

# COMPLIANCE MANUAL

PREPARED BY:	REVIEWED BY:	APPROVED BY:
External consultant	Chief Executive Officer	Management Board

Description of amendments	Revision Edition	Date
N/A	1st edition	April, 2020
Scope, stakeholders, inclusion of new criminal offences	2nd edition	October, 2020
Investigations carried out by compliance body and modifications in the complaint channel	3rd edition	January, 2021
Adapting the template of the procedure; new branches	4th edition	January, 2022
Modification of complaints channel	5th edition	June, 2022

Revision of template format; modification of posts compliance body	6th edition	January, 2023
Deletion of the member of the compliance body: Person in charge in "Finance and Accounting department"	7th edition	March, 2023
incorporation of criminal types of environmental offences; incorporation changes channel of complaints	8th edition	April, 2023

## Index

1.What is a Compliance Manual	4
2.Context	4
2.1 History	4
2.2 Context	5
2.3 Scope	5
2.4 Objectives	6
2.5 Parties interested	6
2.6 SWOT Analysis	6
3. Leadership	7
3.1 Compliance figures	8
3.2 Roles and responsibilities	11
4. Planning	12
4.1 Objectives	12
4.2 Identification of risk activities	12
5. Support elements	30
5.1 Planning Train	31
5.2 Communication channels	31
5.3 Investigation of complaints	32
6. Operation	39
6.1 Risks treatment Plan	32
6.2 Code of Conduct	33
6.3 Disciplinary system	33
7. Performance evaluation	41
7.1 Monitoring and measurement of the system	34
7.2 Audit plan	34
8. Improvement	41
8.1 Review and update plan	35
8.2 Continuous improvement	35
8.3 Non-conformities and corrective actions	35
9. Resources	42

**This Document is the exclusive property of ODILO TID and its reproduction is prohibited.**

## **1. What is a compliance manual**

The Compliance Manual is a guide that contains the set of procedures, instructions of the fundamental aspects of the compliance system.

It is an organised guide that helps to understand the functioning of the criminal compliance management system and that educates all members of ODILO TID about its practical use and operating methodology in an orderly and concise manner.

## **2. Context**

### **2.1 History**

Odilo TID is a private Spanish company that provides services to more than 2,000 centers in 43 countries. Leader in digital content lending solutions in Spanish. Odilo currently offers more than 1.2 million digital titles, including e-books, audiobooks, videos, magazines, national and international press and educational pills.

Odilo TID created the first digital lending platform for libraries in Spain and digital content called OdiloTK. Later the OdiloTT platform was developed, it is the first platform that in a single product manages the physical loan and loan of digital content. Odilo was also a pioneer in creating the first open platform for selling digital content in Spanish for OdiloPlace libraries.

In 2016 OdiloLeisure was introduced, it is a digital content lending platform for Leisure. It has been implemented by Iberia and several hotel groups. Odilo Leisure was presented as a complementary leisure offer:

It's hotels. A leisure offer designed to improve the guest experience by offering them a range of current digital content: eBook, newspapers and magazines.

I'm transporting. We provide a personalised content consumption service during the journeys. This creates a closer relationship with travelers.

Services for corporate: We offer content to companies for customer loyalty or for transversal training and leisure of their employees.

In addition to all the above solutions, ODILO offers its customers the possibility of having their own APPs, bringing and promoting user immersion to new technologies.

Odilo offers innovative solutions, especially taking care of the quality and design of its products making them easy to use and responding to the needs of its customers.

In the field of education in 2017, the technology that allows to offer digital content to the entire education of the country with more than 500,000 students was implemented in Uruguay.

Also highlighted as historical milestones are the portal of the digital library for education of the Junta de Extremadura, the Departments of Education of Madrid, the Balearic Islands and Galicia.

## 2.2 Context

Odilo is a company with a legal form of limited company, incorporated in 2011 whose share capital is EUR 224.754.60.

It has a total of 111 employees and the management body is the Board of Directors. The complete structure of the organisation can be seen in the register through an organisation chart of the organisation.

As business partners we find customers and suppliers. Clients are legal entities such as public administration.

Odilo has a branch incorporated in Chile (ODILO TID S.L. SUCURSAL CHILE) and in the USA.

In 2021 it joined as a branch Colombia.

In 2022, the branches of London and the Philippines.

These branches have joined the criminal compliance of the ODILO matrix, without prejudice to the fact that they carry out their own risk analysis since in Chile a system of criminal liability of legal persons is regulated, applicable only to the crimes of money laundering, financing of terrorism and bribery to national and international public officials, specifying that only legal persons under private law and State companies can commit these offences.

The offices of ODILO TID S.L. are located in Cartagena located at Av. Luxembourg s/n. CE Cartagena Plaza Cartagena Murcia 30353 and in Madrid at C/Jenner °3, 2nd floor, 28010, Madrid. The latter has its registered office.

The main activity of ODILO is the development of software and the distribution and sale of digital content.

Odilo has a legal, contractual and professional commitment to help any company or organisation manage its knowledge and provide a digital content service for its internal use or for that of its users or clients who have to make investments in technology or sign multiple distribution agreements.

The company specialises in the development, evolution and support of applications for the management of digital content as a SAAS service.

As a legal commitment it is to comply with the Spanish legislation in criminal matters such as the Criminal Code and in the contractual sphere, with the civil code and the contracts signed between the parties.

The purpose of the company is to:

1. The realisation of computer and documentary services.
2. The sale and operation as a service of software to both public and private entities.
3. All kinds of complementary transactions derived from or related to the above.
4. Distribution and sale of digital content.

It specifically refers to the development, evolution and support of applications for the management of digital content in libraries, platforms for the physical management of the library, as well as file management. It also provides archive and library consulting services.

Regarding the complexity of the activities described above, ODILO uses a Web Platform Service, which makes available digital libraries involving publishers and distributors, with different interactive functionalities (APPS). And, on the other hand, the management of the electronic archive and preservation of documentation, always dealing with legal entities and public entities.

Odilo is involved with public officials in the provision of their services through their own administrative procedures in the area of Finance and Social Security, and by tendering together with other procedures in public tenders.

## 2.3 Scope

The Manual is developed in accordance with standard UNE 19 601 "Criminal Compliance Management Systems: Requirements with guidance for its use'.

This Management System covers:

DEVELOPMENT OF SOFTWARE FOR FILE MANAGEMENT. THE PROVISION OF PHYSICAL AND DIGITAL FILE SERVICES IN THE CLOUD. THE PROVISION OF THE SERVICE OF SALE AND LOAN OF DIGITAL CONTENT IN THE CLOUD'

**Applicability:**

Odilo applies in its management system all points of UNE 19601.

This manual is mandatory and of global application to the entity.

The members of the organisation must comply with their content, regardless of the position they occupy and the territory in which they are located.

This Manual is complemented by the Crime Prevention Policy (SG.PD.01 Crime Prevention Policy)

## 2.4 Objectives

Odilo by establishing an adequate organisational culture of compliance aims to avoid or at least reduce the risk of committing unlawful conduct.

Odilo, sensitised to such purposes, has a management system that allows it to achieve its objectives and its commitment to integrity.

Policy, objectives, processes and procedures form the core of a management system for the prevention, detection and management of criminal risks, thus avoiding possible economic, reputational or other harm.

The objectives of ODILO have the following characteristics:

- 1) They are consistent with the provisions of the compliance policy together with the analysis of criminal risks
- 2) They are measured
- 3) Monitored
- 4) They can communicate
- 5) Can be updated

The objectives are documented in the measurable objectives procedure.

## 2.5 Parties interested

The stakeholders that may be affected or affected by the decision to implement the criminal compliance management system are defined in a register.

The stakeholders in ODILO are the management team, the development, content, operations, CSM, marketing, management and control departments, sales, investors and partners, clouds and partners.

On the other hand, the stakeholders that depend on ODILO are private and public entities such as customers and employees.

Stakeholders who have an indirect interest in ODILO with competitors, public administrations and society. However, those who have a direct interest are suppliers, cloud providers, partners and banking entities.

## 2.6 SWOT Analysis

It regulates in a procedure the activities, criteria and responsibilities for carrying out the analysis of threats and opportunities and the management of them.

The SWOT analysis consists of: Weaknesses, Threats, Strengths and Opportunities.

Strengths are all those internal and positive elements that can differentiate ODILO from other companies.

Weaknesses are all internal and negative elements that constitute barriers to crime prevention.

Opportunities are external elements that involve changes in the environment, which if taken advantage of can improve the competitive situation of the company.

Threats are external elements that involve changes in the environment, which, if not addressed in time, can place the company at a competitive disadvantage.

The conclusions of the above identification of factors, according to their scores, will be included in a record.

From the SWOT matrix, conclusions should be drawn, and the most appropriate strategy should be defined according to the characteristics of the company and those of the market in which it moves.

## 3. Leadership

### 3.1 Compliance figure and Bodies

In order to facilitate the development and implementation of the Compliance Manual, the entity will create a control body represented by a Compliance Body.

The Compliance Body shall consist of:



Director of Legal Counsel: Person in charge in “Legal, Internal Operations”

5 Vocals:

- Person in charge in “Manager, Internal Operations”
- Person in charge in “Internal operations”
- Person in charge of “Chief Finance and Strategy Officer”
- Person in charge of “Chief Delivery Officer, Project Manager”

Secretary and Senior Management: “Business Manager”

The Compliance Body jointly with senior management shall hold an annual meeting for scrutiny; being able to meet extraordinarily; at the request of any member, if circumstances so advise.

Planned annual internal audits will be carried out on an annual basis.

The meetings held, the topics discussed and the agreements adopted must be recorded in writing by means of minutes signed by those present. These records must be made available to the judicial authorities; The secretary shall take care of its drafting and custody.

The constitution of the Compliance Body must be approved by the Board of Directors, being the director of the legal advice in charge of informing the Board of Directors for its ratification.

### 3.2 Roles and Responsibilities

The responsibilities of the Compliance Body shall include, without limitation, the following:

- Continuously promote and supervise the implementation and effectiveness of the criminal compliance management system in the different areas of the organisation.
- Ensure ongoing training support to members of the organisation in order to ensure that all relevant members are regularly trained.
- Promote the inclusion of criminal compliance responsibilities in job descriptions and in the performance management processes of the members of the organisation.
- Document and inform the criminal compliance system.

- Adopt and implement processes to manage information, such as complaints or comments received from hotlines as well as a reporting channel.
- Establish indicators of penal compliance performance and measure it in the organisation.
- Analyse performance to identify the need for corrective actions.
- Identify and manage criminal risks including those related to business partners.
- Ensure that the criminal compliance management system is reviewed at planned intervals.
- Inform the board of directors on the results of the application of the criminal compliance system.
- Ensure the integrity and commitment of the compliance body with criminal compliance, as well as demonstrate effective communication skills, ability to influence, capacity and prestige and necessary competence.
- Direct and immediate access to the board of directors in case it is necessary to raise suspicious facts or conduct or matters related to the objectives of criminal compliance, the criminal compliance policy and the management system.
- Request and receive full cooperation from the other organs of the organisation.
- Contribute to the identification of criminal compliance obligations, support with the necessary resources and collaborate so that these obligations are translated into viable policies, procedures and processes.
- Provide objective advice to the organisation in matters related to criminal compliance.
- Ensure that there is adequate professional advice for the adoption, implementation and maintenance and continuous improvement of the compliance management system.

The responsibilities of the Management Board (governing body) shall include, but not limited to, the following:

- Establish and defend that the actions of the members of the organisation, are in conformity with criminal law, promoting an adequate culture of compliance in the organisation.
- Provide the criminal compliance management system and compliance body with adequate financial and human resources for its effective functioning.
- Approve the organisation's criminal compliance policy.

- Periodically review the effectiveness of the criminal compliance management system, modifying it if necessary when serious non-compliances are detected or changes occur in the organisation.
- Establish a criminal compliance body entrusted with the supervision of the functioning and execution of the criminal compliance management system, granting it autonomous powers of initiative and control in order to carry out its work effectively.
- Ensure that decision-making and enforcement procedures are established, promoting a culture of compliance that guarantees these compliance standards.

The responsibilities of senior management shall include, but not limited to, the following:

- Ensure that the compliance management system is properly implemented to achieve the objectives of criminal compliance established in the compliance policy and effectively address the criminal risks of the organisation.
- Ensure that the requirement derived from the criminal compliance management system is incorporated into the processes and procedures of the organisation.
- Ensure the availability of adequate and sufficient resources for the effective enforcement of the criminal compliance management system.
- Comply and enforce, internally and externally, the policy of criminal compliance.
- Communicate internally the importance of effective compliance management, consistent with the objectives and requirements of the compliance policy.
- Direct and contribute to staff in order to achieve compliance requirements and effectiveness according to their role in the organisation.
- Promote continuous improvement and support the various management roles to demonstrate leadership in crime prevention and criminal risk detection in their areas of responsibility.
- Encourage the use of procedures for the disclosure of potentially criminal behaviors that may affect the organisation.
- Ensure that no member of the organisation is subjected to retaliation, discrimination or disciplinary punishment for communicating in good faith, violations or substantiated suspicions of violations of the criminal compliance policy or for refusing to participate in criminal proceedings.

In cases where the senior management delegates decision-making in areas where there is a higher criminal risk, ODILO TID has established a delegation of powers procedure and a system of controls that ensures delegation itself.

This delegation does not exempt senior management from its own duties and responsibilities for the prevention of criminal risks. Nor does it transfer to the delegated persons any legal responsibilities for supervision or decision-making that fall within the scope of their duties.

## 4. Planning

### 4.1 Compliance objectives

Odilo TID has decided to define in this Compliance Manual the guidelines for punishable behaviors, guaranteeing their dissemination and favoring their applicability throughout the entity.

The purpose of this Manual is twofold:

- 1) Assist all employees of the entity in complying with applicable rules by providing them with a clear statement of policies and procedures.
- 2) Assist employees in identifying and correcting any actual or perceived violations by them.

Odilo TID is committed to the legal management of its businesses in accordance with the Code of Conduct.

The first commitment of business conduct of the entity is to comply with the applicable law, with special emphasis on the commitment to prosecute their violations and to collaborate with the Justice in the face of possible violations of law from which direct criminal liability may arise for the entity in accordance with the provisions of article 31 bis of the Spanish Criminal Code in force or any other provision that, in the future, could replace or supplement it.

### 4.2 Identification of risk activities

Odilo TID shall identify, analyse and evaluate its criminal risks.

The method is described in a procedure using the Magerit methodology and analysing and evaluating all the risks of committing criminal offences.

However, a SWOT analysis is also carried out to carry out the analysis of threats and opportunities.

In addition, a SWOT matrix has been developed, with which conclusions should be drawn, and to define the most convenient strategy according to the characteristics of the company and those of the market in which it moves.

This risk assessment is the basis for the entire preparation and implementation of the criminal risk prevention program, since it will serve to plan the allocation of resources and procedures that are appropriate and appropriate to manage the risks identified. In order to identify these risks, the first step that must be carried out will be to relate the compliance obligations of the company with its activities,

products, services and relevant aspects of its operations. All this, in order to identify situations in which they may incur breaches of the defined compliance obligations.

The causes and consequences of these non-compliances should be identified.

In this way, when analysing each of the risks or non-compliances identified, the following must be assessed:

causes and sources

severity of its consequences

C) Probability of the occurrence or materialisation of the risk

This compliance manual carries out an analysis of the most likely criminal types included in the reform of the Criminal Code operated at the entry into force of Organic Law 5/2010, of 22 June, with the possible criminal actions that could be carried out in ODILO and its measures and preventive actions to prevent them.

By way of example, but not limited, the following types of criminal offences are defined:

— **Article 197 of the Criminal Code. Crime of Cover-up and Disclosure of Secrets**

Criminal type

Any person who, in order to discover the secrets or violates the privacy of another, without his consent, takes possession of his papers, letters, e-mail messages or any other documents or personal effects or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or image, or any other communication signal.

The person who, without being authorised, acquires, uses or modifies, to the detriment of a third party, reserved data of a professional, personal or family nature of another that is registered in files or computer, electronic or telematic media, or in any other type of file or public or private register. Likewise, anyone who, without being authorised, accesses them by any means and who alters or uses them to the detriment of the owner of the data or a third party.

The person who, by any means or procedure and violating the security measures established to prevent it, accesses without authorisation to data or computer programs contained in a computer system or in part thereof or remains within it against the will of those who have the legitimate right to exclude it.

— Possible criminal actions that could be carried out in the entity:

Violation of correspondence secrecy.

Wiretapping.

Disclosure, dissemination or transfer of personal data information.

Improperly seize papers, letters, emails or any other document to uncover secrets.

— Procedures and controls:

The Code of Conduct must be complied with by all employees.

All employees must sign when joining the entity: Confidentiality clause.

All employees, complying with the provisions of the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD) and with the European Data Protection Regulation (GDPR), will sign a user engagement sheet.

ISO 9001 Organisation Quality Management

ISO 27017 Security Controls for Cloud Services

ISO 27018 Code of Practice for the Protection of Organisation's Personally Identifiable Information (PII)

— **Article 197 bis of the Criminal Code. Crime of computer raiding**

1. Anyone who, by any means or procedure, in breach of the security measures established to prevent it, and without being duly authorised, accesses or facilitates access to the whole or part of an information system or is maintained in it against the will of those who have the legitimate right to exclude it, shall be punished by imprisonment from six months to two years.

2. Any person who, through the use of devices or technical instruments, and without being duly authorised, intercepts non-public transmissions of computer data from, to or within an information system, including electromagnetic emissions thereof, shall be punished by a prison sentence of three months to two years or a fine of three to twelve months.

— Possible criminal actions that could be carried out in the entity:

Improperly seize information on computer support such as e-mail messages or confidential documents.

Violation of user access permissions

Disclosure, dissemination or transfer of personal data information.

— Procedures and controls:

The Code of Conduct must be complied with by all employees.

All employees must sign when joining the entity: Confidentiality clause.

All employees, complying with the provisions of the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD) and with the European Data Protection Regulation (GDPR), will sign a user engagement sheet.

ISO 27018 Code of Practice for the Protection of Organisation's Personally Identifiable Information (PII)

ISO 27701 Organisation Privacy Information Management

**— Arts. 248-251 of the Penal Code. Fraud Offences**

Criminal type:

Fraud is committed by those who, for profit, use deception enough to produce error in another, inducing him to perform an act of disposition to his own or others' detriment.

Scam inmates are also considered:

a) Those who, for profit and using some computer manipulation or similar artifice, obtain a non-consensual transfer of any asset to the detriment of another.

B) Those who manufacture, introduce, own or provide software specifically intended for the commission of the scams provided for in this article.

C) Those who, using credit or debit cards, or traveler's checks, or the data in any of them, carry out operations of any kind to the detriment of their holder or a third party.

— Possible criminal actions that could be carried out:

Use deception to cause error in another and induce him to perform an act of disposition to the detriment of himself or a third party, for profit.

Perform computer manipulations or similar devices to obtain a non-consensual transfer of any assets to the detriment of third parties for profit.

— Procedures and controls

The entity will carry out checks on signatures, codes and passwords.

The required Audit of Accounts of the entity will be carried out.

Internal Audits will be carried out periodically by the Audit and Control Directorate of the entity.

ISO 9001 Organisation Quality Management.

**— Articles 270 to 288 of the Criminal Code. Crimes related to intellectual and industrial property, against the market and consumers.**

Criminal type:

It is considered the perpetrator of an offence against intellectual property who, for profit and to the detriment of a third party, reproduces, plagiarises, distributes or publicly communicates, in whole or in part, a literary, artistic or scientific work, or its transformation, interpretation or artistic execution fixed, in any type of medium or communicated through any medium, without the authorisation of the owners of the corresponding intellectual property rights or their assignees.

Any person who, in order to discover a business secret, takes possession by any means of data, written or electronic documents, computer media or other objects relating thereto shall be punished by imprisonment. Likewise, anyone who, with knowledge of its illicit origin, and without having taken part in its discovery, disseminates, reveals or yields it shall be punished.

— Possible criminal actions that could be carried out in the entity:

1) Unauthorised copies of information relevant to the company through computer support or paper.

“Download” from the company or from the outside of pirated files or reproductions that do not comply with current law.

Use of illegal software.

— Procedures and controls:

All employees must sign the Confidentiality Clause.

Restrictions on access to applications.

Internal communications will be made indicating the patterns of use of the computer equipment.

Firewall systems are established to prevent unauthorised access.

ISO 27001 Information Security Management System.

— **Arts. 305-310 of the Penal Code. Crimes against the public finances and against social security**

Criminal type:

The person who, by act or omission, defrauds the state, regional, regional or local public finances, avoiding the payment of taxes, amounts withheld or that should have been withheld or income on account, wrongly obtaining refunds or enjoying tax benefits in the same way, provided that the amount exceeds EUR 120,000.



The person who, by act or omission, defrauds the Social Security by avoiding the payment of the contributions of this and concepts of joint collection, obtaining unduly refunds of the same or enjoying deductions for any concept also unduly, provided that the amount exceeds EUR 120,000.

Anyone who obtains subsidies, reliefs or aid from public administrations of more than EUR 120,000 by distorting the conditions required for its concession or hiding those that prevented it.

Who obtains, for himself or for another, the benefit of the Social Security System, the undue prolongation of the same, or facilitates to others its obtaining, through the error caused by the simulation or misrepresentation of facts, or the conscious concealment of facts of which he had the duty to inform, thereby causing harm to the public administration.

Who, being obliged by the tax law to keep commercial accounts, books or tax records when the amount exceeds EUR 240.000 and in addition:

It completely fails to comply with that obligation by means of direct estimation of tax bases.

Keep separate accounts which, relating to the same business and financial year, conceal or simulate the true situation of the undertaking.

He has not entered in the books compulsory business, acts, operations or, in general, economic transactions, or has entered them in figures other than the true ones.

Has made fictitious accounting entries in the compulsory books.

— Possible criminal actions that could be carried out in the entity:

The falsifying of documents for workers to fraudulently obtain or benefit from benefits.

Connivance for the obtaining of undue or higher benefits than those applicable in each case, or to avoid the fulfilment of the obligations that correspond to any of them in terms of benefits.

Make statements or record false or inaccurate information in the contribution documents, or in any other document, that cause fraudulent deductions or compensations in the contributions to be paid to the Social Security, or incentives related to them.

Obtain or unduly receive any type of reductions, bonuses or incentives in relation to the amount of social contributions that correspond.

Fraud to the Public Treasury by avoiding the payment of taxes, amounts withheld or that should have been withheld or income on account, wrongly obtaining refunds or enjoying tax benefits in the same way.

Obtain or unduly benefit from subsidies, employment promotion aid or any other provided for in programmes to support the creation of employment or occupational or continuing vocational training granted, financed or guaranteed, in whole or in part, by the State or by the Autonomous Communities

in the framework of the implementation of labour legislation, outside the economic system of social security.

Do not apply for initial membership or registration of workers entering the company.

Do not pay, in the form and statutory deadlines, the corresponding fees collected for all concepts by the General Treasury of Social Security.

— Procedures and controls:

Periodically Internal Audits.

Internal recruitment procedures.

External controls of customers.

Annual external audits.

ISO 9001 Organisation Quality Management

— **Arts. 311-318 bis of the Penal Code. Crimes against workers' rights**

Criminal type:

Those who, through deception or abuse of a situation of necessity, impose on workers at their service working conditions or social security conditions that harm, suppress or restrict the rights they have recognised by legal provisions, collective agreements or individual contract.

Those who traffic illegally with labor.

Those who produce serious discrimination in employment, public or private, against any person on account of their ideology, religion or belief, their belonging to an ethnicity, race or nation, their sex, sexual orientation, family situation, illness or disability, because they have legal or trade union representation of the workers, because of their relationship with other workers of the company or the use of any of the official languages within the Spanish State, and do not restore the situation of equality before the law after request or administrative sanction, repairing the economic damage that has arisen.

Those who, by deceit or abuse of a situation of necessity, prevent or restrict the exercise of freedom of association or the right to strike.

those who, acting in groups or individually, but in agreement with others, coerce other people to initiate or continue a strike.

Those who, in breach of the rules on the prevention of occupational risks and are legally obliged, do not provide the necessary means for workers to carry out their activities with appropriate safety and hygiene measures, in such a way as to seriously endanger their life, health or physical integrity.

— Possible criminal actions that could be carried out in the entity:

Impose on workers a service in working or social security conditions that harm, suppress or restrict the rights they have recognised by legal provisions, collective agreements or in the individual contract.

Employment discrimination based on racial or ethnic origin, religion, belief, disability, age, sexual orientation, etc.

Sexual harassment.

Prevent or limit the exercise of freedom of association or the right to strike.

Breaches of occupational risk prevention regulations, provided that they have serious significance for the physical integrity or health of workers.

Failure to comply with the specific rules on the protection of workers' health during periods of pregnancy and lactation.

Failure to provide the necessary means for workers to carry out their activities with appropriate safety and hygiene measures, in such a way as to seriously endanger their life, health and physical integrity.

Breach of the duty of confidentiality in the use of data relating to the health surveillance of workers.

Failure to take measures on first aid, firefighting and evacuation of workers.

Not take collective or individual protection measures that are of serious importance to the physical integrity or health of workers.

The assignment of workers to jobs whose conditions are incompatible with their known personal characteristics or that are manifestly in states or transitional situations that do not meet the psychophysical requirements of the respective jobs, which have a serious significance for the physical integrity or health of workers.

Failure to comply with the applicable rules on the coordination of business activities.

The hiring under irregular conditions of foreign workers who do not possess the legally required documentation.

— Procedures and controls:

— Internal audits.

—Signature channels.

—Checks carried out by the Joint Committees.

—External controls of customers.

— Existence of an internal protocol of prevention and action in case of situations of workplace harassment.

— Equality Plan.

— **Arts. 368-369 of the Penal Code. Drug Trafficking Crimes**

Criminal type:

Those who carry out acts of cultivation, processing or trafficking, or otherwise promote, favor or facilitate the illegal consumption of toxic drugs, narcotic drugs or psychotropic substances within the Group, or possess them for those purposes.

— Possible criminal actions that could be carried out in the entity:

Introduction and trafficking of toxic drugs, narcotic drugs or psychotropic substances in the premises of the entity.

— Procedures and controls:

- Express prohibition contained in the Code of Conduct.
- Complaints channel
- Control exercised by the controllers and by the customers.

— **Arts. 264 to 264 quater of the Penal Code. Crimes of computer damage**

Criminal type:

1. Anyone who, by any means, without authorisation and seriously erases, damages, deteriorates, alters, deletes or makes inaccessible third-party computer data, software or electronic documents, when the result is serious, shall be punished by imprisonment from six months to three years.

Where, in accordance with Article 31a, a legal person is liable for the offences covered by the three preceding articles, the following penalties shall be imposed on him:

a fine of two to five years or a maximum of twelve times the value of the damage caused, if it results in a higher amount, in the case of offences punishable by imprisonment of more than three years.

a fine of one to three years or three to eight times the value of the injury caused, if it results in a higher amount, in the rest of the cases.

Subject to the rules laid down in Article 66a, judges and courts may also impose the penalties referred to in Article 33(7)(b) to (g).

— Possible criminal actions that could be carried out in the entity:

- 1) Delete, damage, deteriorate, alter, delete or make inaccessible computer data, software or electronic documents
- 2) Illicit use of another person's personal data to facilitate access to the computer system or to gain the trust of a third party
- 3) Unauthorised access to applications, software
- 4) Using third party passwords
- 5) Discovery of secrets

— Procedures and controls:

The Code of Conduct must be complied with by all employees.

All employees must sign when joining the entity: Confidentiality clause.

All employees must comply, in the interest of the entity, with the Code of Conduct.

All employees, complying with the provisions of the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD) and with the European Data Protection Regulation (GDPR), will sign a user engagement sheet.

ISO 27018 Code of Practice for the Protection of Organisation's Personally Identifiable Information (PII)

ISO 27701 Organisation Privacy Information Management

ISO 9001 Organisation Quality Management.

### — Arts. 301 of the Penal Code. Money-laundering offences

Criminal type:

Anyone who acquires, possesses, uses, converts, or transmits property, knowing that it originates from a criminal activity committed by him or by any third party, or performs any other act to conceal or conceal his or her unlawful origin, or to assist the person who has participated in the offence or offences to avoid the legal consequences of his or her actions, shall be punished by imprisonment from six months to six years and a fine of up to three times the value of the property. In such cases, judges or courts, taking into account the seriousness of the act and the personal circumstances of the offender, may also impose on the offender the penalty of special disqualification from the exercise of his profession or industry for a period of one to three years, and may decide on the temporary or final closure of the establishment or premises. If the closure is temporary, its duration may not exceed five years.

— Possible criminal actions that could be carried out in the entity:

Outcropping of amounts of money of some importance

Volume of transactions carried out by customers does not correspond to their activity or is disproportionate

Transactions which give rise to certain irregularities outside common market practice

Relationship of irregular amounts of money to trafficking in prohibited substances

Transactions involving the movement of metallic coins, banknotes, travel cheques or other bearer documents issued by a credit institution, with the exception of those which are credited or debited to a customer's account, for an amount exceeding EUR 30.000 or their equivalent in foreign currency.

— Procedures and controls:

The anti-corruption policy must be complied with by all employees.

All employees must sign when joining the entity: Anti-corruption policy.

— **Arts. 262 of the Penal Code. Price alteration offences in public tenders and auctions**

Criminal type:

1. Those requesting gifts or promises not to take part in a public tender or auction; those who seek to keep the bidders away from it by means of threats, gifts, promises or any other artifice; those who agree with each other in order to alter the price of the auction, or those who fraudulently break or abandon the auction having obtained the award, shall be punished by imprisonment of one to three years and a fine of 12 to 24 months, as well as special disqualification from bidding in judicial auctions between three and five years. In the case of a competition or auction organised by the public authorities or public authorities, the agent and the person or company represented by him/her shall also be subject to the penalty of special disqualification, which shall in any case include the right to contract with the public administrations for a period of three to five years.

— Possible criminal actions that could be carried out in the entity:

Request for a benefit in exchange for not participating in a public tender

Avoiding the participation of other or specific third parties in a public tender as tenderers; with threats, gifts or promises.

— Procedures and controls:

Signature of the Code of Conduct

Conduct of internal audits

ISO 9001 Organisation Quality Management

— **Arts. 294 of the Penal Code. Offences of refusal to conduct inspectors**

Criminal type:

Those who, as de facto or legal administrators of any company incorporated or in formation, subject to or operating in markets subject to administrative supervision, refuse or preclude the action of persons, bodies or inspection or supervisory entities, shall be punished by imprisonment of six months to three years or a fine of 12 to 24 months.

In addition to the penalties provided for in the preceding paragraph, the judicial authority may order some of the measures provided for in article 129 of this Code.

— Possible criminal actions that could be carried out in the entity:

Action to deny or prevent the inspection or supervisory activity of certain bodies of the administration

— Procedures and controls:

Signature of the Code of Conduct

Development and approval of internal procedures.

— **Arts. 424 of the Penal Code. Offence of bribery**

Criminal type:

An individual who offers or delivers a gift or remuneration of any other kind to an authority, public official or person who participates in the exercise of the civil service to perform an act contrary to the duties inherent in his or her office or an act specific to his office, so that he does not perform or delay the one he should perform, or in consideration of his or her office or function, shall in their respective cases be punished with the same prison sentences and a fine as the corrupted authority, official or person.

Where an individual delivers the gift or remuneration at the request of the authority, public official or person involved in the exercise of the civil service, the same prison sentences and fines shall be imposed on them.

If the action taken or intended by the authority or official relates to a procurement procedure, subsidies or auctions convened by the public authorities or public authorities, it shall be imposed on the individual and, where appropriate, on the company, association or organisation to represent the penalty of disqualification from obtaining subsidies and public aid, to contract with entities, bodies or entities that are part of the public sector and to benefit from tax benefits or incentives for a period of five to ten years.

— Possible criminal actions that could be carried out in the entity:

Action to deliver compensation to delay or not perform inherent functions at the expense of the authority or public official.

— Procedures and controls:

Signature of the Code of Conduct

The required Audit of Accounts of the entity will be carried out.

Internal Audits will be carried out periodically by the Audit and Control Directorate of the entity.

Development and approval of internal procedures

— **Arts.419 of the Penal Code. Crime of bribery**

Criminal type:

A public authority or official who, for his own benefit or a third party, receives or requests, by himself or by an interposed person, a gift, favour or remuneration of any kind or accepts an offer or promise to perform in the exercise of his office an act contrary to the duties inherent therein or to not unreasonably perform or delay that which he should perform, shall be liable to imprisonment from three to six years, a fine of 12 to 24 months, and special disqualification from employment or public office and from the exercise of the right to stand for a period of nine to twelve years, without prejudice to the penalty corresponding to the act carried out, omitted or delayed on account of remuneration or promise, if it constitutes an offence.

— Possible criminal actions that could be carried out in the entity:

Action to hand over gifts to officials to act irregularly.

Action of acceding to handing out gifts to officials so that they may become corrupted

— Procedures and controls:

Signature of the Code of Conduct

Development and approval of internal procedures

The required Audit of Accounts of the entity will be carried out

Internal Audits will be carried out periodically by the Audit and Control Directorate of the entity.

— **Arts.429 of the Penal Code. Offence of trade in influences**

Criminal type:

An individual who influences a public official or authority taking precedence of any situation arising from his personal relationship with him or with another public official or authority in order to obtain a decision



that could directly or indirectly generate an economic benefit for himself or for a third party, shall be punished by imprisonment of six months to two years, a fine of both the duplicate of the profit pursued or obtained, and the prohibition of contracting with the public sector, as well as the loss of the possibility of obtaining public subsidies or aid and the right to benefit from tax benefits or incentives for a period of six to ten years. If it obtains the benefit pursued, these penalties shall be imposed on its upper half.

— Possible criminal actions that could be carried out in the entity:

An individual who seeks to influence a public official or authority by taking precedence of any situation arising from his personal relationship with him or with another public official or authority in order to obtain a resolution that could directly or indirectly generate an economic benefit for himself or for a third party.

— Procedures and controls:

Signature of the Code of Conduct

Development and approval of internal audit procedures

#### — Arts.510 of the Penal Code. Hate crime

Criminal type:

a) Those who publicly promote, promote or incite directly or indirectly to hatred, hostility, discrimination or violence against a group, a part of it or a person determined by reason of its membership, on racist, anti-Semitic or other grounds relating to ideology, religion or belief, family situation, membership of its members to an ethnicity, race or nation, national origin, sex, sexual orientation or identity, on grounds of gender, illness or disability.

B) Those who produce, prepare, possess for the purpose of distributing, facilitating access to, distributing, disseminating or selling writings or any other material or media which, by reason of their content, are suitable for promoting, promoting, or inciting directly or indirectly to hatred, hostility, discrimination or violence against a group, a part thereof, or against a person determined by reason of their membership, for racist, anti-Semitic or other reasons relating to ideology, religion or belief, family situation, membership of its members to an ethnicity, race or nation, national origin, sex, sexual orientation or identity, due to gender, illness or disability.

publicly deny, seriously trivialise or exalt crimes of genocide, against humanity or against persons and property protected in the event of armed conflict, or exalt their perpetrators, when they have been committed against a group or part thereof, or against a person determined by reason of his or her belonging to it, on racist, anti-Semitic or other grounds relating to ideology; religion or belief, family status or membership of its members to an ethnicity, race or nation, national origin, sex, sexual orientation or identity, on grounds of gender, illness or disability, where this promotes or favours a climate of violence, hostility, hatred or discrimination against them.

those who harm the dignity of persons by actions involving humiliation, contempt or discredit of any of the groups referred to in the preceding paragraph, or of a part thereof, or of any person determined by reason of their belonging to them on racist, anti-Semitic or other grounds relating to ideology, religion or belief, family status, membership of their members in an ethnic group, race or nation, their national origin, sex, sexual orientation or identity, for reasons of gender, illness or disability, or produce, elaborate, possess for the purpose of distributing, facilitating access to, distributing, disseminating or selling writings or any other material or media that by their content are suitable for injuring the dignity of persons by representing a serious humiliation, contempt or discredit of any of the aforementioned groups, of a part of them, or of any person determined by reason of their belonging to them.

e) Those who exalt or justify by any means of public expression or dissemination the crimes committed against a group, a part thereof, or a person determined by reason of their belonging to that group on racist, anti-Semitic or other grounds relating to ideology, religion or belief, family situation, membership of their members to an ethnicity, race or nation, their national origin, sex, sexual orientation or identity, on grounds of gender, illness or disability, or those who participated in its execution.

— Possible criminal actions that could be carried out in the entity:

Any criminal offence, including infractions against persons or property, where the victim, local or purpose of the infraction is chosen for its, actual or perceived connection, sympathy, affiliation, support, or membership of a group (based on a common characteristic of its members, such as their actual or perceptive race, national or ethnic origin, language, color, religion, sex, age, intellectual or physical disability, sexual orientation or other similar factor).

— Procedures and controls

Signature of the Code of Conduct

Knowledge and dissemination of the protocol against workplace harassment

— **Arts.432-435 of the Penal Code. Offence of embezzlement of funds**

Criminal type:

The provisions of this chapter are extensive:

1° to which they are entrusted for any concept of funds, income or effects of public administrations.

2° To individuals legally designated as depositaries of public flows or effects.

3° To the administrators or depositaries of money or property seized, abducted or deposited by public authority, even if they belong to private individuals.

4° To the insolvency administrators, in relation to the insolvency estate or the economic interests of the creditors. In particular, the interests of creditors will be considered affected when the order of payment of the claims set out in the law will be intentionally altered.

5° To legal persons who, in accordance with the provisions of Article 31 bis, are responsible for the offences referred to in this Chapter.

— Possible criminal actions that could be carried out in the entity:

Use of public funds for purposes other than those granted

Use of grants for other purposes

Breach of contract terms

— Procedures and controls:

Signature of the Code of Conduct

Securing and retaining public funds in deposit

Apply public goods for agreed purposes in procurement

Allocate the subsidies for the purposes for which they were awarded

Comply with the terms established in the contracting with companies, bodies and administrations

Document economic processes related to the management of public funds or assimilated funds

Diligently administer public assets and insolvency estates.

— **Arts.259 et seq. of the Penal Code. Punishable insolvency offence**

Criminal type

Hide, cause damage or destroy property or property that is included, or would have been included, in the mass of the competition at the time of its opening.

2nd Perform acts of disposition by handing over or transferring money or other assets, or by assuming debts, that are not proportionate to the debtor's property status, or to his income, and which lack economic or business justification.

3 rd Performs sales or services at a price lower than its cost of acquisition or production, and which in the circumstances of the case lacks economic justification.

4th Simulate third party credits or proceed to the recognition of fictitious credits.

Participate in speculative business, where this lacks economic justification and results, in the circumstances of the case and in the light of the economic activity carried out, contrary to the duty of diligence in the management of economic affairs.

Fails to comply with the legal duty to keep accounts, keep double accounts, or commit irregularities that are relevant to the understanding of your property or financial situation. It will also be punishable for the destruction or alteration of the accounting records, when this makes it difficult or significantly impairs the understanding of their equity or financial situation.

Hide, destroy or alter the documentation that the employer is obliged to keep before the expiry of the period to which this legal duty extends, when this makes it difficult or impossible to examine or assess the real economic situation of the debtor.

Formulate the annual accounts or accounting books in a manner contrary to the rules governing commercial accounts, in such a way as to make it difficult or impossible to examine or assess the debtor's actual economic situation, or fails to fulfil the duty to formulate the balance sheet or inventory within a period of time.

9<sup>a</sup> Performs any other active or omissive conduct that constitutes a serious breach of the duty of diligence in the management of economic affairs and which is attributable to a decrease in the debtor's assets or by means of which the real economic situation of the debtor or his business activity is concealed.

— Possible criminal actions that could be carried out in the entity:

Conceal, destroy assets included in the estate of the Contest of Creditors when it is open

Perform disposition acts by handing over or transferring money or other assets

Simulate third-party credits or recognise fictitious credits

Failure to comply with the obligation to keep an accounting or double accounting

Destroy, hide documentation that the employer is obliged to carry.

— Procedures and controls:

Internal and external audits

Signature of the Code of Conduct

Prior to the realisation of any act of encumbrance, disposition or lease of a movable or immovable property, the ownership of the same in favor of ODILO must be verified.

— **Arts.576 of the Penal Code. Crime of financing terrorism**

#### Criminal type

1. A term of imprisonment of five to ten years and a fine of threefold to fivefold of its value shall be punishable by any means which, directly or indirectly, collects, acquires, possesses, uses, converts, transmits or engages in any other activity with property or securities of any kind with the intention of being used, or knowing that they will be used, in whole or in part, to commit any of the offences covered by this Chapter.

4. Any person who, being specifically subject by law to cooperate with the authority in the prevention of terrorist financing activities, gives rise, for serious recklessness in the performance of those obligations, to the failure to detect or prevent any of the conduct described in paragraph 1 shall be punishable by one or two degrees less than that provided for therein.

— Possible criminal actions that could be carried out in the entity:

Carrying out actions, as well as their provocation or collaboration to be carried out, which individually or collectively may endanger the prevention of money laundering or involve any action to finance terrorism

— Procedures and controls:

#### Signature of the Code of Conduct

Prohibition of any movement, transfer, alteration, use or transaction of capital or financial assets that gives or may result in a change in the volume, amount, location, ownership, possession, nature or destination of such capital or assets, or of any other change that could facilitate their use, including the management of a portfolio of securities.

Prohibition of the opening of accounts in financial institutions or their branches operating in Spain where they appear as holders, authorised to operate or representatives.

**Contraband** (Organic Law 6/2011 of 30 June 2011 amending Organic Law 12/1995 of 12 December 1995 on the suppression of smuggling)

- This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

#### **Article 184(1) of the Criminal Code. Offence of sexual favours:**

#### Criminal type

1. A person who seeks favours of a sexual nature, for himself or for a third party, in the context of an employment, teaching, service-providing or similar relationship, continuous or habitual, and with such conduct causes the victim an objective and gravely intimidating, hostile or humiliating situation, shall be punished, as the perpetrator of sexual harassment, by imprisonment of six to twelve months or a fine of 10 to 15 months and special disqualification from exercising the profession, trade or activity of 12 to 15 months.

2. If the person guilty of sexual harassment has committed the act by virtue of a situation of superiority at work, teaching or hierarchical, or on a person subject to his or her custody or custody, or with the express or tacit announcement of causing the victim an evil related to the legitimate expectations that the victim may have within the scope of the aforementioned relationship, the penalty shall be imprisonment for one to two years and special disqualification for the exercise of the profession, trade or activity from 18 to 24 months.

3. In addition, if the person guilty of sexual harassment has committed it in centres for the protection or reform of minors, a centre for the detention of foreign persons, or any other detention, custody or reception centre, including temporary stay, the penalty shall be imprisonment from one to two years and special disqualification from exercising the profession, trade or activity from 18 to 24 months, without prejudice to the provisions of Article 443.2.

4. When the victim is in a situation of special vulnerability because of his age, illness or disability, the penalty shall be imposed on his upper half.

— Possible criminal actions that could be carried out in the entity:

Favours of a sexual nature, for themselves or for a third party, in the field of an employment relationship

— Procedures and controls:

Workplace Harassment Protocol

### **Article 197(7) of the Criminal Code. Sexting Crime:**

Criminal type

7. A term of imprisonment of three months to one year or a fine of six to twelve months shall be punishable by any person who, without the authorisation of the person concerned, disseminates, discloses or transfers to third parties images or audio-visual recordings of the person obtained with his consent in a home or in any other place beyond the sight of third parties, where the disclosure seriously undermines the personal privacy of that person.

Possible criminal actions that could be carried out in the entity:

Disseminate, disclose or assign to third parties images or recordings that you have obtained with your consent

— Procedures and controls:

Workplace Harassment Protocol

**Article 173(1) of the Criminal Code. Offence of humiliation:**

Criminal type

1. Anyone who inflicts degrading treatment on another person, seriously impairing his or her moral integrity, shall be punished by imprisonment from six months to two years.

Possible criminal actions that could be carried out in the entity:

Persons who, in the context of any employment relationship, and taking precedence of their situation of superiority, carry out “repeatedly hostile or humiliating acts” involving “serious harassment” against the victim

— Procedures and controls:

Workplace Harassment Protocol/Actions Deriving from the Equality Plan (Awareness)/Sign Code of Conduct

**Article 325 of the Criminal Code. Environmental crime**

Criminal type

1. Shall be punished by imprisonment of six months to two years, a fine of 10 to 14 months and special disqualification for a period of one to two years for a period of one to two years which, in contravention of laws or other general provisions protecting the environment, directly or indirectly causes or carries out emissions, discharges, radiation, extractions or excavations, terrifications, noises, vibrations, injections or deposits; in the atmosphere, soil, subsoil or land, ground or sea waters, including the high seas, with an impact even on transboundary spaces, as well as water abstractions which, by themselves or together with others, cause or may cause substantial damage to air, soil or water quality, or to animals or plants.

Possible criminal actions that could be carried out in the entity:

In contravention of laws or other provisions of a general nature that protect the environment, directly or indirectly cause or carry out emissions, discharges, radiation, extractions or excavations, terrations, noise, vibrations, injections or deposits, into the atmosphere, soil, subsoil or land, ground or sea waters, including the high seas, with an impact including on transboundary spaces, as well as water abstractions which, by themselves or jointly with others, cause or may cause substantial damage to air, soil or water quality, or to animals or plants, or to animals or plants.

— Procedures and controls:

ISO 14001 — environmental management organisation

### **Article 326 bis of the Criminal Code. Storage of hazardous substances**

Criminal type

1. They shall be punished by the penalties provided for in the preceding article, in their respective cases, who, in contravention of laws or other provisions of a general nature, collect, transport, recover, transform, dispose of or exploit waste, or do not adequately control or monitor such activities, in such a way that they cause or may cause substantial damage to the quality of air, soil or water, or to animals or plants, death or serious injury to persons, or may seriously impair the balance of natural systems.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

### **Article 330 of the Criminal Code. Cause of damage in a protected natural area**

Criminal type

They shall be punished by the penalties provided for in Article 325, in their respective cases, who, in contravention of laws or other provisions of a general nature, carry out the operation of installations in which a dangerous activity is carried out or in which dangerous substances or preparations are stored or used in such a way as to cause or may cause substantial damage to the quality of air, soil or water, animals or plants, death or serious injury to persons, or could seriously damage the balance of natural systems.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

### **Article 329 of the Criminal Code. Environmental administrative prevarication**

Criminal type

1. A public authority or official who knowingly has informed favourably of the granting of manifestly illegal licences authorising the operation of the polluting industries or activities referred to in the preceding articles, or who, on the occasion of his inspections, has silenced the infringement of laws or regulations of a general nature governing them, or who has failed to carry out mandatory inspections, shall be punished by the penalty provided for in Article 404 of this Code and, in addition, by imprisonment of six months to three years and a fine of eight to twenty-four months.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.



## **Art. 156 bis Criminal Code. Crime of illegal trafficking organs**

### Criminal type

1. Those who in any way promote, favour, facilitate, publicise or execute trafficking in human organs shall be punished by imprisonment of six to twelve years in the case of the organ of a living person and imprisonment of three to six years in the case of the organ of a deceased person.

For this purpose, trafficking in human organs means:

the illicit extraction or procurement of other human organs. Such extraction or acquisition shall be unlawful if it occurs under any of the following circumstances:

1st that has been carried out without the free, informed and express consent of the living donor in the manner and with the legally prescribed requirements;

2nd that has been carried out without the necessary authorisation required by law in the case of the deceased donor,

Third that, in exchange for the extraction or obtaining, for their own benefit or others, it is requested or received by the donor or a third party, by itself or for an interposed person, gift or retribution of any kind or offer or promise is accepted. A gift or remuneration shall not be understood as compensating for expenses or loss of income arising from the donation.

the preparation, preservation, storage, transport, transfer, reception, import or export of illicitly extracted organs.

the use of illicitly extracted organs for the purpose of transplantation or for other purposes.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

## **Art. 189 bis Criminal Code. Offences relating to minor prostitution and corruption:**

### Criminal type

a) The person who captures or uses minors or persons with disabilities in need of special protection for purposes or in exhibition or pornographic shows, whether public or private, or to produce any kind of pornographic material, whatever its support, or finances any of these activities or profits from them.

B) Anyone who produces, sells, distributes, exhibits, offers or facilitates the production, sale, dissemination or display by any means of child pornography or in whose elaboration persons with disabilities in need of special protection have been used, or possesses it for these purposes, even if the material has its origin abroad or is unknown.

For the purposes of this Title, child pornography or the elaboration of which persons with disabilities in need of special protection have been used:

any material which visually represents a minor or a person with a disability in need of special protection by engaging in sexually explicit, actual or simulated conduct.

any representation of the sexual organs of a minor or person with disabilities in need of special protection for primarily sexual purposes.

any material that visually depicts a person who appears to be a minor engaging in sexually explicit, actual or simulated conduct, or any representation of a person's sexual organs that appears to be a minor, for primarily sexual purposes, unless the person who appears to be a minor actually turns out to be eighteen years or older at the time the images are obtained.

realistic images of a minor engaging in sexually explicit conduct or realistic images of a minor's sexual organs, for primarily sexual purposes.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

**Art.177 bis Criminal Code. Crime of trafficking in human beings:**

Criminal type

1. A sentence of five to eight years' imprisonment shall be punishable as a prisoner of trafficking in human beings, whether in Spanish territory, whether from Spain, in transit or for its destination, by using violence, intimidation or deceit, or by abusing a situation of superiority or need or vulnerability of the national or foreign victim, or by handing over or receiving payments or benefits to obtain the consent of the person holding control over the victim, capture, transport, transfer, welcome, or receive, including the exchange or transfer of control over such persons, for any of the following purposes:

the imposition of forced labour or services, slavery or practices similar to slavery, servitude or begging.

B) Sexual exploitation, including pornography.

C) Exploitation to carry out criminal activities.

D) The removal of their bodily organs.

the conclusion of forced marriages.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

**Article 319 of the Criminal Code. Crimes of construction, building and urbanisation**

Criminal type

1. Prison sentences of one year and six months to four years, a fine of 12 to 24 months, unless the benefit obtained for the offence exceeds the resulting amount in which case the fine shall be up to three times the amount of that benefit, and special disqualification for the profession or trade for a period of one to four years, promoters, builders or managerial technicians carrying out urbanisation works, construction or building not authorised on land intended for roads, green areas, public property or places that have legally or administratively recognised their landscape, ecological, artistic, historical or cultural value, or for the same reasons have been considered of special protection.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

**Article 343 of the Criminal Code. Offences relating to nuclear energy:**

Criminal type

1. Any person who, through the discharge, emission or introduction into the air, soil or water of a quantity of materials or ionising radiation, or exposure by any other means to such radiation endangers the life, integrity, health or property of one or more persons, shall be punished by imprisonment of six to twelve years and special disqualification from public office, occupation or occupation for a period of six to ten years. The same penalty shall be imposed when such conduct jeopardises the quality of air, soil or water, animals or plants.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

**Article 348 of the Criminal Code. Risk crimes caused by explosives**

Criminal type

1. Those who, in the manufacture, handling, transport, possession or placing on the market of explosives, flammable or corrosive substances, toxic and asphyxiating substances, or any other materials, apparatus or devices which may wreak havoc, contravene established safety standards, in particular endangering the life, physical integrity or health of persons, or the environment, shall be punished by imprisonment from six months to three years, a fine of 12 to 24 months and special disqualification to public employment or office, profession or office for a period of six to twelve years. The same penalties shall be imposed on those who unlawfully produce, import, export, market or use ozone-depleting substances.

This illegal activity does not apply in the entity because, due to the entity's own activity, this type of crime cannot occur.

**Article 399 bis of the Criminal Code. Falsity means of payment**

Criminal type

1. Anyone who alters, copies, reproduces or otherwise falsifies credit or debit cards, traveler's cheques or any other payment instrument other than cash shall be liable to imprisonment from four to eight years.

The penalty shall be imposed in its upper half where the falsified effects affect a generality of persons or when the acts are committed within the framework of a criminal organisation dedicated to these activities.

Where, in accordance with Article 31a, a legal person is liable for the above offences, he shall be fined from two to five years. Subject to the rules laid down in Article 66a, judges and courts may also impose the penalties referred to in Article 33(7)(b) to (g).

Possible criminal actions that could be carried out in the entity:

Alter, copy, reproduce or otherwise falsify credit or debit cards or travel cheques; who, without having intervened in the counterfeiting, will use, to the detriment of another and to sa-  
biendas of falsehood, credit or debit cards or falsified traveler's cheques

— Procedures and controls:

Powers of authorisation of expenditure; expenditure policy (Policy travel); policy training on expenditure

#### **Article 445 of the Criminal Code. Corruption to foreign officials**

Criminal type

The provocation, conspiracy and proposition to commit the offences provided for in this Title shall be punishable, respectively, by the lower penalty of one or two degrees.

Possible criminal actions that could be carried out in the entity:

Corrupting or attempting to corrupt; Respond to requests from authorities or officials (directly or through intermediaries)

— Procedures and controls:

Code of conduct; reporting channel

## **5. Support elements**

### **5.1 Training plan**

Odilo TID aspires to establish a culture of compliance and continuous improvement within the entity and the instrument to achieve these objectives, is the training plan.

The training aims to know how certain actions carried out (in many cases, out of ignorance) by the members of the organisation may lead to the commission of crimes for which the perpetrator himself and, in addition, the entity and its administrative body will have to respond criminally.

Odilo TID will develop a procedure with the training plan whose contents will be:

- Learning
- Awareness
- Awareness
- Commitment
- Culture of compliance
- Continuous improvement

Another objective that is pursued with the training plan is that the members of the entity appreciate the value of good corporate practices and ethical principles for their own personal development and for the sustainability of the organisation.

In addition, the training will be understood as a process of continuous improvement and through a register the times in which it is intended to provide such training are established.

The training should be addressed to the different compliance actors. These are:

- The compliance body
- Managers and middle managers.
- Company staff.

## 5.2 Communication channels

Odilo has opted for the creation of an email address: [politicaanticorrupcion@odilo.us](mailto:politicaanticorrupcion@odilo.us) for sending/receiving complaints by your employees and other interested parties.

The sending will be made through a direct email to the aforementioned email address or through the mailbox established on the ODILO website for this purpose, which will be permanently available both to employees of the entity and to the rest of the interested parties.

Access to this enabled email address will only be allowed by the secretary of the compliance body, who will access it with a single password known by it. In the case of obligation by regulations on data protection, it will comply with it, which may affect the complaint channel procedure.

Confidentiality and anonymity shall be ensured in such a way that only the content of the form or e-mail will be reported, and transcribed by the clerk without giving it to 'resubmit' and without indicating the (invented) mail of the person sending the form or e-mail if applicable to the e-mail address.

Once reported to the compliance body for the evaluation of the content of the form or email received, the email will be deleted from the mailbox in order not to store the received emails.

Through a follow-up of the complaints received by email and the mailbox, and their subsequent referral to the compliance body, it is possible to obtain reports of the activity of the channel where the number of complaints sent, opened, finalised, etc.

These reports may be used as evidence of the functioning of the channel in order to demonstrate the degree of compliance with the obligations relating to the criminal liability of the legal person.

The investigations of the illegals that are communicated through the complaints channel, will be carried out by the compliance body and in accordance with the procedure of post-criminal actions.

### 5.3 Investigation of complaints

The compliance body responsible for carrying out the investigation, which shall have a sufficient mandate to enable them to access and carry out all the necessary evidence.

Once it has been agreed to open an internal investigation, it is appropriate to determine to which employees of the company will be communicated (all or only one party), and whether or not that decision will be made public.

Likewise, the employee under investigation must have knowledge at the beginning of the investigation, and therefore, it would be advisable to specify in advance:

- The scope and subject matter of investigation
- The maximum duration of the same
- The powers or powers that correspond to the investigating body together with the personal and material resources with which it will have

- The system of organising the registration, archiving and preservation of documents that examines the obligations of the employees of the company to cooperate with the investigation and at what point in time a sanctioning file can be opened, if necessary, to the employee under investigation.

The compliance body shall have at its disposal all the evidence necessary to carry out the investigation.

It will be possible to use the means of proof consisting of ICT media such as the intervention of media and worker information such as corporate mail as reflected in the procedure PE SGI-A09 Access Control, PE SGI-A05 Information Security Policies, PE SGI-A07 Security Linked to Human Resources, PE SGI-A13 Communications Security Implementation of ISO 27001 Information Security Management.

Such interventions of the company's devices do not violate the right to privacy since the worker has been informed and warned that these devices cannot be used for personal use.

However, the intervention of the devices will be carried out under the criteria of proportionality, of least possible intervention and of rationality, respecting the rights of:

- Rights of defence during the investigation.
- Right to be informed.
- Right to access the evidence and the file of the investigation.
- Right to make allegations and present evidence.
- Right to legal assistance.

## 6. Operation

### 6.1 Risk treatment plan

In order to achieve the regulatory compliance objectives defined in this manual on the prevention of criminal risks, the decision-making of ODILO TID in any of its activities or departments shall be carried out in accordance with the management of the Compliance Manual, the Criminal Risk Prevention Policy and the Code of Conduct.

The procedures should provide for how each of the company's options should be treated when making a decision within its policy areas, so that the criminal risks inherent in that decision are minimised.

However, a SWOT analysis is also carried out to carry out the analysis of threats and opportunities.

For the analysis it will be followed according to the procedure described for risk management.

### 6.2 Code of Conduct

The ODILO TID Code of Conduct aims to establish the guidelines of conduct that must govern the ethical behavior of all its directors, employees, associates and members of the Board of Directors in their daily performance and in the relationships and interactions that the entity maintains.

These groups are formed by the persons mentioned above and also by suppliers, external collaborators, public and private institutions, and civil society in general to the extent that they relate to the entity.

This Code of Conduct is based on the definition of the security policy of ODILO TID to which it complements and which constitutes a guide of action to ensure adequate behavior in the professional performance of all the persons mentioned above.

The Code reflects the due diligence principle applied by ODILO TID for the prevention, detection and eradication of irregularities arising from criminal offences.

This due diligence requires ODILO TID to design and implement control models that periodically analyse risks, ensure knowledge of the organisation's standards, define responsibilities and establish procedures that allow confidential reporting and irregularities, investigation and adoption of measures.

Odilo TID understands that the procedures it has in place allow it to respond to the above objectives.

### 6.3 Disciplinary system

Failure to comply with the principles, rules, policies and protocols indicated in this Compliance Manual may result in labor sanctions against ODILO staff, without prejudice to any administrative or criminal penalties that may correspond.

The only body competent to impose disciplinary sanctions is the Board of Directors of the entity.

The procedure to be followed for the imposition of disciplinary sanctions, as well as the initiation and development, where appropriate, of the relevant disciplinary proceedings, or for the imposition and communication of the sanction, shall be governed by the provisions of the Workers' Statute, the applicable Collective Agreement and the internal agreements with the corresponding workers' representatives, if any.

The disciplinary system can only reach employees, i.e. those linked by some type of employment relationship.

The penalties that may be imposed depend on the seriousness of the fault, as well as on other factors such as the repetition of the infringement, the recidivism or the entity of the damages in your case.

In any of the cases, the burden of proof of the labor violation justifying the dismissal or disciplinary sanction shall be borne by the entity.

As for the limitation of offences and misdemeanours committed, it will be as provided for in the collective agreement, in the Statute of Workers and in the rest of the applicable legislation.



## 7. Performance evaluation

### 7.1 Monitoring and measurement of the system

Odilo TID has identified in its Crime Prevention System indicators that show how effective and efficient the criminal compliance management system is and what levels of implementation and maturity have been achieved.

The information to be obtained is:

- Activity indicators: Percentage of staff trained effectively; level of use of mechanisms for obtaining opinions; number and type of corrective actions that were taken against non-conformities.
- Predictive risk indicators: Measuring the loss of long-term target potential;
- Indicators on effectiveness: time used to inform and take corrective action; consequences deriving from conformity

The analysis carried out will be evidenced in the procedure of metrics and indicators. This analysis can result in corrective or preventive actions.

Odilo TID will establish a procedure to seek and receive information and opinions from different interested parties and third parties, through questionnaires from sources of opinion about the opinion of the criminal compliance.

### 7.2 Audit plan

In addition to the regular reports of the compliance body, internal audits should also be planned at a two-year interval;

These audits will be aimed at ensuring that compliance with the provisions of the criminal risk prevention programme is maintained, and that it is in fact being monitored and updated in relation to the relevant changes.

An audit plan shall be established in order to plan the corresponding ones to verify the degree of compliance, as well as the follow-up of the resulting non-conformities.

## 8. Improvement

### 8.1 Review and update plan

The Board of Directors has delegated to the compliance body the tasks of data collection, establishment of objectives and goals, improvement actions, monitoring and their communication to the staff of the organisation.

Each and every one of the objectives and targets that have been set are measurable and consistent with criminal crime prevention policies.

## 8.2 Continuous improvement

The programme for the prevention of criminal risks should be continuously improved.

Odilo TID must ensure at all times that it is suitable, adequate and effective to prevent the existence of criminal risks.

The information collected and analysed in the follow-up actions, and especially in the reports prepared by the compliance body, as well as internal audits, should be used as a basis to identify opportunities for improvement of the criminal compliance management system.

## 8.3 Non-conformities and corrective actions

Where a non-conformity is known, the organisation shall react to the non-conformity, and as applicable:

- a) Take action to control and correct it  
coping with the consequences

Once the non-conformity has been reacted to, the need for further action should be assessed to prevent it from occurring again. To this end, a complete evaluation of the programme in relation to the identified non-conformity must be carried out to eliminate the risk of recurrence.

The lack of prevention or detection of timely non-conformity does not necessarily mean that the criminal risk prevention programme is not effective in preventing and detecting criminal risks at a general level. However, prompt action should be taken when a non-conformity is detected, in order to mitigate the effects of non-compliance and to amend the criminal risk prevention programme where appropriate.

## 9. Resources

The organisation is committed to providing the necessary resources for the establishment, development, implementation, evaluation, maintenance and continuous improvement of the penal compliance management system, according to the size of the company, its structure, activity and complexity.

The governing body and senior management of the company will ensure that the necessary resources are deployed, effectively to ensure that compliance objectives are achieved.

For the correct development of the program for the prevention of criminal risks, as well as for the implementation of a true culture of compliance with criminal regulations within ODILO TID, the following resources will be made available to the criminal risk prevention plan:

- financial
- human rights
- external advice
- organizational infrastructure
- updated reference material
- training
- technology