEM

Various sections of the Workers Statute establish that good faith must govern the relationship between the company and employees, and is a basic duty of the latter, given that employees must comply with the specific obligations of their post, in accordance with the rules of good faith and diligence (sections 5, 20 [2] and 54. [2]).

Any gross breaches of the Code of Ethics will be considered a breach of contractual good faith, and will therefore entail the adoption of the corresponding disciplinary measures.

VI.- VALIDITY

The Code of Ethics enters into force after its approval by the Board of Directors, and its compliance will be enforceable against all employees, or persons or entities that adhere to it, from the moment they are aware of it.

The Board of Directors will periodically review the content of the Code to update those matters that require it as a result of the entity's own activity or legal modifications. *This version was approved by the Board of Directors of CEDINSA CONCESSIONARIA, S.A. on 17 March 2016.*

Regulation on the Ethics Channel of CEDINSA CONCESSIONARIA, S.A. and its investee companies

I.- INTRODUCTION

In accordance with its *compliance* policy, CEDINSA CONCESSIONARIA, S.A. and its investee companies (we will refer to the entire group as "CEDINSA") has a strong commitment to complying with the applicable legislation and the ethical values and guiding principles determined by its Articles of Association and that are included in the Code of Ethics.

In line with this commitment, a compliance model has been developed to prevent and avoid behaviour contrary to these principles and regulations, and it is of vital importance that all members of the entity participate in achieving the objectives.

In addition, following the reform of the Spanish Criminal Code in 2010 and, in particular, following the amendment implemented by Organic Law 1/2015, there is a need for organisations to have criminal risk prevention models, and one of the essential elements in any compliance system is the collaboration of all employees of the entity to detect situations of risk of breach and to allow management to address the actions necessary to correct them, and under these terms legislation imposes an obligation to disclose any breach.

Along these lines, CEDINSA has a Code of Ethics that expressly establishes that employees are obliged to disclose any breach of the Code of Ethics of which they are aware. In order to communicate these possible incidents and in compliance with the Criminal Code, these Ethics Channel Regulations have been implemented.

III. ETHICS CHANNEL DEFINITION

The Ethics Channel consists of the series of measures adopted by CEDINSA to allow directors, executives and employees to communicate confidentially, and in exceptional circumstances, anonymously, irregularities of potential criminal significance, and any serious breaches of the Code of Ethics.

III. COMMUNICATION CHANNELS

To comply with the obligation to report irregularities of potential criminal significance, or possible serious breaches of the Code of Ethics, which follows from the Code of Ethics, employees have different channels:

1.- COMMUNICATION THROUGH SUPERIORS.

The ordinary channel of communication will be the transfer of the information to the hierarchical superior, which must transfer the content of the information to the various higher instances and to

the SUPERVISION AND OVERSIGHT BODY so that the competent managers will adopt the appropriate measures to correct the situation and adopt the corresponding measures.

2.- SPECIFIC COMMUNICATION CHANNEL: ETHICS CHANNEL.

However, and in view of CEDINSA's stated interest that there should be no obstacles to the communication of information in this field, a direct communication mechanism has been established with the SUPERVISION AND OVERSIGHT BODY, which may be used by any employees, directors and Board members if they consider that, due to the nature of the information, because of the possibility of a conflict of interest of the recipient, or for any other reason, this channel is safer or more effective.

This direct communication mechanism is the ETHICS CHANNEL.

IV. LEGAL SYSTEM OF THE ETHICS CHANNEL.

1.- BODY IN CHARGE OF MANAGEMENT

The recipient and controller of the ethical channel is the SUPERVISION AND OVERSIGHT BODY, which is configured as an autonomous body, which reports solely to the Board of Directors, and that is responsible for proactively ensuring regulatory compliance, configured in accordance with CEDINSA's internal regulations (Criminal Risk Management and Compliance Manual, Procedures Manual, Code of Ethics, etc.).

2.- OBJECT OF COMMUNICATIONS

Any breach, risk of breach or irregularity that employees, directors and Board members may detect with potential criminal significance, and gross breaches of the Code of Ethics, may be communicated through the mailbox.

3.- COMMUNICATION CHANNELS.

Communications through the ETHICS CHANNEL may be submitted via three channels:

- Via email to: organsupervisio@cedinsa.cat

- Telephone: 932291060

- Or by post to:

Supervisory and oversight body
CEDINSA CONCESSIONARIA, S.A.
Avda. Josep Tarradellas, 38, planta 6

4.- USERS.

Access and use of the Ethics Channel is reserved to the employees, executives and members of the Board of Directors of CEDINSA.
Anyone using the Ethics Channel through any of the channels mentioned in the previous point will be considered Users of the Ethics Channel.

5.- ACCEPTANCE OF OPERATING RULES AND OTHER ETHICS CHANNEL CONDITIONS.

Use of the Ethics Channel entails the full and unqualified acceptance of the operating rules contained in this Regulation, as it stands at any given time. Consequently, employees using the Ethics Channel agree to make diligent use of it, in accordance with the law and these Regulations.
CEDINSA will be considered the manager of the Ethics Channel, under the conditions and authority envisaged in these regulations, and reserves the right of interpretation in the event of a doubt or disagreement about its use.

6.- CONTENT OF COMPLAINTS. CONFIDENTIALITY OF CLAIMANTS.

Complaints must include at least the following information:

- Identifying information of the claimant:
    - Name
    - National Identification Document or equivalent document
- Grounds for the complaint, specifying where possible the infringement and the possible perpetrators.
- Date and signature.

The identity of the claimant will be considered confidential information, and no type of disciplinary action may be taken, either directly or indirectly, due to the fact of the complaint, without prejudice to the rights corresponding to those reported in accordance with the legislation in force.
As an exception, and if - despite the confidentiality commitment - claimants believe they may be harmed by having their identity revealed, anonymous complaints will be admitted if they meet minimum standards of credibility given the information provided.

7.- PROCESSING OF COMPLAINTS

7.1. Acceptance of complaints for processing

1. Once a communication has been sent to the ETHICS CHANNEL, the SUPERVISION AND OVERSIGHT BODY will determine whether or not it should be processed.

2. The SUPERVISION AND OVERSIGHT BODY will not process the complaint if it does not constitute a breach of the internal rules of CEDINSA, or a behaviour that may imply the commission of any irregularity, or of any act contrary to the law or the rules of action of the Code of Ethics, or with significance in the professional functions of the perpetrator of the breach within CEDINSA, or in the interests and image of CEDINSA.

7.2 Processing of the case

1. Once the complaint is processed, the SUPERVISION AND OVERSIGHT BODY will assign it a case number and carry out the corresponding investigation, respecting the rights of the person investigated at all times, and it will process the case.

2. The SUPERVISION AND CONTROL BOARD will verify the veracity and accuracy of the information contained in the communication, and in particular, of the alleged behaviour, with regard to the rights of the persons involved. From there, all of the affected parties and witnesses will be heard, and the formalities considered necessary will be performed. All CEDINSA employees, the members of the governing body and anyone else related to CEDINSA and related to the complaint, are obliged to cooperate with the investigation. The participation of witnesses and those affected will be strictly confidential.

3. The hearing process, which must be held within 60 days of the reception of the communication/complaint, must include, as a minimum, whenever possible, an interview with the person supposedly responsible for the reported conduct in which, with regard to the presumption of innocence, the accused will be informed of the facts that are the subject of the case, and will be invited to present his complete version of the facts, provide the relevant means of proof, and he will be asked the corresponding questions depending on the circumstances of the case and the facts reported.

4. All investigations must ensure the right to privacy, the right to defence and the presumption of innocence of the persons investigated.

5. Once the investigation has been concluded, the SUPERVISION AND OVERSIGHT BODY will issue a report that will be submitted to the Board of Directors for its decision as appropriate. That report must contain:

a) copy of the complaint filed (respecting, where applicable, the confidentiality of the complainant)

(b) a transcription of interviews and questionings conducted (respecting the confidentiality of the persons interviewed and questioned, who must not be able to be identified directly or indirectly)
(c) a copy of the version of the facts in the case as presented by the person investigated
(d) a copy of the documents collected as evidence during the examination of the case
(e) proposal for resolution
(f) Any other document and information that the SUPERVISION AND OVERSIGHT BODY considers appropriate to decide the case.

7.3 Resolution of the case

1. Once the report issued by the SUPERVISION AND OVERSIGHT BODY has been received, the Board of Directors will proceed to decide on the case based on the facts.

2. If the processing of the case affects any Board member, that Board member must be absent from the meeting where it is discussed and the corresponding resolution is passed.

3. If the decision issued concludes that the employee has committed an irregularity or any act contrary to the law or the applicable rules of action, the Board of Directors will resolve to adopt the appropriate disciplinary measures, informing the SUPERVISION AND CONTROL BOARD of the adoption and content of the disciplinary measure.

4. If the decision issued concludes that a Board member has committed an irregularity or any act contrary to the law or the applicable rules of action, the Board of Directors will adopt any corrective measures it considers appropriate, it will inform the SUPERVISION AND OVERSIGHT BODY of the adoption and content of the measure.

8. DATA PROTECTION

1. Sending personal information through the complaints box may require express and unequivocal consent to process the personal data of the employee who sent the communication, as well as those of the accused. To this end, the SUPERVISION AND OVERSIGHT BODY must provide the mechanisms necessary to obtain prior consent to the commencement of actions, in accordance with personal data protection legislation.

2. In general, the defendant will be informed of the existence of the complaint when it is admitted to processing. However, in those cases in which the SUPERVISION AND OVERSIGHT BODY considers that the notification entails a risk that jeopardises the ability to effectively investigate the allegation or collect the necessary evidence, the notice to the accused may be delayed. In any case, this period may never exceed 60 calendar days.

3. The data processed within the framework of the investigations will be cancelled as soon as they end, unless the measures adopted result in, or may result in, administrative or court proceedings. However, CEDINSA will store such data duly frozen during the period in which the complaints or actions carried out by CEDINSA, or by its professionals, could give rise to liability.

4. Users of the complaints box may exercise their rights of access, rectification, erasure and objection with regard to their personal data by sending a written communication to the same report box, complying with the requirements established by the law in force at any given time and indicating the specific right they wish to exercise.

ANNEX NO. 3

CRIMINAL RISK MATRIX TABLE

SPECIFIC RISK/MEASURES MATRIX TABLE

AREA / PROCESS	SECTION	CRIMINAL RISK	SITUATION	SPECIFIC MEASURES
	197, 197[a] and 197[b]	Offences against privacy and unlawful access to data and computer programs	- Obtaining or intercepting communications to discover secrets or violate the privacy of others - Obtaining, using or modifying, to the detriment of a third party, personal or family data of someone else that are recorded in files - Disseminating, disclosing or assigning to third parties data or facts discovered or images captured by the above practices. - Accessing, or facilitating access to, an information system by breaching the security measures established to prevent this, and without authorisation - Producing, acquiring or providing third parties with computer programs designed to carry out such behaviour, or passwords or access codes	A) Keep the data protection measures up-to-date, and in strict compliance with current legislation. B) Periodic and documented IT audits by IT Department personnel, in order to review the status of the information storage systems and periodic password changes. C) Warn workers who have PCs connected to the network of the use of USB or other removable storage devices. D) Signature by employees of the contractual annexes in the matter and strict archiving of them. E) Lock up all relevant and sensitive documents. F) Use the destruction devices authorised for this purpose to dispose of confidential documents.
	248 and 251	Scams	- Deceiving third parties to make acts in their own detriment or the detriment of others. - Manipulating computers to obtain unauthorised transfers. - Using a credit card or travellers cheques to carry out transactions detrimental to their owner or a third party. - Manipulating evidence in court proceedings for the Judge to pass a decision detrimental to a third party. - Disposing of assets over which that power is not available. - Entering into a simulated agreement to the detriment of others.	A) Strict compliance with the procedures manual B) Train employees involved in such transactions so that they are aware of the types of crimes and prohibited practices.
	257, 258 and 258 bis	Fraudulent conveyance	- Absconding with assets to the detriment of creditors. - Disposing of assets in any way that generates obligations that entail hindering an attachment or executive or enforcement procedure. - Making disposals, assuming obligations or hiding assets, for the purpose of avoiding the payment of civil liabilities arising from an offence the perpetrator committed or should be accountable for.	A) Take special care in the event of attachment of property. B) With regard to responses to requests and summons received by CEDINSA from official bodies, it is recommended that a formal written

			- Failing to provide judicial or official authorities a list of assets or presenting an incomplete or mendacious equity relationship in an enforcement proceeding, to hinder or prevent the satisfaction of a creditor. - Using property seized by public authorities and deposited without authorisation.	response procedure be included in the procedures manual so that all employees are aware of and can duly comply with them.
	259, 260 and 261	Negligent insolvency	- In a current or imminent insolvency situation, concealing assets, disposing of goods or providing services without justification or for a price lower than market price, simulating credits, engaging in speculative business against the duty of care, breaching accounting duties or hiding documents, or any other act or omission that constitutes a serious infringement of the duty of care in the management of economic matters and that results in a decrease in the debtor's equity or through which the real economic situation of the debtor or its business activity is concealed. - Causing grounds for insolvency by any of the practices referred to in the preceding paragraph. - Favouring any creditors by making an act of asset disposal or settling obligations aimed at paying an unenforceable loan or providing it with a guarantee to which it was not entitled, in the case of a transaction that lacks economic or business justification. - Committing any act of asset disposal or obligation generator, intended to pay one or several creditors, with postponement of the rest, once an application for insolvency has been admitted - Submitting false information relating to the accounting statement in insolvency proceedings, to unduly obtain its declaration.	
	264, 264bis and 264ter	Criminal misuse of computer systems	- Deleting, damaging, impairing, altering, deleting, or rendering inaccessible others' data, computer programs or electronic documents where the result is serious - Obstructing or interrupting the operation of a third-party computer system, by introducing, transferring, damaging, erasing, impairing, altering, deleting or rendering inaccessible, computer data. - Procuring or acquiring for use a computer program designed to commit any of the aforementioned offences or a password or code that allows access to all or part of a system, by a person who is not duly authorised, as well as providing them	A) Maintenance and strict compliance with the existing measures. B) Periodic IT audits by IT Department personnel, in order to rule out the use of potentially hazardous programs and verify C) Regularly verify with those responsible for preparing the website compliance with the legal provisions, in particular, Law 34/2002 of 11 July on Information Society Services and Electronic

			to third parties, with the intention that they carry out any of the aforementioned practices.	Commerce [*Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y del Comercio Electrónico*] and the other regulations in this regard.
	270 273, 274 and 275	Intellectual Property offences Industrial property offences	- Reproducing, plagiarising, distributing, and publicly communicating, a literary, artistic or scientific work, or its transformation or interpretation established in any type of medium or communicated through any means, without the authorisation of the holders. - Facilitating the access or location on the Internet of works or services subject to intellectual property rights without the authorisation of their owners and to the detriment of a third party - Exporting, importing or storing copies of the works, productions or performances, and erasure of the technological measures available to avoid the typical practices or facilitate the evasion of those measures available to prevent the practices in question. - Manufacturing, or having any means specifically intended to facilitate the unauthorised removal or neutralisation of any technical device that has been used to protect computer programs or any other protected works. - Manufacturing, importing, possessing, using or offering in trade industrial or artistic objects or procedures, models or drawings, protected by patent rights, utility models, industrial drawings or topography rights - Reproducing, imitating, modifying or usurping an identical or confusing distinctive sign, to distinguish the same or similar products, services, activities or establishments. Manufacturing, producing or importing products that incorporate an identical or confusing distinctive sign. - Offering, distributing or selling wholesale, products that incorporate an identical or mistaken distinguishing sign or storing them for this purpose. - intentionally using and without being authorised to do so, in economic traffic, a designation of origin or a geographical indication representing a given legally	A) Review and confirm the existence of licenses for all computer programs used, as well as to have their location identified, for possible inspections. B) Warn employees that they may not use images, texts or designs protected by intellectual and industrial property law C) The Systems Department should evaluate software purchases, authorise their acquisition, conduct the necessary installations, and maintain the licenses.

			protected quality to distinguish the products covered by them, with knowledge of this protection. - disclosure of an invention subject to an application for a secret patent in breach of patent law.	
	278 - 285	Crimes against the market and consumers	- Obtaining data or written documents to discover a trade secret. - Disseminating, disclosing or assigning to third parties, the secrets discovered. - Disposing of, disclosing or assigning of a trade secret by a person legally or contractually obliged to keep it secret. - Taking essential raw materials or products off of the market with the intention of refuting a sector of it, forcing a change in prices, or seriously harming consumers - Making false representations or making false claims about products, such that they can cause serious and obvious harm to consumers - False economic-financial information on securities traded on the securities markets for the purpose of attracting investors or obtaining financing by any means - Altering automatic devices to invoice higher amounts for products or services. **- A**ltering the prices resulting from the free concurrence of products or goods with violence, threats or deception - Disseminating news or rumours about persons or undertakings in order to alter or preserve the price of a security or financial instrument, obtaining an economic benefit greater than EUR 300,000 or causing harm of an identical amount. - Performing transactions or ensure a dominant position in the stock market using inside information. - Using any information relevant to the share price of any type of securities or traded instruments, to which reserved access was obtained during the performance of the perpetrator's professional or business activity, obtaining a financial benefit greater than EUR 600.000 or causing harm of identical amount, - Facilitating access to a broadcasting service, television, or other services provided electronically, without the consent of the service provider and for commercial purposes, or using the equipment and programs that make this possible.	Include an appendix in employment contracts that prohibits the use of confidential information from previous work in other undertakings (there is currently a prohibition on the use of information obtained at CEDINSA).

			- Altering or duplicating the identification number of telecommunications equipment, or selling equipment that has been fraudulently altered for profit.	
	286 bis and 286 ter	Corporate corruption	- Receiving, requesting or accepting an unjustified benefit or advantage of any nature in order to favour, vis-à-vis third parties, whoever grants it or from whom the benefit or advantage is expected - Promising, offering or granting executives, directors, employees or associates of a company or of a company or association, a benefit or advantage to obtain a favourable treatment of one's own or for a third party. - Deliberately and fraudulently predetermining or altering result of a sport competition of special economic and sporting relevance, with the above practices. - Corrupting a public authority or official by granting any undue benefit or advantage, so that they act or refrain from acting to obtain a contract, business or any other competitive advantage in the performance of international economic activities.	A) It is recommended to include rules of action regarding the possibility of giving gifts to executives, directors, employees or associates of third commercial entities, where applicable, creating a register of the recipient of the gift, entity and position. B) Express prohibition on requesting an unjustified benefit or advantage from CEDINSA companies as consideration for such gifts. C) It is also recommended to include rules of action regarding the possibility of accepting gifts from executives, directors, employees or associates of a commercial company or a company, that may claim an unjustified benefit or advantage in favour of those entities. D) Establish a representation expense policy that establishes: a) Authorised persons B) Types of authorised expenses and limits C) Control procedures (authorisations, registers, etc.) E) Identification of procurement action protocols (need for alternative offers above certain limits and supplier approval) F) Maintenance of a register of authorised suppliers. G) Have the Legal Advisory Department revise and approve the contracts executed by the entity.

				H) Detail the expenses on an expense sheet, making them only reimbursable if authorised and validated according to the approval circuit. N) Receive authorisation for advances through a document approved by the superior of the employee requesting them.
298	301	Money laundering	- Acquiring, owning, using or transferring property, knowing that it originates from a criminal activity, or performing any act to hide the illicit origin of the property. - Helping someone who participated in an infringement avoid the legal consequences of their actions.	A) Strict compliance with legislation on money laundering B) Training on the subject of those responsible for relations with banks.
	304 bis	Unlawful political funding	- Providing donations or contributions to a political party in breach of section 5(1) of Organic Law 8/2007, of 4 July, on Funding of Political Parties [*Ley Orgánica 8/2007, sobre financiación de los partidos políticos*].	absolute prohibition on making donations or contributions intended for a political party, federation, coalition or group of electors directly or through intermediaries.
	305 - 310	Offences against the Public Treasury and Social Security System	- Defrauding the Public Treasury by avoiding the payment of taxes in an amount greater than EUR 120,000. - Defrauding or unduly obtaining funds from the general budget of the European Union in an amount greater than EUR 50,000 - Defrauding Social Security by avoiding the payment of contributions, unduly obtaining returns or taking deductions in an amount greater than EUR 50,000. - Obtaining for one's self or others Social Security System benefits by simulating or concealing facts. - Obtaining grants, deductions or aid from public authorities by distorting the conditions required, in an amount greater than EUR 120,000 - Keeping separate accounts in order to conceal the situation of the company, not to record business or economic transactions or to make fictitious accounting entries, in breach of tax law	A) Have the labour consultancy regularly verify compliance with Social Security obligations. B) Compliance with the annual audit obligation. C) Strictly complying with the procedures manual D) Maintenance of restrictions on access to the accounting system and periodic change of the passwords used. E) All communications sent or received by external tax advisers must be documented in writing, avoiding undocumented oral communications, and they must be duly filed. F) It is recommended that, with the approval of the external advisers, the possibility of the

				company adhering to the Code of Good Tax Practice should be assessed. G) Taxes should be filed by authorized personnel digitally using Digital Certificates. H) Income tax filings should be reviewed by a specialised external adviser.
	311 - 316	Offences against workers' rights	- Imposing employment or Social Security conditions on workers in their service that harm, suppress or restrict the rights they have recognised, by deception or abuse of a situation of necessity. - Simultaneously employing multiple employees without communicating their registration in the social security scheme. - Maintaining the aforementioned conditions imposed by another, in the event of transfer of undertakings - Engaging or employing foreign citizens or minors without a work permit, repeatedly. - Illegally trafficking employees. - Recruiting persons or encourage immigration by offering deceptive or false employment or working conditions, and employing foreign nationals without a work permit in conditions that harm, suppress or restrict the rights they have recognised for them. . - Gross discrimination in employment, public or private, against any person on the grounds of their ideology, religion or belief, belonging to an ethnic group, race or nation, sex, sexual orientation, family situation, illness or disability, due to being a legal or union representative of employees, because of their kinship with other workers in the company, due to the use of any of the official languages within the Spanish State, or for any other personal circumstance. - Preventing or limiting the exercise of trade union freedoms or the right to strike, by deception or abuse of a situation of necessity. - Coercing other people to initiate or continue a strike, in a group or in collusion with others.	A) Need for occupational risk prevention management in strict compliance with the regulations in this area, in accordance with the instructions of the External Prevention Service. B) Periodic audits are recommended. C) Take actions to prevent harassment in the workplace D) Establish processes for the selection and hiring of personnel, with special rigour in obtaining and keeping documents of personnel of foreign origin.

			- Not providing the resources necessary for workers to carry out their activity with the appropriate health and safety measures, in breach of the occupational risk prevention rules.	
	318 bis	Offences against the rights of foreign citizens	- Intentionally assisting a non-national of an EU Member State in entering or passing through Spanish territory, infringing Spanish legislation on the entry of foreigners.	
	319	Urban development offences	- Carrying out unauthorised urban development, construction or works, on land intended for roads, green areas, public property or classified with special protection, as well as on land that may not be developed.	Continuous training and conscious raising is recommended of persons with responsibilities in the design, implementation and supervision of construction with regard to unlawful practices.
	325, 326, 326 bis and 327	Offences against natural resources and the environment	- Acting in breach of laws or other general provisions protecting the environment, which may cause substantial harm to the quality of air, soil or waters, or animals or plants - Collecting, transporting, removing or using waste, or not adequately controlling or monitoring such activities, in breach of laws or other general provisions, and in a way that causes or may cause substantial harm. - Operating installations where a hazardous activity is carried out or where hazardous substances are stored or used, in breach of laws or other general provisions.	A) Strictly comply with the relevant administrative legislation. B) Update and maintain a register of authorised waste management centres with which the company works C) Request and file of waste delivery certificates. D) Training of personnel with responsibility in this area.
	386	Counterfeiting	- Altering currency or making fake currency. - Bringing into the country, transporting or distributing, altered or false currency. - Distributing fake currency received in good faith, after confirming it is counterfeit.	Avoid committing the practices described as constituting offences, which will require the correct training of employees with payment responsibilities.
	399 bis	Falsification of bank cards and	Altering, copying, reproducing or falsifying credit or debit cards or travellers cheques. Having those effects for distribution or traffic.	

		travellers cheques	Using, to the detriment of a third party, forged credit or debit cards or travellers cheques.	
	419 to 427 and 428 to 430	Bribery and influence peddling	- Offering or delivering a gift or remuneration of any other type in order to have a national or foreign public authority or official perform an act contrary to the duties inherent to his post or an act characteristic of his post, so that he does not perform or delay that which he should perform, or in consideration of his position or function. - Delivering a gift or remuneration in accordance with the request of the public authority or official. - Influencing a public official or authority taking advantage of any situation arising from one's personal relationship with him or with another public official or authority to obtain a resolution that could directly or indirectly generate an economic benefit. - Offering to perform the practices described in the two preceding sections, requesting from third parties gifts, present or any other remuneration, or accepting offers or promises.	A) Develop an anti-corruption policy and draft a protocol for dealing with public officials and authorities, which addresses, among other aspects, the prohibition on making gifts. B) Inclusion of clauses in contracts with advisers and, where applicable, suppliers, specifying that both parties will not tolerate, with regard to corruption and the prohibition on offering or granting public officials or third parties payments, gifts or other unauthorised advantages for the purpose of obtaining favourable treatment in the granting of public contracts or personal benefits or for the Company. C) Implement a representation expense policy that establishes: A) Authorised persons. (b) The types of authorised expenses and limits. C) Oversight procedures (authorisations, registrations, etc.). D) Restrict, through powers of attorney, the disposal of funds, contracting and representation before Public Bodies and Courts. E) All expenses should be detailed in an expense sheet that will only be reimbursable if it is authorised and validated according to the corresponding approval circuit.

				F) Reduce the use of cash as much as possible.

1.- This table reflects the specific controls for specific types of crimes, and the general criminal risk prevention measures are transversal: Organisational structure/Code of Ethics and Procedures Manual/Communication Channel/Training