



Crime Prevention Policy

Telefónica, S.A.

Country-level Policy

Approved by the Board of Directors of Telefónica, S.A.

5th Edition - January 2025

Control de cambios

Edición	Modificaciones
1.0	February 2012
2.0	December 2015
3.0	September 2016
4.0	November 2020
5.0	January 2025

1. Contenido

1	Explanatory preamble	4
2.	Purpose.....	5
3.	Scope of Application.....	6
4.	Crime Prevention Programme	6
5.	Crime Prevention Function.....	19
6.	Audit of the Operation of the Programme.....	21
7.	Entry into force.....	21

1 Explanatory preamble

Following the entry into force of the reform of the Criminal Code by Organic Law 5/2010 of 22 June, the Telefónica Group undertook a process, focused mainly in Spain, of reviewing and updating its control systems to ensure their adaptation to these new legal requirements, in particular with regard to the provisions of Article 31 bis of the Criminal Code (CC), taking further preventive measures to prevent the commission of possible criminal offences in its environment. Subsequently, successive reforms of the Penal Code have generated a process of continuous revision of this control environment. Specifically, following the approval of Organic Law 1/2015 of 30 March, and, in particular, of the new Articles 31 ter and 31 quater, the environment has been revised and, subsequently, both the Attorney General's Office and case law have developed some issues in relation to this matter. The control environment has also been reviewed, following the various amendments made to the Criminal Code through successive legislative amendments in this area, notably those arising from Law 2/2023 of 20 February, regulating the protection of persons who report regulatory offences and the fight against corruption (hereinafter, Law 2/2023).

In this regard, and with the encouragement and supervision of the Audit and Control Committee of the Board of Directors of Telefónica, S.A., a complete and updated crime prevention programme (hereinafter, Crime Prevention Programme or Programme) was formalised and subsequently reviewed in the Group companies in Spain, with application, where appropriate, of the corresponding criminal compliance management system, a programme that in each of these companies has and will take into account its own conditions and characteristics (type of activity, products and services offered, where appropriate, purpose of the business relations, duration or volume of its operations, etc.). The other Group companies have formalised or will formalise a crime prevention programme in accordance with the legal requirements applicable to them.

To this end, in the case of the Telefónica Group companies in Spain (hereinafter, each of them, the Company), the possible criminal risks have been reviewed, recorded and assessed (or, where appropriate, the review, recording and assessment process will be carried out with respect to those companies recently incorporated or acquired) as well as the scenarios that may give rise to such risks, which the Company faces depending on its activity, as well as the existing controls aimed at mitigating these risks, taking the necessary measures to update and strengthen these controls in light of the risks identified. These activities include, but are not limited to, those related to negotiating and contracting with third parties, whether customers or suppliers, the development, purchase or marketing of products or services, the management of financial resources, the management and processing of privileged and personal information, relations with public entities and authorities and the management of human resources.

In accordance with our Crime Prevention Policy for the Telefónica Group in Spain, the Telefónica Group follows a zero tolerance policy with regard to possible criminal

offences, as reflected in the Responsible Business Principles that make up the Group's fundamental values, promoting an ethical and responsible business culture in each of the companies that make up the Group. And, in line with this policy and with a preventive and control purpose, the Board of Directors, at its meeting held on 2 February 2012, approved this Crime Prevention Policy, subsequently revised in successive editions (second edition, approved by the Board of Directors on 16 December 2015, third edition, approved by the Board of Directors on 28 September 2016, fourth edition, approved by the Board of Directors in November 2020 and the present fifth edition, approved by the Board of Directors on 29 January 2025).

2. Purpose

The purpose of this policy is to present a detailed description of the main components of the Crime Prevention Programme of Telefónica Group companies in Spain, without prejudice to the internal implementing regulations. This Programme is conceived as a framework comprising the regulations, procedures and other specific controls that make it possible to reasonably ensure that the risks of committing crimes affecting the Group's companies in Spain are adequately identified, documented, assessed, controlled and mitigated, in an environment of permanent review, updating and continuous improvement.

This Crime Prevention Programme, in accordance with the aforementioned articles of the Criminal Code, has a dual function:

- To prevent offences being committed on behalf of or for the account of the various companies comprising the Telefónica Group in Spain, and for their direct or indirect benefit, by their legal representatives or by those who, acting individually or as members of a body of the legal person, are authorised to take decisions on behalf of the legal person or have powers of organisation and control within the legal person; furthermore, that offences may be committed, in the performance of corporate activities and on behalf of and for the direct or indirect benefit of the legal entities that make up the Telefónica Group in Spain, by those who, being subject to the authority of the legal representatives and de facto or de jure directors, may carry out such acts due to a serious breach by the former of their duties of supervision, monitoring and control of their activity in view of the specific circumstances of the case.
- Establish mechanisms to ensure that, in the event that, despite this preventive function, the aforementioned persons commit crimes, measures are taken to investigate and, if necessary, to protect the informant and other measures established in Law 2/2023.

The Crime Prevention Programme is conceived as a framework comprising regulations, procedures and other specific controls that make it possible to reasonably ensure that the risks of committing crimes affecting the Group's companies in Spain are appropriately

identified, documented, assessed, controlled and mitigated, in an environment of permanent review and updating.

The Programme is based on the creation and continuous reinforcement of the Compliance culture, which is based on the Responsible Business Principles that form the core values of the Group, fostering ethical and responsible conduct in the organisation.

Within the framework of said Crime Prevention Programme, it is important to highlight the need to maintain and continuously improve the Programme and, where appropriate, the associated management system, which guarantees the definition of crime prevention objectives, including, where appropriate, the specific objectives of the criminal compliance management system, the identification and implementation of the actions necessary to achieve them and the review of the effectiveness of said actions and objectives on a regular basis, in accordance with the provisions of this policy.

3. Scope of Application

This Policy is applicable to all Telefónica Group companies in Spain in which it has a direct or indirect majority shareholding and in all other companies in which, although the shareholding is lower, it has effective control over management.

As the Group's parent company, Telefónica S.A. is responsible for laying down the guidelines necessary for appropriate and efficient coordination between this Company and the other companies which make up its Group; all without prejudice or detriment to the autonomous decision-making capacity of each of these companies, in accordance with the corporate interests of each one, and with the fiduciary duties that the members of their management bodies perform for all their shareholders.

4. Crime Prevention Programme

The Crime Prevention Programme is composed of:

- The **general control environment** in place in Telefónica Group companies
- The **criminal risk registers** in which the **risks** of committing criminal offences affecting the Group companies are recorded, as well as the **controls** in place to minimise their exposure to such offences
- The set of internal **rules and regulations** referred to in point 4.3 which, in view of their relevance to this Programme, are attached as annexes to this Policy.
- **The processes**, which implement and develop in practice the provisions of the regulations, and which include controls that mitigate the identified risks, and which aim to ensure compliance with internal regulations and policies.

– The **disciplinary system** in place, where applicable, in the applicable collective bargaining agreements and, in general, in the Corporate Policy on the Comprehensive Disciplinary Programme and in the Corporate Regulation for the preparation and organisation of the regulatory framework in order to ensure compliance by all employees with the rules and processes in place in the Group companies.

– The existence of a **Crime Prevention Function**, at corporate level and in each of the companies concerned, with responsibility for its implementation, development, compliance and continuous review and improvement.

The existence of an Internal Reporting System (which includes the whistleblowing channel) compliant with Law 2/2023 of 20 February, regulating the protection of persons who report breaches of regulations and the fight against corruption, through which directors, executives and employees must report confidentially and/or anonymously any indication that a crime has been committed. The complaints channel is available to third parties on Telefónica's corporate website (www.telefonica.com) and those Spanish companies that have a website.

– The **protection of the informant**, in accordance with the timely and continuous monitoring of the regulations provided for in Law 2/2023.

– **Training and information** for all employees of Telefónica Group companies in Spain in relation to compliance with the internal regulatory regime (including training on crime prevention, which in particular is the subject of this Policy).

4.1 The general control environment

Beyond the specific crime prevention, it is necessary to refer to the control environment which, in general, Telefónica S.A. and the other companies in its Group possess and which forms part of its corporate governance structure. This environment is largely determined by the fact that, at the date of approval of this Policy, Telefónica, S.A. is listed in several markets (Spain, the United States and Peru), which means that the Group is subject to the strict control requirements established by the law of all three countries.

Thus, firstly, the Board of Directors of Telefónica, S.A. has among its responsibilities, the creation, maintenance and supervision of this general control environment.

The key elements of this control environment are, inter alia, the following::

a) Committees of the Board of Directors:

The Committees of the Board of Directors are vested with specific powers in matters of control; in particular, in relation to the following:

(i) The Audit and Control Committee, with specific responsibilities in this area, and with direct responsibility, inter alia, for supervising the effectiveness of the Company's internal control, internal audit and risk management systems, including tax risks.

(ii) The Appointments, Remunerations and Corporate Governance Committee, which has, among other duties, the supervision of compliance with corporate governance policies and rules, as well as with the Company's internal codes of conduct in force from time to time, it also ensures that the corporate culture is aligned with its purpose and values.

(iii) The Sustainability and Regulation Committee, whose main function is to carry out, through study, analysis and discussion, the permanent monitoring of the main sustainability and regulatory issues affecting the Group at any given time, including the supervision and review of the strategies and policies derived from the Responsible Business Principles.

b) Specific organisational units:

(i) Independent Compliance Unit, which reports directly to the Board of Directors through the Audit and Control Committee, responsible for generating and reinforcing a general culture of compliance with regulations (both legal and Telefónica's internal regulations) by all Group employees.

(ii) Internal Audit Unit, which reports directly to the Board of Directors through the Audit and Control Committee, which independently supervises the Group's internal control structures in accordance with its Work Plan and functions.

(iii) Global Sustainability Department, which, among other responsibilities, manages the opportunities linked to the impact of the services provided by Telefónica, S.A. and the other companies in its Group on society, and the "Stakeholder engagement".

(iv) Other corporate units that control specific compliance risks related to, among others, insurance, regulatory, privacy, competition, environmental, supply chain, commercial, tax, capital markets and finance, securities or other legal risks, security and systems, and labour relations.

c) Risk management model:

Risk Management is an essential internal control instrument for Telefónica, S.A. and the other companies in its Group, which enables them to identify and manage risks. The Telefónica Group has a Risk Management Policy to regulate this essential instrument of internal control, whose basic principles are as follows:

(i) Train and involve employees in the Risk Management culture, encouraging them to identify risks and actively participate in their mitigation.

(ii) Systematise and structure the risk management activities and processes in a methodical way in the organisation.

(iii) Facilitate the identification, assessment (in terms of impact and likelihood of occurrence), reporting and management of the following risk categories: Business, Operational, Financial and Legal, and Compliance.

This Policy establishes the principles for the identification, assessment, management and reporting of risks that could affect the achievement of the Group's main objectives and strategy, as well as those of its component companies.

The Corporate Risk Management Model is based on the COSO framework (Committee of Sponsoring Organisations of the Treadway Commission) and aligned with international best practices.

To support the development of risk management supervision activities by the Audit and Control Committee, a risk management function has been established within the Internal Audit department, independent of management, to promote, support, coordinate and verify the application of the provisions of the Risk Management Policy, both at Group level and in its main operations.

d) Internal regulation:

Within the control environment described above, the set of internal regulations that Telefónica, S.A. and the other companies in its Group have and through which their operations are organised is of particular importance. This general regulatory framework, as well as the specific rules of relevance within the Crime Prevention Programme, are described in detail in section 4.3 below. The organisation and production of regulations is governed by the provisions of the Corporate Regulations on the preparation and organisation of Internal Regulations and other Organisational Documents. The Compliance department carries out the function of coordination and review of the consistency of the Telefónica Group's internal Regulatory Framework through encouraging the development and supervision of standards, simultaneously promoting actions that promote the updating and communication of said standards, always in line with the provisions set out in the Telefónica regulatory framework's organisation and preparation regulations.

e) Complaints Channel:

At Telefónica, we have an Internal Information System to promote compliance in the Group with the provisions of the Principles for Responsible Business, the law and other applicable internal regulations by employees, executives, directors of Group companies and other stakeholders, which has the appropriate mechanisms to guarantee confidentiality and, where appropriate, anonymity of the communications and reports sent through it, as well as due protection for the informant, the reported party and the other persons involved in the communication of any conduct that may come within its scope of application.

The Whistleblowing Channel forms an integral part of Telefónica's Internal Information System and is the preferred mechanism that Telefónica makes available to all employees, managers and directors of Group companies and third parties related to them and, in particular, to suppliers and contractors, shareholders, volunteers, interns

and workers in training periods so that they can report any information related to any Group company that may involve.

(i) a possible irregularity or act contrary to the Principles for Responsible Business or any other applicable internal regulation;

(ii) a potential irregularity relating to accounting, auditing matters and/or internal control over financial reporting matters referred to in the Sarbanes-Oxley Act of the United States of America and other regulations applicable to such matters; or

(iii) a possible irregularity or unlawful act, including conduct that may constitute a serious or very serious criminal or administrative offence, as well as an infringement of European Union law, in relation to activities subject to European Union law.

f) Specific controls over the financial and accounting reporting process:

Telefónica Group companies have a specific internal control system over financial and accounting information, which, in accordance with Spanish and US legal requirements, is assessed annually by Internal Audit, for the purposes of the internal control system over the Telefónica Group's consolidated financial information, in order to detect any deficiencies or weaknesses that may exist; this assessment is also validated by the external auditor in their report.

g) Specific controls over non-financial processes:

In addition, Telefónica Group companies have a series of non-financial controls that form part of their internal control environment.

In relation to non-financial information, the Telefónica Group publicly reports sustainability information in accordance with current legislation, for which the external verifier issues an independent review report.

h) Regular training and information:

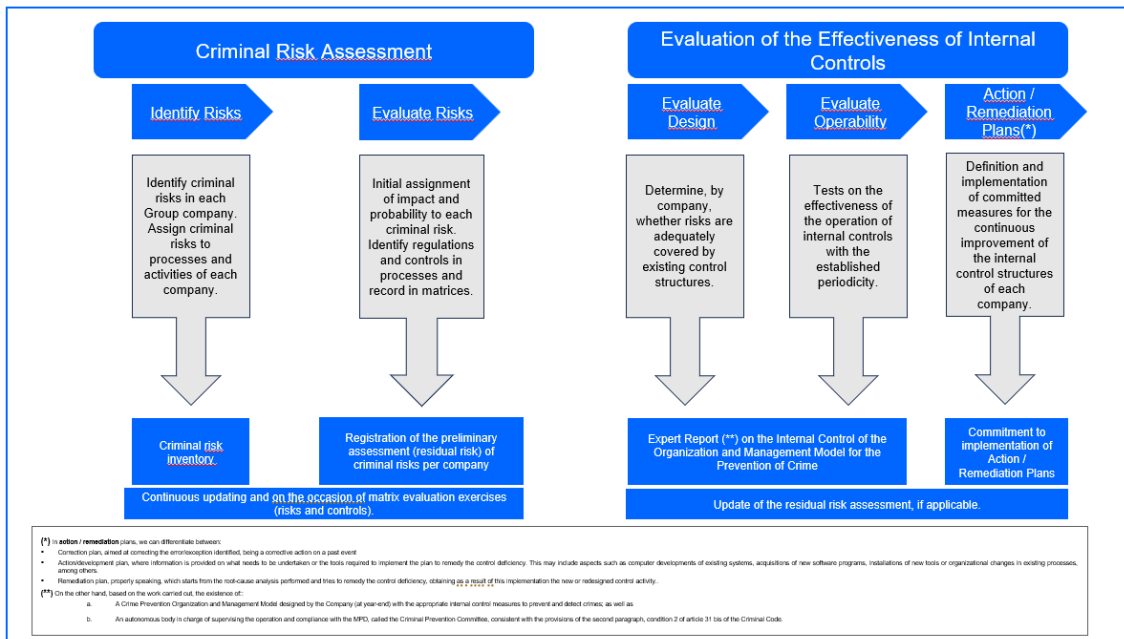
It is carried out in the context of a permanent awareness-raising activity (information through ad hoc communications, publication on websites, specific training, etc.) aimed at all employees, and which deals with Telefónica's regulatory environment and its implications. It includes training and information specifically related to Crime Prevention, which is the subject of this Policy.

4.2 The criminal risk register: identifying and assessing risks

On the occasion of the entry into force of the criminal law reform, Telefónica and the various Group companies domiciled in Spain set in motion a process to identify the

criminal risks that could affect the Group, setting up a register of criminal risks that has been updated on an ongoing basis. The ‘criminal risk register’ means the written record, after detailed analysis, of the possible criminal contingencies that may affect the various legal entities of the Telefónica Group in Spain, with specific identification and assessment of the existing risk. In particular, the controls in place in the various Telefónica Group companies in Spain to mitigate these risks have been identified and the effectiveness of these controls has been audited periodically.

The criminal risk register has been developed according to the following outline:



Within the framework of the activities envisaged in the Telefónica Group's Risk Management Policy, the criminal risk register is not a static register; on the contrary, the Telefónica Group companies in Spain keep these registers periodically updated so that they are, at all times, a true reflection of the possible criminal contingencies they face and, in accordance with which, and with a preventive purpose, the control mechanisms described in this Policy have been established.

4.3 Internal regulations

As indicated in section 4.1 above, Telefónica Group companies have a complete set of internal regulations integrated into their corporate governance structure, which defines the internal control system. These regulations, and the control system established by them, go beyond the minimum measures required from a crime prevention point of view.

Compliance with internal regulations is required of all employees of Telefónica Group companies, without exception.

As a fundamental rule, and the basis of all existing regulations, Telefónica, S.A. and the other companies in its Group have a code of ethics known as the Responsible Business Principles, the monitoring, control and implementation of which is the responsibility of the [corporate Responsible Business Principles Office]. The Principles of Responsible Business group together a set of guidelines or directives that should guide and orient the employees of the Group's companies in their daily work, both in their decision-making and conduct, and in the way in which they interact with customers, suppliers, shareholders, employees and society in general. This code of ethics was established in December 2006 to be applied in all countries in which the Telefónica Group operates. The Responsible Business Principles, last updated in June 2022, together with the values, vision and behaviour of Telefónica Group companies, make up its corporate culture.

In addition, a series of internal regulations have been established, as well as organisational documents that define the internal control environment of Telefónica Group companies and through which: (i) it establishes the organisational structure and internal functioning, as well as the minimum criteria for decision-making and governance of the Telefónica Group, (ii) it regulates the procurement of goods and services, reception, invoicing and payments, (iii) it establishes the general provisions on comprehensive security in the Group, (iv) it develops the principles of integrity commitment and transparency in operations, principles established at a programmatic level in the Principles of Responsible Business of the Group's companies, guaranteeing their practical compliance, (v) general criteria are established on the preparation and reporting of information and its review by the external auditor and (vi) the criteria to be followed by employees for the development of the working environment are established.

In this way, and analysing at a specific level the criminal risks included in the aforementioned registers, the internal regulations of Telefónica, S.A. applicable to the other companies in its Group cover the following criminal risks, grouped for this analysis on the basis of the legal assets affected:

a) General protective framework

Telefónica Group companies have a regulatory framework with a suitable procedure for managing complaints through the Internal Information System. Specifically, these regulations are composed of:

- Internal Information System Management Policy and Procedure.

There are specific regulations regarding the framework of powers of attorney for employees of Telefónica Group companies, as well as control of the different responsibilities within the Group, delimited in their hierarchical and control relationships, and the delegation of responsibilities, where permitted, among others:

- Corporate Regulations for the Preparation and Organisation of Internal Regulations and other Organisational Documents.
- Telefónica Group Corporate Internal Control Policy.
- Statute and regulations for the implementation of the compliance function.

- Internal Audit Organisation Policy
- Corporate Operation Regulations with centralised decision-making (NCC-001).
- Executive Proxy Circular (SGYC- 002).
- Payment Control Regulations (NCC-002).
- Corporate Regulation for Procurement of Goods and Services (NCC-003).
- Regulation of operations in companies with little structure, or in special situations (NCC-010).

In addition, there is a Risk Management Policy, which establishes the basic principles that guide the Telefónica Group's general risk management activities.

b) Right to privacy, secrecy of communications and data protection

Telefónica Group companies have regulations on privacy and protection of personal data, privacy, protected files, guarantees against - among others - the crime of discovery and disclosure of secrets, etc. (art. 197 PC and related); protection against computer damage of any kind including inaccessibility, alteration, etc. (art. 264 PC and concordant); protection against credit card abuse, alteration, copying, reproduction, etc. (art. 399 bis PC and concordant); protection against the seizure of data and discovery of company secrets, dissemination of company secrets (arts. 278, 279, 280 PC and similar articles); among other regulations:

- Global Security Policy.
- Global Security Regulation.
- [Instruction on Personal Data Security Measures].
- Global Privacy Policy.
- Regulations of the Governance Model for the Protection of Personal Data.
- Social Networking Regulations.
- Information Classification and Processing Regulations
- Security Incident Management Regulations
- Business Continuity Regulations
- Global Security Risk Analysis Regulations
- Cybersecurity Regulations
- Supply Chain Security Regulations.

c) Capital Markets Telefónica Group companies have regulations on guarantees of accurate economic-financial information in the prospectuses (art. 282 bis PC and similar articles), protection against abuse of privileged information (art. 285 CC

and similar articles), protection against obstruction of inspection or supervisory activity (art. 294 CC), as well as against the alteration of prices by means of rumours, false news, or abuse of information to secure a dominant position in the market, etc. (art. 284.2 and 3 CC and other similar provisions); among other regulations:

- Regulations on disclosing information to markets.
- Regulations on Recording, Reporting and Control of Financial and Sustainability Information (NCC-005).
- Single Treasury System and Credits through Telfisa Regulations (NCC-004).
- Intragroup operations regulations (NCC-006).
- Regulation on the investment process, the management of fix assets and divestments (NCC-009).
- Regulations for operations in companies with little structure, or in special situations (NCC-010).
- Internal code of conduct regulations in matters relating to securities markets.

There is also an Accounting Policies Manual based on IFRS (the International Financial Reporting Standards), whose aim is to homogenise and establish standards of compliance with accounting regulations, as well as Instructions for the closing and auditing of the consolidated annual accounts for each financial year. There is also a Consolidation Reporting Manual, which is updated periodically, and which enables the consolidated accounting information to be standardised..

d) Anti-fraud and anti-corruption in the broad sense, as well as the crime of illegal financing of political parties

Telefónica Group companies are protected, among others, against the crime of frustration of execution (art. 257 et seq.), against intellectual or industrial property fraud (arts. 270 et seq.), corruption in business dealings (art. 286 bis and quarter CC and similar articles), as well as corruption of officials, bribery or influence peddling (arts. 424 et seq., 427, 429, 430 CC and other similar articles), at national level and in international commercial transactions (art. 427 CC and other similar articles); also protection against the offence of embezzlement of public funds (art. 432 and similar articles); protection against the offence of fraud (art. 248, 249, 250, 251, 251 bis PC and other similar provisions), against the crime of price manipulation (art. 284.1 PC and other similar provisions) or possible manipulation in the supply of raw materials or basic necessities (art. 281 CC and other similar provisions); protection against the crime of corruption or urban or regional planning prevarication (art. 319 CC and other similar provisions); likewise, guarantees against money laundering (art. 301 CC and other similar provisions) and against the crime of illegal financing of political parties (art. 304 bis CC); among other regulations:

- Regulations on the approval of sponsorship and patronage (NCC-012).
- Regulations on travel and representation expenses (NCC-007).

- Anti-Corruption Policy.
- Regulations on the certification of executives regarding anti-corruption.
- Relationship with public entities regulations.
- Procurement regulations in relation to Public Entities.
- Corporate Regulations on Conflicts of Interest.
- Corporate Regulation for Procurement of Goods and Services (NCC-003).
- Payment Control Corporate Regulations (NCC-002).
- Single treasury system and credits through Telfisa Corporate Regulations (NCC-004).
- Regulation on Recording, Reporting and Control of Financial and Sustainability Information (NCC-005).
- Intragroup Operations Regulations (NCC-006)
- Regulation on the investment process, the management of fix assets and divestments (NCC-009).
- Regulation of operations in companies with little structure, or in special situations (NCC-010).
- Performance and transparency protocol in resource management.

e) Environment

Telefónica Group companies have regulations on protection against environmental damage in a broad sense (arts. 325, 326, 327, 328 CC and concordant), including protection against the emission of ionising radiation (art. 343 CC and other similar articles); among other regulations:

- Global Environmental and Energy Policy.
- Environmental Management System Manual.
- Sustainability in the Supply Chain Policy.

f) Crimes against persons, against the rights of workers, nationals and foreign nationals, and of harassment at work and sexual harassment

Telefónica Group companies have regulations on protection against illegal exploitation of people, against the rights of workers, in the broadest sense, national or foreign nationals, and against harassment in the workplace and sexual harassment (arts. 173, 177 bis, 184 and other similar provisions); it comprises, among other regulations:

- Equality Policy.
- Human Rights Global Policy.

- Diversity and Inclusion Policy.
- Sustainability in the Supply Chain Policy.
- Diversity and Board Members Selection Policy
- Occupational Health, Safety and Well-Being Policy
- Policy for the recruitment of former Telefónica Group Directors and Employees
- Regulations for the formalisation of contracts with former directors and former managers
- Local and International Procurement Regulations
- Occupational hazards in the procurement of works and services Instruction (ICC-001).
- Protocol for handling workplace or moral harassment, sexual harassment and discrimination
- Protocol for action in situations of sexual and gender-based harassment.

g) Protection against misleading advertising

Telefónica Group companies have regulations on protection against misleading advertising (art. 282 CP and other similar provisions), the most important of which are the following:

- Telefónica Group Responsible Communications Policy.

h) Protection against the use of the companies' media and against the incitement of discrimination, hatred or violence against persons

Telefónica Group companies have regulations on protection against the use of the companies' technical means and media against any type of sexual or pornographic offences involving minors (art. 189 bis CC and other related articles), and against the provocation of discrimination, hatred or violence against people (arts. 510 et seq. CC); in addition to the regulations already cited in part, it consists of, among other regulations, the following:

- Policy on the acceptable use of internet services.
- Equality Policy
- Telefónica Group Responsible Communications Policy.

i) Protection against tax risks

Telefónica Group companies have regulations on protection against tax risks (arts. 305 et seq., 310 bis CC and other similar provisions), among others, in particular:

- Tax control corporate policy.

- Regulations on Disclosing Information to the Markets.
- Payment Control Corporate Regulations (NCC-002).
- Corporate Regulation for Procurement of Goods and Services (NCC-003).
- Regulations for joining the single treasury system and applying for credits through Telfisa (NCC-004).
- Corporate regulations on the recording, communication and control of financial and sustainability information of Telefónica Group companies (NCC-005).
- Intra-group operations regulations (NCC-006).
- Regulation on the investment process, the management of fix assets and divestments (NCC-009).
- Regulation of operations in companies with little structure, or in special situations (NCC-010).

j) Protection against consumer fraud through the fraudulent use of automatic devices or fraud in the provision of communications

In this area, there are numerous processes in the area of Telefónica España aimed at protecting consumers in the provision of telecommunication services provided by Telefónica in its capacity as a communications carrier (Articles 283 CC and other similar articles, and Articles 286 PC and other similar articles, Article 162 CC). The main processes that can be considered relevant for this purpose are the following: (i) management and use of IT systems; (ii) staff obligations in the use of IT tools; (iii) security for systems development; (iv) fraud control caused by sending unsolicited messages (spam); (v) plant and service monitoring.

k) Other offences

The zero tolerance environment created and, among others, the Responsible Business Principles that apply to other criminal offences, which are also outlawed even though, due to their nature and in the context of Telefónica, and except in exceptional cases, it is very unlikely that they could occur, being considered as residual. Among these offences are those relating to trafficking in human organs (art. 156 bis CC and other similar articles), genetic manipulation (arts. 159 et seq. CC), to trafficking in human beings (art. 177 bis CC), to the promotion of prostitution, sexual exploitation or corruption of minors (arts. 187 et seq. CC), punishable insolvencies (art. 259 et seq. CC, offences against the rights of foreign citizens (art. 318 bis), offences against animals (art. 340 bis et seq. CC), risks caused by explosives and other agents (art. 348 CC), drug trafficking and against public health (arts. 359, following and other similar articles of the CC), counterfeiting currency (art. 386 CP), nor, finally, the crimes of terrorism (art. 570 quater, 576 CC and other similar articles), terrorist organisations and groups (art. 572 and other similar articles) and smuggling (art. 2 of the Law for the repression of smuggling), since, we reiterate, these are risks far removed from the sphere of action of the Telefónica

Group companies. However, for all of them, the Code of Ethics called Responsible Business Principles applies as a general preventive system.

4.4 The processes

The internal processes established in the different companies that make up the Telefónica Group in Spain establish controls to mitigate the criminal risks that could affect Telefónica Group companies, always taking into account the requirements established in current legislation.

Telefónica Group companies have their main business and support processes duly documented and updated, with specific units responsible for maintaining these descriptive processes.

In addition, it is necessary to point out that these processes are, for the most part, supported by computer systems and applications that facilitate the control of the different areas.

4.5 Communication and training

All employees of Telefónica Group companies have a legal obligation to know and comply with the internal regulatory system, depending on their position and responsibility.

Likewise, everyone must collaborate in its most effective implementation and compliance, which includes the obligation to report any potentially improper fact or conduct through the Whistleblower Channel.

To this end, Telefónica Group companies will carry out the relevant information and continuous training work for all staff.

4.6 Disciplinary regime

In accordance with the corporate regulations on the drawing up and organisation of the Internal Regulations and other Organisational Documents, and, within their scope, the Organisational Documents that comprise the Regulatory Framework of the Telefónica Group are mandatory for all Group employees, each of which is applicable within the scope of their respective roles and responsibilities.

In this context, the Telefónica Group has a Corporate Policy regarding the Comprehensive Disciplinary Regime, applicable to all Group employees, which defines the basic principles of the disciplinary system of the Group. This Policy establishes that breaches of the Internal Regulations are considered breaches of terms and conditions of employment which may be penalised in accordance with the specific provisions of said legislation and the Internal Regulations that may be applicable. In the case of the

Organisational Documents, compliance with them shall apply to those employees to whom they are applicable. Depending on the circumstances, a breach thereof may be classified as an employment offence and subject to appropriate penalties.

This policy, which is on a de minimis basis, establishes the disciplinary system applicable to all Telefónica Group employees, without prejudice to the provisions of any applicable laws and regulations, collective bargaining agreements, collective covenants or similar agreements, as well as any criminal and labour legislation that may be applicable.

In addition, Telefónica has a corporate Disciplinary Action Committee, which is the body responsible for ensuring the effective development of this Policy at a global level.

The disciplinary regime associated with the Crime Prevention Programme will be that resulting from the application of the Corporate Policy on the Comprehensive Disciplinary Programme. With regard to conduct that may eventually give rise to criminal liability of natural persons and, by derivation, of the legal persons to which they are linked, the sanctioning regime shall be that corresponding to offences or misdemeanours classified as very serious, with the additional consequences that may apply in terms of disciplinary actions.

Furthermore, the disciplinary regime is applicable not only to the direct perpetrators of the conduct involving non-compliance, but also to those persons who induce, cooperate with, or in any way assist them, as well as those who, having evidence or knowledge of any breach, contribute to preventing or hindering its discovery (including, where appropriate, through conduct involving reprisals against whistleblowers), fail to report them or do nothing to prevent them. Disciplinary action may also be taken against any employee who, intentionally and in bad faith, make a false accusation or report with the intention of harming another person.

Finally, and without prejudice to the foregoing, Telefónica has a zero tolerance towards penalties or any type of retaliatory measure against whistleblowers who report any impropriety, in strict compliance with Law 2/2023, on the Protection of the Informant.

5. Crime Prevention Function

The Crime Prevention Function is carried out by the Compliance Unit (Compliance), which, in collaboration with the Internal Audit Directorate and the Legal Services Directorate, carries out the functions related to the design, documentation, updating and monitoring of Telefónica's Crime Prevention Programme. To carry out the Crime Prevention Function, a Crime Prevention Committee has been set up, which will include managers from the Compliance Department, the Internal Audit Department and the Corporate Legal Services Department, each within the scope of their respective responsibilities.

This Crime Prevention Committee meets as often as necessary for the proper operation of the Programme, and at least quarterly, except in circumstances that make such quarterly meetings impossible due to force majeure or unforeseen circumstances, in which case, such meetings shall in any case reach the number of four in the financial year of the calendar year. Telefónica Group companies to which this Policy applies may

choose to have their own specific crime prevention committee after consultation with the Crime Prevention Committee.

The Crime Prevention Function has, in relation to each company or business unit, among others, the following powers:

- a) Supervise the operation, implementation, development, compliance and communication of the Crime Prevention Programme.
- b) Promote and coordinate the review and update and improvement of the Crime Prevention Programme, including updating the risk register. This review will be carried out on the basis of a model that establishes a variable review periodicity for each company depending on its volume and risk, as well as when regulatory changes or jurisprudential developments make it advisable.
- c) Define the objectives, scope and priorities of the evaluation model of the Crime Prevention Programme and, where appropriate, of the criminal compliance management system that may exist and monitor them.
- d) Propose the necessary changes or updates to the Crime Prevention Programme, and in particular, the improvements that should be undertaken in view of the conclusions reached in previous reviews, as well as any breaches that have been detected through the continuous monitoring of the Model.
- e) To receive all suggestions made in relation to the Crime Prevention Programme, as well as to process these suggestions so that they are appropriately taken into account.
- f) To know, in as much detail as required, and to evaluate, the results of the tests carried out in the course of the Programme review.
- g) Be aware of and follow up on internal investigations into suspicious actions, situations or events that may arise in relation to these tests and controls or, in general, to the implementation of the Programme, insofar as the implementing procedures so provide.
- h) Be aware of and follow up on cases in which a judicial body may initiate legal proceedings affecting the company to which the Programme refers, regardless of whether or not it has been identified as an area of risk or improvement, or whether or not the corresponding internal investigation has been opened.
- i) In general, to promote and supervise the remediation of control deficiencies, where appropriate, as well as the implementation, monitoring and review of the recommendations for improvement of the Programme that may have been identified or formulated, either as a result of the audit referred to in the following section, or as a result of any other matter agreed in the Crime Prevention Committee.
- j) Ensure the protection of those persons, whether members of Telefónica or not, who report irregularities through the whistleblowing channels provided, preventing the adoption of any type of reprisal, insofar as the complaints are within the scope of the Committee's analysis in accordance with the development procedures.

k) Report regularly to the Audit and Control Committee of Telefónica, S.A. on the operation of the Programme, including any breaches or material incidents detected, as well as the action plan or measures adopted to resolve them.

6. Audit of the Operation of the Programme

The operation of the Crime Prevention Programme shall be audited as often as necessary in view of the circumstances of each company, although its appropriateness shall be considered especially on the occasion of:

- i) Changes in the organisation or control structure.
- ii) Changes in the activity carried out by the company which could eventually result in a necessary extension of the scope of control.
- iii) Amendments to the Criminal Code or its interpretation in case law in areas affecting the company's business.
- iv) Any other objective circumstances that may substantially alter the company's risk profile.

7. Entry into force

This Policy will enter into force on the day of its approval by the Board of Directors.



www.telefonica.com