Leading by example

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

8 DECENT WORK AND ECONOMIC GROWTH

5 GENDER EQUALITY

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

17 PARTNERSHIPS FOR THE GOALS

2.16. Governance and culture of sustainability

GRI 2-24

KEY POINTS

- ☆ In 2022, 91,347 employees received training in our Responsible Business Principles, Telefonica's code of ethics, based on integrity, transparency and commitment.
- ☆ Our Responsible Business Plan is approved and monitored at the highest level and on a regular basis. It translates our code of ethics into targets and KPIs, which are then incorporated into the Company's strategic plan.
- ☆ We ensure sustainability is part of our culture by integrating the pillars of ESG within our businesses, our processes, our variable remuneration and via training and awareness-raising initiatives for our employees.

2.16.1. Governance

GRI 2-9, 2-12, 2-13, 2-14, 2-16, 2-23

The Telefónica Group has a code of ethics and conduct: our Responsible Business Principles. The Principles form part of our sustainability policy as they help guide us to act with integrity, commitment and transparency.

To ensure that our Responsible Business Principles are the common thread guiding everything we do, we de have a **Responsible Business Plan**. This includes targets and projects in the key areas of our strategy's three pillars: leading by example, helping society thrive and building a greener future.

The priorities of the Responsible Business Plan form part of the **Company's Strategic Plan**, which contains the non-financial indicators that we cover in this Report. Some of the targets are also incorporated into the variable remuneration of all employees, including members of the Executive Committee.

For further information, see chapter 1.5. Strategy

The main governing bodies for sustainability are as follows:

Approval	Board of Directors
Supervision	Sustainability and Quality Committee Audit and Control Committee Nominating, Compensation and Corporate Governance Committee
Follow-Up	Responsible Business Office Due Diligence Office Energy and Climate Change Office
Implementation	Corporate Business and Support Areas Country Operators

The **Board of Directors** approves the Responsible Business Principles, the Responsible Business Plan and the most important ESG policies (anti-corruption, environmental management, privacy, diversity, equality and sustainable management of the supply chain). This forms our ethical and responsible business framework and the roadmap for all employees, which is complemented by training and awareness-raising.

For further information, see chapter 4.4. The organisational structure of the Administrative Bodies

The **Sustainability and Quality Committee** oversees the implementation of the Responsible Business Plan at its monthly meetings. In addition, the **Audit and Control Committee** has an additional role in sustainability, as it oversees certain aspects related to non-financial information such as regulatory compliance, the risk analysis and management process, and the Company's reporting processes. On the other hand, the **Nominating, Compensation and Corporate Governance Committee** oversees the variable compensation system.

The **Responsible Business Office**, which brings together four times a year the heads of the areas of Global Sustainability, Compliance & DPO, Internal Audit, General Secretariat, Human Resources, Communication, Security, Procurement, Data & Analytics, Global Consumer, Technology and Information, Legal Services, Strategy, Finance, Telefónica Foundation, Telefónica Tech and Telefónica Infra, among other functions, monitors the Responsible Business Plan. This Office reports to the **Sustainability and Quality Committee** through the Global Sustainability Officer.

There are two bodies under the Responsible Business Office, the **Due Diligence Office**, responsible, among other activities, for monitoring Telefónica's sustainability due diligence process, and the **Energy and Climate Change Office**, responsible for monitoring the implementation of the Climate Action Plan, among others.

The Corporate Business and Support Areas and the Country Operators' executive committees are responsible for implementing the targets of the Responsible Business Plan.

2.16.2. Telefónica Group's main policies and regulations related to sustainability

Ethics

- Global Anti-Corruption Policy.
- Policy on Compliance Function (new).
- Rule on Compliance Function (new).
- Crime Prevention Policy.
- Internal Rules of Conduct.
- Regulation on the Prevention and Management of Fraud in Telecommunications.
- Regulations on Relations with Public Entities.
- Complaints Channel Management Policy.
- Corporate Policy on the Comprehensive Discipline Programme.
- Fiscal Control Policy.
- Policy on Risk Management.
- Policy on Competition Law (new).
- Regulation on Sanctions (new).

Supply chain

- Policy on Supply Chain Sustainability.
- Regulation on Supply Chain Sustainability.
- Global rule on security in the supply chain.
- Low Carbon Procurement Instruction.
- Procurement of Goods and Services Regulations.

Privacy and freedom of expression

- Global Privacy Policy.
- Personal Data Protection Governance Model Regulations.
- Regulations on Requests from Competent Authorities in Security (new).
- Global Security Policy

Human capital	Human rights	Responsible communication	Environmental management and climate change
• Protocol for Action in Situations of Workplace or Moral Harassment, Sexual Harassment and Discrimination • Regulation on Occupational Health, Safety and Well-being • Diversity and Inclusion Policy • Equality Policy (new) • Diversity Policy in relation to the Board of Directors and Selection of Directors • Remuneration Policy of the Directors of Telefónica, S.A.. • Regulation on Telefónica Group Reinstatement of Former Managers and Former Employees	• Global Human Rights Policy • Principles of Artificial Intelligence	• Market Disclosure Regulations • Shareholder Communication Policy • Responsible Communication Regulations • Social Media Regulations	• Global Environmental Policy • Energy Management Policy

COVERAGE OF POLICIES AND REGULATIONS: The main policies and regulations indicated above are applicable to Telefónica Group companies within the scope of consolidation.

For further information, see Appendix I: Scope of consolidation.

2.16.3. Culture aligned with ethical and sustainable management

Beyond ensuring ethical behaviour and responsible business management, we aim to make sustainability a **cornerstone of our culture**. In doing so, we seek to align behaviours, processes and targets with the Company's purpose and values.

We are guided by our Responsible Business Principles, which are developed across 10 areas:

1. Ethical and responsible management.

2. Corporate governance and internal control.

3. Respect for and promotion of human and digital rights.

4. Our commitment to the environment.

5. Innovation, development and responsible use of technology.

6. Responsible communication.

7. Our commitment to our customers.

8. Our commitment to our employees.

9. Our commitment to the societies in which we operate.

10. Responsible supply chain management.

To align **internal culture with ESG** (Environmental, Social and Governance) **factors**, we demonstrate their long-term business value. In fact, we ensure **that every internal process or activity is in line with this vision.** Moving the organisational culture forward and embedding a commitment to sustainability is a long-term task that requires shared vision and commitment at every level of the organisation.

We would like to highlight several lines of work that show in a tangible way how the Group's management is 100% aligned with sustainability criteria:

Training and awareness raising: we continuously train our entire workforce (part-time and full-time employees) in Responsible Business Principles and Human Rights. The course is mandatory and is monitored by the Responsible Business Office. Completion of the course implies the employee's acceptance of the Principles. In the case of new employees, in addition to finding the Responsible Business Principles document in the welcome pack, they are required to take the specific course within a maximum period of three months from their incorporation. The course as well as the Responsible Business Principles are translated into English, German and Portuguese.

In addition, strategic training is given annually on key issues such as privacy, digital security, ethics and artificial intelligence, environmental management, accessibility and diversity, as well as on specific ethical and sustainability issues related to the design of our products and services, such as impact on human rights, ecodesign, accessible products and services, social impact and data ethics.

Training is reinforced by internal awareness-raising campaigns on conflicts of interest, gifts and invitations, responsible purchasing, environment, privacy, customer promise, etc.

- **Internal processes and activities:** our aim is for every employee to understand that sustainability is part of our daily activities. Sustainability is an element that brings value and differentiation to the different areas of the business. One example is the incorporation of ethical and sustainability aspects into product and service development processes.

For further information, see chapter 2.12. Responsibility in our products and services.

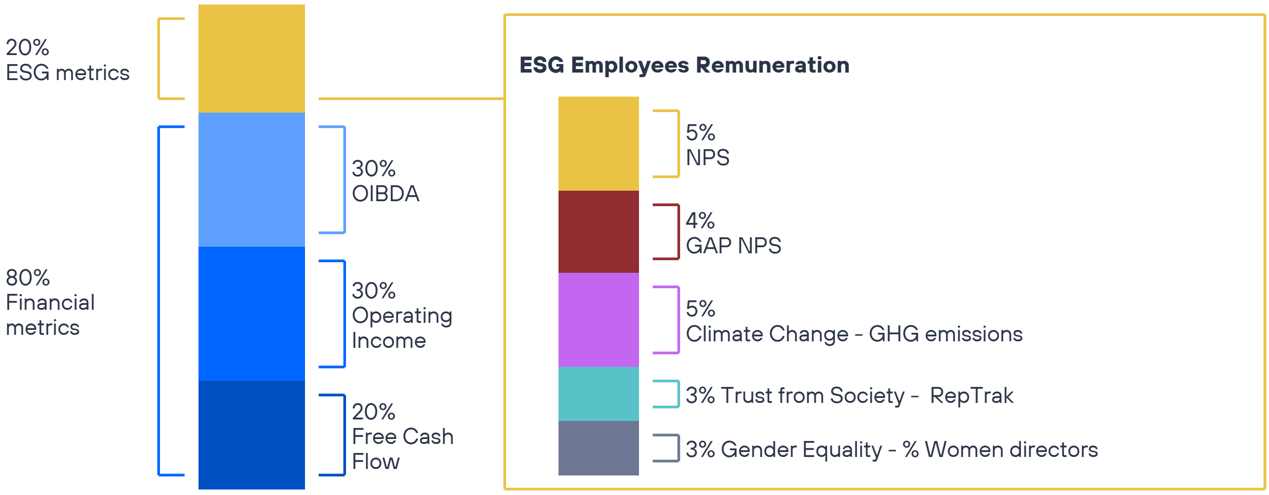
- **Alignment with business priorities:** we show business use cases with the benefits quantified in figures. An example would be Eco Smart services, digital solutions that help our customers reduce their impact on the environment, which is measurable.

For further information, see chapter 2.4. Digital solutions for the green transition.

- **Control processes and indicators:** we ensure the robustness of non-financial indicator control processes.
- **Remuneration scheme**: 20% of the performance appraisal (short-term variable remuneration) of our employees includes sustainability indicators. A further 10% relates to in long-term remuneration, applying to senior management.

For further information, see chapter 5.1. Annual Report on Remuneration.

Annual variable remuneration



Long term incentive (2021-2026)

50 %
Relative TSR

40 %
Free Cash Flow

10 %
Neutralising of CO_2 emissions (10%)

2.16.4. Progress

GRI 3-3

RBP training

In June, a new edition of the course was launched and assigned to all employees, incorporating the updates to the Responsible Business Principles implemented in 2021.

An extensive internal communication campaign was carried out and compliance was closely monitored.

In 2022, 91,347 employees received training, representing 89% of the average workforce[1] totalling 163,125 hours.

Training in Responsible Business and Human Rights through the Principles Course

Number of employees who received training on responsible business and human rights through the Principles Course	91,347
Percentage of employees who received training in responsible business and human rights through the Principles Course	89
Hours of training on responsible business and human rights through the Principles course	163,125

Other ESG training

We conducted various internal training sessions related to ESG issues:

Environment (E):

- Low carbon procurement: aimed at operations, procurement and sustainability teams to integrate internal carbon pricing into procurement in order to select more energy efficient equipment with lower associated CO_2 emissions.

For further information, see chapter 2.2. Energy and climate change

- Environmental management: internal training aimed at all Company personnel who have any duties related to the operation of the Environmental Management System, so that they can collaborate to manage environmental aspects and improve the organisation's performance.

For further information, see chapter 2.1. Responsibility towards the environment

- Climate change: training for marketing and communication teams as part of the Planet Pledge initiative.

For further information, see chapter 2.4. Digital solutions for the green transition

Society (S):

- Accessibility: guidelines and training sessions to ensure inclusive communication with our stakeholders.

For further information, see chapter 2.10. Digital inclusion

- Disability: workshops and courses for employees, leaders and Human Resources areas to ensure the successful integration of talent with disabilities.
- Diversity: awareness-raising initiatives on gender, LGBT+, racial and generational diversity.

For further information, see chapter 2.7. Diversity and inclusion

Governance (G):

- Ethics: in addition to the Responsible Business Principles course, anti-corruption training was provided.

For further information, see chapter 2.17. Ethics and compliance

MILESTONES

→ Formalisation of Due Diligence and Energy and Climate Change Offices.

→ 89% of employees received training through the Responsible Business Principles course in 2022.

→ New training courses on ESG issues.

[1] Including within the "average workforce" those employees newly hired in the last quarter, those on paid leave during the training period and those from newly acquired companies in the process of integration whose deadline for training has not yet ended.

2.17. Ethics and compliance

GRI 2-25

KEY POINTS

- We have zero tolerance for corruption and bribery.
- Training and awareness are key elements underpinning our culture of compliance. 94,840 employees received anti-corruption training in 2022.
- Our Concern and Whistleblowing Channel ensures that our stakeholders have the opportunity to share their concerns, complaints and/or claims anonymously or personally.

2.17.1. Vision

Our vision is to strengthen our **culture of ethics and compliance** by bolstering the standards of adherence to mandatory rules and maintaining best in class ethical and business practices.

2.17.2. Governance

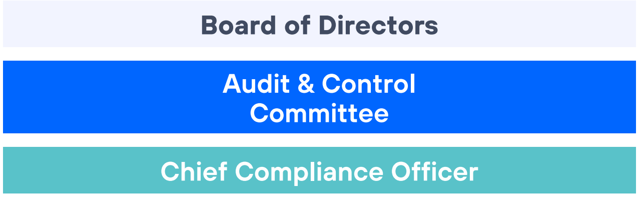
GRI 2-12

Our culture of ethics and compliance is **led** and driven by the **highest level of our Company** with a **firm commitment to zero tolerance of corruption and bribery**, and to other best business practices. We have clear lines regarding responsibility and the definition of key risks in this area.
The commitment of the Telefónica Group to fighting corruption and bribery, and to regulatory compliance in general, led the **Board of Directors of Telefónica, S.A. to approve** the creation of an **independent regulatory compliance area** on 16 December 2015, and subsequently the appointment of the **Chief Compliance Officer of the Telefónica Group;** this officer reports directly to the Board of Directors through the Audit and Control Committee.

The goal pursued was to continue to implement a compliance model at Telefónica in a much more targeted way, with due regard for all the activities performed up until that point by other areas of the Company in order to prevent corruption and bribery (for example: the internal audit, sustainability and legal areas). Both the appointment and the removal of the Chief Compliance Officer fall within the remit of the Board of Directors of Telefónica, S.A., at the proposal of the Audit and Control Committee and, where appropriate, of the rest of the competent bodies in this process.

The **Compliance Function** of the Telefónica Group **reports** directly to the **Board of Directors** through the **Audit and Control Committee**. Its purpose is to manage the preventive and reactive environments related to compliance with (a) legislation and (b) Telefónica's internal regulations, both at the Corporation and at a Operational level (countries and businesses) in general, while focusing specifically on those that are more sensitive according to the circumstances.

Governance of ethics and compliance


Board of Directors

Audit & Control Committee

Chief Compliance Officer

2.17.3. Policies

The internal regulations which implement the Responsible Business Principles, our code of ethics, with regard to integrity, ethics and compliance are listed below:

- Anti-Corruption Policy.
  - Regulations on Anti-Corruption Certifications for Management.
- Compliance Function Policy.
  - Compliance Function Charter.
  - Compliance Function Organisational Manual.
- Local crime prevention policies and regulations.
- Internal Code of Conduct for Securities Markets Issues.

- Regulations on Relations with Public Bodies.
- Regulations on Procurement Related to Public Bodies.
- Concern and Whistleblowing Channel Management Policy.
- Responsible Business Principles Channel Management Regulations.
- Corporate Policy on the Comprehensive Discipline Programme.
    - Disciplinary Action Committee Manual.
- Conflict of Interest Regulations.
- Rules on Sanctions.
- Competition Law Policy.

2.17.4. Risks and opportunities

One of our main challenges is to consolidate a culture of ethics and compliance designed to ensure the Company's future and sustainability, and contribute to guaranteeing the trust of all our stakeholders.

The nature of our business, **compliance with various national and extraterritorial regulations,** and the progressive demand for specific compliance programmes, represent a challenge to implementing this culture. Therefore, we must constantly adapt our compliance activity to the prevailing needs of each company or business unit.

We also foster training and awareness-raising initiatives, as a basic element of our compliance programme, in order to consolidate this culture so that our employees can adopt ethical and responsible decisions in the face of the dilemmas and conflicts they face during their daily activities.

2.17.5. Action plan and commitments

GRI 2-23

To ensure ethical behaviour throughout our Company, we take several lines of action: the Compliance Function, identification of non-compliance risks, policies and procedures, due diligence controls, training and awareness-raising, consultation, internal reporting mechanisms for potential infringements, discipline and recognition, as well as possible remediation plans.

Targets

- Develop and implement training on integrity and compliance for suppliers and other commercial partners.
- Continue training specific groups of employees within the Group on issues related to international economic sanctions.

2.17.5.1. Compliance

GRI 205-1, 205-2, 206-1

The Compliance Function Charter , approved by the Board of Directors, defines the main lines of Telefónica Group's Compliance Programme, its interaction with the Company's business processes and other areas, and the matters identified as particularly relevant. The starting point for compliance management is risk assessment and the protection of integrity.

The function of compliance, in accordance with the current Compliance Function Charter, is deployed on two levels:

- **Preventive control** in order to generate a culture of compliance. It involves training and awareness-raising activities on issues such as anti-corruption, criminal prevention and sanctions, as well as supporting other Company training. It also includes **continuous assessment** of compliance risk.

    It is also worth highlighting the **consultative activity** conducted through channels available to employees to make queries related to compliance issues (mainly related to the application of the Anti-Corruption Policy and other related internal regulations).

    We also develop compliance-based **protocols for assessing suppliers and business partners**, which are put into practice in a context of continuous improvement. These include the assessment protocols applied to corporate transactions (mergers and acquisitions), in which we assess anti-corruption aspects and the risks of money laundering and terrorist financing.

For further information, see chapter 2.20. Responsible supply chain management.

Finally, we must mention other activities, such as internal regulatory monitoring, the preventive control model, management of conflicts of interest, and criminal prevention.

- **Reaction and response** through action protocols for situations in which there is sufficient evidence of non-compliance. Response refers to the correction of the consequences through action: mitigating all the consequences associated with a possible breach, or a breach already evidenced, and ensuring the consistent application of the consequences for said breaches, as well as promoting the recognition of employees with outstanding behaviour in terms of their commitment to compliance.

In a dynamic prioritisation exercise, subject areas were identified in which compliance-based training is needed that extends beyond simply preserving integrity or international sanction regimes.

Compliance programme subjects

Integrity and sanctions	**Privacy and personal data protection**	**Relations with competitors**	**Security**
	Labour	**Sustainability, supply chain and human rights**	**Compliance with sector-specific regulations and customer promise**
	Tax	**Compliance with specific financial regulations - money laundering and terrorist financing**	**Regulated areas**[1]

This chapter features the following topics: (a) anti-corruption (integrity), (b) competition (relations with competitors) and (c) money laundering.

> Anti-corruption compliance

The Compliance area oversees and bases a large part of its policies, procedures and controls on **integrity**. It includes, among other initiatives, those that implement our fight against corruption and bribery.

With regard to the policies and procedures implemented in the Telefónica Group to combat corruption and bribery, it is worth highlighting, as a basis for the activities described above, the specific internal regulations in this area, the most significant being the Anti-Corruption Policy.

Among other aspects, the Anti-Corruption Policy sets out the guidelines on conduct which must be followed at Telefónica with regard to accepting or offering gifts or invitations and prohibiting any type of bribery; in the case of offering gifts or invitations to employees and public officials, this aspect is developed specifically by the Regulations on Relations with Public Bodies.

The regulatory framework on this subject is complemented by the Conflict of Interest Regulations[2] and the Corporate Policy on the Comprehensive Discipline Programme, among others.

As the parties responsible for establishing adequate controls and procedures to ensure compliance with the Anti-Corruption Policy, the Company's directors and executives certify their knowledge of and commitment to comply with the Responsible Business Principles and said policy on an annual basis, and with the associated policies, practices and regulations. In 2022, 100% of the executives signed the anti-corruption certificate.

Corruption risk analysis is another of the focus areas of Telefónica's Compliance Programme.

As part of the Risk Management Model, based on the guidance from the Committee of Sponsoring Organizations of the Treadway Commission (COSO), and which has been implemented homogeneously throughout the Group's main operations, senior Company management perform timely identification, assessment, response and monitoring of the compliance risk, within their scope of action. This includes the particularly important subject of integrity and encompasses the obligations associated with the Responsible Business Principles, in particular those relating to practices that prevent corruption. In 2022, the annual assessment of the aspects related to compliance risks and therefore with corruption risks covered the entirety (100%) of our operations.

[1] Regulated areas: this refers to compliance with legislation applicable to insurance and reinsurance companies, and pension fund and investment fund management companies.

[2] Telefónica's Conflict of Interest Regulations address situations in which an employee's personal interest (whether direct or indirect) influences or could influence – or creates the perception that it may influence – professional decisions to be made by that employee, where that personal interest or benefit may conflict with the interests of any of the companies belonging to the Telefónica Group. Our regulations make it a requirement to act at all times, and particularly in the case of a conflict of interest, in accordance with the corporate principles of loyalty, confidentiality and integrity.

	2022
Assessed operations based on risks related to corruption.	100%

For further information, see chapter 3. Risks.

The following Group companies are UNE 19601:2017 Criminal Compliance Management certified: Telefónica S.A. (obtained in 2021), Telefónica de España, S. A.U and Telefónica Móviles España, S.A.U. (both renewed in 2020), alongside companies in its perimeter such as Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U. and Telyco, S.A.U. (obtained in 2020).

In 2022, Colombia Telecomunicaciones was awarded the ISO 37001:2016 Anti-bribery Management Systems certification and Telefónica del Perú S.A. renewed that certification.

In 2022, Telefónica's commitment in this matter was recognised in the context of its participation in a project launched by "Business at OECD" with the aim of evaluating the role that technology can play in the fight against corruption. Telefónica's initiatives in this regard stood out among the different use cases identified in the private sector.

> Sanction compliance

At the present time, international sanction regimes – namely the commercial and/or financial and economic restrictions and/or prohibitions imposed by governments, regulators and/or other international organisations against governments, countries, individuals, entities and/or business sectors – constitute an increasingly important and highly complex reality.

Telefónica is committed to conducting its business in compliance with the international sanction regimes that may apply to it at any given time. Therefore, in 2022 the Board of Directors, as part of the evolution and continuous improvement of the Compliance Programme that Telefónica has implemented in this respect, approved new Rules on Sanctions which define the main controls in this area and reinforces Telefónica's commitment to compliance with applicable sanction regimes.

> Competition compliance

Fair competition is one of our Responsible Business Principles, and is integrated transversally in several policies and processes within the Company.

In 2022, in order to strengthen Telefónica's compliance programme in this area, the Board of Directors of Telefónica, S.A. approved the first **Competition Law Policy of the Telefónica Group**. This formalised the Telefónica Group's commitment to the principle of fair competition, enshrined in the Responsible Business Principles, in a rule that both demonstrates and facilitates the fulfilment of that commitment to fair competition practices in all markets, as well as reflecting our belief in free markets and fair conditions of competition.

On the basis of the approval of the Competition Law Policy, the course on competition law, which is included in the Training Opportunities Scheme and is aimed at all Telefónica Group employees, was reviewed and updated. Training sessions are also given on specific areas previously-identified.

In addition, the Group has guidelines in place for participation in industry organisations and meetings with competitors, where clear rules are laid down to ensure compliance with competition law regarding the exchange between competitors of sensitive information. This is complemented in some countries by specific competition compliance programmes under local legislation (e.g. Chile).

In 2022, no (0) material judicial proceedings[3] in progress for infringement of competition law regulations were identified and a fine was paid (€67 million) for anti-competitive practices in relation to the formal procedure opened in 2011 by the European Commission for the contract for the sale of the participation of Portugal Telecom in Brasilcel, N.V.

For further information, see the Consolidated Financial Statements.

> Money laundering compliance

With regard to money laundering, the Company has **payment controls** in place that include due diligence procedures for suppliers and business partners, defined from a compliance viewpoint, and controls on payments to certain high-risk countries. These are then complemented by activities specifically aimed at fulfilling the requirements of the legislation in each country, and/or certain regulations on this topic applicable to the type of company or entity in question (when under local legislation it is considered to be subject to the requirements in this area).

[3] Taking into account issues whose materiality meets the reporting rules for the Consolidated Annual Accounts (whether it is greater than €40 million and classified as probable or €100 million and the risk classified as possible).

In this regard, in accordance with the Telefónica Group's internal regulations on payment control, the Company monitors the definition of minimum controls on payments to prevent the risk of **money laundering**, both at Group level and by jurisdiction and/or type of entity or activity.

In particular, in 2022, under its continuous improvement strategy, on a Group-wide level Telefónica implemented, as part of the process, a new control on certain payments, stemming from previously-undertaken analysis regarding the need to strengthen the corresponding control model.

2.17.5.2. Training

GRI 205-2

A key element in promoting a culture of ethics within the Company is anti-corruption training. This training includes the following courses:

- The **Responsible Business Principles and Human Rights Course** (see chapter 2.16), covering aspects relating to anti-corruption and bribery in the section entitled 'Ethical and Responsible Management'.

For further information, see chapter 2.16. Governance and culture of sustainability

- The **Foreign Corrupt Practices Act (FCPA) Course,** in online and in-person format, on the law against corrupt practices abroad. This course is aimed at certain areas of the Company that present a higher potential risk due to their greater exposure to the risk of public corruption.
- Other **local courses** on anti-corruption and crime prevention. Other specific training courses (including aspects relating to criminal prevention) are in most of the countries in which the Telefónica Group operates. In some cases, they are taught on an in-person basis and/or targeted at certain groups of employees whose activity may present a higher potential risk. Here we highlight the training on criminal liability given in Peru, Argentina, Chile and Ecuador, and at Telefónica Spain and the companies within its scope of consolidation which began training in 2021.

In 2022, stemming from the updating of the Responsible Business Principles, certain training courses which are particularly important for the efficiency of the Group’s compliance model were reviewed, updated and launched. Specifically, the courses on the Responsible Business Principles, competition law, the FCPA and criminal prevention at Telefónica S.A. and the Spanish companies within its corporate scope, were incorporated into the Training Opportunities Scheme which was launched in June 2022 on a Group-wide basis.

As of December 31, 2022, 94,840 employees had received anti-corruption training, which represents 93% of the average workforce.

All the members (15) of the Board of Directors received anti-corruption training.

In addition, in 2022, a new course began on **cybersecurity for employees: personal protection and co-responsibility,** and the training on **privacy** was continued and extended to Group companies in the Hispanoamerica region. Other training activities also began for certain areas and relevant executive personnel of the Company concerning international sanction programmes.

Anti-corruption training in 2022

Number of employees trained in anti-corruption matters.	94,840
Percentage of employees trained in anti-corruption matters.	93

> Raising awareness

Another of the crucial elements of the compliance programme is that of raising awareness. There are various initiatives, at both global and local level, which target fostering a culture of compliance among employees. These include:

a. **Compliance Day**, a day designed to familiarise the business with the function of Compliance and raise awareness among employees about the main issues that this area addresses. In 2022, we instituted the **Compliance Quiz**. One employee from each of the different units of the Group sent in a multiple-choice question related to compliance matters; some of the questions submitted were used to create a Compliance Quiz, which was launched to coincide with Compliance Day.

b. The **'Five Stars' Recognition Programme,** developed to promote and recognise behaviour that stands out thanks to its commitment to the issues of integrity and sanctions, privacy and security. In 2022, we held the fourth edition of these awards, in which 63 employees from different operations and companies were recognised as deserving Five Stars.

Also in 2022, we conducted a global compliance survey in order to measure the level of internal awareness about the different elements that make up Telefónica's Compliance Programme, and identify and undertake future awareness-raising and improvement activities.

Employees receiving anti-corruption training in 2022 by professional category and region

Country	Executives	Middle management	Other professionals	Total
Germany	152	519	4,325	4,996
Brazil	1,693	2,459	28,708	32,860
Spain	1,581	2,809	22,176	26,566
Hispam	747	2,592	26,758	30,097
Others	54	153	114	321
Total	**4,227**	**8,532**	**82,081**	**94,840**

% of employees receiving anti-corruption training in 2022 by professional category and region

Country	Executives	Middle management	Other professionals	Total
Germany	64%	76%	64%	65%
Brazil	100%	99%	94%	95%
Spain	99%	98%	97%	97%
Hispam	99%	88%	96%	95%
Others	74%	59%	14%	28%
Total	**98%**	**92%**	**92%**	**93%**

2.17.5.3. Complaint and remedy mechanisms: Concern and Whistleblowing Channel

GRI 2-16, 2-26, 3-3, 205-3, 403-2, 406-1, 418-1

> Complaints

Telefónica has a **whistleblowing channel** which is **available to employees and stakeholders** (suppliers, shareholders, customers, investors and society in general), where they can report, on an anonymous or personal basis, any alleged irregularity or act in breach of the law or of internal regulations.

This channel is **available 24/7 on our website and on the Company's intranet** to enable access by all our stakeholders and thus comply with both the European Directive on the protection of persons who report breaches of EU law and also with the updated version of the Good Governance Code for Listed Companies.

When processing the complaints reported, the **principles of confidentiality of the data provided**, respect and substantiation apply. In cases where a significant or relevant irregularity is identified, the Audit and Control Committee, which reports to the Board of Directors, is informed. All individuals who report a breach are protected in accordance with applicable legislation or regulation.

The complaint may fall into the following categories:

- Labour dispute
- Labour conditions
- Information security/privacy
- Acts contrary to the integrity of the Company
- Asset fraud
- Favourable treatment
- Financial reporting
- Regulatory/contractual/legal non-compliance

The above categories also include any irregularities relating to accounting matters, auditing matters and/or internal control over financial reporting in compliance with section 301 of the US Sarbanes-Oxley Act and other requirements in this regard.

The channel makes it possible to consult the status of a complaint, add information and contact the auditor responsible for analysing the complaint.

In accordance with our Zero Tolerance policy on corruption, bribery and discrimination, Telefónica has **specific controls in place to detect and remedy possible cases**. This takes the form of disciplinary action and/or termination of contract.

In 2022 we received 808 complaints through this Channel. As a result of the investigations, 374 were founded. Among the measures adopted as a consequence of the founded reports, there were 118 terminations of employment contracts.

Complaints

	2021	2022
Nature of substantiated complaints	**% of total substantiated complaints**	**% of total substantiated complaints**
Failure to comply with regulations	12%	15%
Fraud	23%	21%
Workplace/sexual harassment and/or discrimination	1%	3%
Conflict of interest	4%	5%
Information security/privacy	2%	3%
Inappropriate behaviour and other workplace disputes	38%	41%
Other	20%	12%
Total	**389**	**374**

Main indicators on complaints

	2021	2022
Complaints received	955	808
Substantiated complaints	389	374
Termination of employment measures taken as a result of substantiated complaints	152	118
Confirmed cases of corruption	0	0
Disciplinary measures taken or terminations of contract carried out in connection with confirmed cases of corruption	0	0
Cases of discrimination detected	0	0
Disciplinary measures taken or terminations of contract in relation to confirmed discrimination cases	0	0

VMED O2 UK

	2022
Confirmed cases of corruption	0

> Queries

We have a channel through which all our stakeholders can **make queries, give notice of or report**, either anonymously or personally, queries, requests or complaints about any aspect related to the Responsible Business Principles.

In 2022, we received 711 valid queries, of which 698 have been resolved as queries related to the themes of this channel. The themes into which the closed queries have been divided are those represented in the following table:

Queries

	2021	2022
Responsible communication	5	6
Integrity	5	9
Environment	11	66
Supply chain	1	14
Privacy	9	30
Accessibility	3	5
Sustainable innovation	2	3
Human rights	2	5
Children's rights	1	0
Freedom of expression	2	0
Diversity and talent management	2	14
Others (for example, responsibility towards the customer, infrastructure)[4]	153	546
Total	**196**	**698**

In 2022, as in previous years, the handling of these queries has made it possible to identify improvements in complaint and remedy mechanisms, but also in policies and procedures for the internal management of enquiries submitted by stakeholders.

Our Concern and Whistleblowing Channel is available in various languages and open to anyone, including our suppliers' employees.

2.17.5.4. Political neutrality

GRI 415-1

Telefónica is politically neutral. We do not take a direct or indirect position for or against any political party and we do not make donations (0€) to political parties or to organisations, whether public or private, linked to political parties. This does not prevent us, in compliance with prevailing legislation, from making our views known on matters that may affect the management and sustainability of the Company, through lobbying activities.

We are registered as a lobbyist in the voluntary transparency register of the European Union and in the register of interest groups of the CNMC (National Commission on Markets and Competition).

Our total expenses in relation to contributions to sectoral organisations are widely distributed because: (a) Telefónica is present in many countries and each country has its own local sectoral organisations, and (b) Telefónica provides many types of services affected by different business sectors (fixed and mobile connections, television and digital services).

Our expenditure on contributions to industry bodies and to organisations or individuals performing representative activities for Telefónica amounted to €6,095,148 in 2022, 92% of which was allocated to industry bodies, including GSMA, SindiTelebrasil, ETNO and Bitkom, among others.

2.17.5.5. Responsible communication

We promote freedom of expression, pluralism and diversity, and we are committed to truthful information, education and inclusion.

We assume our responsibility to promote responsible, ethical and quality communication through the content we generate (entertainment, cultural, sporting, advertising and other content). Our **Responsible Communication Regulation** offers general guidelines for when we communicate with our customers and other stakeholders, use our social media, generate and disseminate content, generate our own advertising, or broadcast that of third parties.

We also have a **specific Responsible Communication Code for Movistar Plus+**, approved by the Executive Committee of Telefónica Spain with the following lines of action:

- Publication in different public media to enable consultation by any user.

[4] The 'Others' category currently includes queries related to 'responsibility towards the customer' and 'infrastructure', which we redirect internally for resolution by the appropriate channels.

- Implementation. It has been shared with all Movistar Plus+ stakeholders to ensure that it is accepted and respected on a daily basis by employees, suppliers and external collaborators, analysts, customers and society in general.

Possible complaints/enquiries are channelled through the Concern and Whistleblowing Channel.

Movistar Plus+ Responsible Communication Code

We are a television platform with ethical editorial criteria for all our productions, whether our own, purchased or outsourced. We promote these principles:

Legality

We comply with the rules, we protect intellectual property and we do not encourage illegal, irresponsible or discriminatory.

Neutrality

We promote freedom of expression and creativity, while respecting the right to honour and privacy.

Protection of minors

We manage content responsibly and have preventive, safe advertising and awareness-raising measures.

Integrity and transparency

We ensure compliance with Telefónica's Anti-Corruption Policy.

Diversity

We promote equality and social integration in our programme schedule.

Values and talent

Our business commitment to creativity and innovation is reflected in the content.

We have pre-broadcast controls, a Content and Production Officer, and anti-piracy mechanisms in place.
All our activities are based on Telefónica's Responsible Business Principles and our Responsible Communication Regulation.

For further information, see chapter 2.11. Customers.

2.17.5.6. Internal control

As set out in the Internal Control Policy, the Company has an internal control model defined in line with the COSO Internal Control — Integrated Framework.

Thus, internal control at the Telefónica Group is defined as the process undertaken by the Board of Directors, management and the rest of the Company's personnel, designed with the goal of providing a degree of reasonable assurance for meeting the targets relating to operations, information and compliance.

Internal control is designed to be a process that is integrated into the Company's day-to-day activities in which all the areas, within their areas of action (managers), are responsible for internal control and must take into consideration among their tasks the assurance elements necessary to achieve operational targets (effectiveness), with the least use of resources (efficiency), the availability of appropriate information for decision making and external reporting (information - accuracy) and the observance of laws and rules (compliance). These aspects, above all, must take into consideration the possible contingencies that may arise in their development (risks), incorporating assurance elements with regard to possible contingencies (Internal Control structures), as well as for monitoring (supervision) activities and its own internal control structures within its area of responsibility

The areas of action performed by Internal Audit include coordination of the Telefónica Group's regulatory framework by supervising the process of defining internal regulations, as set out in the policy governing the creation and organisation of the regulatory framework. In turn, the regulatory framework promotes actions that favour the updating and communication of said standards.

Specific reviews are also performed that are of interest to the Board of Directors or the Company's management, which include investigations stemming from the whistleblowing channels provided for the purpose at the Telefónica Group, potential cases of fraud and specific reviews aimed at preventing fraud.

In 2022, the Internal Audit area spent 86,096 workdays on the activities scheduled in the audit plan and, of these, 10,020 were related to fraud prevention and corruption prevention activities.

Number of days

	2021	2022
Fraud/corruption prevention, review of personal actions	10,808	10,020

MILESTONES

- → **We launched a Group-wide Training Opportunities Scheme including essential training for the compliance model.**
- → **Our Board of Directors approved the Competition Law Policy and the Rules on Sanctions.**

2.18. Fiscal transparency

KEY POINTS

☆ Telefónica's tax contribution in 2022 amounted to €7.7 billion globally: €19.2 per every €100 of turnover.

☆ Taxes paid during the year amounted to €2.4 billion and taxes collected amounted to €5.2 billion.

☆ Each year we publish the fiscal contribution per country: we highlight the €2.3 billion contributed in Spain and the €2.8 billion paid in Brazil.

2.18.1. Vision

GRI 207-1

Telefónica's taxation is based on our Responsible Business Principles, the guidelines that inform our daily activity and define how we conduct our business. In accordance with these guidelines, we are committed to honesty, respect for the law and transparency in the conduct of our fiscal affairs.

At Telefónica, we are committed to the OECD guidelines for multinational companies to ensure strict compliance with our **tax obligations**. We strive to be a best-practice benchmark, ensuring that we contribute faithfully and loyally to the public finances of the countries and territories in which we operate, our compliance with the tax legislation and the principles that drive sustainability. The Company's fiscal contribution is one of its main contributions to the economic and social development of the environment in which it operates. Accordingly, in line with our commitment to fiscal transparency and our contribution to the UN Sustainable Development Goals (SDGs), we publish our total economic and social tax contribution on our corporate website in the section on sustainability-innovation/how-we-work/sustainability-strategy.

In this regard, the statements contained in this GRI 207 standard enable Telefónica to achieve some of the SDG targets it has set itself.

2.18.2. Governance

GRI 207-1, 207-2

The **bodies responsible for the fiscal control framework at Telefónica** are as follows:

The determination of the Group’s tax policy and strategy is the responsibility of the **Board of Directors** and cannot be delegated; therefore, the Board of Directors is also responsible for their approval and any future modifications. The **Group's Tax Department leads**, develops and reviews the tax strategy.

The Group’s Tax Department and the Regional Divisions report on a yearly basis to the Audit and Control Committee and, where appropriate, to the Board of Directors, on the following matters:

- The tax policies and criteria followed by the Group in order to facilitate the task of supervising the tax risk management system, entrusted to the Audit and Compliance Committee by the Spanish Corporations Act, in accordance with the provisions of the Code of Good Tax Practices.
- The status and development of tax risks.
- The tax impacts of all relevant transactions submitted for approval in accordance with Section 529 Ter of the Spanish Corporations Act.
- Transactions that are particularly important from a tax perspective.

The **Group's Tax Department and the Regional Divisions** detect and report on mechanisms subject to notification under Council Directive (EU) 2018/822 of 25 May 2018 (DAC 6) and **coordinate with the Group's Internal Audit function** on the review and analysis of procedures necessary to achieve the control objectives of the Fiscal Strategy and Fiscal Control Framework.

Those responsible for the tax area in each subsidiary put in place the necessary management procedures to ensure that fiscal control is performed in accordance with the defined principles and operating regulations.

> Assessment of compliance with the fiscal governance and control framework

The Group's Tax Department and the Regional Tax Divisions perform the analyses and verifications deemed appropriate to verify the correct application of the aspects contained in the regulations, tax strategy and tax control policy, and to guarantee control targets set by the Group.

In addition, as indicated in the Annual Corporate Governance Report, Telefónica annually validates compliance with the content and commitments contained in the Code of Good Tax Practices and, therefore, that it is complying with its governance framework.

> Integration of the fiscal approach in the Telefónica Group

Telefónica will ensure that the departments involved in tax issues have the necessary means to guarantee compliance with tax obligations in all the countries in which the Company operates.

Those responsible for the tax area at each company participate in analysing all transactions that may have tax implications. For this purpose:

- They have the necessary financial, human and material resources.
- They can and should, where necessary, establish permanent computer links with the information systems of Group companies.
- They receive maximum support and assistance from the Group companies.
- They may require the participation and collaboration of Group company employees.

For further information in this regard, Telefónica develops the core principles of the fiscal control function within the Fiscal Control Policy (available on the corporate website in the section on sustainability-innovation/how-we-work/ sustainability-strategy.

2.18.3.Policies

GRI 207-1

The **Fiscal Control Policy**,approved by the Board of Directors and available on the Telefónica website, has the following objectives:
• Correct fulfilment of tax obligations in due time and form.

• Effectiveness and efficiency of operations with regard to tax matters.

• Position-taking or tax strategy duly supported and documented.

• Reliability of tax information.

• Transparency vis-à-vis third parties, especially the tax authorities.

• Tax risk management.

2.18.4.Risks and opportunities

GRI 207-2

As mentioned on the corporate website in the section Commitment/ How we work, we manage tax risks to prevent and reduce tax litigation to the extent necessary to defend tax positions legitimately taken by Telefónica. Accordingly, at Telefónica, we have a **Risk Management Model** in place based on COSO (Committee of Sponsoring Organizations of the Treadway Commission), which enables the identification, assessment and management of the different risks (as explained in chapter 3. Risks).

Under this Model, we have defined **four risk categories: business, operational, financial** and, lastly, **legal and compliance**. The **latter category includes tax risks**.

Typology of tax risks and associated controls In relation to their origin, risks of a fiscal nature are classified as follows:

- **Compliance risk**: relating to the fulfilment of obligations in taxation (filing of returns, information requirements, etc.).
- **Interpretative risk**: the possibility of interpreting tax laws differently from the tax authorities.
- **Regulatory risk**: associated with legislative activity and regulatory volatility and complexity.
- **Reputational risk**: related to the current context of demands and public scrutiny in terms of transparency and perception of fair compliance with the companies' tax obligations by the different stakeholders.

Although risk identification is a continuous process and requires the involvement of the entire organisation, in the case of tax risks the Corporate Tax Department promotes and coordinates their identification and regular updating.

The policy of control, evaluation and management of tax risks is developed in the Fiscal Control Policy available on the corporate website, in the section sustainability- innovation/how-we-work/ sustainability-strategy

> Reporting obligations

On a quarterly basis, those responsible for the tax control function at each of the Group's companies inform the Tax Department—through the Regional Tax Divisions—of the main conclusions from the process of identifying and assessing tax risks, including those related to:

- Litigation in court/arbitration.
- Litigation in administrative proceedings prior to judicial proceedings.
- Transactions with implicit risk that may be examined by the tax authorities.

They also report on external tax audits and tax administration inspection processes.

Furthermore, as a consequence of the entry into force of DAC 6, we have developed a procedure for detecting and reporting notifiable mechanisms.

2.18.5. Action plan and commitments

GRI 207-2, 207-3

Pursuant to Section 529 Ter of the Spanish Corporations Act, on 14 December 2016 the Board of Directors of Telefónica approved the Group's tax strategy as published on our corporate website.

> Regulatory compliance

At Telefónica, we are committed to complying with all national and international legislation, regulations and tax obligations, respecting both their letter and their spirit. In fact, we devote the necessary resources and take the appropriate measures to make a reasonable interpretation of the rules, taking into account the legislator's intention in accordance with the interpretative criteria established by the competent tax authorities and the legislative background. We also adopt the necessary control mechanisms to ensure compliance with these regulations as part of good business management.

Relationship between taxation, sustainable development and business

At Telefónica, we are committed to all tax positions being taken up for commercial and business reasons, paying taxes according to their true legal nature and economic substance, and avoiding abusive tax planning schemes or practices. In this respect, the tax component of any transaction cannot be justified separately from the commercial and business reasons for the transaction in question.

Telefónica also applies the arm's length principle in its transactions with related entities, aligning taxation in each country and territory according to its business there and the generation of value, in accordance with local tax legislation and the international taxation standards established by the OECD.

> Stakeholder engagement and management of tax concerns

Relationship with tax authorities

At Telefónica, we are committed to fostering a cooperative relationship with the tax authorities inspired by the principles of collaboration, trust, good faith, loyalty, professionalism, mutual respect and dialogue.

Since 2010, and in order to apply the highest standards of tax transparency, Telefónica, S.A. has adhered—by resolution of the Board of Directors—to the Code of Good Tax Practices drawn up by *Foro de Grandes Empresas* (Forum for Large Enterprises) in conjunction with the Spanish tax authorities.

Based on the principles of transparency and mutual trust, we have voluntarily filed Transparency Reports with the Spanish tax authorities since the 2016 financial year, with the prior authorisation of the Audit and Control Committee, as part of the functions delegated by the Board of Directors. Our corporate website provides further information on the subject in the section sustainability-innovation/how-we-work/sustainability-strategy.

Our approach to matters relating to the Spanish tax authorities also applies internationally. In this regard, Telefónica participates in various international fora to promote and develop the OECD's good practice recommendations.

We also participate in the cooperative compliance programme in the UK.

Contribution to legislative initiatives in tax matters

Telefónica actively participates in the *Foro de Grandes Empresas*. This allows us to intervene in tax legislation initiatives, highlight current problems that may arise in the application of the tax system and propose new tax measures to increase legal certainty.

We contribute to the committees of telecommunications industry organisations such as ETNO (European Telecommunications Network Operators' Association) and GSMA.

We are active collaborators in various industries and economic forums, such as DigitalES (Spanish Association for Digitalisation) and Adigital (Spanish Association of the Digital Economy).

The Telefónica Group is also actively involved in tax policy through the respective committees of the CEOE (Spanish Confederation of Business Organisations) and DET3 (Digital Economy Taxation Think Tank).

Stakeholder dialogue

Telefónica's stakeholder engagement strategy is based on **increasing transparency and effective dialogue to build relationships of trust** in the countries in which we operate.

We maintain a constructive dialogue and collaborate with various key stakeholders, such as non-governmental organisations – such as Intermon Oxfam, the Haz Foundation and the Tax and Competitiveness Foundation - and government agencies through the Forum of Large Companies, which was created in 2009 as a body for cooperation between Spain's largest companies and the Spanish tax authorities. Likewise, we obtain all stakeholders' views on their expectations and perceptions about fiscal transparency in the consultation process that we perform for our materiality analysis.

For further information, see chapter 1.4. Materiality.

This relationship makes it possible to identify which aspects are considered most significant and which are the new trends in the field of sustainability. In this way, we set our targets, define the strategic plan and, in addition, assess our ability to meet society's expectations.

In fact, thanks to the progress made, we achieved the highest score in the S&P DJSI, MSCI and Sustainalytics indices.

Reporting unethical behaviour

As described in section 2.8.5 of the Non-Financial Information Statement, Telefónica has public complaint and remedy mechanisms in place (the Concern and Whistleblowing Channel) to report concerns about unethical or illegal behaviour and the organisation's integrity in relation to taxation.

For further information, see chapter 2.17. Ethics and compliance.

Telefónica's Concern and Whistleblowing Channel handles any tax issues reported by our various stakeholders

2.18.6. Progress in 2022

GRI 201-4, 207-2, 207-4

> Contribution to the development of local economies and finances

In 2022, our Total Tax Contribution (TTC) amounted to €7.7 billion (€2.4 billion in taxes incurred and €5.2 billion in taxes collected), accounting for 48% of our distributed value[1] (value distributed as input and output taxes levied on the total value distributed, the latter being the sum of the following items: shareholder value -profit after tax-, wages and salaries net of taxes levied, net interest and input and output taxes levied).

Total subsidies received by Telefónica in 2022 amounted to €17 million (€16 million in 2021), which includes the receipt of capital grants and subsidies as other income.

The Group did not use any tax deductions in the latest corporation tax return filed in Spain.

For every €100 of turnover, we pay €19 in taxes (€6 incurred and €13 collected).

It is important to note that our economic and social contribution is quantifiable not only through corporate tax revenues but also through other specific contributions in the various countries in which we operate. These include fees (for use of the public domain and for financing the radio and television corporation, among others), local taxes and social security payments, as well as other similar contributions in other countries.

[1] Calculated on the basis of our own methodology.

In addition to these direct taxes, we generate revenue for the public treasury as a result of our business activity and on behalf of other taxpayers, other amounts that must be taken into account in the total tax contribution made by the Company, such as indirect taxes, withholding taxes on employees and other deductions.

For further information, see chapter 2.14. Contribution and impact on communities

> Contribution in countries

The following is a breakdown of the jurisdictions in which the Telefónica Group conducts its main business as a telecommunications services provider. Other jurisdictions where the Group is present, and in which its activities are not the Group's core business, are included under "Other". All amounts are given in millions of euros and refer to the financial year 2021.

The main companies that make up the Telefónica Group, together with their main activity, may be consulted in the 2022 Consolidated Financial Statements.

For further information, see Appendix I: Scope of consolidation

For reconciliation purposes with the figures reported in the Consolidated Financial Statements, consolidation adjustments and eliminations of inter-company transactions between Group companies in different countries are also included under "Other".

However, there are differences with the Group's Consolidated Annual Accounts, which are explained below:

- The Annual Accounts only include information on sales to third parties, whereas the Country-by-Country Report (CbCR) also includes intra-group sales.
- In relation to profit or loss before tax, there is an adjustment for the accrual of coupons corresponding to the subordinated perpetual debentures in the Netherlands.
- The differences in taxes paid are due to the Annual Accounts including not only corporation tax (as in the case of the CbCR), but also telecommunication charges, local taxes, other charges, licence fees and social security, etc.

2021 country-by-country report

Tax jurisdiction	Third-party income	Related-party revenues	Total income	Profit or loss before tax[2]	Tax on profit paid[3]	Profit tax[1]	No. of employees[4]	Tangible assets
Germany	8,642	69	8,711	663	54	41	7,576	3,492
Argentina	2,296	64	2,360	-64	18	117	13,030	1,371
Brazil	7,569	49	7,617	882	44	-30	34,570	5,377
Chile	2,084	59	2,143	372	39	128	4,157	1,068
Colombia	1,335	15	1,349	-20	39	-41	6,114	876
Costa Rica	135	1	136	48	11	16	145	0
Ecuador	408	6	413	-11	11	0	935	238
El Salvador	122	3	126	-26	1	6	190	0
Spain	20,280	2,069	22,349	5,261	197	635	28,668	8,511
Guatemala	5	4	9	1	1	0	10	14
Mexico	1,042	67	1,109	-386	24	22	1,832	158
Panama	3	15	19	2	0	1	26	8
Peru	1,721	30	1,751	-554	41	141	4,810	1,156
UK	7,141	155	7,296	5,200	-7	194	3,008	13
Uruguay	230	109	339	104	14	16	591	309
Venezuela	104	3	108	90	1	30	1,661	40
Others	420	-890	-470	195	20	15	453	93
Total	**53,537**	**1,828**	**55,365**	**11,757**	**506**	**1,293**	**107,776**	**22,725**

[2] Contribution to the consolidated profit before tax and to the tax on profit, adjusted for the allocation to the year of coupons relating to subordinated perpetual bonds. The consolidated financial statements of the Telefónica Group are drawn up in accordance with the International Financial Reporting Standards (IFRS) as adopted by the European Union. The local accounting regulations applicable in each of the countries in which the Group is present may differ from the standards set by the IFRS.
The table above groups together all companies of the Group according to the country of their registered office. This grouping does not coincide with the distribution by segment of the Telefónica Group. The results by country include, as appropriate, the effect of the allocation of the purchase price to the acquired assets and the liabilities assumed. The results by country exclude income generated by dividends of Group subsidiaries, as well as the change in the provision for write-downs of investments in Group companies, which are eliminated in the consolidation process. The withholdings paid to the various administrations have been allocated to the jurisdiction by which they are ultimately paid.

[3] Rebates received from different administrations and corresponding to overpayments from previous years have been excluded in 2021, €30 million in Spain and €17 million in Peru and Chile, to be precise.

[4] The number of employees refers to the average number of employees, distributed by tax jurisdiction.

> Reasons for the difference between the effective rate and the statutory rate

The Group closely monitors the differences between the nominal tax expense and the effective tax expense on a monthly basis.

At year-end 2021, the differences relate to the permanent differences inherent in the preparation of corporation tax. In other words, they comprise all the expenses or income recorded on the income statement that will not be deductible or will not be taxed from a fiscal point of view and will therefore never be reversed in subsequent periods. The most relevant are the deductibility of the amortisation of goodwill in Spain and, in Brazil, the deductibility of the distribution of Juros on capital. There is also a significant difference owing to the non-activation of tax credits in countries with negative results.

In addition, during the 2021 financial year, extraordinary accounting adjustments were made to the corporation tax expense account, representing a significant part of the differences between the statutory and effective rates. In this regard, the effects of the tax assessments from the completion of the tax inspection in Spain for the years 2014 to 2017 were recorded, in addition to a decrease in deferred tax assets in Spain due to the restatement of their recoverability, a tax provision in Peru due to an unfavourable ruling by the Supreme Court and adjustments for tax rate changes in different countries, as well as the effect of non-taxable interests in Brazil. In addition, a substantial portion of the capital gains recorded in 2021 was exempt from corporation tax.

Verification of the contents in terms of taxation has been completed as part of the external verification process carried out by PricewaterhouseCoopers Auditores, S.L.

Tax contribution by country

Millions of euros	Contribution by country to consolidated Group profit before tax (1) 2022	Contribution by country to consolidated Group profit before tax (1) 2021	Total taxes paid 2021	Total taxes collected 2022	Total 2022
Germany	697	663	291	790	1,081
Argentina	-166	-64	165	393	558
Brazil	919	882	1,105	1,648	2,754
Central America	1	25	2	1	2
Chile	64	372	1	97	98
Colombia	118	-20	151	126	277
Ecuador	23	-11	66	25	90
Spain	795	5,261	427	1,847	2,274
Mexico	-228	-386	27	62	89
Peru	-103	-554	143	151	294
United Kingdom	294	5,200	-1	36	35
Uruguay	152	104	32	25	57
Venezuela	95	90	14	16	30
Others	21	195	15	15	30
TOTAL	**2,682**	**11,757**	**2,438**	**5,231**	**7,669**

The breakdown of the corporation tax contribution is as follows:

Tax contribution by region

	2022		2021	
Millions of euros	Contribution by country to consolidated Group profit before tax	Tax on profit[5]	Contribution by country to consolidated Group profit before tax	Tax on profit
Europe	1,786	477	11,124	244
Latin America	874	530	413	229
Central America	1	2	25	13
Other	21	2	195	20
TOTAL	**2,682**	**1,010**	**11,757**	**506**

Contribution to the consolidated profit before tax, adjusted for the allocation to the year of coupons relating to subordinated perpetual bonds. The consolidated financial statements of the Telefónica Group are drawn up in accordance with the International Financial Reporting Standards (IFRS) as adopted by the European Union. The local accounting regulations applicable in each of the countries in which the Group is present may differ from the standards set by the IFRS.

The table above groups together all companies of the Group according to the country of their registered office. This grouping does not coincide with the distribution by segment of the Telefónica Group. The results by country include, as appropriate, the effect of the allocation of the purchase price to the acquired assets and the liabilities assumed. The results by country exclude income generated by dividends of Group subsidiaries, as well as the change in the provision for write-downs of investments in Group companies, which are eliminated in the consolidation process.

The contribution in 2021 from Germany, Spain and the United Kingdom is affected by the capital gains generated on the incorporation of VMED O2 UK and on the sale of the telecommunications towers division of Telxius (see Note 2 Notes to the Consolidated Financial Statements).

MILESTONES

→ We are one of the 34 companies which voluntarily filed the Transparency Report for 2021 with the Spanish tax authorities.

→ Thanks to the progress we have made regarding tax issues, we have achieved the highest score in indices such as S&P DJSI, MSCI and Sustainalytics.

[5] Rebates received from different administrations and corresponding to overpayments from previous years are excluded in 2022, to be precise,€115 million in Spain and €12 million in Peru and Chile. In addition, the extraordinary refund from the Judgement Enforcement Agreement of the Spanish National Court of Appeals (Audiencia Nacional) (€790 million) is excluded in Spain as explained in Note 25 of the Notes to the Consolidated Financial Statements.
With regard to 2021, rebates of €30 million in Spain and €17 million in Peru and Chile have been excluded.
The withholdings paid to the various administrations have been allocated to the jurisdiction by which they are ultimately paid.

2.19. Privacy and security

KEY POINTS

☆ We protect our customers' data, monitored at the highest levels, with high standards of privacy and security, and empower them to have access to, and control of, their personal data.

☆ We are transparent about how, why and when our customers' data is collected, used, stored and disposed of, as well as how we protect the data with a high level of security.

☆ We are committed to increasing the percentage of contracts/RFPs that contain security requirements for the supply chain, with the goal of reaching at least 95% by 2025.

2.19.1. Vision

Technology **improves people's quality of life and generates wealth,** provided that their privacy is respected and the highest level of security is guaranteed throughout the processing of their information and personal data.

We want **our customers to feel confident about using our products and services** and to be aware that we respect their rights at all times as we offer them choices about the use of their personal information.

For this reason, we work on the **privacy and security** of our customers, to generate a relationship of trust with all those we work with are linked, and we focus on the following pillars:

- **Protection:** data must be secure and **the privacy of individuals must be preserved.** This is the basis of our business and our primary consideration when designing our services and collaborating with third parties.
- **Design:** we apply **privacy and security from the design**, that is, from the initial concept of our products and services and throughout the development process.
- **Control:** individuals must be able to manage and **have control over their personal data**. In this way, access to their data, and to additional information on risks and benefits associated with its management, is made possible.
- **Transparency:** the **principle of transparency** is about making simple tools available to people in order for them to control their data with the appropriate technological developments to generate maximum respect for privacy and information security.

We are also strongly committed to the right of children to privacy and security, to protecting their personal information and to fostering a safe use of technology.

For further information, see section 2.10.4.4. Secure and responsible use of technology

In addition, Telefónica is a global leader in the development and commercialisation of **cybersecurity and managed security products and services**. We provide more detail of our portfolio and achievements in this field in chapter 1.6 Organisation.

For further information, see chapter 1.6. Organisation.

This chapter describes the different aspects related to our internal privacy and security operations, which are applicable to our processes, products and infrastructure.

2.19.2. Privacy

2.19.2.1. Vision

Telefónica respects the fundamental rights and freedoms of individuals, including the fundamental right to the protection of personal data. The Responsible Business Principles, the Group's code of ethics, envisage the need to **preserve this fundamental right** and establish common guidelines of behaviour for all the companies that form part of the Company.

2.19.2.2. Targets

In order to reduce risk exposure and raise digital trust, we continuously update our processes and policies:

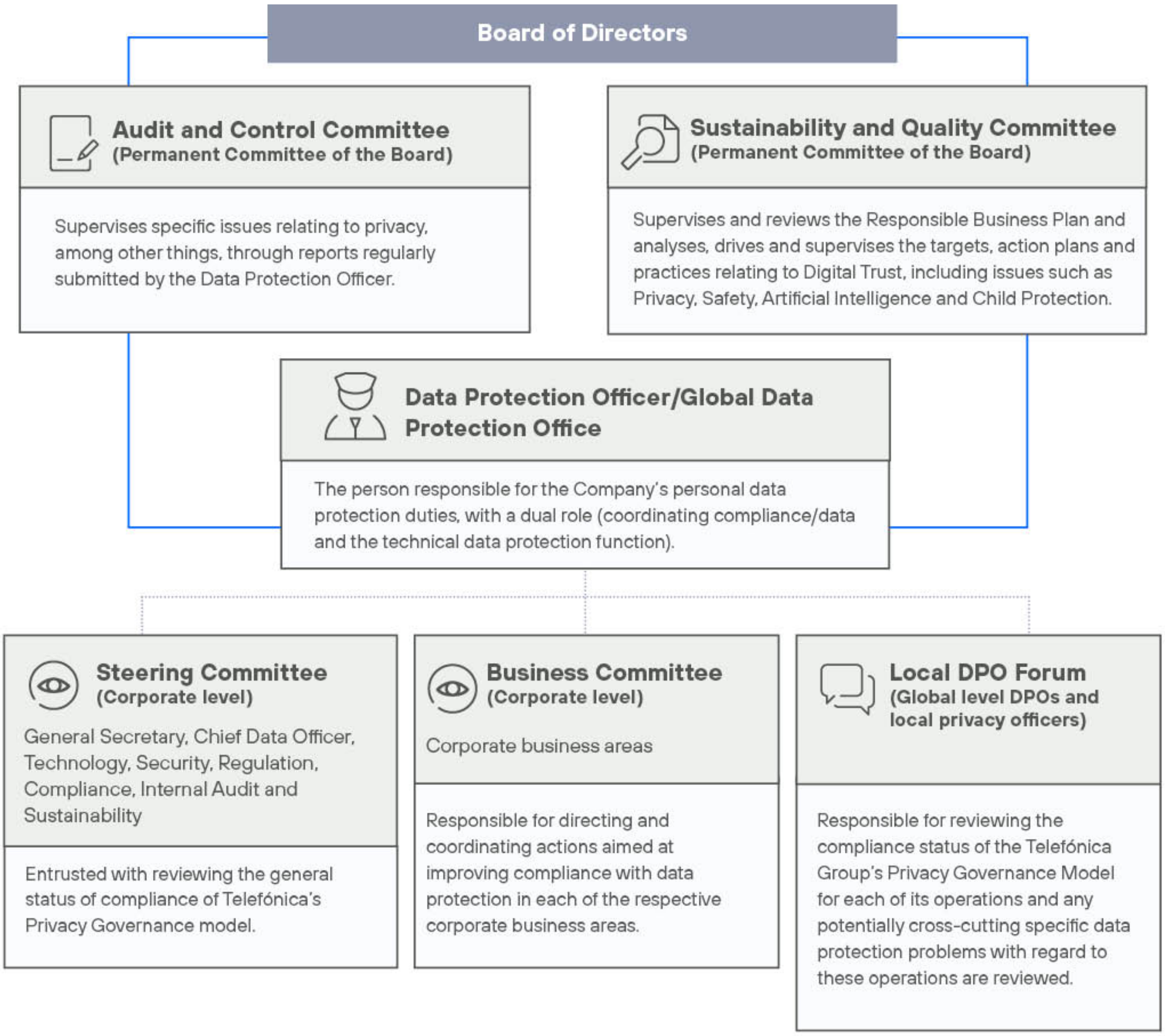
- Update the Group's Privacy Policy.
- Approve Binding Corporate Rules (BCRs).
- Update the Global Privacy Centre.
- Create the regulations for the Artificial Intelligence Governance Model.
- Updated and refresh training, while expanding reach.

2.19.2.3. Governance

At Telefónica, we have a governance model for the management of Personal Data Protection aimed at ensuring effective and efficient management of privacy and that the model is aligned with the Group's strategy.

The person in charge of personal data protection at the Group is the **Global Data Protection Officer**, who reports directly to the Board of Directors of Telefónica, S.A., through the Audit and Control Committee. To ensure compliance with this function, the different corporate areas meet twice yearly as part of the Governance Model Steering Committee, the Business Committee and through the Local Data Protection Officers.

In addition, the Board´s Sustainability and Quality Committee is responsible for promoting and monitoring the implementation of Telefónica's Global Responsible Business Plan, which includes specific targets on privacy. The Board is informed monthly about the implementation of the Plan by the Corporate Sustainability Department, which is run by the Responsible Business Office and includes the heads of the global operational areas.



Board of Directors

Audit and Control Committee
(Permanent Committee of the Board)

Supervises specific issues relating to privacy, among other things, through reports regularly submitted by the Data Protection Officer.

Sustainability and Quality Committee
(Permanent Committee of the Board)

Supervises and reviews the Responsible Business Plan and analyses, drives and supervises the targets, action plans and practices relating to Digital Trust, including issues such as Privacy, Safety, Artificial Intelligence and Child Protection.

Data Protection Officer/Global Data Protection Office

The person responsible for the Company's personal data protection duties, with a dual role (coordinating compliance/data and the technical data protection function).

Steering Committee
(Corporate level)

General Secretary, Chief Data Officer, Technology, Security, Regulation, Compliance, Internal Audit and Sustainability

Entrusted with reviewing the general status of compliance of Telefónica's Privacy Governance model.

Business Committee
(Corporate level)

Corporate business areas

Responsible for directing and coordinating actions aimed at improving compliance with data protection in each of the respective corporate business areas.

Local DPO Forum
(Global level DPOs and local privacy officers)

Responsible for reviewing the compliance status of the Telefónica Group's Privacy Governance Model for each of its operations and any potentially cross-cutting specific data protection problems with regard to these operations are reviewed.

2.19.2.4. Policies

We promote and review different global and local policies, processes and procedures, as depicted in the chart below:

Privacy regulations

Global Privacy Policy

Corporate Rule

Approved by the Board of Directors

Telefónica S.A.

Establishes the mandatory rules for all of the company's entities, in order to create a privacy-focused Company based on the principles of legality, transparency, security, limitation of storage time and commitment to the data subjects rights

Regulation of the Governance Model on Personal Data Protection

Corporate Rule

Approved by the DPO Office Department

Telefónica S.A.

Establishes the strategic, organisational and operational, and management framework applicable to the different actions in the field of data protection.

Regulations Governing Enquiries from the Competent Authorities

Corporate Rule

Approved by the Ethics and Sustainability Department

Telefónica S.A.

Sets out the principles and minimum guidelines that must be referred to in the internal procedures of each of the Group's companies/Business Units/OB to comply with their duty to cooperate with the competent authorities as regards our customers' data.

In addition, we have so-called **'Operational Domains'**, which are privacy procedures defined and implemented throughout the data life cycle and which regulate, among other issues, the recording of processing, risk analysis and impact assessments, international transfers, personal data security breaches, third party management, internal audit plans, training and awareness, data subjects' rights, and data retention and deletion.

2.19.2.5. Risks and opportunities

Rapid technological progress and regulatory dynamics in the field of data protection pose significant challenges in adapting and responding to the evolving changes in the field of privacy. This entails the need to **identify risks, assess and mitigate them** and also to leverage opportunities related to Telefónica's commitment to protecting the privacy of its stakeholders.

Further information on this issue can be found in chapter 3. Risks.

For further information, see chapter 3. Risks.

2.19.2.6. Action plan and commitments

The privacy strategy is based on three pillars:

- **Protection:** protect our customers' personal data through robust policies and processes.
- **Transparency:** be transparent about how and why we collect, use, store and delete our customers' personal data.
- **Empowerment:** empower our customers through simple and secure tools so that they are able control the use of their personal data.

Our main lines of action are:

- Privacy by Design
- Digital privacy
- Transparency initiatives
- Customer empowerment
- Consultation and complaint mechanisms
- Binding Corporate Rules
- Monitoring and training of suppliers

> Privacy by Design

The principle of **Privacy by Design** is one of Telefónica Group's key strategic pillars and is defined in our mandatory internal regulations.

The concept of Privacy by Design entails the obligation of the whole organisation to establish, in the design of products and services, procedures that primarily take into account two aspects: first, the implementation of privacy protection measures from a legal and security point of view in the early stages of any project; and, secondly, that all business processes and practices involved in each activity or processing that may affect personal data are covered.

We have our own Privacy by Design guidelines to define the set of rules, standards and legal and security processes that must be taken into account to comply with our **Global Privacy Policy.** All of this is to ensure that the rights and freedoms of individual´s personal data are guaranteed as from the initial definition of any processing project or activity.

These practical guidelines stand as reference documents for the Group's professionals in charge of developing and implementing products and services, as well as for internal use cases that directly or indirectly involve the processing of personal data.

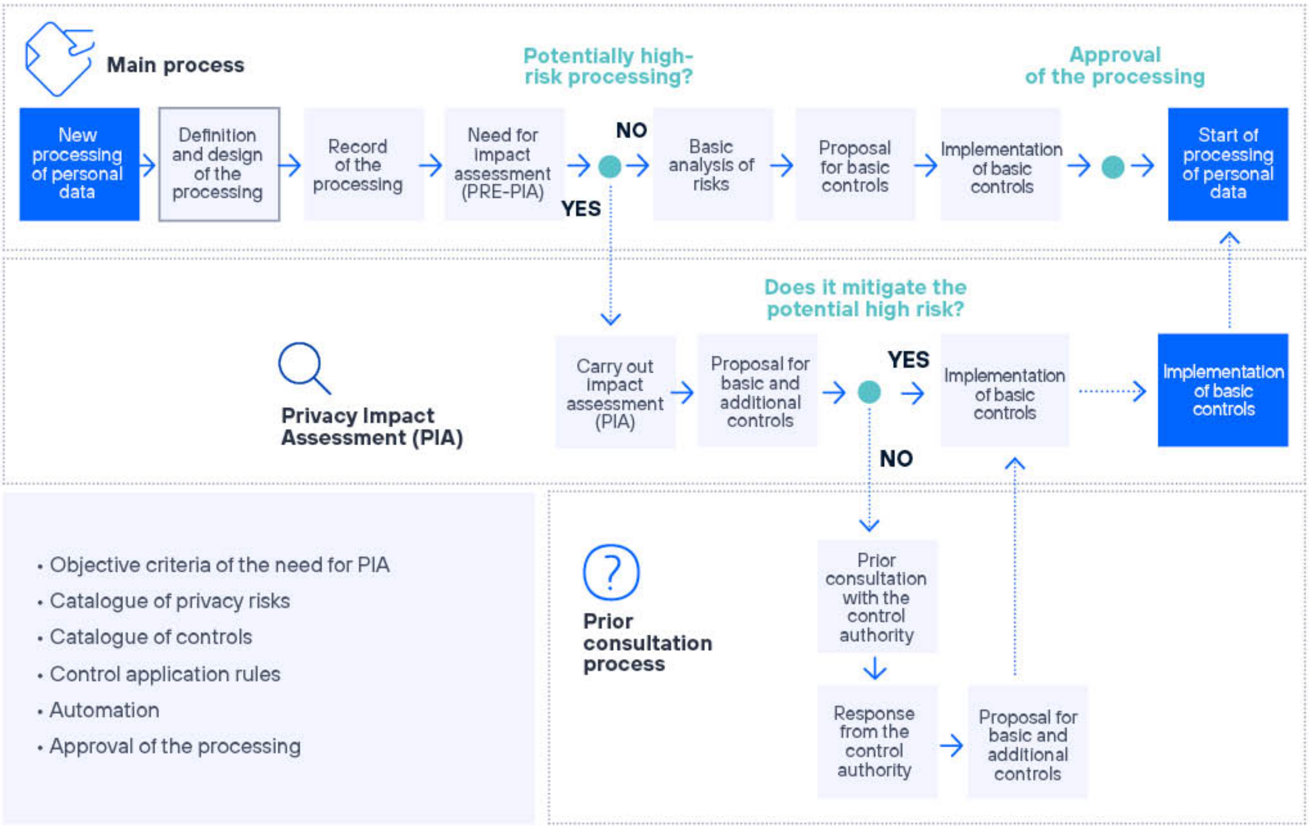
In addition, product managers are supported by the privacy and security specialists in the area of each company and/or business unit of the Group, in order to ensure that all the necessary privacy-related legal and security requirements are taken into account from the start of relevant projects.

We use a **risk management-oriented approach of proactive responsibility** (critical and continuous self-analysis in the fulfilment of the obligations required by the regulations) to establish strategies for each product or service that incorporate privacy throughout the entire data life cycle: collection and obtaining, processing, exercise of rights, and retention and deletion.

When defining or developing any product or service, the practical application of Privacy by Design involves aspects such as: the lawfulness and definition of the grounds legitimising the processing; the guarantee that the data is secure and that the most appropriate security measures are being applied according to the potential risks; transparency in the privacy clauses and policies; the **minimisation of data** in that it must be strictly necessary for the purposes of processing; the commitment to the data subjects' rights; and the limitation of the period of retention, among others.

The Privacy by Design process that was defined by the Telefónica Group's Global Data Protection Office includes the following activities:

Privacy by design process


Main process
Potentially high-risk processing?
Approval of the processing
New processing of personal data
Definition and design of the processing
Record of the processing
Need for impact assessment (PRE-PIA)
NO
YES
Basic analysis of risks
Proposal for basic controls
Implementation of basic controls
Start of processing of personal data
Does it mitigate the potential high risk?
Privacy Impact Assessment (PIA)
Carry out impact assessment (PIA)
Proposal for basic and additional controls
YES
Implementation of basic controls
Implementation of basic controls
NO
• Objective criteria of the need for PIA
• Catalogue of privacy risks
• Catalogue of controls
• Control application rules
• Automation
• Approval of the processing
Prior consultation process
Prior consultation with the control authority
Response from the control authority
Proposal for basic and additional controls

For further information, see chapter 2.13. Sustainable innovation.

Digitalisation of Privacy by Design (Digital Privacy Framework– DPF)

The DPF is Telefonica´s framework for the global legal and privacy strategy with respect to the General Data Protection Regulation (GDPR) and the ePrivacy regulation on data processing platform products and systems.

In the DPF we adapt the privacy legal compliance guidelines to a technological reality to standardize and conceptualize the functional and technical requirements of the dynamics of privacy systems, and apply them automatically and digitally in the processing of personal data.

This digitilisation is implemented from design, and naturally enables a dynamic and automatic privacy process to be built between the customer and the systems to carry out the processing of personal information and compliance with the GDPR.

We are implementing this digitalisation framework in our systems and platforms where data processing takes place, for example, in Kernel,Telefónica's big data platform. The Digital Privacy Framework made significant progress in Spain during 2022 and will continue to do so during 2023 in operators with more demanding data protection jurisdictions, for example, with respect to anonymisation requirements.

> Transparency initiatives

At Telefónica, we make privacy more human and understandable by **focusing our design principles on people** (human-centred design). In this regard, we are committed to putting transparency into practice by including it as one of the principles of the Global Privacy Policy and developing different initiatives to implement this principle:

Global Privacy Centre

The Global Privacy Centre is a public reference point for our policy and processes. Available at www.telefonica.com, our stakeholders can find all the information they need easily and in a simple format by means of visual and graphic resources. Our objective during 2023 is to continue improving on this centralized channel including linking all of the Groups Transparency centres to present all the relevant information centrally.

Operators' Privacy and Security Centres

The purpose of these centres is to enable both our customers and any stakeholders to obtain information, in a simple, digital and understandable way, with regards to the processing of their personal data and other relevant information on privacy and security matters. The Information available includes data on channels and avenues to excercise rights, the security and confidentiality measures adopted to process data, the privacy terms and conditions applicable to our products and services, transparency reports and our Artificial Intelligence principles, as well as the **child security and protection** issues that apply in each case in digital environments.

The Privacy and Security Centres are currently available on the websites of all the operators. They are updated regularly in accordance with regulation and stakeholder analysis,

The **Transparency Centre** has also been launched on for our **content platform, Movistar+.** The service is available through the Mi Movistar section and allows customers control their data.

Telecommunications Transparency Report

We publish an annual report on the requests we receive from the competent authorities in the countries where we operate. This report includes information on the number of requests for lawful interception, access to metadata associated with communications, content blocking and restriction, and geographical and temporary suspension of service.

We follow a strict procedure for any request, which is laid down in the Regulations on Requests from Competent Authorities. This guarantees, in equal measure, the fulfilment of our obligations in terms of collaboration with these authorities and the **protection of the fundamental rights** of the people affected, in accordance with our commitment to respect for human rights.

For further information, see chapter 2.15. Human Rights.

In 2022, a total of 3,761,918 requests for customer information from competent authorities (lawful interception and access to metadata) were recorded. Of these applications, 230,226 were rejected, which was 94% of the requests dealt with. The number of accesses/customers affected was 4,003,851.

> Customer empowerment

As part of the principle of transparency, Telefónica provides customers with access to the data they generate during the use of our products and services, data that are collected in the so-called 'Personal Data Space' of Kernel and which are accessible through different channels.

The **Transparency Centre** in Spain, which offers all customers access to their privacy preferences and management of the data collected in the 'Personal Data Space', is currently available to a group of users through the Mi Movistar app (in the Security and Privacy section of the User Profile) and has been available through the television channel in Spain since 2022.

In the Transparency Centre, through the Privacy Permissions section, customers can manage the legitimising grounds relating to the use of their data for certain purposes. In addition, the Access and Download section includes useful views of different types of data, with a user-friendly experience, in compliance with privacy criteria; there is also the option of downloading a more detailed document.

The Transparency Centre experience has been designed to **give users confidence,** with clear language, explaining the purpose for which their data is processed and its nature within Telefónica.

The Transparency Centre represents the first steps towards fulfilling our promise to give our customers features for them to control and ensure the transparency of their data, albeit in accordance with applicable regulations on privacy. For example, in Europe this processing will be fully aligned with the GDPR.

> Consultation and complaint mechanisms

Besides the mechanisms established in the privacy policies and privacy centres, Telefónica has implemented other consultation and mediation methods to deal with any incidents in this area:

Responsible Business Channel

We have a public channel on our website where all our stakeholders can enquire or complain about any aspect related to the Responsible Business Principles. In 2022, 30 communications on privacy and 0 on freedom of expression were processed.

Voluntary mediation system with AUTOCONTROL
This system has been operational since January 2018, and is designed to provide a swift response to complaints related to **identity theft and the receipt of unsolicited advertising**. The procedure was developed by the *Asociación para la Autorregulación de la Comunicación Comercial* (AUTOCONTROL) in collaboration with the Spanish Data Protection Agency (AEPD). It also involves the participation of Orange, Telefónica and Vodafone, and is open to other entities. This information can be found in the Movistar Privacy Centre. In 2022, 227 requests for mediation were processed.

> Binding Corporate Rules

Binding Corporate Rules (BCRs) are designed to permit the international movement of data within the Telefónica Group in accordance with article 47 of the GDPR, in particular the data from the European Economic Area (EEA) to countries outside the EEA.

The implementation of the BCRs will foster an improvement in compliance with the European regulations throughout the Telefónica Group, by enabling Telefónica to transfer personal data swiftly regardless of the place where the recipient Telefónica subsidiary is located.

In addition, the BCRs will provide more legal certainty by facilitating the alignment with the Group's organisational model.

In 2022, Telefónica began the process of approving its BCRs and has followed the following steps:

- Analysis of international intra-group transfers.
- Drafting of Binding Corporate Rules.
- Designation of the AEPD as the lead supervisory authority, responsible for leading the process, as well as the interested supervisory authorities for cooperation in the approval procedure, following a proposal by Telefónica.
- Sending the BCRs and complementary documentation to the lead authority for approval.

> Management of our supply chain

One of Telefónica's priorities in ensuring privacy is successful management of the supply chain in relation to the processing of personal data by third-party contractors. To this end, we have incorporated common data protection agreeements across the whole Group and included specific commitments asssumed by suppliers with regards to international transfers. .

In 2022, a series of automated control measures were implemented to ensure successful processing of personal data before, during and after the provision of the service by the supplier. Additionally, to ensure protection of personal data managed by third parties, automated mechanisms were developed to enable the optimisation of training initiatives.

2.19.2.7. Progress in 2022

Telefónica has developed an internal tool to facilitate compliance at the Group with the data protection regulations and, in particular, in order for each area to perform the following tasks, among others: creating the Record of Processing Activities (ROPA) and keeping it updated; management and recording of security breaches; recording requests to exercise GDPR data subject rights; management of electronic signatures of data protection agreements (DPAs); and management of privacy indicators.

Proof of our progress in terms of privacy and freedom of expression is that in 2022, and for the third consecutive year, we were first among all telecommunications companies in the Ranking Digital Rights (RDR). This ranking assesses corporate commitments, policies and practices that affect freedom of expression and customer privacy, including governance and oversight mechanisms.

2.19.3. Security

2.19.3.1. Vision

Security aims to protect against potential damage to people and property, and to guarantee the confidentiality, integrity and availability of the Company's information assets.

At Telefónica, security is approached as an **integral concept** which includes physical and operational security (of people and goods), digital security (encompassing information security and cybersecurity), business continuity and fraud.

The increase in the number, complexity and type of threats makes it necessary to apply security measures and review them in a **cycle of continuous improvement**. Our strategy is based on a number of security activities that reinforce both the Company's processes and its transformation initiatives, compromising a security management system in line with international reference frameworks and standards such as **ISO 27001 and NIST (National Institute of Standards and Technology)**

2.19.3.2. Targets

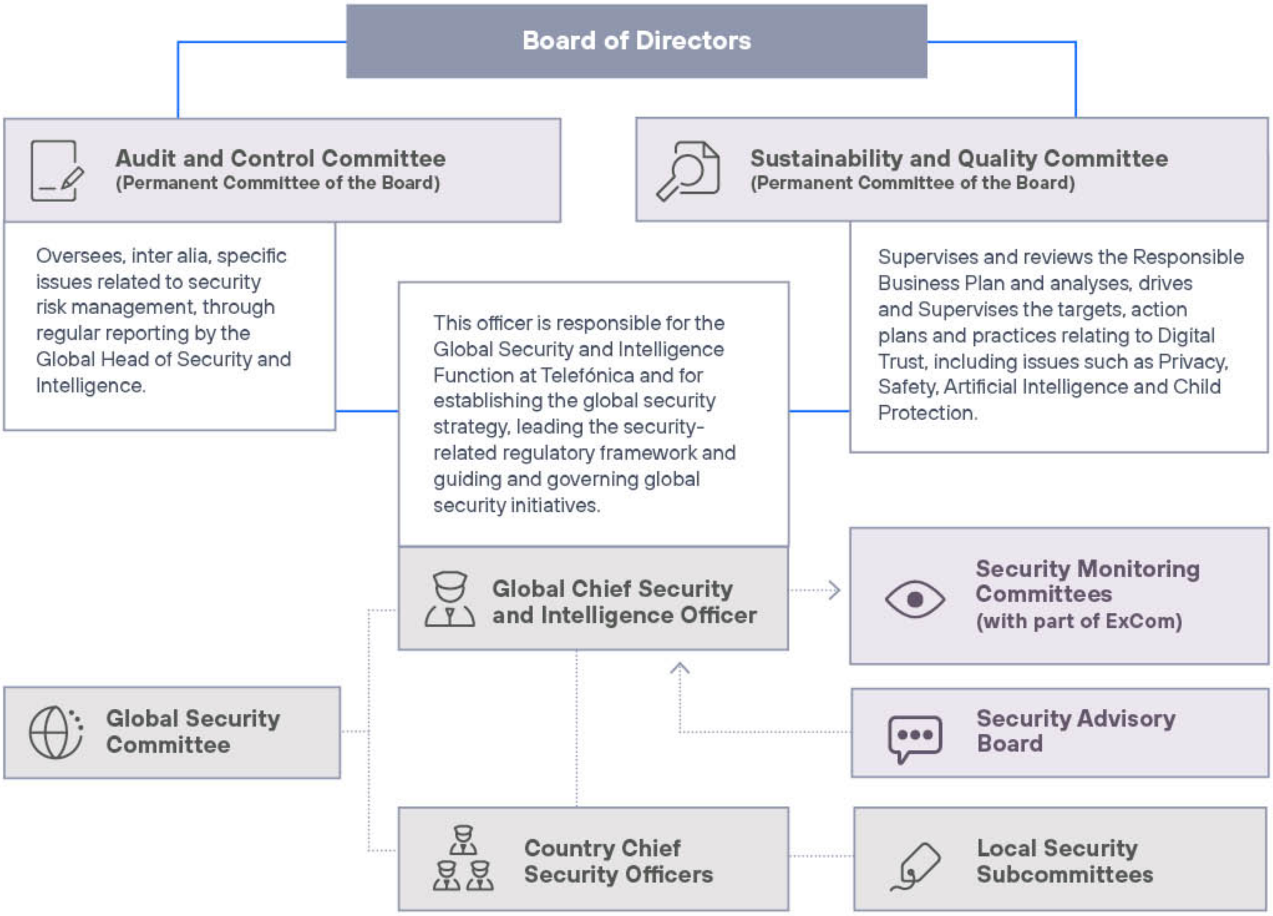
In the short and long term, the targets we have set are to:

- Review the global regulatory framework on security to align it with new versions of international standards, such as ISO 27001.

- Move forward in deploying the Zero Trust[1] model to control IT system access and implement tools to govern the security of cloud environments.
- Increase the percentage of contracts/RFPs that contain security requirements for the supply chain, with the goal of reaching at least 95% of suppliers by 2025.

2.19.3.3. Governance

The global Security and Intelligence Area has the backing of the Company's management and reports to the Board of Directors through the Sustainability and Quality Committee and the Audit and Control Committee. It also coordinates with the local security departments, as shown in the following diagram:



Board of Directors

Audit and Control Committee (Permanent Committee of the Board)

Oversees, inter alia, specific issues related to security risk management, through regular reporting by the Global Head of Security and Intelligence.

Sustainability and Quality Committee (Permanent Committee of the Board)

Supervises and reviews the Responsible Business Plan and analyses, drives and Supervises the targets, action plans and practices relating to Digital Trust, including issues such as Privacy, Safety, Artificial Intelligence and Child Protection.

This officer is responsible for the Global Security and Intelligence Function at Telefónica and for establishing the global security strategy, leading the security-related regulatory framework and guiding and governing global security initiatives.

Global Chief Security and Intelligence Officer

Security Monitoring Committees (with part of ExCom)

Global Security Committee

Security Advisory Board

Country Chief Security Officers

Local Security Subcommittees

The head of security at the Company is the **Global Chief Security and Intelligence Officer (the Global CSO)**, who has been delegated, by the Company's Board of Directors, the authority and responsibility to establish the global security strategy. **The Global CSO leads, monitors and supervises** implementation of the policy framework and that of the global initiatives. The Global CSO nominates a local security manager at each Telefónica Group company. The nominations are submitted for a decision from the corresponding company's management bodies.

The Global Security Committee coordinates and governs activities. The Committee is and is chaired by the Global Director of Security and Intelligence. The local Chief Security Officers **(local CSOs)** and the corporate heads of different areas of the Company (Compliance, Audit, Legal, Technology and Operations, People, Sustainability, etc.) are committee members.

There are also local security sub-committees chaired by the local CSOs, which take part in defining strategic initiatives and global guidelines and implement them in each Telefónica Group company.

In addition, the Global Security and Intelligence Area promotes and drives the Global Digital Security Committee in which several members of the Company's Executive Committee participate.

[1] Zero Trust is a security strategy applied to access to information, which will be provided through "minimum privilege" control techniques. It will be end-to-end encrypted and guided by the principle of "never trust, always verify".

The Global Security and Intelligence Area reports to the Board of Directors through the Sustainability and Quality Committee and the Audit and Control Committee.

Telefónica also has a **Security Advisory Board** made up of major figures from outside the Company, in the field of security and intelligence, with the aim of contributing best practices, increasing the efficiency of capabilities and procedures, and enhancing the quality of our strategy in this area.

2.19.3.4. Policies

At Telefónica we foster regulatory security policies that are **mandatory for all Group companies**. All the documents are reviewed and updated as a result of a cycle of continuous improvement. In these reviews, account is taken of periodic measurements and audits of security activities, changes in context and newly-identified risks, as reflected in the following diagram:

Security regulations

Governance
Security Committees

Global policy

Global Security Policy

Governed by national and international standards and regulations on physical and digital security and lays down the guiding principles applicable to all the companies that make up the Group.
Updated and approved by the Board of Directors of Telefónica in 2021.

Global rules

Global Security Regulations

Develops the principles and general guidelines of the Global Security Policy, establishes rules of conduct and general responsibilities, and refers to global regulations on different subjects.
Updated in 2022 by the Secretary of the Board, it includes alignment with the global policy, review of obligations and responsibilities, and global and local security departments.

Global regulations

- Management of Incidents and Emergencies
- Analysis of Security Risks
- Business Continuity
- Security in the Development Life Cycle
- Security in the IT Infrastructure
- Security in Networks and Communications
- Cybersecurity
- Security in Change Management
- Classification and Processing of Information
- Security in Asset Management
- Access Control
- Physical Security
- People's Safety
- Prevention and Management of Fraud in Telecommunications
- Security in the Supply Chain
- Governance of Security

These establish the controls necessary to guarantee security in each specific domain. Based on the provisions of the global regulations, local procedures and documents are generated which contain the details of the actions to be performed to ensure compliance with the security controls.
In 2022, a review of eight regulations was approved, with a range of updates.

Security activities

Monitoring and measuring (security Indicators)
Audit and Control

Changes in context and new risks

Continuous improvement

In certain domains, including products and services, official certifications are held such as **ISO 27000, PCI-DSS, and national security system (ENS)** certifications in applicable countries. The decision to obtain certification is based on legal compliance, business requirements or customer demands. In turn, depending on the service provided, we require third-party certification or reports from our suppliers (for example, ISAE 3402 or similar).

2.19.3.5. Risks and opportunities

Information technology is an important element of our business and is exposed to **cybersecurity risks**. For this reason, it is included in the Company's basic risk map, which defines guidelines to facilitate uniform reporting, alignment with business objectives and corporate risk tolerance criteria.

For further information, see chapter 3. Risks.

2.19.3.6. Action plan and commitments

At Telefónica, we understand security as a comprehensive concept aiming to protect our **assets, interests and strategic objectives**, ensuring their integrity, and protecting them from potential threats that could damage their value, affect their confidentiality, reduce their effectiveness or alter their operability and availability.

Comprehensive security encompasses:

- Physical and operational security (of people and assets)
- Digital security
- Business continuity
- Fraud prevention
- Any other relevant area or function aimed at corporate protection against potential damage or loss.

In turn, the concept of digital security integrates aspects related to information security and cybersecurity and is applied to the media, systems, and technologies and elements that make up the network.

Our security provisions apply to all the entities involved in the supply chain, focusing especially on companies that manage data of the Telefónica Group or its customers.

Security activities are governed by the **principles of legality, efficiency, co-responsibility, cooperation and coordination**.

The most recent review of the Company's Global Strategic Security Plan, approved by the Global Security Committee on 28 September 2022, pursues the implementation of the basic principles laid down in the Security Policy and identifies and prioritises the main lines of action.

> Digital security or cybersecurity

Digital security is a key element of our business. Its ultimate goal is to **ensure our resilience**, in other words, the ability to withstand and contain attacks so that our business is not affected or is affected to a degree that is tolerable. This is put into practice in processes, tools and capabilities that aim to anticipate and prevent cybersecurity risks.

The activities in this respect are coordinated by the global area with the various digital security units of the Group's companies. We hold annual meetings with the digital security teams of all Telefónica units in order to align strategies and share experiences.

We have a public mailbox for reporting weaknesses or threats and a bug-bounty program consisting of rewards for finding them.

Particular emphasis is placed on the following aspects:

Cyber-intelligence and incident management

We have tools and capabilities for the entire cycle of potential incidents:

- **Anticipation**, before they can impact the Company.
- **Prevention**, ensuring the protection of both facilities and assets, as well as customer data and identities.
- **Detection and response,** through a network of 17 Incident Response Centres (Cybersecurity Incident Response Teams, CSIRTs)

Our approach to cyber-intelligence is proactive, applying knowledge and technology to achieve the required levels of protection by quickly detecting breaches or attacks on assets. We also build the technical and human capabilities needed to **respond effectively and quickly** to any breach or incident in order to minimise attacks and their consequences.

We have a **public mailbox**, available to all , so that bugs or threats that could affect Telefónica's technological infrastructure can be reported. This mailbox can be found on Telefónica's global website and on those of its operators in the Global Privacy Centre/Security section. We also have a **bug-bounty reward program**, managed by selected companies acknowledged as industry leaders, enabling us to rely on input from cybersecurity experts (ethical hackers) worldwide.

The CSIRTs work in a coordinated manner to understand and analyse the risks of potential cyber-threats, monitor serious bugs in the most critical technological assets and establish relationships with other national and international CSIRTs/Computer Emergency Response Teams (CERTs) in the public and private sectors. Cyber-exercises are performed once a year to train the CSIRTs in all the countries in handling potential incidents.

During 2022, 2 **significant security incidents** were dealt with (we consider significant incidents to be those that meet certain criteria at a global level, such as their economic, legal, service, or media impact). The 2 incidents affected customer data. One occurred in Telefónica Peru and the other in Telefónica Spain. Neither of the incidents had a sufficiently material impact to be reported to the financial market supervisory authorities.

Lessons learned from incidents help us to improve the security of both processes and technological capabilities and platforms.

We followed the transparency protocols, notifying the affected users and, where appropriate, the data protection agencies of the incidents. Incident management protocols are also followed in terms of detection, analysis and response, establishing the appropriate mitigation measures.

The Company has various **insurance programs and coverages** in place that could mitigate the impact on the income statement and balance sheet of the materialisation of a large number of risks. In particular, there is cover for cyber-risks that could cause a loss of income, loss of customers, extra costs or recovery costs for digital assets, among others, and cover for Technological Errors and Omissions in the event of claims for damages to customers and third parties in general. The current global insurance limits range in value from €100 million to €500 million.

> Network security

Our approach to networks and communications is based on a good understanding of our assets and sites, as well as their characteristics and their importance for the business. The aim is for the networks to be properly planned and deployed in keeping with applicable security requirements that minimise the risk of downtimes, unauthorised access or destruction.

We also perform security controls on associated service platforms, such as video and the Internet of Things (IoT), to manage the risks associated with attacks and the exploitation of bugs and weaknesses in networks and protocols. To this end, we work with technological partners and international organisations (for example, GSMA). Examples can be found in the work done on 4G/LTE, SS7, BGP, and other critical-enabling technologies.

At Telefónica, we want to contribute to making 5G networks safe. The Company's technological developments in this area, such as the evolution of our network virtualisation platform (UNICA NEXT), network splitting, and new radio access technologies, take into account Security by Design.

> Physical and operational security

At Telefónica, we make a continuous effort to improve our capabilities for the physical protection of infrastructure and assets. Among the programs we develop, the following stand out:

- The interconnection of control centres to create a resilient network that reinforces the availability of infrastructure for surveillance and protection services.
- The management of travel security for Telefónica personnel, which substantially improves response time and the mechanisms for action in the event of any incident.
- The implementation of consistent digital procedures and tools for global security monitoring.

> Security by Design

Security is considered at the earliest stages in all areas of activity to ensure that it is an **integral part of the entire technology life cycle**. This approach is based on the following aspects:

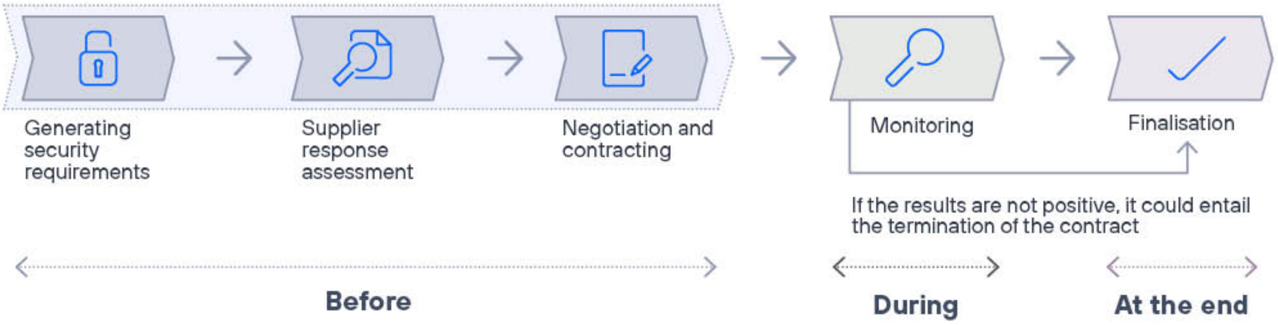
- The risk analysis and management process.
- Commitment to innovation, including the development of proprietary technologies.
- Raising employee awareness.
- The security requirements demanded of our supply chain.

In this way, the security requirements are a consideration from the design phase of applications and systems, incorporating controls against known bugs, and ensuring that there are no security weaknesses at source. This results in systems and applications that are more resistant to malicious attacks.

> Supply chain security

At Telefónica, we have security requirements for our suppliers and we identify the risks associated with the provision of a service/product. We continue to develop **3PS+**, our security process digitalisation tool in the supply chain. Its main characteristics are as follows:

Supply chain security process


Generating security requirements
Supplier response assessment
Negotiation and contracting
Monitoring
Finalisation
If the results are not positive, it could entail the termination of the contract
Before
During
At the end

- **Prior to contracting**, the application makes it possible to generate the security requirements for new procurement processes. It incorporates the responses given by suppliers, providing objective assessments about compliance levels and access to the mitigation measures proposed by the suppliers.
- **During the provision of the service**, it offers the possibility of monitoring the security requirements. To this end, the system generates alerts based on the start date of the service and the selected monitoring period. This allows the user to record relevant information that may pose a risk to Telefónica's processes.
- **On completing the provision of the service**, it is possible to control how the removal of the supplier is executed and to mitigate or even avoid the most common security risks at service termination: failure to block physical and logical access, failure to check VPNs/ports/systems used for services, etc.

All Telefónica Group employees have access to this tool.

> Business continuity and crisis management

The business continuity function integrates various activities and processes aimed at improving our resilience, and crisis management makes it possible to tackle any serious incident that affects the organisation in an effective manner.

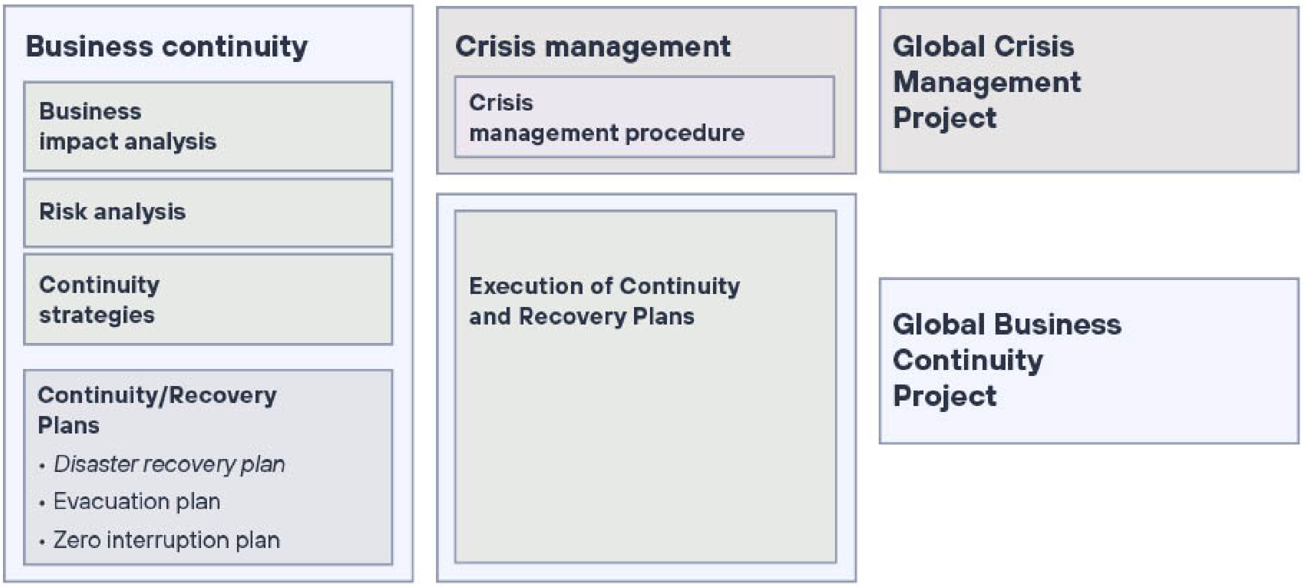
In the event of a crisis, the priorities are:

- **Protect people**, ensuring the well-being of employees and collaborators.
- **Provide the agreed services** to our customers, with the agreed availability and quality.
- **Protect and look after the interests** of our shareholders and institutional investors.
- **Comply with our** regulatory and legal **obligations**.
- **Protect and secure business** from a sustainability point of view.

The business continuity function is included in the Global Security Policy. The details are defined in the Global Business Continuity Regulation and in a range of documentation, both globally and locally, for each business unit.

The Global Crisis Management Plan, which is made up of the Global Crisis Management Project and the Global Business Continuity Project, is part of the Strategic Plan of the Global Security and Intelligence Directorate. For the execution of the crisis management plan, the processes of each of the areas are identified, detecting scenarios that could lead to their interruption; potential treatment plans are considered; the business continuity strategies to be applied are decided; and, if necessary, business continuity plans are generated with the appropriate actions to be taken.

Global Crisis Management Plan


Business continuity
Business impact analysis
Risk analysis
Continuity strategies
Continuity/Recovery Plans
· *Disaster recovery plan*
· Evacuation plan
· Zero interruption plan
Crisis management
Crisis management procedure
Execution of Continuity and Recovery Plans
Global Crisis Management Project
Global Business Continuity Project

Our strategy is evolving by strengthening the following aspects:

- **Strategic vision:** global threats require global action. Having a strategic vision of business continuity enables global decisions to be taken that result in greater resilience.
- **Effectiveness in crisis management:** we have a proven crisis management model, common to the entire Company, both in its definitions and in the execution of its procedures.
- **Coordination and collaboration:** the organisational model guarantees, aligns and promotes the homogeneous development of business continuity in the various business units.
- **Standardisation of measurement:** this allows us to measure, without bias, various indicators that show us the degree of maturity from the business continuity point of view and the level of resilience of the Company. It also provides us with the necessary information to be able to establish medium and long-term objectives.

This is based on international standards such as ISO 22301 for business continuity management and ISO 22320 for emergency management.

Each year, several global and local exercises are conducted to check the business continuity mechanisms, simulate crisis scenarios and identify opportunities for improvement with regard to real incidents.

> Governance model

The **Global Business Continuity Committee,** the highest governance body, defines the global strategy from design, as well as the prioritisation and availability of the necessary resources.

The **local business continuity committees,** the bodies responsible for ensuring business continuity in each business unit, guarantee the implementation of the strategic decisions taken at global level and transfer the needs, achievements and maturity indicators that allow a holistic view of business continuity in the Company.

The committees, whether at global or local level, prioritise and focus the resources where they can generate the greatest impact and value for the Company, based on:

- Strategic services.
- Strategic projects.
- Strategic suppliers.
- Organisational aspects.

Each business unit has its own **Local Business Continuity Office (LBCO)**, and all local offices are aligned and coordinated through the **Global Business Continuity Office (GBCO)**. The GBCO is functionally located in the Global Security and Intelligence Directorate, which is part of the Company's corporate area. It coordinates the LBCOs and transfers the various strategic decisions defined by the Global Business Continuity Committee.

> Global Business Continuity Program

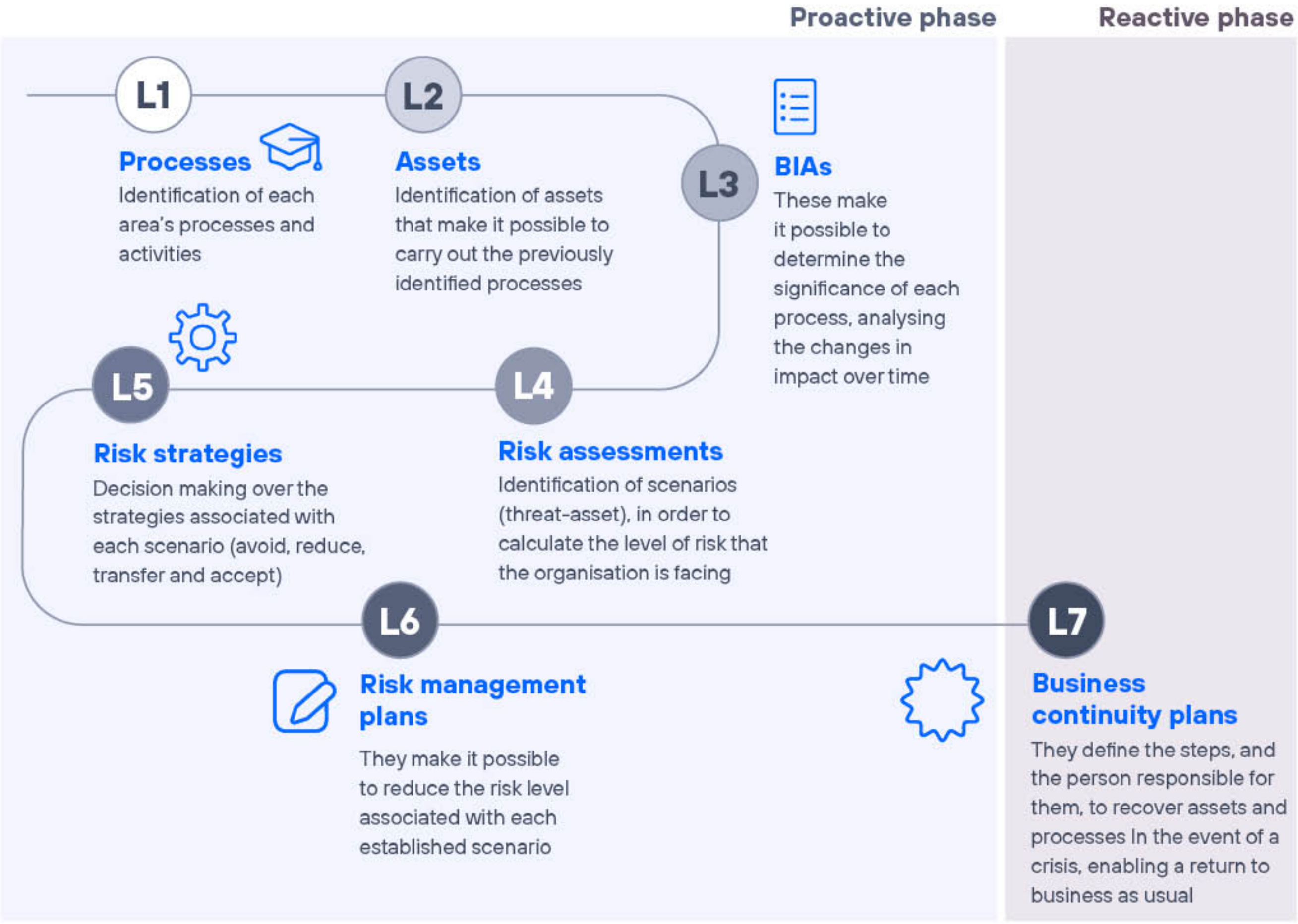
Our **Global Business Continuity Program** is aligned with the standard ISO 22301 and is made up of the following phases:

1. **Planning:** a Statement of Work (SoW) detailing the scope of business continuity and an annual activities plan.

2. **Implementation and operation:** deliverables aimed at establishing and documenting the business continuity mechanisms such as a Business Impact Analysis (BIA) identifying the major processes and services, risk analysis, continuity plans, return to normality plans, etc.
3. **Monitoring and evaluation:** assessment of the effectiveness of the business continuity arrangements in place by testing them in realistic and bounded scenarios. Indicators are available to assess the performance, maturity level and implementation of the overall business continuity project.
4. **Maintenance and improvement:** encompassing lessons learned and opportunities for improvement from business continuity testing and crisis simulation, the execution of the continuous improvement process for business continuity management, training and awareness raising.

The LBCOs are responsible for ensuring and driving the proper implementation of the business continuity management process, which starts with the identification of processes/services. The process is shown in the following image:

Business continuity management system

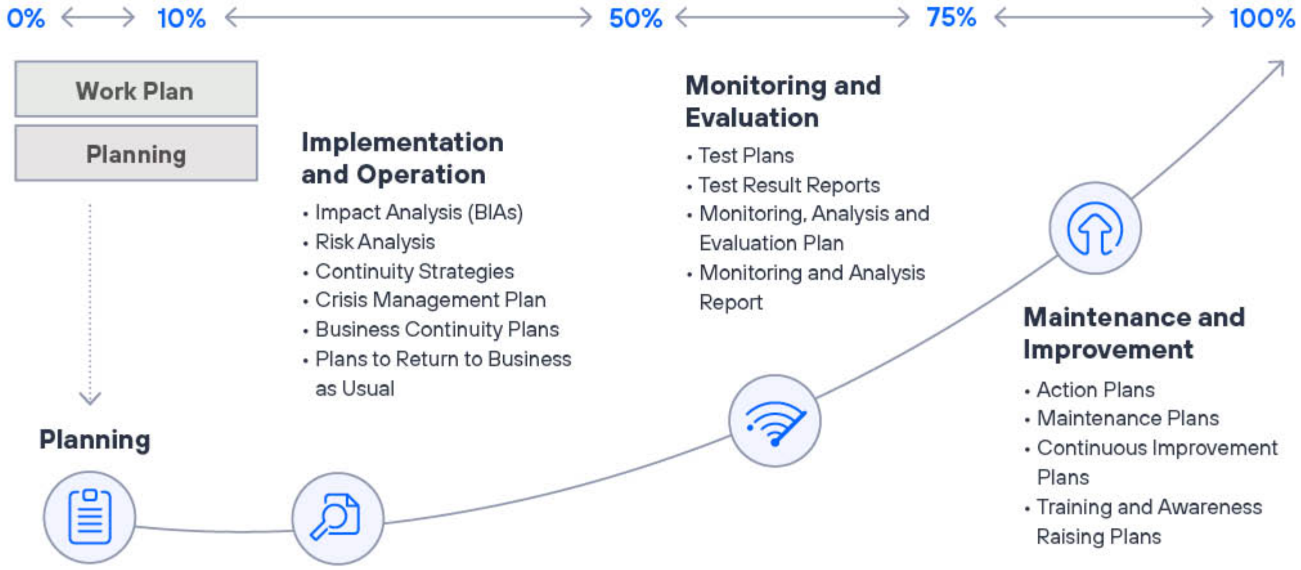


Proactive phase
Reactive phase
L1
Processes
Identification of each area's processes and activities
L2
Assets
Identification of assets that make it possible to carry out the previously identified processes
L3
BIAs
These make it possible to determine the significance of each process, analysing the changes in impact over time
L4
Risk assessments
Identification of scenarios (threat-asset), in order to calculate the level of risk that the organisation is facing
L5
Risk strategies
Decision making over the strategies associated with each scenario (avoid, reduce, transfer and accept)
L6
Risk management plans
They make it possible to reduce the risk level associated with each established scenario
L7
Business continuity plans
They define the steps, and the person responsible for them, to recover assets and processes In the event of a crisis, enabling a return to business as usual

> Business continuity maturity monitoring

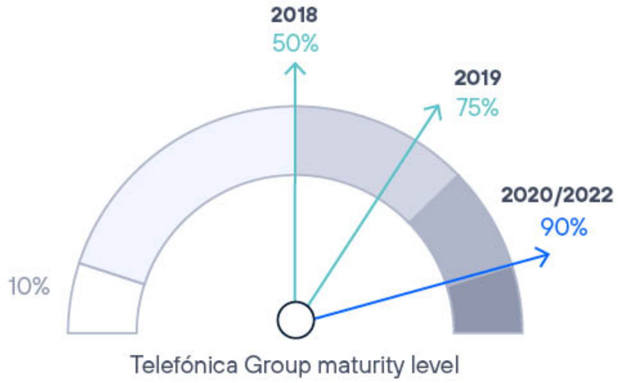
In order to have a homogeneous process for measurement of the correct execution of the management process by the LBCOs, the 'degree of maturity' has been defined.

Business continuity maturity model


0%
10%
50%
75%
100%
Work Plan
Planning
Planning
Implementation and Operation
• Impact Analysis (BIAs)
• Risk Analysis
• Continuity Strategies
• Crisis Management Plan
• Business Continuity Plans
• Plans to Return to Business as Usual
Monitoring and Evaluation
• Test Plans
• Test Result Reports
• Monitoring, Analysis and Evaluation Plan
• Monitoring and Analysis Report
Maintenance and Improvement
• Action Plans
• Maintenance Plans
• Continuous Improvement Plans
• Training and Awareness Raising Plans

Over the past years, we have reached and maintained an 'optimised' maturity level. This means that we have established, tested and gained lessons learned on the defined business continuity mechanisms:

Evolution of the degree of maturity



> Crisis management

The Global Crisis Management Project includes all aspects related to the successful coordination and management by senior management of events that could have a major impact on the Company, and which have to be treated as a crisis.

The structure contains four layers.

1. The first layer defines and classifies the crises, their typology and the general strategy for dealing with them.

2. The second layer defines the roles, responsibilities, means and channels involved in crisis management, as well as the relationship and responsibilities between crisis committees.

3. The third layer groups together the procedures, plans and documentation necessary to manage crises.

4. The fourth layer defines, on a global basis, the architecture of warning systems, secure communication and, in general, the aspects related to digitalisation that support the activities of the different crisis committees.

Layers of Crisis Management

Crisis

- Definition
- Classification (Local, Regional, Global)
- Overall strategy

Crisis Committee

- Chairman
- Members and boards
- Media and channels

Procedures

- Crisis response procedures
- Business continuity drills/plans
- Communication plans

Architecture

- Alert system
- Secure communication system
- Crisis committee support system

The global crisis management project provides additional and complementary mechanisms to business continuity, making it possible to manage incidents with a broad impact on the Company.

Three types of crises are described as part of the model:

- **Local crisis:** confined to one organisation or business unit in one country.
- **Regional crisis:** confined to several countries belonging to the same geographical region.
- **Global crisis:** confined to several companies or business units of the Telefónica Group in more than one country and geographical region.

Depending on the type of crisis, there are active protocols and means of alert, notification, management and coordination, which are known to all those involved in the overall Crisis Management Project.

The main role in this management process is played by the members of the crisis committee, at global or local level. There is a differentiation between permanent members who participate in any activation, ad hoc members who participate depending on the typology of the crisis, and working groups or task forces to support these members.

The **Global Crisis Management Project** enables us to:

- Accelerate the decision-making process.
- Manage any crisis as a unit.
- Centralise the receipt of information.
- Act as a unified tactical and decision-making figure.
- Decide how to act based on the crisis scenario faced, building on the business continuity aspects worked on previously.
- Reliably transmit information about what has happened to customers, authorities, organisations or any other stakeholders.

Finally, it defines the obligation to conduct **tests and drills** on different scenarios potentially harmful to the Company. The drills will be carried out at least once every six months, unless a crisis situation is declared in the same period. This makes it possible to:

- Evaluate reactions to particular circumstances.
- Evaluate the preparation of documentation supporting the crisis management activity.
- Evaluate coordination mechanisms.
- Prepare crisis committee members to act.

The events discussed by the crisis committee are detailed below:

Events discussed by the crisis committee

GLOBAL – MONITORING CRISIS, COVID-19 – January to March 2022	
Description	**COVID-19**
Type of crisis	Health and Safety
Impact	Monitoring of the development and level of impact of COVID-19 on the employees of the Telefónica Group at a global level, as well as the level of impact on the in-person presence of employees at Telefónica facilities and the opening levels of the Company's stores.
Actions	Monitoring of COVID-19 in each country, showing that although there was an increase in cases after Christmas, it was a lot less serious; therefore, in March it was decided not to continue regular monitoring, the situation being kept open to observe developments. The recommendation of wearing masks at Telefónica was upheld until September, thereby avoiding possible increases in infection levels among the workforce. In December, the incident was closed.

GLOBAL – UKRAINE– March to June 2022	
Description	**Conflict between Ukraine and Russia**
Type of crisis	Political-social
Impact	Monitoring of the development and level of impact of the conflict on the Telefónica Group's activities at a global level and its employees, as well as the level of impact on the countries where it operates.
Actions	The crisis committee was activated on 7 March 2022. Monitoring of the conflict, with the aim of analysing different scenarios that could affect the Telefónica Group. The various local crisis committees were involved so as to obtain information about the impact in their countries. In June, the crisis committee was wound up as there were no changes in the impact, while continuing to monitor the situation. In December, the incident was closed.

BRAZIL (LOCAL) March 2022	
Description	**Unavailability of access to VPN**
Type of crisis	Technological
Impact	Affecting approximately 60% of the customer care service level, due to it being impossible for employees and collaborators working remotely to connect and perform that service. The duration of the incident was 1 hour and 15 minutes, and it had no economic impact.
Actions	The committee was activated on 8 March 2022. The VPN IP was gradually restored by the technical teams, with the supplier of the solution service providing support. As part of the work, the configuration and updating parameters of technical components were corrected.

ECUADOR (LOCAL) June 2022	
Description	**Public demonstrations**
Type of crisis	Political-social
Impact	Services to customers were not affected, but there were financial losses due to the commercial impact and impact on sales. In some cases, customer services at offices had to be restricted.
Actions	The crisis committee was activated on 20 June 2022. The physical security and monitoring levels at technical sites/stations were reinforced. In addition, where possible, remote working was put in place. The main concerns were the impact on people's safety, the impact on the preventive and corrective maintenance services due to difficulties in accessing the facilities, and the possible shortage of fuel, as well as impact on the power supply due to vandalism. The preventive measures for security and monitoring avoided incidents affecting the health and safety of staff and critical services. On 30 June 2022, the incident was closed. As a result, action plans were prepared, some of which have already been completed while others are under study and/or being executed, which are still being monitored.

CHILE (LOCAL) September 2022	
Description	**Data centre power cut**
Type of crisis	Operational continuity
Impact	Due to a power cut on 14 September, there was a failure at a data centre which affected several IT systems and the continuity of the WiFi. Although the most critical IT systems were restored in the first few days, in accordance with the priority set in the Business Continuity Plans, there were systems which exceeded the recovery time objectives (RTO), leading to the activation of the crisis committee.
Actions	The crisis committee was activated on 23 September 2022. This committee supported the technology team, which dealt with restoring the applications and systems. On 27 September 2022, the incident was deemed closed and, from that point, the action relating to the completion phases was carried out (analysis of root cause, etc.).

BRAZIL (LOCAL) September 2022	
Description	**Failure in authentication and integration of users**
Type of crisis	Technological
Impact	Impact on the customer care service, field and stores (B2B and B2C) due to login failure for several applications. Duration of approximately 1 hour, without an economic impact.
Actions	The committee was activated on 28 September. The operations restored the platforms, simultaneously validating the systems involved.

BRAZIL (LOCAL) December 2022	
Description	**Failure in the national mobile network**
Type of crisis	Technological
Impact	Intermittent unavailability of fixed, mobile and TV network services at a national level, with different impact scenarios according to region due to the deconfiguration of 400 Nokia routers. Approximate duration 1 hour 15 minutes, with an approximate economic impact of €3,700.
Actions	The committee was activated on 1 December. The incident was addressed immediately by the operation and support teams to evaluate the causes. The back-up copy of the configuration was restored and they proceeded to complete manual activation. After executing the procedure, the teams managed to perform mass activation of the routers through the Nokia platform and service was restored.

PERU (LOCAL) December 2022

Description	**Political instability and public demonstrations**
Type of crisis	Political-social
Impact	Services to customers were not impacted. However, owing to the demonstrations, there was damage to premises.
Actions	The crisis committee was activated on 8 December 2022. Periodic sessions were held, adopting security measures to protect staff and reinforce technical sites. Access to critical technical sites was restricted and, in the regions outside Lima, teleworking was put in place for staff. It coordinated actions with government authorities to ensure continuity of the services. In addition, all travellers were recommended to leave the country due to the risk to their safety. Those who wished to visit the country were warned about the risk to their safety and required to undergo a consultation process to authorise their trip.

2.19.3.7. Progress in 2022

Throughout 2022, we continued to adjust our security measures linked to **remote access and teleworking**.

We continued to promote Local Business Continuity Offices in recently-created companies of the Group, as well as the participation of the Global Business Continuity Office in cross-cutting projects at a corporate level.

The management of global and local crises, after satisfactorily activating the management process and the available resources, made it possible to maintain the service levels agreed with customers at all times and adapt the network capacity to changes in demand.

During 2022, the improvement, support for, and broadening of, the supply chain security initiative continued. We consolidated and evolved the **3PS+** tool, which makes it possible to digitalise the entire security risk management process in our purchasing.

2.19.4. Cross-cutting privacy and security issues

2.19.4.1. Internal Control

In order to address and comply with the legal provisions of the countries related to local **data protection and privacy** laws and regulations, within the 2022 Annual Plan, a total of 748 specific audit days were used to verify compliance, as well as the identification of best practices in data protection issues.

The most significant aspect for European operators, which are affected by the new data protection legislation (GDPR), was to review the implementation of the documentation in Privateca of the data processing corresponding to year 2 of the GDPR audit cycle, as well as the successful execution of the controls on the reviewed processing and, within the governance model, the implementation of the data deletion procedure. In the rest of the countries affected by local data protection laws, the most important aspects reviewed were verification of the application of security measures in the processing of personal data, verification that the integrity and quality of the information is assured, and verification that the consent of users has been obtained for the processing of their personal data.

The Annual Plan has also promoted **auditing work related to cybersecurity and security in networks and systems,** with the aim of validating mainly the security of remote access to the infrastructure and its security configuration (bastioning), as well as the resistance of the technological perimeter to incidents due to the exploitation of vulnerabilities. Another objective, related to the infrastructure configuration, is to review the stored information to ensure that it is sufficiently secure in terms of access permissions and profiles to prevent tampering or unauthorised deletion. In 2022, a total of 5,088 specific audit days were used to verify the control environment as regards cybersecurity and the security in networks and systems.

2.19.4.2. Training and awareness-raising

We ran awareness-raising and training campaigns for employees on the subject of privacy and security, as well as for relevant third parties (sub-contractors, service providers and similar).

For further information, see chapter 2.20. Responsible supply chain management.

With regard to employee training, in 2022, 126,948 participants completed their training on privacy, data protection, security and cybersecurity. These courses amounted to a total of 119,639 training hours provided.

In addition, we reinforced communication and awareness-raising programs in this area through different channels and techniques to ensure that the messages reached all the levels and locations of the Company:

- Phishing campaigns applied to all the employees of the Group, to raise awareness and educate them about cybersecurity risks.
- Annual surveys to measure knowledge levels concerning security and privacy.
- Knowledge pills on security, targeting the entire workforce, containing short messages to raise awareness about specific aspects.
- Gamification techniques, which include the elements and dynamics that are typical of games and leisure, in order to foster motivation and reinforce behaviour in information security and Company asset protection practices.

2.19.4.3. Stakeholder relations

Telefónica actively participates in various international organisations and forums, most of which are multi-stakeholder bodies. In 2022, the following were noteworthy:

Internet Governance Forum in Spain

In 2022, we participated in the organisation of the Spanish edition of the Internet Governance Forum (IGF). This year, with the theme "Technology and people, more connected than ever", we actively contributed to the debates on such different issues as: challenges and opportunities of the metaverse, digital sovereignty and Internet fragmentation, and the contribution of Over-The-Top (OTT) services to the financing of European telecommunications infrastructures.

Council of Europe

We have been a member of the partnership between digital companies, operators, industry organisations and the Council of Europe since its inception in 2017, so as to cooperate on the development of recommendations and proposals related to technology and human rights in democracy and the rule of law.

Over 2022-2023, Telefónica has been participating in the Committee on Artificial Intelligence (CAI) in the work to prepare the Convention on Artificial Intelligence, which is intended to become the legal framework of reference on a global scale to tackle the challenges posed by AI with regard to human rights, democracy and the rule of law.

Cybersecurity Tech Accord

Telefónica is a founding member of this private sector initiative. It is a joint effort of more than 160 companies from around the world whose main objective is to protect internet users against the growing evolution of cyber-threats. Consumer awareness and "cyber-hygiene" are two of the tasks on which the organisation focuses its efforts. The Tech Accord is unique in its aim to accelerate the implementation and improvement of cybersecurity globally, through the participation of businesses, governments and individuals.

The Cybersecurity Tech Accord was one of the first to support the Paris Call for Trust and Security in the Cyberspace, a forum created in 2018. In 2022, Telefónica continued our active participation in coordination between companies and governments, with the goal of enhancing security in an increasingly-connected environment. Noteworthy aspects of Telefónica's contribution include the dissemination of a Zero-Trust culture and progress as regards security in the supply chain, and in promoting participation by women in the area of cybersecurity.

Organization for Economic Co-operation and Development (OECD)

We are a member of Business at OECD and Vice-Chair of its Committee on Digital Economy Policy.

In 2022, the Ministerial meeting of the Committee on Digital Economy Policy was held, in which a statement was approved whereby the OECD includes, in its work, consideration of people's rights in the digital world, following the Spanish proposal of a charter of digital rights. Telefónica was an active participant in the preparatory workshops and made a substantial contribution to the debates relating to the digital rights of people. We also participated in other OECD programs such as the Declaration on Government Access to Personal Data Held by Private Sector Entities, one of the most significant agreements of this Ministerial meeting. We continued to participate in the Working Party on Artificial Intelligence Governance (AIGO), as well as initiatives associated with digital technologies and anti-corruption measures.

International Telecommunication Union (ITU)

In 2022, we took part in the ITU Plenipotentiary Conference and its World Telecommunication Standardization Assembly, both of which are held every four years, where countries come to agreement, among other things, on which security aspects are the responsibility of telecommunications operators. Cooperation between agents, coordination and adoption of risk-based measures is essential in order to improve cybersecurity at a global level.

Centre for Information Policy Leadership (CIPL)

We are part of the CIPL organisation, an international think tank based in Washington D.C., Brussels and London that works with industry leaders, regulators and policymakers to develop global solutions and best practices in the field of privacy and responsible use of data in the new digital environment.

Global System for Mobile Communications Association (GSMA)
We participate in the GSMA (the global organisation representing mobile operators and organisations) not only in the special groups and topics of the Fraud and Security Group (FASG), but also its other working groups. José María Álvarez Pallete is currently the Chairman of the GSMA and will hold the position for two years as of 1 January 2023.

ENISA Ad-Hoc Working Groups
We participate in the working groups that ENISA, the European Union Agency for Cybersecurity, has created with different European operators and manufacturers, with the aim of defining a 5G security certification scheme which will be mandatory for all European Union countries.

2.19.4.4. Main indicators

GRI 418-1

Summary of key indicators on privacy and security

	2021	2022
Number of attendees on training courses in data protection and cybersecurity[2]	67,880	126,948
Number of hours of training in data protection and cybersecurity	81,460	119,639
Number of open procedures due to data protection issues	68	49
Number of fines for data protection issues	24	18
Sum of fines (euros) due to data protection issues	436,714	318,059
Number of confirmed fines due to data protection issues as a result of a security breach or incident (physical or cybersecurity) affecting personal data of customers, employees or others	0	0
Number of queries/complaints on data protection/privacy issues in the Responsible Business Channel	9	30
Number of queries/complaints on freedom of expression issues through the Responsible Business Channel	2	0
Number of days devoted to data protection and cybersecurity by Internal Audit	5,822	5,836
Total number of relevant information security/cybersecurity incidents classified as serious	3	2
Number of high-impact information security or cybersecurity incidents/breaches that affected customers' personal data	1	2
Number of customers affected by data breaches[3]	157,217	1,407,257
Percentage of clients whose information is used for secondary purposes[4]	-	69 %

MILESTONES

- → **In 2022, for the third consecutive year, we were first in the sector in Ranking Digital Rights (RDR).**
- → **We consolidated and evolved the 3PS+ tool, which makes it possible to digitalise the entire security risk management process in our purchasing, with the goal of reaching at least 95% by 2025.**
- → **We have extended our training and awareness programmes in privacy and security for our employees and relevant third parties.**

[2] .An employee may have taken more than one privacy and/or security course.

[3] In 2022, 2 incidents affecting personal data were identified. The first incident affected 1.4 million customers' WiFi connectivity data in Spain. The incident was reported to each customer affected. Additionally, the continuous improvement in Telefónica's cyberintelligence tools enabled the detection of a publication containing basic data from 2016 pertaining to customers in Hispam which was eliminated. As the published data were of a basic nature they were deemed as being inconsequential from a regulatory standpoint. Furthermore, no potential impacts on the rights and freedoms of the persons affected have been detected. However, in the interests of transparency, Telefónica has decided to voluntarily report this incident.

[4] This percentage has been calculated based on the total number of Telefónica customers likely to receive commercial communications.This indicator has been calculated in line with the TC-TL220a.2 standard of the Sustainability Accounting Standards Board (SASB) and reflects the proportion of customers who, in accordance with legislation, do not object to the use of their information for uses such as commercial communication of the company's products and services. In particular, this indicator does not presuppose the use of customer information by third parties. Telefónica only processes personal data for secondary purposes in those cases permitted by current legislation or with the consent of customers. Telefónica also provides information on the processing of its customers' data in the Privacy Policy of each of its operations. In any case, the reported figure (69%) demonstrates that the tools we make available to our customers are useful to them and that customers are exercising their rights effectively.

2.20. Responsible supply chain management

GRI 2-6, 2-20

KEY POINTS

☆ We require 100% of our suppliers to operate with stringent sustainability standards similar to our own.

☆ We engage with our key suppliers on specific topics (Scope 3 emissions, occupational health and safety standards, zero child labour, etc.) in order to join forces to achieve our targets.

☆ We collaborate with other telcos in industry initiatives to enhance our positive impact on the sustainable transformation of the ICT supply chain as a whole.

2.20.1. Vision

Telefónica has set **ambitious sustainability targets**, be it in relation to reducing CO_2 emissions, promoting decent working conditions or designing sustainable digital solutions. In order to meet them, **we cooperate closely with our suppliers** on these issues. That is why we see them as **partners** in our common journey towards a **more sustainable economy**.

We have developed robust policies and processes with a dual purpose in order to build trusting relationships with our suppliers. First, to **jointly identify potential sustainability risks** common to our supply chain in order to address them effectively. Secondly, to **collaborate proactively on key issues** (e.g. CO_2 emissions) to turn the ICT supply chain into a driver for sustainability. This dual approach guarantees our customers **products and services** which not only have a **positive impact** on society and the planet, but have also been **developed in a responsible manner**.

2.20.2. Governance

GRI 3-3, 2-12

The sustainable management of our supply chain is part of the **Responsible Business Plan**, which is led by the Board of Directors. The **Sustainability and Quality Committee of the Board of Directors** supervises its implementation and monitors its goals.

2.20.3. Policies

GRI 3-3

Our key policies and standards related to responsible supply chain management are:

- Supply Chain Sustainability Policy.
- General conditions for the supply of goods and services.
- Low Carbon Procurement Instruction.
- Human Rights Policy.
- Global Privacy Policy.
- Global Security Policy.
- Occupational Health, Safety and Well-being Regulation.
- Global Environmental Policy.

2.20.4. Risks and opportunities

The **main sustainability risks** in our supply chain relate to **working conditions, environmental impacts and data privacy and security**. Failure to adequately address these risks may result in adverse impacts, not only for society and the planet, but also in terms of business disruption along our supply chain. In other words, sustainable supply chains allow for better identification of risks and higher avoidance of business disruptions resulting from pandemics, natural disasters and other geopolitical events.

For further information, see chapter 1.4. Materiality.

Our approach is to **turn these risks into opportunities** by **working closely** with our suppliers. In doing so, we can create **efficiencies** and, for example, reduce material, energy and transport costs. We can also increase labour productivity by ensuring decent working conditions in our supply chain. Lastly, we can **innovate together** in the face of changing markets and meet the growing demand for sustainable solutions in the transition to a more sustainable economy.

2.20.5. Action plan and commitments

Telefónica's purchasing strategy is mainly based on:

- **Global management** by Telefónica Global Services, an organisation made up of a team of buyers specialised by product/service category. This team leads the negotiations of products and services that require more technical knowledge and are more critical for the business, with in-depth knowledge of the market and a focus on capturing synergies.

  Coordination with the operators is coordinated through the local procurement teams in each country, making it possible to anticipate demand and supervise the execution of contracts and supplier performance.

- **Internal efficiency** through the optimisation of procurement processes and systems, by symplifying process initiatives and developing support systems.

This is complemented by a **commitment to innovation and sustainability,** present throughout the entire process of our relationship with our suppliers and developed through our sustainable management model. This is all based on generating a positive impact, favouring economic and social development based on digitalisation.

As part of our management model, we pay special attention to issues associated with the supply chain which have a **high social and environmental impact** and are **significant** for **both the sector** and the **Company's strategy.** In particular the following:

Our commitments according to the key sustainability aspects in our supply chain

Aspect	Our commitments	You can find more information on how we manage this in:
Abolition of child/forced labour	To contribute to the abolition of forced labour through specific projects focused on the protection of children's human rights (e.g. on-site audits of high-risk suppliers).	**2.15**. Human Rights **2.20.5.1.** Risk management, **2.20.6.1.** Risk management in 2022 **2.20.6.2.** Engagement in 2022
Working conditions	To promote decent working conditions among our suppliers, especially for those suppliers of labour-intensive services (contractors and subcontractors).	**2.20.5.1.** Risk management, **2.20.6.1.** Risk management in 2022 **2.20.6.2.** Engagement in 2022
Occupational health and safety	To promote best practices in health and safety among our suppliers, with the common aim of achieving zero accidents.	**2.20.6.1.** Risk management in 2022 **2.20.6.2.** Engagement in 2022
Conflict minerals	To strengthen control over the use of 3TG minerals (tin, tantalum, tungsten and gold) throughout our value chain.	**2.20.6.2.** Engagement in 2022
Waste management	To work hand in hand with our suppliers to digitalise our waste management in order to improve traceability and seize the opportunities. presented by the circular economy.	**2.3.** Circular economy
CO_2 emissions - Scope 3	To improve emissions management in our supply chain and increase engagement with our suppliers both globally and locally.	**2.2.** Energy and climate change **2.20.6.2.** Engagement in 2022
Data privacy and security	To work with our suppliers, with a particular focus on those who have access to customer data, to ensure compliance with applicable regulations and security requirements.	**2.19**. Privacy and security

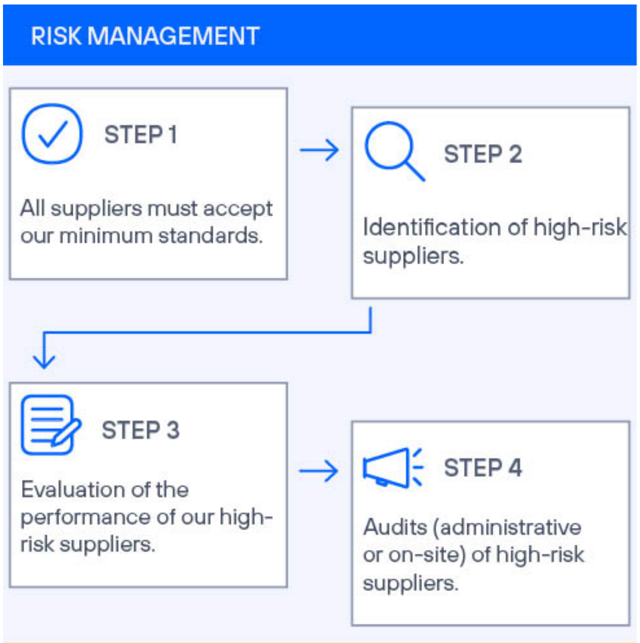
In doing so, we continue to rely on a Company-wide **common procurement model**. This model is **aligned** with our **Responsible Business Principles** and is based on transparency, equal opportunities and non-discrimination, objective decision making and sustainable management of our supply chain.

Our suppliers have all the information available on our Supplier Portal.

In accordance with international standards such as ISO 20400 and the OECD Due Diligence Guidance for Responsible Business Conduct, we base our sustainable management model on risk mitigation and trusting relationships with our suppliers.

Our approach

Sustainable supply chain management



RISK MANAGEMENT

STEP 1

All suppliers must accept our minimum standards.

STEP 2

Identification of high-risk suppliers.

STEP 3

Evaluation of the performance of our high-risk suppliers.

STEP 4

Audits (administrative or on-site) of high-risk suppliers.

ENGAGEMENT

Every stage of our sustainable management model is complemented by training and engagement with our suppliers. This enables us to raise awareness and develop capabilities to improve the sustainability of the supply chain.

Our approach is based on two pillars:

- Risk management
- Engagement with suppliers

We protect children's rights in the supply chain. Zero tolerance of child labour is a mandatory requirement for our suppliers.

2.20.5.1. Risk management

GRI 308-2, 407-1, 408-1, 409-1

> Step 1. Minimum standards required

We require 100% of our suppliers to conduct their business activities in accordance to ethical standards similar to ours. Thus, ensuring respect for core human rights and labour rights, as well as the protection of the environment.

Therefore, **all Telefónica suppliers must accept** the following upon registering and/or renewing in our Procurement platform:

- Supply Chain Sustainability Policy, where we set out the minimum criteria for responsible business that our suppliers must comply with.
- Anti-corruption Policy (certified).

Prior acceptance of these minimum conditions means that successful suppliers are assessed in relation to the social and environmental impacts set out in our regulations.

SUMMARY OF OUR MINIMUM RESPONSIBLE BUSINESS CRITERIA

- Zero corruption and conflicts of interest.
- Respect for human rights.
- Zero child labour.
- Fair treatment of employees.
- Freedom of association.
- Zero tolerance of forced labour.
- Diversity, gender equality and non-discrimination.
- Zero tolerance for violence and harassment at work.
- Health and safety.
- Minimum environmental impact.
- Waste management.
- Reduction of single-use plastics.
- Management and reduction of hazardous substances.
- Fewer emissions.
- Eco-efficiency.
- Responsible sourcing of minerals.
- Privacy, confidentiality of information, freedom of expression and artificial intelligence.
- Management of the supply chain.

> Step 2. Identification of high-risk suppliers

We focus on our main suppliers according to their level of risk and impact on our business, given the volume of purchases awarded.

To do so, we carry out the following process to analyse the overall sustainability risk of our individual suppliers, according to our **risk analysis** methodology:

First criterion: an initial assessment of the possible risk level given the products/services supplied to us and based on the following specific sustainability aspects in our supply chain, as set out in our **Minimum Responsible Business Criteria**: working conditions, health and safety, environmental, human rights (child/forced labour), conflict minerals, privacy and data protection, and customer responsibility.

Second criterion: an analysis of the potential risk is then carried out taking into account the **origin of the service or product** (and its components). In this analysis, we have also incorporated the impact of potential risks associated with the pandemic by country of origin.

Third criterion: finally, we assess the potential **reputational impact on Telefónica,** should the risks analysed materialise**.**

This three-step analysis allows us to identify potential high-risk suppliers in our supplier base from a sustainability perspective.

> Step 3. Performance assessment of our high-risk suppliers

We monitor the possible risks associated with our potential high-risk suppliers identified in the initial analysis. Our buyers in different countries can view the results directly on the purchasing platform:

External assessment platform

We conduct an external 360° **assessment** of our main high-risk suppliers based on 15 **sustainability criteria** that cover ethical, social, environmental and supply chain management aspects.

Performance-based actions

Performance Sustainability	Action
ADVANCED	• Collaborate with the supplier to identify possible improvements or sharing of best practices.
PARTIAL	• Request a commitment from the supplier to implement an improvement plan in the coming year, with the aim of improving its level of performance.
INSUFFICIENT	• Preventive blocking of the supplier in the purchasing system. • Report and agree an improvement plan with supplier.

Dow Jones Risk & Compliance Service

We cross-check our supplier database with Factiva, a database developed by Dow Jones Risk & Compliance. This comparison takes place on a regular basis from the time the supplier is registered. This tool allows us to **identify possible risks related to ethical behaviour and corruption**, thereby reinforcing processes already in place for compliance with our Anti-Corruption Policy.

We identify the potential ethical and corruption risks of 100% of our suppliers when they register on our procurement platform.

If a supplier does not reach the **required level in the external assessment platform** or is unable to provide the information requested, we require their **commitment to implementing improvement plans** to ensure compliance with our standards. If **the comparison with Dow Jones Risk & Compliance** results in **adverse information** about the supplier, an **analysis of this information is carried out** to assess this adverse information and **its significance** in relation to the specific contract.

In extreme cases, when this is not feasible, all further business with the supplier is **suspended** until they prove they have rectified the situation and/or corresponding actions have been taken to mitigate the identified risks, as stated in the terms and conditions signed by both parties.

> Step 4. Audits of high-risk suppliers

The performance assessments are complemented by our **annual audit plan** to verify **compliance with the critical aspects identified** according to (i) type of supplier, (ii) service and product provided, and (iii) the risks of each region or country. These audits are mainly carried out through the internal Allies Programme (for service suppliers) and the sectoral Joint Alliance for CSR (JAC)[1] initiative (for product manufacturers).

The audits include improvement plans agreed with 100% of the suppliers that do not comply with any of the aspects that may have a negative social or environmental impact.

[1] Joint Audit Cooperation has been transformed into a legal entity under the legal form of an international non-profit association under the new name "Joint Alliance for CSR" (JAC).

2.20.5.2. Engagement with suppliers

We strive to understand the importance of **material issues** for our suppliers, as well as their perception of Telefónica's performance in this regard.

For further information, see chapter 1.4. Materiality.

Telefónica is firmly committed to an **open and collaborative relationship** with its suppliers. Our commitment to them is based on establishing relations that enable us to have a joint positive impact on our surroundings through close collaboration and the sharing of good practices, fostered through different initiatives and meetings with our suppliers.

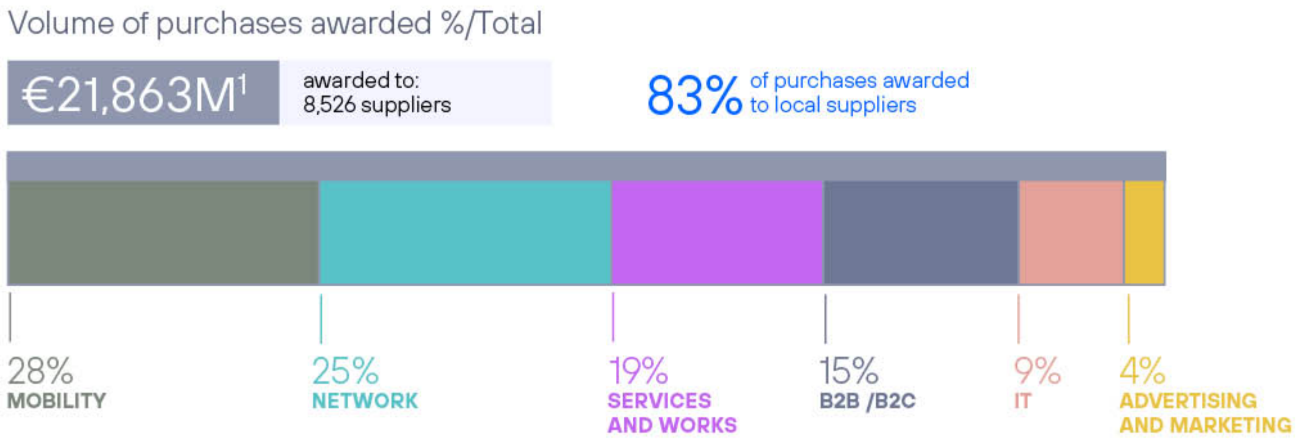
One example is the management of our third-party and collaborating companies through the **Allies Programme**. The way we engage with these companies has allowed us to foster a culture of sustainability, raising awareness among suppliers about compliance with our standards, while we jointly establish mechanisms for early detection and prevention of possible risks in our contractors and subcontractors (most of them in direct contact with our customers).

Another example of this is our participation in the **Joint Alliance for CSR (JAC) industry initiative**, together with 26 other telecommunications operators. Through this initiative, we join forces to verify, assess and develop the implementation of sustainability standards in factories of mutual suppliers, mainly in at-risk areas such as Asia, Latin America and Eastern Europe. To this end, we carry out on-site audits of direct suppliers, tier 2, 3, etcetera, implement improvement plans to rectify non-conformities and form specific working groups (climate change, human rights and circular economy) to implement best practices in our supply chains.

Targets

- 100% of high-risk suppliers assessed on sustainability aspects in the external assessment platform by the end of 2024.
- Promote audits of Tier 2, 3, etc. suppliers in the ICT supply chain through cooperation with direct suppliers as part of the JAC sector initiative.
- Promote the participation of SMEs in specific procurement processes in order to strengthen our positive impact on local economies.
- Improve due diligence processes carried out by our suppliers, through proactive engagement, to ensure traceability of minerals and mitigate risks of human rights violations linked to components or products they sell to us.
- Reduce CO_2 emissions in our value chain (Scope 3) by 56% by 2030 compared to 2016, and achieve net-zero emissions by 2040.

Impact of our business on society



(1) Agreements negotiated in Procurement with impact in 2022.

2.20.6. Progress in 2022

GRI 3-3

As explained above, our approach is based on two complementary pillars, namely risk management and supplier engagement.

2.20.6.1. Risk management in 2022

GRI 3-3, 308-1, 403-7, 407-1, 408-1, 409-1, 414-1, 414-2

In 2022, **100% of our suppliers accepted the minimum standards** set out in our Supply Chain Sustainability Policy **(step 1)**.

Based on our **global risk analysis** of suppliers awarded contracts in 2022, we identified **768 suppliers** that provide us with products or services which were classified as **potentially high risk** from a **sustainability perspective**. In 2022, we maintained our analysis methodology in order to focus on those suppliers with a significant impact on the business as well as the Company's strategy **(step 2)**.

Of the suppliers identified, **72%** have been externally **assessed on sustainability aspects** through an external platform, namely EcoVadis or IntegrityNext (including those that are in progress, pending analysis of the information provided).

Over the past year, taking into account the new requirements included in the **proposed EU Directive on Corporate Sustainability Due Diligence**, we started to improve the tools we have been using to work with our suppliers on sustainability. This improvement will progressively allow us to **incorporate all our suppliers into our process for external assessment of sustainability aspects**. It will also enable us to select **the aspects to be included in each assessment according to the potential level of risk to Telefónica** identified in our overall risk analysis.

According to the information available in the procurement system at the end of this reporting period, **6 suppliers** were **blocked** in our database **due to integrity/ sanctions, sustainability risks or non-compliance**. These were 100% of the suppliers with identified risks, either relating to integrity/sanctions or sustainability issues (social or environmental reasons), which had not yet remedied the situation or shown a commitment to implement improvement plans to ensure compliance with our standards (step 3).

In addition, we complement the risk management of our suppliers with audits that allow us to verify their level of compliance with the various sustainability aspects that we require of them, including respect for human rights.

In 2022, we conducted **18,578 administrative** or on-site audits. Given the results obtained in these audits, at the end of the year we had **879 suppliers with improvement plans** (10% of those awarded contracts) **(step 4)**.

See breakdown of audits by theme in the table below.

Details of the Annual Audit Plan

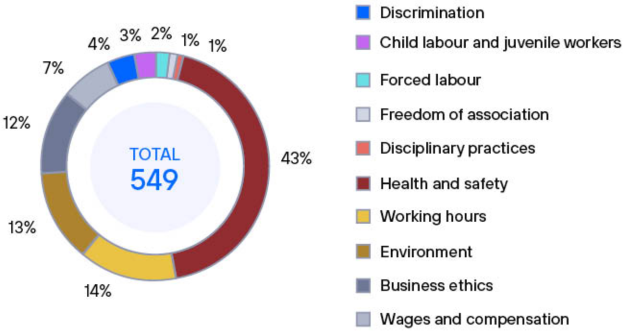
			Audited risk aspects							
Type of supplier	**Region/ country**	**Ongoing audits and improvement plans**	**Ethics**	**Labour**	**Health and Safety**	**Supply chain management**	**Human rights(child /forced labour)**	**Conflict minerals**	**Environmental**	**Security, privacy and PbD**
ALLIES PROGRAMME Labour-intensive collaborator companies.	Spain and six countries in Latin America[2]	LOCAL • 8,479 administrative audits. • 9,090 on-site audits. • 268 suppliers with improvement plans.		√	√		√			
	Germany, Spain and six countries in Latin America[3]	CORPORATE • 68 on-site audits. • 66 suppliers with improvement plans.	√	√	√	√	√		√	√
JAC INITIATIVE Manufacturing centres in the ICT sector.	54% in China and the rest in 12 countries[4]	• 59 on-site audits: 62% on TIER 2 or 3 suppliers. • 24 suppliers with improvement plans.	√	√	√	√	√	√	√	
OTHER LOCAL AUDITS Due to risks associated with the product or service.	Brazil, Colombia, Mexico and Peru	• 135 administrative audits. • 124 suppliers with improvement plans.							√	
	Brazil and Colombia	• 8 on-site audits. • 1 supplier with improvement plans.								
	Brazil, Chile, Ecuador and Germany	• 271 on-site audits. • 106 suppliers with improvement plans.			√					
	Brazil, Colombia, Ecuador and Germany	• 450 on-site audits. • 283 suppliers with improvement plans.								√
	Chile and Peru	• 18 on-site audits. • 7 suppliers with improvement plans.		√						
								Social	**Environment**	
Total audits per aspect								**17,985**	**270**	
Suppliers with improvement plans								**471**	**215**	

The decision on how to conduct on-site audits has always been subject to compliance with local mobility restrictions for COVID-19 and to ensuring at all times the health of the people involved in the process.

> Details of JAC audits (product manufacturers)

In total, 549 corrective action plans were carried out as a result of the 98 audits carried out by the JAC sector initiative in 2022 (59 of the audits were at Telefónica suppliers). The following graph shows the breakdown of these plans by topic:

Corrective action plans in 2022



[2] Argentina, Brazil, Chile, Colombia, Mexico and Venezuela.
[3] Argentina, Brazil, Colombia, Ecuador, Mexico and Peru.
[4] Brazil, Mexico, Italy, Poland, Romania, Tunisia, Nigeria, Bangladesh, Taiwan, India, Vietnam and the United States

The following table provides additional information on the four audited aspects with the most corrective action plans raised in this audit campaign:

Aspect	Non-compliance	Corrective action	Status at the end 2022
Health and Safety	Some emergency exits not properly functioning/installed.	Emergency exits can now be passed appropriately (e.g. doorways open outwards, that is, away from the room).	Closed
	No proper personal protective equipment used where required to control safety hazards and worker exposure.	Training provided for workers on proper use of personal protective equipment, supervision mechanism installed so that workers use it where required.	Closed
Work schedule	The working-hour management and control system is not effective.	Establish systems to record, manage and monitor working hours, including overtime, with reliable and detailed records of workers' working hours.	Closed
	Workers' overtime hours exceeded local legal requirements and their weekly working hours exceeded 60 hours.	Development of a reasonable production plan, increasing productivity using positive measures (such as bonuses), reducing overtime to no more than three hours per day and training employees on the health and safety hazards posed by excessive overtime.	Closed
Environment	No identification of opportunities/ measures to reduce greenhouse gas emissions; no setting of corresponding reduction targets.	Development of energy savings plan with concrete measures and emissions targets.	Closed
	The factory does not have a process in place to involve its suppliers in reducing greenhouse gas emissions in their operations.	Development of processes to oblige its suppliers to reduce greenhouse gas emissions in their operations.	Closed
Wages and remuneration	Workers' wages are not regularly reviewed to ensure that a living wage is paid.	Completion of regular surveys/ reviews with workers to guarantee living wages.	Closed
	Insufficient social security provided to workers.	Social security now provided to all workers.	Closed

> Details of corporate audits within the Allies Programme (labour-intensive services)

We closely monitor that service providers comply with our standards, including contractors. In 2022, we incorporated Germany into our audit process, promoted to the corporate level within the Allies Programme. In this way, the audit process covered each of our main markets: Brazil, Spain and Germany, and five countries in Hispanoamerica (Argentina, Colombia, Ecuador, Mexico and Peru).

Throughout 2022, **we audited 68 labour-intensive suppliers**. As in previous years, a high level of compliance was achieved, standing at over 87% in the five areas audited (Responsible Business Principles, human resources, health and safety, environment, and security and data protection). These results reflect the good performance of our partners, thanks to the work they continue to do each year.

If we take into account the average number of risks per issue identified in each of the countries, the **health and safety** section was the one with the highest number, with the risks concentrated around aspects of industrial hygiene and safety, verification and planning.

Regarding the **human resources** section, the most common risks were detected mainly in compliance with the required percentage of staff with disabilities and the lack of programmes for work climate measurement, guarantees and/or insurance taken out for labour claims, in addition to a lack of staff performance evaluation programmes. In **environmental** processes, the most common risks were related to the environmental management system (failure to identify and/or assess all applicable environmental requirements) and waste management. With regard to the section on **security and data protection**, the most common risks related to the lack of procedures establishing the criteria for action in the event of security breaches and the lack of employee training on data protection or information confidentiality.

Taking into account the potential social or environmental[5] impacts of the risks identified, the most significant issues were as follows:

- The most significant social impacts are mainly related to industrial hygiene and safety, emergency control and accident assessment and control management.
- The environmental impacts are in the noise section.

> Tier 2, 3 supplier management

Our supply chain management goes beyond our direct suppliers.

As part of the **JAC initiative**, we place particular emphasis on carrying out audits of manufacturers that supply components and/or equipment to our suppliers. In 2022, **61% of the audits were conducted at Tier 2 or 3 suppliers.**

In addition, **in Spain**, we continue to develop our **Comprehensive Prevention and Sustainability Project**. Through this initiative, we aim to assess and recognise the performance in prevention and sustainability, with a special focus on aspects related to **occupational risk prevention**, of the main sub-contractors that collaborate with our contractors in the deployment and maintenance of our network. In 2022, we brought 11 new sub-contractors into the project, bringing the total to **106 Tier 2 suppliers and having an impact on 2,216 employees**. The **results of the assessments carried out** during the first phase of the project allowed us to **identify the need for improvements in two processes**: (i) communication of the specific prevention measures that sub-contractors' employees must comply with, and (ii) creation of a channel for communicating any incidents detected regarding occupational risk prevention. To this end, **we have begun to work with our contractors** to identify the current status of each of these processes and **to establish the necessary improvement plans in each case** to ensure their proper development in the day-to-day relationship between the contractor and their respective sub-contractors.

2.20.6.2. Engagement in 2022

GRI 204-1

For yet another year, we promoted new capabilities among our suppliers to improve their performance on key sustainability-related issues.

> Supply chain emissions

We work on emissions management in the supply chain. Globally, we have two collaborative programmes on climate change to which we invite our most significant suppliers in terms of emissions:

- Firstly, we continued our **Supplier Engagement Programme** to understand the maturity level of each supplier's corporate-level climate strategies and help them set more ambitious emissions reduction targets. For this purpose, we invited the most significant suppliers in terms of emissions to the CDP Supply Chain Programme. In total, 218 suppliers participated, representing 97% of the emissions from our supply chain.
- In addition, we are working on a new **Carbon Reduction Programme,** together with our strategic suppliers, on the analysis and reduction of emissions at the product level.

In addition, we encouraged decarbonisation among our SMEs and invited them to join the **SME Climate Hub,** where they can sign the SME Climate Commitment (through the Hub) and have access to the tools made available to help them achieve their climate goals.

We continued to participate in initiatives such as **1.5°C Supply Chain Leaders** to reduce CO_2 emissions from small and medium-sized suppliers in the **SME Climate Hub** and in the **climate change working group of the JAC initiative.**

For further information, see chapter 2.2. Energy and climate change.

[5] Critical non-conformities identified during audits in each area are considered significant impacts, either social or environmental.

Telefónica has implemented a new climate requirement within its procurement process, asking its key suppliers for a decarbonisation plan aligned with SBTi.

> Labour conditions

Under the JAC initiative, we collected **direct feedback** from **20,634 employees** at 15 supplier factories through an **anonymous survey** conducted on their own mobile phones. In this way, we assessed aspects related to working conditions, especially with regard to issues concerning the number of hours worked, rest periods, harassment, discrimination, treatment and relationship with their direct manager, overtime, the handling of chemical materials, etc.

In the new **Living Wage Working Group within the JAC initiative**, we are working to ensure a living wage in the ICT supply chain. Through the JAC protocol, which we apply to all audits conducted under the initiative, we ensure that suppliers pay a **fair and reasonable wage** to employees that is high enough to maintain a **decent standard of living**.

> Human rights

We are part of the **human rights working group created in 2021 within the JAC initiative** to promote respect for human rights throughout our **value chain**. Together we analyse new regulations and trends that may have an impact on our suppliers, and implement initiatives to counteract potential risks in the ICT supply chain.

Supplier Development Programme

We regard our suppliers as partners and help them to meet our high sustainability standards. As a sign of this commitment, since 2019 we have been part of the Supplier Development Programme promoted by JAC and involving other telecommunications operators, a training programme for key suppliers that goes beyond an audit.

The aim is to provide support to the supplier for two years in order to enhance its sustainability performance.

By participating in this programme, suppliers have been able, for example, to reduce worker turnover and workplace accidents in factories, as well as improve employee satisfaction and productivity rates.

For further information, see chapter 2.15. Human rights.

> Responsible sourcing of minerals

Although we do not have direct business relationships with smelters or refiners, we work actively to tighten controls on the use of these minerals across our value chain.

1.Policy and clauses

Our Minerals Policy is set out in our Supply Chain Sustainability Policy and is based on the OECD Due Diligence Guidance regarding minerals. All our suppliers have to accept this Policy and therefore commit to responsible sourcing of minerals.

In addition, any supplier that submits an offer to us must meet **minimum sustainability** requirements in the supply chain. These are **set out in the Telefónica Group's General Conditions for the Supply of Goods and Services**. They include a contractual minerals clause whereby we require our suppliers to carry out effective due diligence processes to ensure traceability of 3TG minerals and mitigation of associated risks (such as human rights violations).

2. Identification and management of high-risk suppliers

1. We identify mineral risk suppliers according to our risk analysis methodology.

2. We assess performance based on the CMRTs (Conflict Minerals Reporting Templates) that we request from these suppliers.

3. We engage with those suppliers whose due diligence needs to be improved.

4. We verify compliance of some key suppliers through on-site audits under the JAC sector initiative.

3. Commitment initiatives

We support, and participate in, major international and sector initiatives to reduce this type of risk, such as:

a. The **Responsible Minerals Initiative** (RMI): our activities regarding smelters and refiners are supported by industry initiatives such as the RMI, in which audits are performed, best practices shared, and stakeholder dialogue promoted.

b. The **Public-Private Alliance for Responsible Minerals Trade** (PPA): we participate in the PPA, a multi-sector, multi-stakeholder initiative that improves conflict-free mineral supply chains.

4. Complaints

We have a Concern and Whistleblowing Channel through which our stakeholders can consult us and submit complaints in this regard.

5. Information

We report on the due diligence of the supply chain through various channels (this Report, the website, dialogue with stakeholders, etc.).

Furthermore, as a company listed on the New York Stock Exchange, we comply with Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

> Occupational Risk Prevention

Once again this year, we have focused on fostering best practice regarding **safety, health and well-being** in our **supply chain**, with a particular **focus on contractors** who assist us in the deployment and maintenance of the network, activities where the main risks are present (work at height, electrical risk and confined spaces).

In 2022, we maintained a series of initiatives with our suppliers depending on the situation in the different countries:

- Specific and direct **communication with our suppliers**, through face-to-face sessions, to address the most significant aspects to work on in order to avoid possible accidents arising from the risks inherent in each activity. For example, last October, we held a **workshop** with our partner companies in **Spain** on **specific prevention measures for work at height**.

  Furthermore in **Colombia**, we organised a **technical round table** where we presented new **instructions for the management of serious or fatal accidents** to our suppliers.

- Occupational health and safety **audits** specifically adapted to each country, in order to verify compliance with the procedures and protocols established for the prevention and safety of employees at the facilities (see the table "Details of the Annual Audit Plan" for a breakdown by country of the audits carried out on occupational health and safety aspects).

- **Follow-up** and monitoring of the corresponding indicators to analyse the trends in accident rates throughout the year.

OHS+ Project at Telefónica España

> What is it?

Initiative for the coordination of business activities which seeks to create a community of dialogue, sharing practices, addressing queries, proposals for improvement, etc., on an equal footing between supplier and customer.

> Targets

Identify levers that lead to a reduction in the number of OHS incidents detected and the volume and severity of occupational accidents until it reaches zero accidents.

- **Encourage participating companies to conduct audits of their own suppliers.**

> 2022 results

- **100% of the companies once again met the monitoring target, and some even exceeded it.**
- **Accident frequency rate (in the workplace) of 1.27. The target set for 2023 is 0.9.**

> Diversity

We see diversity as a competitive advantage, which creates business value and positively impacts our results. Therefore, in addition to promoting it internally in the Company, we also encourage it among our suppliers, as stated in our Supply Chain Sustainability Policy.

In this regard, we promote "**Mujeres en Red**", a project that we implement in **Colombia and Peru** in collaboration **with our partner companies** to promote the **employability and training of women** in technical positions in the telecommunications sector, promoting **equal opportunities** in roles where women are under-represented. By the end of 2022, in both countries, more than 1,000 female technicians had been hired by our partners and over 7,000 people (both technicians and administrative staff) had received training on topics such as "Unconscious Biases", "Female Empowerment" and "New Masculinities".

For further information, see chapter 2.7. Diversity and Inclusion.

> Training and communication

To **update the Low Carbon Procurement Instruction,** we conducted **internal training sessions for the different countries** in which we operate. **Over 500 purchasers** and key **internal contract managers,** involved in the purchase of equipment consuming energy and/or containing refrigerant gases, participated in the sessions.

In **Brazil**, we trained **internal contract managers** on how to **manage our partners** through an **online course** on our SuccessFactors platform.

Also, complementing the training of our buyers and internal contract managers, we maintained our **supplier training** and **communication channels** with our suppliers for another year.

In 2022, we delivered 11,936 in-person courses and 14,766 online courses involving over 349,001 participants from partner companies in Latin America.

These trainings were delivered in-person or online for our suppliers, addressing the specific needs in each country and the most critical issues according to the service they provide. For example, in **Peru**, we organised **two workshops on "Regulation, Control and Good Practices in Environmental Matters"**, with the aim of providing a knowledge base for the staff of the collaborating companies, in which 60 people took part. They learned about the **main regulatory changes in the environmental field** (comprehensive solid waste management, the circular economy, WEEE management, etc.). In addition, the workshop "**Our Chain's Footprint**" was also held, in which 14 people took part, with the aim of raising awareness and informing Telefónica's key suppliers about the **importance of measuring and reporting the carbon footprint.**

In Spain, we provide privacy trainings to suppliers with whom we have a high number of contracts in force and that provide us with **services involving the processing of personal data.**

In **Colombia**, through an **online course** on **digital security**, we improved our partners' knowledge of information security by addressing topics such as the workstation, secure passwords, how to change your password and security in the workplace.

For further information, see chapter 2.19. Privacy and security.

Furthermore, under our **Supplier Engagement Programme,** and as part of the **annual CDP Supply Chain campaign**, we trained our **key suppliers on carbon footprint management and reporting**.

As part of the **SME Climate Hub initiative, we invited our SMEs to our "Small Business Saturday"** seminar, where we presented the tools that the hub makes available to SMEs **to help them achieve their climate goals**.

We also promoted continuous communication as a key lever to boost their engagement through different channels, such as our newsletter to Allies, the Allies' Portal and the Supplier's Portal. The Supplier's Portal contains all our global policies, as well as specific local requirements.

Our suppliers have a confidential channel for queries and complaints related to compliance with our Minimum Standards for Responsible Business.

We also organise in-person and online events (global and local) with suppliers, such as:

13th Telefónica Global Energy and Climate Change Workshop
An annual meeting point for leaders of the Company's energy transformation and the main collaborating companies in the field. This is a workshop that reviews and sets out the challenges for the Company in this area. Around **200 professionals** from different internal areas and **30 technology partners participated** in this edition. During the workshop, multiple initiatives from our different markets were broken down, focusing on reducing fuel consumption (in buildings and mobile sites), the impact of refrigerant gases (reducing leakage), optimising consumption and increasing the use of renewable energy. Changes in the global energy model were also analysed, as well as, the energy market situation, and developments in the industry relating to energy procurement. In addition, for yet another year, the

Company's **climate change targets were reviewed** and the **importance of the work carried out by our suppliers to achieve them** was made clear.

For further information, see chapter 2.2. Energy and climate change.

Workshop on human rights in Brazil

This was **attended by nearly 125 people from 68 companies exposed to practices that may violate human rights**, including issues related to occupational health and safety. The event aimed to provide a general understanding of the **importance of human rights** within the Telefónica business environment and **how they affect the Company's relationship with its suppliers**.

4th Forum on the Prevention of Occupational Risks in Spain

The event **brought together Telefónica Spain, its supply chain (main contractors and sub-contractors)**, the most prominent operators in the sector, trade unions and ADEMI, the sector's employers' association. All of them **share the target of achieving zero accidents in the sector**. During the forum, dedicated to the key players in prevention, the close coordination between all the actors in the telco sector was revealed, highlighting the great extent to which managers are involved in achieving the targets set and the importance of, and trust in, people as the cornerstone on which the culture of prevention is built. Another of the aspects addressed was Telefónica Spain's Comprehensive Prevention and Sustainability Plan, which is based on our Responsible Business Principles, the importance of sustainability for the progress of society, and our commitment to the prevention of occupational hazards. For the third consecutive year, an **award was presented to one of the companies in our supply chain** based on the **results obtained in its prevention management**, which this year went to the prevention services of the company Cobra Instalaciones y Servicios, S.A. Lastly, a tribute was paid to all those people who throughout the pandemic and especially at the beginning, when as a society we were largely unaware of how to proceed, did not hesitate to continue working to ensure that we remained connected.

Summary of key indicators

	Indicators	2021	2022
Activity[6]	Volume of purchases awarded.	23,737M	21,863M
	Suppliers awarded contracts.	9,368	8,526
	% purchases awarded locally.	81%	83%
Ethics and Compliance	Sustainability risk-related suppliers identified in our global analysis.	810	768
	% high-risk suppliers assessed on sustainability aspects through EcoVadis o IntegrityNext.	71%	72%
	% suppliers assessed through Dow Jones Risk & Compliance.	100%	100%
	Suppliers blocked due to integrity/sanctions, sustainability risks or non-compliance.	9	6
	Total audits of suppliers.	17,960	18,578
	High-risk suppliers with improvement plans.	610	879

[6] Considering that the activity of Telefónica UK Limited has not been included in the 2022 reporting scope, comparability between the two years is not guaranteed.

MILESTONES

- → We continued minimising sustainability risks within the procurement process, with 100% of our suppliers accepting our sustainability standards as part of their contractual obligations.
- → We improved our supplier assessment processes in order to be able to meet new requirements on supply chain due diligence.
- → In collaboration with the other telcos in the JAC initiative, we audited 98 companies in the ICT sector and surveyed 20,634 employees at 15 supplier factories in 2022, to work across different levels of our supply chains.
- → As part of our supply chain decarbonisation strategy, we required our key suppliers to commit to emission-reduction targets validated by the Science Based Targets initiative.
- → We obtained a 75% response rate in the second year of CDP Supply Chain reporting, with 100% participation of our high-priority suppliers and 82% of our mid-level priority suppliers.
- → We reduced CO2 emissions from our value chain by 32% compared to 2016, with emissions from our supply chain being the most significant of our Scope 3 emissions (64%).