

# Leading by example



## 2.15. Governance and culture of sustainability

### Key points

92,401

employees have received training in our code of ethics, our Responsible Business Principles.

20%

of our professionals' variable remuneration is linked to ESG targets such as reductions in carbon emissions and gender equality.

3,300

courses on sustainability were taken by our employees in 2023 through the Company's newly launched ESG Academy.

### 2.15.1. Governance

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

Telefonica's Responsible Business Principles are our code of ethics and conduct. The Principles also form the basis of our sustainability policy as they guide us to act with integrity, commitment and transparency.

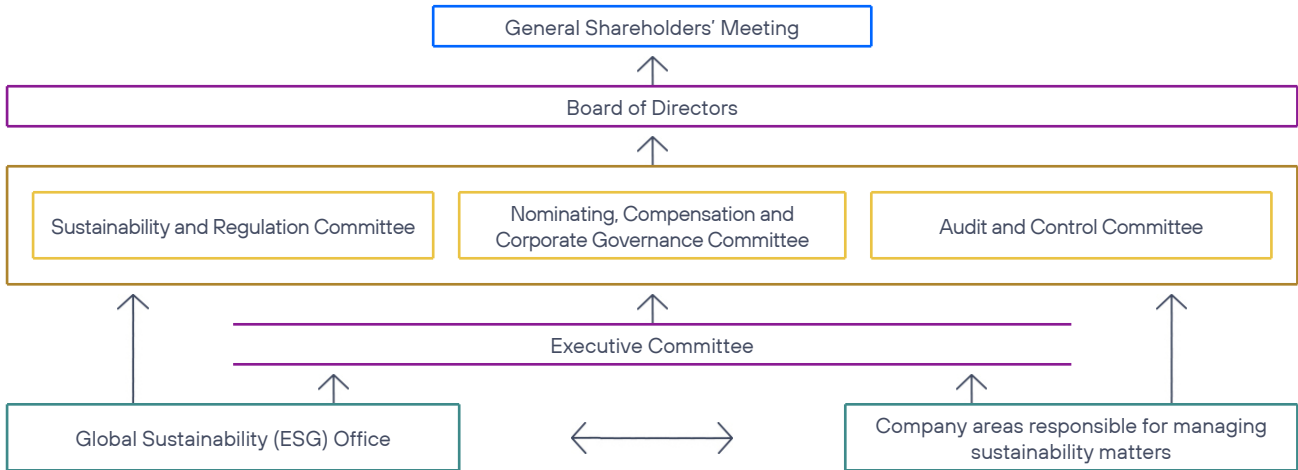
To ensure that our Responsible Business Principles are the common thread running through everything we do, we have a **Responsible Business Plan**. This includes targets and projects across the key areas of our strategic plan, Growth, Profitability and Sustainability (GPS): to transform the relationship with our customers (Growth), to streamline the operating model (Profitability) and to create long-term value (Sustainability).

In turn, the priorities of the Responsible Business Plan form part of the **Company's Strategic Plan**, which contains the sustainability indicators that we cover in this report. Some of the targets also form part of the variable remuneration of our employees, including members of the Executive Committee.

 For further information, see 1.5. Strategy

Sustainability management is a cross-cutting issue, involving various governance and management bodies from the corporate and local areas.

**Main bodies of the sustainability governance model**



The **General Shareholders' Meeting** is the Company's highest decision-making body. This is the platform through which corporate will is expressed and shareholders' right to participate in the Company's decision-making processes is exercised. Among its functions is the approval of the Sustainability Report.

The **Board of Directors** approves the Responsible Business Principles, the Responsible Business Plan and the relevant ESG policies and regulations (anti-corruption, environmental management, privacy, diversity, equality or sustainable management of the supply chain, among others). These documents form our ethical and responsible-business framework and our roadmap for employees, which is supplemented by training and awareness-raising.

The **Sustainability and Regulation Committee**, created under its new structure on 13 December 2023, oversees implementation of the Responsible Business Plan at its monthly meetings, among other tasks. In addition, the **Audit and Control Committee** has an extra role to play in the area of sustainability, as it oversees certain matters related to sustainability information, regulatory compliance, the risk analysis and management process and the Company's reporting processes. The **Nominating, Compensation and Corporate Governance Committee** oversees the variable remuneration system, which includes sustainability-related targets, among other things.

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

The **Executive Committee**, one of the Telefónica Group's highest management bodies, which twice a month brings together the main people responsible for managing the various areas of the Company, monitors the business and the Responsible Business Plan, as well as

other issues related to the management of sustainability targets that are deemed necessary in this area.

The **Global Sustainability (ESG) Office** is responsible for monitoring and coordinating:

- The development of the Responsible Business Plan (based on materiality analysis) which includes objectives, tracking indicators, and action plans related to ESG matters.
- The reporting of sustainability information to various stakeholders and its verification.
- The management of sustainability risks, impacts, and opportunities and ESG governance.
- The ESG culture (purpose, Responsible Business Principles, variable remuneration system, policies, training, and internal awareness regarding ESG matters).
- The communication for engagement with stakeholders (ratings, rankings, analysts, investors, society, regulators, or customers)
- The sustainable financing.
- The measurement of the company's reputation and the assessment of its social and environmental impact, among other aspects.

Finally, the **Company areas responsible for managing sustainability matters** are those that undertake the implementation of the objectives of the Responsible Business Plan and generate and manage quantitative or qualitative indicators of this nature (ESG) within their competence (for example, corporate areas such as Environment and Human Rights, ESG Development and Impact, ESG Consumer and Business Development, Procurement, Compliance, Privacy, Tax, Human

Resources, Inspection, Investor Relations, Strategy, Infrastructure and Operations, General Secretary, Management Control, or Security, as well as local

subsidiaries or operators that also participate in sustainability management.

## 2.15.2. The Telefónica Group's main sustainability-related policies and regulations

GRI 2-24, 3-3

 <b>Ethics</b>	 <b>Supply chain</b>	 <b>Privacy and freedom of expression</b>	
<ul style="list-style-type: none"> <li>• Global Anti-Corruption Policy.</li> <li>• Compliance Function Policy.</li> <li>• Compliance Function Regulations.</li> <li>• Crime Prevention Policy.</li> <li>• Internal Rules of Conduct.</li> <li>• Regulation on the Prevention and Management of Fraud in Telecommunications.</li> <li>• Regulations on Relations with Public Bodies.</li> <li>• Complaints Channel Management Policy.</li> <li>• Corporate Policy on the Comprehensive Discipline Program.</li> <li>• Fiscal Control Policy.</li> <li>• Risk Management Policy.</li> <li>• Competition Law Policy.</li> <li>• Rules on Sanctions.</li> <li>• US Clawback Rules.</li> <li>• Telefónica's Internal Information System Management Policy and Procedure.</li> </ul>	<ul style="list-style-type: none"> <li>• Supply Chain Sustainability Policy.</li> <li>• Supply Chain Sustainability Regulations.</li> <li>• Supply Chain Security Regulations.</li> <li>• Low Carbon Procurement Instruction.</li> <li>• Procurement of Goods and Services Regulations.</li> </ul>	<ul style="list-style-type: none"> <li>• Global Privacy Policy.</li> <li>• Personal Data Protection Governance Model Regulations.</li> <li>• Regulation on Requests by Competent Authorities.</li> <li>• Global Security Policy.</li> </ul>	
 <b>Human Capital</b>	 <b>Human Rights</b>	 <b>Responsible Communication</b>	 <b>Environmental Management and Climate Change</b>
<ul style="list-style-type: none"> <li>• Protocol for Action in Situations of Workplace or Moral Harassment, Sexual Harassment and Discrimination.</li> <li>• Occupational Health, Safety and Well-Being Regulation.</li> <li>• Diversity and Inclusion Policy.</li> <li>• Equality Policy.</li> <li>• Diversity Policy in relation to the Board of Directors and Selection of Directors.</li> <li>• Remuneration Policy for Telefónica, S.A. Directors.</li> <li>• Rules on the Hiring of Former Executives and Former Employees of the Telefónica Group.</li> </ul>	<ul style="list-style-type: none"> <li>• Global Human Rights Policy.</li> <li>• Artificial Intelligence Principles.</li> </ul>	<ul style="list-style-type: none"> <li>• Regulations on the disclosure of information to the markets and other stakeholders.</li> <li>• Shareholder Communication Policy.</li> <li>• Responsible Communication Regulation.</li> <li>• Regulations on the recording, reporting and control of financial and sustainability information.</li> <li>• Social Media Regulations.</li> </ul>	<ul style="list-style-type: none"> <li>• Global Environmental Policy.</li> <li>• Energy Management Policy.</li> </ul>

Coverage of policies and regulations: the main policies and regulations listed are applicable to Telefónica Group companies within the scope of consolidation.

 For further information see Appendix I: Scope of consolidation

### 2.15.3. Impacts, risks and opportunities

We are committed to a strong, efficient and comprehensive ESG (*Environmental, Social & Governance*) governance model and an ethical corporate culture in which respect and inclusion are paramount. We believe that this can have a positive **impact** on the satisfaction of our employees, customers, shareholders, suppliers and other stakeholders.

Furthermore, we identify **risks** related to governance and accountability so that we can manage and mitigate them. For example, we encourage transparency through regular sustainability reporting and disclosures as we believe a potential risk is the loss of engagement with stakeholders due to ineffective communication with them.

We also analyse sustainability governance **opportunities** and seek to leverage them throughout the Group. For example, we believe that linking a percentage of variable remuneration to ESG criteria will help to ensure our long-term future while having a positive impact on society and the environment.

### 2.15.4. A culture aligned with ethical and sustainable management

Beyond ensuring ethical behaviour and responsible business management, our goal is to make sustainability a cornerstone of our culture. Therefore, we seek to align behaviours, processes and targets with the Company's purpose and values.

We are guided by our Responsible Business Principles (RBPs), which are spread 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 our **internal culture with ESG** (environmental, social and governance) factors, we clearly communicate their long-term business value. In fact, we ensure **that every internal process or activity is in line with this vision**. Developing organizational culture and enhancing commitment to sustainability is a continuous work that requires a shared vision and commitment at every level of the organisation.

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

**Training and awareness raising:** we provide Responsible Business Principles and Human Rights training to our entire workforce (part-time and full-time employees) on an ongoing basis. The course is mandatory. Completion of the course implies the employee's acceptance of the Principles. In addition to receiving the Principles in their welcome pack, new employees are required to take the specific RBP course within three months of joining the Company. Both the course and the RBPs have been translated into the main languages of the Telefónica Group: English, German and Portuguese.

In addition, specific strategic training in key issues such as privacy, digital security, ethics and artificial intelligence (AI), environmental management, accessibility and diversity is delivered on an annual basis. We also train employees in specific ethical and sustainability issues related to the design of our products and services, such as the 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, our customer promise, the environment, privacy, diversity and inclusion, accessibility, etc.

- **Internal processes and activities:** our aim is for every employee to understand that sustainability is part of their day-to-day activities, that it adds value and sets the different areas of our business apart. One example is the incorporation of ethical, social and environmental aspects into product and service development processes.

- **Alignment with business priorities:** we quantify benefits and include them in our business use cases. Examples include Eco Smart services, digital solutions that help our customers reduce their impact on the environment and the value that our sustainability strategy provides our customers as a distinguishing feature in procurement processes.

**+** For further information, see 2.11 Sustainable offering and innovation

- **Control processes:** we promote the robustness and efficiency of our internal control processes by closely monitoring and managing sustainability indicators. We are committed to ensuring the integrity, quality, accessibility, comparability and transparency of our information, thereby contributing to informed decision-making and the sustainable achievement of our strategic targets.

- **Remuneration scheme:** as part of variable remuneration, 20% of the performance appraisal of our employees includes sustainability indicators. In addition, 10% is included in long-term remuneration and this applies to senior management.

**+** For further information, see 5.1. Annual Report on Remuneration

In early 2024, following the Board of Directors' approval of the proposal put forward by the Nominating, Compensation and Corporate Governance Committee, the remuneration scheme was modified to align it with our GPS strategic plan. The **new model** focuses on three essential sustainability indicators:

In the short term:

- **NPS:** this key lever to strengthen our relationship with our customers now represents 10% of the short-term variable remuneration system, compared to 9% under the previous scheme.
- **Women executives:** this indicator will now represent 5% (compared to 3% up until the end of 2023) in the short term. We are thereby awarding more importance to gender equality through an indicator which we have also linked to sustainable financing.
- **Carbon emissions:** emissions reductions continue to be part of our employees' variable remuneration, at 5%.

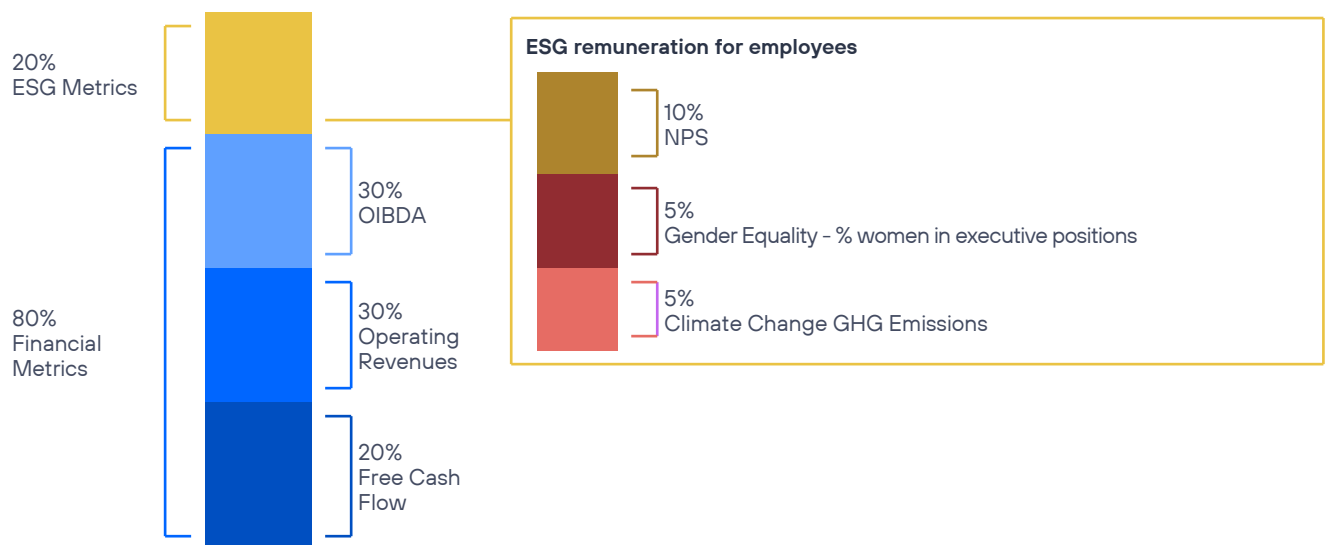
In the long term:

A proposal is expected to be put forward at the forthcoming 2024 General Shareholders' Meeting for a 2024-2028 Long-Term Incentive Plan that, with similar characteristics to previous plans, contains certain adaptations, including the following:

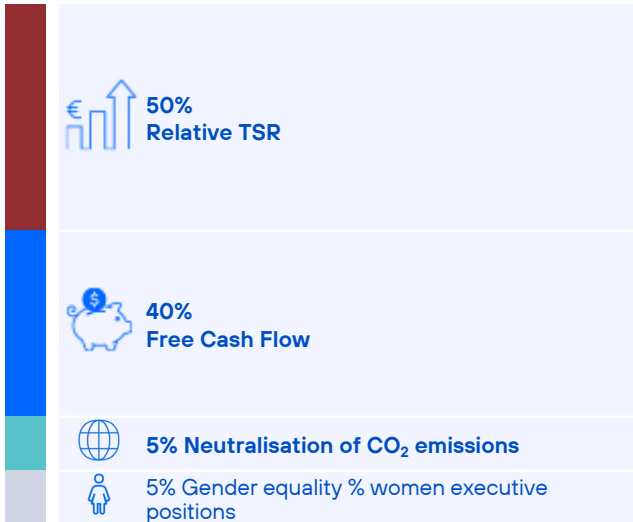
- **Women executives:** due to its importance, this will represent 5%.
- **Carbon emissions:** instead of 10%, this will change to represent 5%.

The following graph shows how the scheme will be structured:

**Annual variable remuneration**



**Long-term Incentive (2021-2026)**



Our target in 2024 is to develop and implement a new training program to refresh knowledge on Responsible Business Principles.

**2.15.5. Progress in 2023**

**2.15.5.1. Training**  
GRI 3-3

**Training Responsible Business Principles**

Internal communication campaigns were run to highlight the importance of doing the course on Responsible Business Principles and Human Rights; we also carried out close monitoring of course uptake.

- In 2022 we launched a new edition of the course, which was scheduled to be in force for three years. Over a six-month period, we managed to train 91,347 employees, representing 89% of the average workforce<sup>1</sup> (102,483 employees).
- As the workforce is constantly experiencing turnover, in 2023 we continued to press ahead in instructing the highest possible number of employees, adding a further 13,581 trained employees. Taking into account employee exits and new hires, the net increase amounted to 1,054 employees since its launch.
- The cumulative total since the 2022 launch is 92,401 trained employees, which represents 89% of the average workforce<sup>1</sup> and a total of 183,489 hours. It is important to bear in mind the difficulties involved in calculating the total workforce, as this includes employees on paid leave during the training period, recently acquired companies undergoing the integration process and recently hired employees (where the deadline for training of the latter two has not yet ended).
- The course is mandatory and compliance was closely monitored by a multidisciplinary team made up of the Compliance, People and ESG Departments.

<sup>1</sup> 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.

**Training in Responsible Business and Human Rights through the Principles Course**

Training	2022	2023
Number of employees who received training on responsible business and human rights through the Principles Course in the reporting year	91,347	13,581
Number of employees who have received training on responsible business and human rights through the Principles Course since its launch	N/A	92,401
Percentage of employees who received training in responsible business and human rights through the Principles Course in the reporting year	89	13
Percentage of employees trained in responsible business and human rights through the Principles Course since its launch	N/A	89
Hours of training in responsible business and human rights through the Principles Course in the reporting year	163,125	20,364
Hours of training in responsible business and human rights through the Principles Course since its launch	N/A	183,489

The objective of the ESG Academy is to promote a culture of sustainability through training in ESG topics.

**ESG Academy**

In 2023, we launched ESG Academy, a space for training aimed at Telefónica's entire workforce. There are two formats:

- **Online:** a space inside Telefónica's learning platforms which brings together internal training relating to sustainability, along with external training courses and a number of different resources of interest. The content is in Spanish and is intended for self-learning. We have run a communication campaign to publicise both its launch and the content it offers. We delivered more than 5,500 hours of training, involving 2,500 employees, and over 3,300 courses were completed.
- **Live:** in collaboration with Universitas (Telefónica's corporate university) and with other areas of the Company, we held live-format courses featuring in-house and external speakers. Training content was based on the basic ESG's pillars of our business and

how we approach them as for example: environment, digital inclusion, privacy or security. Through this method, we trained 1,054 employees in Spain, Hispanoamérica and Brazil.

**Other ESG training**

We conducted various internal training sessions related to ESG issues:

**Environment (E):**

- **Environmental management:** internal training aimed at employees holding responsibilities in the operation of the Environmental Management System, in order to improve the Company's performance.



For further information, see 2.1. Responsibility to the environment

- **Waste management:** sessions designed for the heads of different areas regarding use of the waste management platform at all our operators.
- **Climate change:** specific training was given on managing climate change to the members of the Board of Directors. There was also a training course for the marketing, communication and branding team as part of the Planet Pledge initiative.



For further information, see 2.11. Sustainable offering and innovation

**Society (S):**

- **Responsible use of technology:** training to help employees and their families to make healthy use of digital devices.
- **Accessibility:** awareness-raising sessions through dynamic, enjoyable formats, such as video pills featuring people with physical, audiovisual, organic, intellectual and mental disabilities. There was also training for departments and roles with direct responsibility, such as branding and product development areas.



For further information, see 2.12. Digital inclusion

- **Disability:** we enhanced our awareness programme for all employees, with information on the different types of disabilities and tools to promote equal treatment.
- **Diversity:** the value of differences, awareness of unconscious bias and prejudice, and the importance of inclusive leadership are some of the issues we address in our workshops, manuals and online courses. We have also provided training sessions for our Board of



Directors and have continued to consolidate the employee resource groups for LGBT+ employees, employees with disabilities, employees of different ethnicities, young people and women.

**+** For further information, see 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 2.16. Ethics and compliance

- **Privacy and security:** courses aimed at all our employees about data protection, roles in processing and other security matters.

**+** For further information, see 2.18. Privacy and security

**2.15.5.2. Awareness campaigns**

We ran a number of internal campaigns related to ESG issues (strategy, significant progress, rankings, recognition, awareness on key dates, etc.) targeting the entire workforce.

In the case of the ESG Academy, the communication campaign focused on publicising the platform as well as on disseminating short videos and short courses on each of the topics. The main channels used were our internal social network (Workplace) and newsletters. The posts, which all featured a manager as spokesperson, achieved over 40,000 views.

**Environment (E)**

- The campaigns run centred on the circular economy, climate change and specific dates such as that of Earth Hour. We also held the fourteenth edition of the Energy and Climate Change Workshop.

**+** For further information, see 2.2. Energy and climate change

**Society (S)**

- **Diversity and inclusion:** we participated in celebrating the International Day of Persons with Disabilities and International LGBT+ Pride Day through internal communication campaigns. We were also the hosts of the REDI to Connect Employees event, the largest event for LGBT+ employee resource groups in Spain.
- **Disability and accessibility:** video pills featuring people with physical, audiovisual, organic, intellectual and mental disabilities, who explain their needs and what they expect from their teams and their company, in a simple and enjoyable format.
- **Work-life balance:** we conducted an internal analysis to ascertain what barriers there are to achieving a good work-life balance. The results were circulated internally.
- **Responsible use of technology:** we shared the thoughts of experts on the topic through an internal newsletter, where we also commemorated significant dates such as Safer Internet Day. We invited our employees to participate directly in the #MalamadreEnModoAvión challenge and event to encourage digital disconnection.

**Governance (G):**

- **Privacy and security:** we reinforced communication and awareness-raising programmes to ensure that messages reach all corporate levels and locations.

**+** For further information, see 2.18. Privacy and security

Milestones

- 1 13% of our employees received training through the Responsible Business Principles course in 2023.
- 2 We launched the ESG Academy for employees.

# 2.16. Ethics and compliance

## Key points

### Zero tolerance

of corruption and bribery throughout the value chain. 5.823 suppliers have received guidance on integrity during 2023.

### 94,990

employees trained in anti-corruption training since the launch of the Training Framework in 2022.

### New Policy

on the Internal Information System Management (Whistleblowing Channel), which defines the principles that govern it, with special reference to whistleblower protection and prohibition of retaliation.

## 2.16.1. Vision

Our vision is to consolidate our **ethics and compliance culture** by strengthening the standards of compliance with mandatory regulations and maintaining best-in-class ethical and business practices.

## 2.16.2. Governance

GRI 2-12, 2-23

Our ethics and compliance culture is **led** and driven from the **highest levels of our Company**. We are **firmly committed to zero tolerance for corruption and bribery** and to other best business practices. Likewise, we have clear lines of responsibility and definitions of key risks in this area.

The Telefónica Group's commitment to fighting corruption and bribery and in general to regulatory compliance led the **Board of Directors of Telefónica, S.A. to approve the creation of an independent regulatory compliance area** on 16 December 2015, as well as the subsequent appointment of a **Chief Compliance Officer of the Telefónica Group** in February 2016. This officer reports directly to the Board of Directors through the Audit and Control Committee.

The goal behind these two developments was to continue with the implementation of a compliance model at Telefónica in a much more targeted way, without prejudice to all the activities carried out to date by other areas of the Company in an effort to prevent corruption and bribery (for example, the Internal Audit, Global Sustainability Management (ESG) and Legal areas).

As well as his appointment, the dismissal of the Chief Compliance Officer is the responsibility of the **Board of Directors of Telefónica, S.A.** through the **Audit and Control Committee**, and its purpose is to manage the preventive and reactive environments related to compliance with (a) legislation and (b) Telefónica's internal regulations at a corporate and operational level (countries and businesses), in general and with a specific focus on those that are more sensitive according to the circumstances.

The Chief Compliance Officer reports regularly to the Audit and Control Committee on the main aspects of the Telefónica Group's compliance programme as well as the Group's practices in terms of integrity and the fight against corruption and bribery.

## Ethics and Compliance governance

### Board of Directors

Audit & Control Committee

Chief Compliance Officer

### 2.16.3. Policies

The internal regulations (drawn up in accordance with the Telefónica Group's Regulatory Framework) which develop the Responsible Business Principles – our code of ethics – with regard to integrity, ethics and compliance are listed below:

- [Anti-Corruption Policy.](#)
  - Corporate Rule Executive Certification in terms of Anti-Corruption..
- Compliance Function Policy.
  - Compliance Function Regulation.
- Local crime prevention policies and regulations.
- Internal Code of Conduct for Securities Markets Issues.
- Regulation on Relationships with Public Entities
- Regulations on Procurement Related to Public Entities.
- Policy on the Internal Information System Management.
  - Regulation on the Management Procedure of the Internal Information System.
- Business Principles Channel Management Regulations.
- Corporate Policy on the Comprehensive Discipline Program.
  - Manual of the Disciplinary Action Committee .
- Conflict of Interest Regulations.
- Regulation on Sanctions.
- Policy on Competition Law.

### 2.16.4. Impacts, risks and opportunities

One of our main challenges in ensuring the Company's future and sustainability and having a positive impact on society is to consolidate a culture of ethics and compliance. This will allow us to contribute to the economic and social development of the local communities in which we operate and ensure 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 programs represent a challenge to implementing this culture. Therefore, we constantly adapt our compliance activity to the prevailing needs of each company or business unit to the applied legislation. Compliance risk is part of the Group's risk map, thus allowing us to achieve our objectives and contribute to the of value creation.



For further information, see 3. Risks

In addition, we promote training and awareness-raising initiatives as key elements of our compliance program. This allows us to consolidate our culture so that our employees can make ethical and responsible decisions when faced with dilemmas and conflicts in their day-to-day work.

### 2.16.5. Action plan and commitments GRI 2-23, 2-25

Our Compliance Program is made up of several lines of action designed to ensure ethical behaviour throughout our Company: 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, and possible remediation plans.

All of this is included in the 2023 Compliance Function Annual Report, which sets out the Compliance area's main lines of action for the year. This information is complemented by the Action Plan for the following year, both documents are presented to the Audit and Control Committee.

#### Objectives

- Develop and implement new training in 2024 to refresh anti-corruption knowledge.
- Reinforce the control environment of the Telefónica Group's procurement model through the definitive implementation of new compliance protocols and/or the adaptation of existing ones.

### 2.16.5.1. Compliance

#### GRI 205-2

The Compliance Function Policy, approved by the Board of Directors in 2016 and last updated in July 2023, defines the main lines of the Telefónica Group's Compliance Program, how it interacts with the Company's business processes and other areas, and the most relevant issues. The starting point for compliance management is risk assessment and the protection of integrity.

In accordance with the current Compliance Function Policy, the Compliance Function is deployed on two levels:

- **Preventive control** to generate a culture of compliance. This is implemented through the following functions:
  - Compliance area: responsible for coordinating the Group's regulatory framework. Plays a key role in establishing regulations and protocols aimed at preventing unlawful and unregulated conduct, with different levels depending on the sensitivity of the situation.
  - Knowledge management: involves training and awareness-raising activities on issues such as anti-corruption, crime prevention and sanctions, in addition to supporting other Company training initiatives.
  - Ongoing assessment of compliance risk and effectiveness of controls.
  - Consultative activities conducted via the channels available to employees for raising queries about compliance issues (mainly concerning the application of the Anti-Corruption Policy and other related internal regulations).

Another line of action is geared towards coordinating all initiatives related to third-party involvement in regulation enforcement. In this regard, Telefónica believes it is of the utmost importance that the third parties with whom it interacts in the context of certain relationships comply with the corresponding standards of business ethics.

Therefore, in addition to implementing measures such as responsible declarations and contractual safeguards, we have developed **protocols for assessing suppliers and business partners from a compliance point of view**. The protocols assess anti-corruption, money laundering and terrorist financing risks and are applied as part of an ethos of continual improvement. Telefónica's procurement and payment controls are particularly important in this context, hence the involvement of Compliance.



For further information, see 2.19. Responsible supply chain management










#### • Reaction and response

- **Reaction** refers to existing action protocols for situations where there are signs of non-compliance. Telefónica has an Internal Information System designed in accordance with Law 2/2023 to promote compliance with the Responsible Business Principles, the law and other internal regulations. The System has mechanisms in place to ensure the confidentiality of the communications and complaints it processes.
 

By appointment of the Board of Directors, the Chief Compliance Officer is responsible for the Internal Information System, carrying out his functions autonomously and having the necessary personal and material resources
- **Response** encompasses the remediation of consequences by mitigating the consequences of all kinds associated with a potential violation or a violation already evidenced, and ensuring uniformity in the application of consequences for such violations, as well as promoting the recognition of employees with outstanding behaviour in terms of their commitment to compliance.

In a dynamic prioritisation exercise, we have identified the areas in which to deploy compliance controls that go beyond the protection of integrity and international sanction systems.

**Compliance Program areas**

Integrity and sanctions	 Privacy and personal data protection	 Relationships with competitors	 Security, including the protection of confidential information	+  Artificial intelligence
	 Labour	 Sustainability and human rights	 Compliance with sector-specific regulations and customer promise	
	 Tax compliance	 Compliance with specific financial regulations – money laundering and terrorist financing	 Regulated areas of Compliance (insurance and pension plans and funds) <sup>1</sup>	

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

**Compliance – anti-corruption**  
GRI 2-23, 205-1

The main aspect supervised by the Compliance area and on which we focus a large part of our policies, procedures and controls is **integrity**. This includes, among others, initiatives that implement our fight against corruption and bribery.

Among the policies and procedures implemented in the Telefónica Group, we have specific internal regulations aimed at combatting corruption and bribery. The most significant of these is the **Anti-Corruption Policy**, which is aligned with the provisions of the 2004 United Nations Convention against Corruption.

Among other aspects, the Anti-corruption Policy sets out guidelines for the conduct to be followed at Telefónica with regard to accepting or offering gifts or invitations and prohibits any type of bribery. In the case of offering gifts or invitations to employees and public officials, this aspect is specifically developed by the Regulations on the Relationship with Public Entities.

The regulatory framework is complemented by the **Conflict of Interest Regulation** and the **Corporate Policy on the Comprehensive Disciplinary Programme**, among others.

The Conflict of Interest Regulation require us to act at all times, and especially in the event of a conflict of interest, in accordance with the corporate principles of loyalty, confidentiality and integrity. It also regulates those situations in which an employee’s direct or indirect personal interest influences, could influence or generates the perception of being able to influence the professional decisions to be adopted by that employee, and this interest or professional benefit may collide with the interests of a company of the Telefónica Group.

The Company’s directors and executives as the parties responsible for establishing the controls and procedures needed to ensure compliance with the Anti-Corruption Policy, certify their knowledge and commitment to the Policy, the Responsible Business Principles and associated policies, practices and regulations on an annual basis. In 2023, 100%<sup>2</sup> of the executives in active employment signed the anti-corruption certificate.

Corruption risk analysis is another focus area of Telefónica’s Compliance Program.

As part of the Risk Management Model, which is based on the guidelines of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and has been implemented uniformly across the Group’s main operations, the Company’s senior management perform timely identification, assessment, response and monitoring of compliance risks within their scope of action. This exercise covers a variety of matters, one of the most important being integrity, which encompasses the obligations associated with the Responsible Business

<sup>1</sup> Regulated areas: this refers to compliance with legislation applicable to insurance and reinsurance companies and pension fund and investment fund management companies.

<sup>2</sup> Only one executive who is on leave from work is pending.

Principles, and those relating to practices that prevent corruption in particular. The exercise to review the operators' risk map, including the basic compliance risk, is carried out on a semi-annual basis.

In 2023, the **annual assessment** of aspects related to compliance risks, and therefore corruption risks, covered 100% of our operations.

	2022	2023
Operations assessed based on corruption-related risks.	100%	100%



For further information, see 3. Risks

The following Group companies have the UNE 19601:2017 Management System for Criminal Compliance certification: Telefónica, S.A. and Telefónica de España, S.A.U., and Telefónica Móviles España, S.A.U. and the companies in its scope of consolidation (Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U. and Teleinformática y Comunicaciones, S.A.U.). All of these companies renewed their certifications in 2023.

Colombia Telecomunicaciones and Telefónica del Perú S.A. also renewed their ISO 37001:2016 Anti-Bribery Management Systems certification in 2023. In addition, Telefónica de España, S.A.U., Telefónica Móviles España, S.A.U. and the companies within its scope (Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U. and Teleinformática y Comunicaciones, S.A.U.), and Telefónica Cybersecurity & Cloud Tech Perú SAC obtained this certification for the first time last year.

### Compliance – sanctions

At present, international sanction regimes – understood to be 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 a highly complex and increasingly relevant situation.

Telefónica is committed to conducting its business in compliance with the international sanctions regimes that may apply to it at any given time. The **Regulation on Sanctions** defines the Company's main controls in this area and reinforces Telefónica's commitment to compliance with the sanction regimes.

### Compliance – competition GRI 206-1

Fair competition is one of our Responsible Business Principles and it is integrated across the entire Company via various internal policies and processes.

In 2022, in order to strengthen our Compliance Programme in this area, the Board of Directors approved the first **Policy on Competition Law of the Telefonica Group**. This formalised our commitment to the principle of fair competition enshrined in the Responsible Business Principles, in a standard that facilitates compliance with fair competition practices in all markets and reflects our belief in free markets and fair competitive conditions.

Following approval of the Policy on Competition Law, the course on competition law, which is included in the Training Framework and is aimed at all Telefónica Group employees, was reviewed and updated. Additionally, training sessions are also to previously identified specific areas.

In addition, specific training sessions have been delivered to different areas of the Company in relation to the new Regulation 2022/2560 of the European Parliament and of the Council on foreign subsidies distorting the internal market to make sure that employees are aware of the new obligations and can comply with them.

The Group also has guidelines in place for participation in industry organisations and meetings with competitors to ensure compliance with competition law regarding the exchange of sensitive information. This is complemented in some countries by specific competition compliance programs in accordance with local legislation (e.g. Chile).

In 2023, no material judicial proceedings<sup>3</sup> were in progress for violation of competition law and no fines were paid for anticompetitive practices.

	2022	2023
Number of material legal proceedings in progress in relation to anti-competitive practices during the last fiscal year	0	0
Total amount of material fines paid for anti-competitive practices in the last fiscal year (€M)	67	0



For further information, see the Consolidated Financial Statements

<sup>3</sup> 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).

**Compliance – money laundering**  
GRI 205-2

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

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

**2.16.5.2. Training**  
GRI 205-2

Anti-Corruption training is a key element of promoting a culture of ethics within the Company. Our training in this area includes the following courses:

- The **Business Principles and Human Rights** course, which covers issues relating to anti-corruption and bribery in the section entitled "Ethical and Responsible Management".

**+** For further information, see 2.15. Governance and culture of sustainability

- The **Foreign Corrupt Practices Act (FCPA)** course, which 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 (that include content related to crime prevention) are given 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. It is worth mentioning the training in criminal liability in Peru, Argentina, Chile and Ecuador, and at Telefónica Spain and its perimeter companies.

- Courses relating to the **sanctions** program. Throughout 2023 we continued to deliver sessions to target areas of the Company.

The Responsible Business Principles, Competition Law, FCPA and Crime Prevention at Telefónica, S.A. courses were integrated into the **Training Framework** that was launched in June 2022 on a Group-wide basis. As of 31 December 2023, 32,432 employees had received anti-corruption training, which represents 31% of the general workforce.

With regard to the Board of Directors, all members have received anti-corruption training, with the exception of the two new members who joined in December 2023. They will receive training at the beginning of 2024.

- **Information on integrity for third parties.** A project was launched in 2023 to share our main integrity regulations and the consequences of non-compliance with our value chain. Under the project, every six months this information is sent to all suppliers selected in the immediately preceding six-month period. At the close of this report, a total of 5,823 suppliers have received this information.

**Anti-corruption training since Training Framework launch**

	2022	2023
Number of employees trained in anti-corruption matters since its launch.	94,840	94,990
Percentage of employees trained in anti-corruption matters since its launch.	93%	91%

**Awareness raising**

Another crucial element of the Compliance Programme is awareness raising. In addition to the publication of news and updates on the Group's internal channels, we have a number of global and local initiatives aimed at fostering a culture of compliance among employees. Of the initiatives carried out in 2023, the following are particularly noteworthy:

- a. **Compliance Day**, a global internal awareness day designed to familiarise the business with the Compliance Function and raise employee awareness of current issues dealt with by our Compliance Programme. As part of this activity, we launched a **Compliance Challenge** featuring five games related to compliance concepts.
- b. The **Five Stars Recognition Programme**, a programme developed to promote and recognize displays of outstanding commitment to the issues of integrity and sanctions, privacy and security. The fifth edition was held in 2023, with 83 employees from our different local and global operations and companies receiving recognition.

c. **Compliance Cafés**, informal meetings aimed at acquainting different areas of the Group with the Compliance Function and raising awareness of the

importance of acting appropriately in certain situations that may arise on a day-to-day basis.

### Employees receiving anti-corruption training in 2023 by professional category and region

Country	Senior Management	Middle Management	Other Professionals	Total
Germany	132	292	2,986	3,410
Brazil	803	967	14,498	16,268
Spain	657	337	4,778	5,772
Hispan	352	390	5,366	6,108
Other	33	99	742	874
<b>TOTAL</b>	<b>1,977</b>	<b>2,085</b>	<b>28,370</b>	<b>32,432</b>

### % of employees receiving anti-corruption training in 2023 by professional category and region

Country	Senior Management	Middle management	Other Professionals	Total
Germany	53%	36%	40%	40%
Brazil	46%	37%	21%	46%
Spain	41%	12%	21%	21%
Hispan	46%	13%	20%	20%
Other	51%	43%	74%	67%
<b>TOTAL</b>	<b>44%</b>	<b>22%</b>	<b>31%</b>	<b>31%</b>

### 2.16.5.3. Complaint and remedy mechanisms: Whistleblowing and Queries Channel

GRI 2-16, 2-26

#### Complaints

GRI 3-3, 406-1

During the 2023 financial year, Telefónica **adapted its Whistleblowing Channel to the new regulatory requirements**. In June 2023, the Board of Directors approved Telefónica's Internal Information System Management Policy and Procedure, aligning them with Spanish Law 2/2023 of 20 February, which regulates the protection of individuals who report regulatory violations and the fight against corruption. In addition, the Board also appointed the Chief Compliance Officer, responsible for the Internal Information System (hereinafter referred to as "the System"). The Policy sets out the general principles governing the System, whistleblower protections, the prohibition of retaliation and the complaints handling procedure.

The Whistleblowing Channel forms part of the System and is the main tool that Telefónica makes available to all employees, managers and directors of its companies, as well as associated third parties, for anonymously or personally reporting any information about the Telefónica

Group that may involve any alleged irregularity or act in breach of the law or internal regulations.

All communications can be made in writing or verbally. The Whistleblowing Channel is **accessible 24/7 via the Company's website and intranet, f numbers and dedicated email accounts**. The channel also allows users to check the status of a complaint, add information and contact the team responsible for the analysis.

The Compliance area investigates the received complaints carefully and promptly, ensuring that are verified and boosts measures to resolve or mitigate them in accordance with the internal regulations and procedures in place.

Complaints can fall into different categories. The main ones are:

- Labour disputes (harassment at work, sexual harassment and discrimination)
- Labour conditions
- Information security/privacy
- Acts contrary to the integrity of the Company (public and private corruption)
- Asset fraud



- Favorable treatment
- Financial reporting, including any irregularities in accounting, auditing and/or internal control over financial reporting, in compliance with Section 301 of the US Sarbanes-Oxley Act, among other requirements.
- Regulatory/contractual/legal non-compliance

In 2023, we received 912 complaints through the Whistleblowing Channel. Following investigation, 328 complaints were substantiated. Regarding the substantiated complaints, the Company established individualised action plans aimed at resolving or mitigating the detected situations. Among the measures taken was the termination of 109 employment contracts.

## Complaints

Nature of substantiated complaints	2022	2023
	% of total substantiated complaints	% of total substantiated complaints
Failure to comply with regulations	15%	17%
Fraud	21%	32%
Workplace/sexual harassment and/or discrimination	3%	8%
Conflict of interest	5%	7%
Information security/privacy	3%	1%
Inappropriate behaviour and other workplace disputes	41%	25%
Other	12%	10%
<b>Total</b>	<b>374</b>	<b>328</b>

## Main indicators for complaints

### GRI 205-3

	2022	2023
Complaints received	808	912
Substantiated complaints	374	328
Termination-of-employment measures taken as a result of substantiated complaints	118	109
Confirmed cases of corruption	0	0
Disciplinary measures taken or contracts terminated in connection with confirmed cases of corruption	0	0
Cases of discrimination detected	0	0
Disciplinary measures taken or contracts terminated in connection with confirmed cases of discrimination	0	0

In 2023 Compliance deployed 9,829 working days (10,020 in 2022) to activities related to Whistleblower management, that are classified according to their nature in the previous table.

## VM02

	2023
Confirmed cases of corruption	0

## Queries

We also have a channel through which all our stakeholders can submit queries, anonymously or personally, about any issue related to the Responsible Business Principles.

In 2023, we received 622 queries related to these Principles. The topics of the queries received are shown in the following table<sup>4</sup>.

### Queries<sup>5</sup> 418-1

	2022	2023
Responsible Communication	6	5
Integrity	9	4
Environment	67	35
Supply chain	14	4
Privacy	32	10
Accessibility	5	11
Sustainable innovation	3	0
Human rights	5	2
Children's rights	0	0
Freedom of expression	0	2
Diversity and talent management	14	18
Network, Infrastructure and Maintenance	N/A	169
Responsibility with the Customer	N/A	85
Partners and suppliers	N/A	5
Responsible use of technology	N/A	0
Repeated incidence	N/A	9
Others	556	263
<b>Total</b>	<b>711</b>	<b>622</b>

In 2023, as in previous years, the handling of these queries led to the identification of improvements not only in our complaint and remedy mechanisms, but also in our policies and procedures for the internal management of stakeholder queries.

In order to improve the management of queries received, the tool was updated in 2023 to allow for two-way communication with stakeholders, among other improvements. The [internal regulation on Queries Channel Management](#) was also updated to bring it in line with this new development.

## 2.16.5.4. Supervision of internal control

The Telefónica Group has an internal control model defined in line with the provisions of the Internal Control - Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The use of this Framework by the Group facilitates the recognition and validity of the company's internal control system before third parties, such as external auditors or supervisory bodies. Thus, for example, the Securities and Exchange Commission (SEC) expressly recognises the COSO integrated framework as a valid internal control model. In accordance with the applicable Corporate Governance frameworks, Internal Control considers both financial and sustainability aspects, including operational, technological, legal, social, environmental, reputational and regulatory compliance aspects.

Telefónica's Board of Directors is the Company's highest supervisory and control body, with the support of the Audit and Control Committee in its supervisory functions. The Internal Audit Department, in turn, supports the Audit and Control Committee in its competencies regarding the assurance of the internal control system, through different channels of action. For further details on the activities of the Internal Audit function, see section 4.7 Internal Control and Risk Management Systems in relation to the Financial Information Issuance Process (SCIIF).

In accordance with the provisions of the US Sarbanes-Oxley Act (the SOX Act), the Telefónica Group is subject to various requirements, pursuant to which it performs relevant and mandatory oversight of the internal control environment for financial reporting and fraud and corruption prevention actions, as well as other, broader aspects of internal control within the Company that may ultimately affect the information to be published. Among other aspects, these oversight procedures aim to:

- Strengthen corporate governance by establishing stricter oversight requirements for Management and the Board of Directors, thereby helping to prevent fraud.
- Increase the accountability of Management at the Company at all levels to ensure the accuracy and completeness of financial reporting by imposing severe penalties for fraudulent activities.
- Protect whistleblowers by encouraging the reporting of corporate fraud and preventing possible retaliation.
- Identify the need to establish and regularly assess an internal control framework over financial reporting to reduce the risk of financial fraud.

<sup>4</sup> In 2023, the topics of the Queries Channel were expanded. This allowed us to improve identification and reduce the number of queries received in the "others" category from the second semester onwards.

<sup>5</sup> Changes are introduced in the reporting methodology, showing the topics of inquiries received instead of those handled. To allow comparability, the 2022 data are recalculated according to this criterion.

These SOX Act-related procedures therefore mandate monitoring of internal control over financial reporting, and of disclosures in general, to identify fraud issues that may have involved Company executives who are in a position to exercise influence over the financial statements or those who prepare them.

From a fraud prevention perspective, these activities have an important role to play in achieving this aim, by ensuring the proper functioning of internal controls and assessing their effectiveness on an annual basis, in order to identify and remedy control deficiencies that could be exploited to commit fraudulent activities.

To comply with the Sarbanes-Oxley Act and other legal requirements, the Telefónica Group, through the Internal Audit area (which is functionally and hierarchically independent as it reports directly to the Audit and Control Committee), annually evaluates the effectiveness of internal controls (on risk management processes, systems and protocols) and entity-level controls, with the Company publicly reporting on this effectiveness.

These oversight activities include reviewing entity-level controls in the field of ethics. They complement other Company fraud prevention and detection procedures, identifying control deficiencies and recommending improvements in relation to aspects related to these potential practices.

In addition, the Internal Audit area carries out different types of activities and review procedures on aspects of fraud to evaluate their impact on the design or operation of internal control. Some of the lines of action of Internal Audit in this area are indicated below:

- Targeted reviews of security settings of network elements and IT systems.
- Technology reviews of key IT processes and applications, as well as cybersecurity and data privacy aspects.
- Regular regulatory compliance reviews in areas such as the prevention of money laundering and terrorist financing.
- GDPR and data privacy compliance reviews.
- Monitoring of controls over the reporting and breakdown of related-party transactions, as well as compliance with the control measures of the crime prevention model.
- Reviews of certain compliance program controls, including specific anti-corruption controls.

In order to carry out its procedures for supervising internal control over financial reporting, the Telefónica Group carries out review activities through the Internal Audit area, allocating over 15,000 working days each year for this on a recurring basis. The Statutory Auditor also publicly issues their own independent conclusions on the internal control environment. These review efforts are designed to provide the necessary coverage for the processes of preparing and reporting the Telefónica Group's consolidated financial information in order to be able to achieve a level of reasonable assurance on the system of internal control over financial reporting (SCIIF).

On the other hand, Internal Audit supervision activities, complementary to the above and corresponding to other technological reviews, audits of reporting and business processes, as well as other Internal Audit activities not included in other sections of this Report, involve recurring efforts of more than 29,500 working days per year.

Our Whistleblowing and Queries Channel is accessible online to all our stakeholders, including suppliers, and is available in different languages.

## Milestones

- ❶ Our Internal Information System has been adapted to Law 2/2023 of 20 February, which regulates the protection of individuals who report regulatory infringements and the fight against corruption.
- ❷ We have shared our main integrity regulations and the consequences of non-compliance with our suppliers.
- ❸ Almost 95% of the queries received through the Queries Channel were resolved during the reporting year.

## 2.17. Fiscal transparency

### Key points

19

euros per every 100 euros of turnover is Telefónica's tax contribution in 2023.

7,580

million euros are the taxes paid during 2023 of which 2,464 million euros are borne taxes and 5,116 million euros are collected taxes.

MSCI

and S&P DJSI has awarded us the highest score, once again, for our tax transparency.

### 2.17.1. Vision

GRI 207-1

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

At Telefónica we adhere to the OECD guidelines for multinational companies in order to ensure strict compliance with our **tax obligations**. We strive to be a model of best practice, ensuring that we contribute faithfully and loyally to the public finances of the countries and territories in which we operate and that we are fully compliant 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 places in which it operates.

Accordingly, and in line with our commitment to fiscal transparency and the UN Sustainable Development Goals (SDGs), we publish our total economic and social tax contribution on our corporate website, in the section sustainability-innovation/how-we-work/sustainability-strategy.

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

### 2.17.2. Governance

GRI 207-1, 207-2

The **bodies responsible for Telefónica's fiscal control framework** are as follows:

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 lead**, develop and review the tax strategy.

Every year the Group's Tax Department and the Regional Divisions report to the Audit and Control Committee and, where appropriate, to the Board of Directors on the following matters:

- The tax policies and criteria that the Group follows in order to facilitate the task of supervising the tax risk management system, which, in accordance with the provisions of the Code of Good Tax Practices, is entrusted to the Audit and Control Committee by the Spanish Corporations Act.
- 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.

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

### 2.17.2.1. 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 criteria 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, every year Telefónica validates compliance with the content and commitments of the Code of Good Tax Practices and, therefore, validates that it is complying with its governance framework.

### 2.17.2.2. Integration of the Telefónica Group's fiscal approach

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 tax at each company participate in analysing all transactions that may have tax implications. When doing this:

- They are provided with 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 about this, see the core principles of the fiscal control function that Telefónica has developed as part of its Fiscal Control Policy (available on the corporate website in the section sustainability-innovation/how-we-work/sustainability-strategy).

## 2.17.3. Policies

### GRI 207-1

The **Fiscal Control Policy**, which is approved by the Board of Directors and available on the Telefónica website, has the following targets:

- Correct fulfilment of tax obligations in due time and form.
- Effectiveness and efficiency of operations from a tax perspective.
- Duly supported and documented position-taking or tax strategy.
- Reliability of tax information.
- Transparency vis-à-vis third parties, especially the tax authorities.
- Tax risk management.

## 2.17.4. Impacts, risks and opportunities

### GRI 207-2

We are aware of the impact we have on society and of our contribution to economic development through taxes and other specific contributions. For this reason, transparency is key to communicating tax information in a visible, understandable and complete manner. This allows us to build trust with all our stakeholders.

With regard to tax risks, and as generally defined for the Company, the Group has a level of risk tolerance or acceptable risk established at corporate level, meaning the willingness to assume a certain level of risk, to the extent that it allows the creation of value and the development of the business, achieving an appropriate balance between growth, return and risk.

In assessing tax risk tolerance, the Company takes into consideration the various circumstances that may affect this type of risk, such as the legal, political and regulatory environment of the country in question. Consequently, this sensitivity threshold is analysed annually on the basis of the aforementioned criteria, both for the Group as a whole and for its main component companies. In any case, the Group always assesses its tax risk tolerance on the basis of correct and strict compliance with tax regulations in each of the countries in which we operate.

As mentioned on the corporate website, in "How we work", we manage tax risks in order to prevent and reduce tax litigation to that which is necessary to defend the tax positions legitimately adopted by Telefónica.

To this end, Telefónica has a **Risk Management Model** based on COSO (Committee of Sponsoring Organizations of the Treadway Commission), which facilitates the identification, assessment and management of the different risks, as detailed in Chapter 3 on Risks.

Under this model, **four risk categories** are defined: business, operational, financial and legal, and compliance. In this respect, the latter category includes **tax risks**.

Tax risk typology and associated controls

In relation to their origin, risks of a tax nature are classified as follows:

- **Compliance risk:** relating to the fulfilment of obligations in the tax field (submission of declarations, information requirements, etc.).
- **Interpretative risk:** the possibility of interpreting tax laws differently from the Administration's criteria.
- **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 the perception by different stakeholders of companies' fair compliance with their tax obligations.

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 Tax Control Policy, available on the corporate website, section Sustainability-Innovation/How we work/Strategy-Sustainability.

#### 2.17.4.1. Reporting obligations

Every quarter those responsible for tax control at each of the Group's companies inform the Tax Department – through the Regional Tax Divisions – of the main conclusions of the tax risk identification and assessment process, 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 inspection processes by the tax authorities.

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

#### 2.17.5. 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.

### 2.17.5.1. Regulatory compliance

At Telefónica we are committed to complying with all national and international tax legislation, regulations and obligations, respecting both their letter and their spirit.

In fact, we devote all necessary resources and take all appropriate measures to make a reasonable interpretation of the rules, taking into account the legislator's intention pursuant to 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 pledge that any position we may take on tax shall serve our commercial and business interests, that we shall pay taxes according to their true legal nature and economic substance, and that we shall avoid abusive tax planning schemes or practices. Consequently, 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 when engaging in transactions with related entities; the tax we pay in each country and territory is relative to the business we do there and the generation of value, as laid down in local tax legislation and the international taxation standards established by the OECD.

### 2.17.5.2. 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 that is inspired by the principles of collaboration, trust, good faith, loyalty, professionalism, mutual respect and dialogue.

In order to apply the highest standards of tax transparency, since 2010 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 Administration.

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, as authorised by the Audit and Control Committee within the functions delegated by the Board of Directors. More information about this can be found on our corporate website, in the section [sustainability-innovation/how-we-work/sustainability-strategy/fiscal transparency](#).

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

We also participate in the cooperative compliance program in UK.

#### Contribution to legislative initiatives on 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 during 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 the European Telecommunications Network Operators' Association (ETNO) 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 Spanish Confederation of Business Organisations (CEOE) and the DET3 (Digital Economy Taxation Think Tank).

#### Stakeholder dialogue

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

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




For further information, see 1.4. Materiality

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

In fact, thanks to our progress in this area, we were awarded the highest score in the S&P DJSI, MSCI and Sustainalytics indices.

### Reporting unethical behaviour

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

 For further information, see 2.16. Ethics and compliance

Telefónica's Whistleblowing and Queries Channel handles all tax issues reported by our various stakeholders.

## 2.17.6. Progress in 2023

GRI 207-2

### 2.17.6.1. Contribution to the development of local economies and local finances

GRI 201-4

In 2023, our total tax contribution (CTT) amounted to EUR 7,580 million (EUR 2,464 million to taxes borne and EUR 5,116 million to taxes collected), representing 50% of our distributed value<sup>1</sup> (distributed value as taxes borne and collected over total distributed value, the latter being the sum of the following items: shareholder value - profit after tax, wages and salaries net of taxes collected, net interest and taxes borne and collected).


The total grants received by Telefónica in 2023 were EUR 28 million (EUR 17 million in 2022), which includes the receipt of capital grants and grants for other income.

The Group has not used any tax deductions in the last corporate income tax return filed in Spain.

For every 100 euros of turnover, we spend 19 euros in taxes (6 on taxes borne and 13 on taxes collected).

It is important to note that our economic and social contribution is not only quantifiable through income from corporate tax, but also through other comparable contributions with an impact on the profit and loss account, taxes, local taxes and social security payments.

In addition to these directly borne taxes, we generate revenue for the public coffers, as a result of our 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, employee withholding taxes and other withholdings.

 For further information, see 2.13. Contribution and impact on communities

### 2.17.6.2. Contribution in the countries

GRI 207-4

The following is a breakdown of the jurisdictions in which the Telefónica Group carries out its principal activity as a telecommunications service provider. Those other jurisdictions where the Group is present and whose activity is not its core business have been included under 'Other'. All amounts are in millions of euros and refer to the year 2022.

The main companies comprising the Telefónica Group, as well as their principal activity, can be consulted in the 2023 Consolidated Financial Statements.

 For further information, see Appendix I: Scope of consolidation

<sup>1</sup> Calculation based on our own methodology.



For the purpose of reconciliation with the figures reported in the Consolidated Financial Statements, consolidation adjustments and eliminations of intercompany transactions between Group companies in different countries, as well as the share in income of investments accounted for by the equity method, are also included under 'Other'.

However, there are differences with the Group's Consolidated Financial Statements, which are explained below:

- The Annual Accounts only include information on sales to third parties, while the CbCR (Country-by-Country Report) also includes a breakdown of intra-group sales.

- In relation to the profit or loss before tax, there is an adjustment for the allocation to the year of the coupons corresponding to the subordinated perpetual bonds in the Netherlands.
- The differences with regard to taxes borne are due to the inclusion in the annual accounts not only of corporate income tax (as in the case of CbCR), but also of telecommunication charges, local taxes, other charges, licence fees, social security, etc.

### Country by country report 2022

Tax jurisdiction	Unrelated parties income	Related parties income	Total Income	Profit or loss before income tax <sup>2</sup>	Income tax paid <sup>3</sup>	Income Tax Accrued	No. of employees <sup>4</sup>	Tangible assets
Germany	8,894	113	9,007	752	103	-174	7,716	3,518
Argentina	2,449	129	2,578	-166	61	34	11,725	1,489
Brazil	9,734	75	9,809	921	250	143	34,666	6,250
Chile	1,957	144	2,101	64	9	-6	4,118	1,165
Colombia	1,687	130	1,817	136	69	134	6,145	734
Ecuador	477	9	485	23	-2	9	940	231
Spain	15,354	1,839	17,193	798	383	77	27,357	8,466
Mexico	1,212	71	1,283	-228	10	9	1,894	134
Peru	1,936	27	1,963	-100	112	259	4,554	1,198
Uruguay	272	143	415	152	15	18	591	339
Venezuela	275	86	361	95	10	50	1,644	50
Other	799	-1,039	-241	236	-8	18	1,134	139
<b>Total</b>	<b>45,046</b>	<b>1,726</b>	<b>46,771</b>	<b>2,682</b>	<b>1,010</b>	<b>571</b>	<b>102,483</b>	<b>23,714</b>

<sup>2</sup> Profit or loss before tax and income tax, adjusted for the allocation to the year of the coupons corresponding to the subordinated perpetual debentures. The consolidated financial statements of the Telefónica Group are prepared in accordance with International Financial Reporting Standards (IFRS) as adopted by the European Union. The local accounting standards applicable in each of the countries in which the Group operates may differ from IFRS. The table above groups all the Group companies according to the country of their tax residence. This grouping does not coincide with the Telefónica Group's segment breakdown. The results by country include, where applicable, the effect of the allocation of the purchase price to the assets acquired and liabilities assumed. Likewise, results by country exclude dividend income from Group subsidiaries, as well as the change in the provision for depreciation of investments in Group companies, which are eliminated in the consolidation process. The differences between the result of the Country-by-Country Report and the contribution per country to the Group's profit before tax correspond to the companies reporting under the equity method.

<sup>3</sup> Excluded in 2022 are refunds received from different administrations, which correspond to overpayments of taxes from previous years, specifically EUR 115 million in Spain and EUR 12 million in Peru and Chile. Also excluded in Spain is the extraordinary refund deriving from the Enforcement Agreement of the National Court Judgment (790 million euros). Withholding taxes paid to the various tax authorities have been allocated to the jurisdiction that actually bears them.

<sup>4</sup> The number of employees refers to the average number of employees, distributed by tax jurisdiction.

### 2.17.6.3. 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 2022, the differences correspond to the permanent differences inherent to the mechanics of corporate income tax preparation. In other words, they comprise all those expenses or income recorded in the income statement that will not be deductible or will not be taxed for tax purposes and will therefore never be reversed in subsequent periods.

The most relevant are: the deductibility of the amortisation of goodwill in Spain and the deductibility in Brazil of the distribution of Juros on capital. There is also a significant difference due to the non-activation of tax credits in countries with negative results.

In addition, during 2022, there were extraordinary accounting entries in the income tax expense account that justify a significant part of the differences between the statutory rate and the effective rate.

In this regard, mainly recorded in Spain were the effects derived from the agreement to enforce the National Court ruling of October 24, 2022 with its corresponding impact on the company's tax credits, the reversal of a tax provision in Germany as a result of the closure of the tax audit of Group 3G UMTS Holding GmbH and the recording of a provision for tax contingencies by Telefónica del Perú.

The verification of the taxation content has been completed as part of the external verification process which has been carried out by PricewaterhouseCoopers Auditores, S.L.

### Tax contribution in each country

Million euros	Contribution by country to consolidated Group profit before tax 2023 <sup>5</sup>	Contribution by country to consolidated Group profit before tax 2022 <sup>5</sup>	Taxes borne 2023	Taxes collected 2023	Total 2023
Germany	624	697	343	905	1,248
Argentina	(167)	(166)	169	241	410
Brazil	1,063	919	679	1,526	2,205
Chile	(122)	64	6	78	84
Colombia	(100)	118	140	123	263
Ecuador	(20)	23	51	18	70
Spain	(1,264)	795	950	1,938	2,887
Mexico	(19)	(228)	21	59	81
Peru	(157)	(103)	30	126	156
Uruguay	148	152	24	35	59
Venezuela	101	95	16	18	34
Other	(1,899)	316	34	48	83
<b>Total</b>	<b>(1,812)</b>	<b>2,682</b>	<b>2,464</b>	<b>5,116</b>	<b>7,580</b>

<sup>5</sup> Profit or loss before tax and income tax, adjusted for the allocation to the year of the coupons corresponding to the subordinated perpetual debentures. The consolidated financial statements of the Telefónica Group are prepared in accordance with International Financial Reporting Standards (IFRS) as adopted by the European Union. The local accounting standards applicable in each of the countries in which the Group operates may differ from IFRS. The table above groups all the Group companies according to the country of their tax residence. This grouping does not coincide with the Telefónica Group's segment breakdown. The results by country include, where applicable, the effect of the allocation of the purchase price to the assets acquired and liabilities assumed. Likewise, results by country exclude dividend income from Group subsidiaries, as well as the change in the provision for depreciation of investments in Group companies, which are eliminated in the consolidation process. The differences between the result of the Country-by-Country Report and the contribution per country to the Group's profit before tax correspond to the companies reporting under the equity method.

The breakdown of the corporate income tax contribution is as follows:

### Tax contribution by region

Million euros	2023		2022	
	Contribution by country to the consolidated Group's profit before tax	Profit tax <sup>6</sup>	Contribution by country to the consolidated Group's profit before tax	Profit tax
Europe	(640)	439	1,492	486
Brazil	1,063	201	919	250
Hispania	(336)	142	(45)	282
Other	(1,899)	9	316	(8)
<b>TOTAL</b>	<b>(1,812)</b>	<b>790</b>	<b>2,682</b>	<b>1,010</b>

The contribution by country to the consolidated Group's profit before tax is adjusted for the allocation to the year of the coupons corresponding to the subordinated perpetual debentures. The consolidated financial statements of the Telefónica Group are prepared in accordance with International Financial Reporting Standards (IFRS) as adopted by the European Union. The local accounting standards applicable in each of the countries in which the Group operates may differ from IFRS.

The table above groups all the Group companies according to the country of their registered office. This grouping does not coincide with the Telefónica Group's segment breakdown. The results by country include, where applicable, the effect of the allocation of the purchase price to the assets acquired and liabilities assumed. Likewise, results by country exclude dividend income from Group subsidiaries, as well as the change in the provision for impairment of investments in Group companies, which are eliminated on consolidation.

## Milestones

- 1 Telefónica is one of the 35 companies that have voluntarily submitted the [2022 Transparency Report to the Tax Authorities in Spain](#).
- 2 Taxes borne and collected amounting to €2,887 million in Spain and € 2,205 million in Brazil.

<sup>6</sup> Excluded in 2023 are refunds received from different administrations, which correspond to overpayments of taxes from previous years, specifically EUR 293 million in Spain and EUR 43 million in Peru and Chile.

Excluded in 2022 are refunds received from different administrations, which correspond to overpayments of taxes from previous years, specifically EUR 115 million in Spain and EUR 12 million in Peru and Chile. Also excluded in Spain is the extraordinary refund deriving from the Agreement for the Enforcement of the National High Court Ruling (790 million euros), as explained in Note 25 of the Consolidated Annual Accounts of 2022. Withholdings paid to the various administrations have been allocated to the jurisdiction that actually bears them.

# 2.18. Privacy and security

## Key points

### Data

monitored at the highest level with high standards of privacy and security.

>95%

of contracts/RFPs with suppliers will contain security requirements by 2025.

75,821

Hours of training for our employees in data protection and cybersecurity with over 94,642 attendees.

### 2.18.1. 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 when 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 endeavour to cultivate our customer's **privacy and security** and generate a relationship of trust with all those with whom we work. In doing so, we focus on the following pillars:

- **Protection:** data must be secure and individuals' privacy must be preserved. This is the foundation of our business and our primary consideration when designing our services and collaborating with third parties.
- **Design:** we apply privacy and security by design, that is, privacy and security are incorporated into the initial concept of our products and services and subsequently throughout the development process.
- **Empowerment:** individuals must be able to manage and control their personal data. This enables access to their data and to additional information about the risks and benefits associated with management thereof.

- **Transparency:** the principle of transparency is about both providing people with straightforward tools that allow them to control their data and having the technological development needed to generate maximum respect for privacy and information security.



For further information, see 2.12.4.4. Secure and responsible use of technology

We also recognise the importance of raising awareness among our employees and relevant third parties and training them on this issue. To this end, we provide specific courses on privacy to employees within the sphere of Telefónica and we also send educational content about the issue to the suppliers we consider most important from a privacy perspective.

In addition, Telefónica is a global leader in the development and marketing of **cybersecurity and managed security products and services**.

This chapter describes the different aspects of our internal privacy and security operations that are applicable to our processes, products and infrastructures.

## 2.18.2. Privacy

### 2.18.2.1. Vision

Telefónica respects individuals' fundamental rights and freedoms, including the fundamental right to the protection of personal data. The Responsible Business Principles, the Group's code of ethics, recognise the need to **preserve this fundamental right** and accordingly establish common behavioural guidelines for all the companies in the Telefónica Group.

### 2.18.2.2. Targets

To reduce exposure to risk and raise digital trust, we are constantly working to update our processes and policies. Our targets are:

- Approve and introduce Binding Corporate Rules (BCRs) in 2024. BCRs are data protection policies adhered to by companies established in the EU to guarantee transfers of personal data outside the EU. These rules include all general data protection principles so as to ensure appropriate safeguards for data transfers. They are legally binding and approved by the competent national authority.
- Update the Group's Privacy Policy to bring it in line with the BCRs in 2024.
- Update the Global Privacy Centre, which is part of the Global Transparency Centre, in 2024.
- Implement the Artificial Intelligence (AI) Governance Model in accordance with internal regulations. To help us achieve this target, we have developed an app to record the AI systems that are developed, used or marketed at the Telefónica Group, and to identify associated risks and applicable requirements in order to both reduce risk and comply with regulations in force.
- Annually update and extend the reach of our training for both employees and third parties.
- Continue to promote annual privacy audit plans across the Telefónica Group, incorporating the BCRs so as to identify best practices.

### 2.18.2.3. Governance

At Telefónica we have a Personal Data Protection Governance Model that is designed to ensure effective and efficient privacy management in alignment with the Group's strategy.

Our global privacy management activities seek to deliver highly transparent data protection in all the Group's companies.

Implementing our BCRs (which are in the process of being approved by the European authorities) will permit us to increase our level of commitment to privacy even further.



For further information, see [2.18.2.7 Progress in 2023 > Binding Corporate Rules](#)

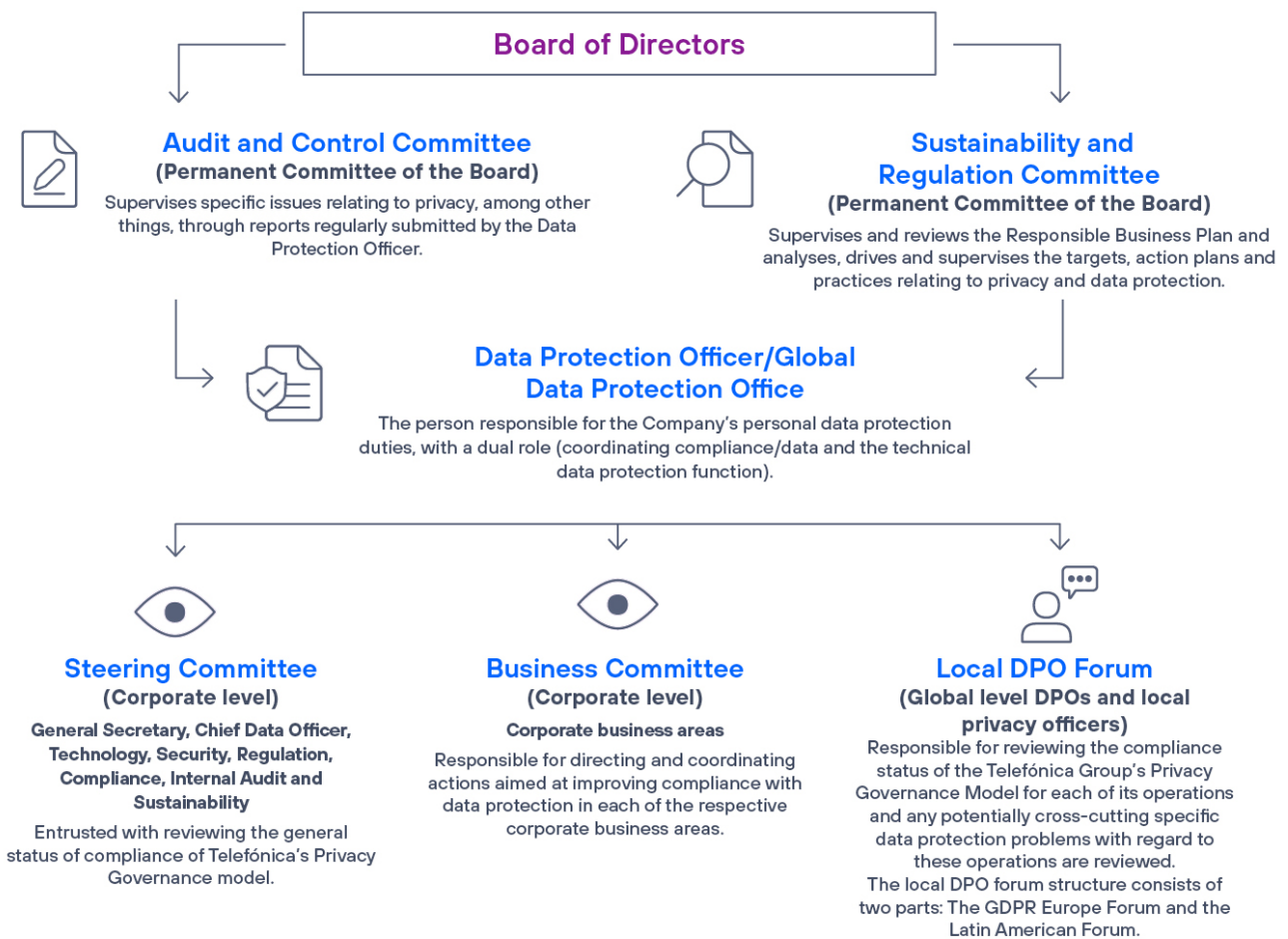
The person in charge of personal data protection for the Group is the global Data Protection Officer (DPO). This person:

- Coordinates regulatory compliance monitoring, and in particular:
- Gathers the information necessary to identify data processing activities.
- Informs and advises the data controller or processor of their obligations.
- Monitors compliance with Company policies and assesses the impact of new projects from a privacy perspective.
- Establishes the guidelines and methodologies pertaining to privacy-related risk management and impact assessments.
- Maintains and stores the documentation required by current regulations, and channels notifications and communications. Updates and maintains the records of processing activities that correspond to these tasks.
- Acts as a point of contact with the supervisory authority, cooperating with them and ensuring consistency in communications.

To ensure these tasks are performed as required, the different corporate areas meet twice yearly as part of the Governance Model Monitoring Committee, the Business Committee and through the Local Data Protection Officers.

In addition, the primary duty of the Audit and Control Committee is to support the Board of Directors in its supervisory duties. **The DPO reports annually to the Board of Directors through the Audit and Control Committee.**

In addition, the Sustainability and Regulation Committee (a standing committee of the Board) is responsible for promoting and monitoring the implementation of Telefónica's Global Responsible Business Plan, which includes specific privacy targets. The Board receives updates about implementation of the Plan from the Global Sustainability (ESG) Office .



### 2.18.2.4. Policies

We promote and review a number of 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 of Telefónica, S.A.



Establishes the mandatory rules for all Company entities, thereby laying the foundations for a privacy culture based on the principles of legality, transparency, security, storage limitation and respect for data subjects' rights.



##### Personal Data Protection Governance Model Regulations

###### Corporate Rule

Approved by the DPO Office of Telefónica, S.A.



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



##### Regulation on Requests by Competent Authorities

###### Corporate Rule

Aprobada por la dirección de Ética y Sostenibilidad de Telefónica S.A.



Establishes the principles and minimum guidelines that must figure in the internal procedures of each of the Group's companies/business units/OB to ensure compliance with their duty to cooperate with the competent authorities as regards our customers' data.

Data subjects can easily obtain access to and additional information about our policies through our [Global Transparency Centre](#), which can be found on our website.

At Telefónica we have what we call Operational Domains – internal procedures that reinforce data protection.

The Operational Domains are published by the Telefónica Group DPO Office and are updated in line with any legislative developments. The most recent update took place in November 2023 and extended application of the Operational Domains to all the data protection jurisdictions of the Telefónica Group.

The Operational Domains regulate the following aspects:

- **The Records of processing activities, risk analysis and impact assessments:** guidelines on making records and inventories of processing activities, identifying and assessing risks and performing assessments of impact on privacy whenever necessary .
- **International transfers:** regulation of the transfer of personal data outside the jurisdiction of origin, ensuring protection of such data in accordance with the applicable privacy laws.
- **Data classification:** categorisation of data types according to level of sensitivity so as to ensure the application of appropriate privacy and security measures.
- **Legitimate basis for processing and duty of information:** establishment of legitimate bases for data processing and general criteria to be followed to fulfil the obligation of informing data subjects about how their data will be processed.

- **Personal data breaches:** procedures to detect, report and manage personal data security breaches.
- **Third-party management:** policies and processes to monitor and ensure compliance with the required privacy obligations by the third parties that process personal data on behalf of Telefónica.
- **Internal audit plans:** planning and execution of regular audits to verify compliance with privacy policies and procedures.
- **Training and awareness:** coordination of employee training on the privacy policies and awareness raising about the importance of protecting data privacy.
- **Data subjects' rights:** protocols to be followed to ensure that data subjects can exercise their data protection rights.
- **Data retention and erasure:** we follow the "storage limitation" principle. In accordance with the specific legislation for each jurisdiction, Telefónica stores the data only as long as needed for the purposes of processing and legal obligations.

Our various operators incorporate specific and detailed information about data retention in their respective Transparency Centres. For further information about storage periods, see the relevant [Transparency Centres](#).

In order to ensure effective implementation of the data protection policies, processes and procedures, the following practices have been put in place:

- **Privacy audits:** conducted annually to assess compliance with the data protection policies and procedures. These audits are included in the Company's annual audit plan. They fall under the management of Internal Audit, which can in turn engage privacy experts to perform them. The audits identify gaps and areas for improvement.

Action plans are established by the areas responsible for implementation. Internal Audit monitors the entire process and conducts the final audit of proper implementation. Other work is done in the area of technology and cybersecurity that covers aspects of privacy from a security perspective. The working process, publication of reports and monitoring of action plans in that area is equivalent to the specific privacy audits.

- **Training and awareness raising:** conducted on a regular basis to ensure employees and stakeholders know about the privacy policies and procedures. This includes raising awareness about the importance of data privacy and how to comply with the policies.
- **Assessment of suppliers and third parties with access to personal data:** performed to ensure they meet the organisation's privacy and compliance standards.

In the interests of access and transparency, [our policies](#) have been translated into the languages of the countries in which we operate.

### 2.18.2.5. Impacts, risks and opportunities

Rapid technological progress and regulatory pressure in the field of data protection pose significant challenges to adapt and respond to regulatory demands.

In this respect, we understand the importance of data privacy and its management. Therefore, with the aim of avoiding or mitigating adverse impacts and enhancing **positive impacts**, we establish protocols and controls to protect personal data. This enables us to achieve a more secure and reliable digital environment.

In addition, the challenges associated with complying with the current privacy and data protection legislation are intensifying. At the same time, our stakeholders' expectations are increasing. In this context, privacy **risk** management has a prominent position in the risk map and in Telefónica's strategy.



For further information, see 3. Risks

We integrate the protection of personal data as a key element in the development of products and services. Our motivation is not limited to regulatory compliance, but we aim to make privacy a sign of trust for our users, thus highlighting the importance of privacy as a core value of our company.



Thanks to the control, transparency, and responsible use mechanisms we implement, we create strategic **opportunities** for the Company in response to the growing demand from society towards telecommunications operators to protect the personal data of their customers.

### 2.18.2.6. 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, as well as when complying with the principle of "data minimisation".
- **Empowerment:** equip our customers with simple and secure tools that enable them to control the use of their personal data.

Telefónica complies with the "Data minimisation" principle of the General Data Protection Regulation (GDPR), the goal of which is to obtain, process and store only the personal data that is necessary and to do so only for a specified time.

Our main lines of action are:

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

### Privacy by Design

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

This concept represents the organisation-wide obligation to establish procedures that primarily take into account two aspects when designing products and services: first, the implementation of privacy protection measures from a legal and security perspective in the early stages of any project; and, secondly, that all business processes and practices involved in each activity or processing operation 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 individuals' personal data are guaranteed from the get-go of any processing project or activity.

These practical guidelines stand as reference documents for the Group 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 experts in each of the Group's companies and/or business units, in order to ensure that all the necessary privacy-related legal and security requirements are taken into account from the design stage of relevant projects.

We use **an approach based on risk management and proactive responsibility** (critical and continuous self-analysis of compliance with the obligations laid down by the regulations) to establish strategies that incorporate privacy throughout the entire data life cycle of each product or service: collection and obtaining, processing, exercise of rights, and storage and erasure of data.

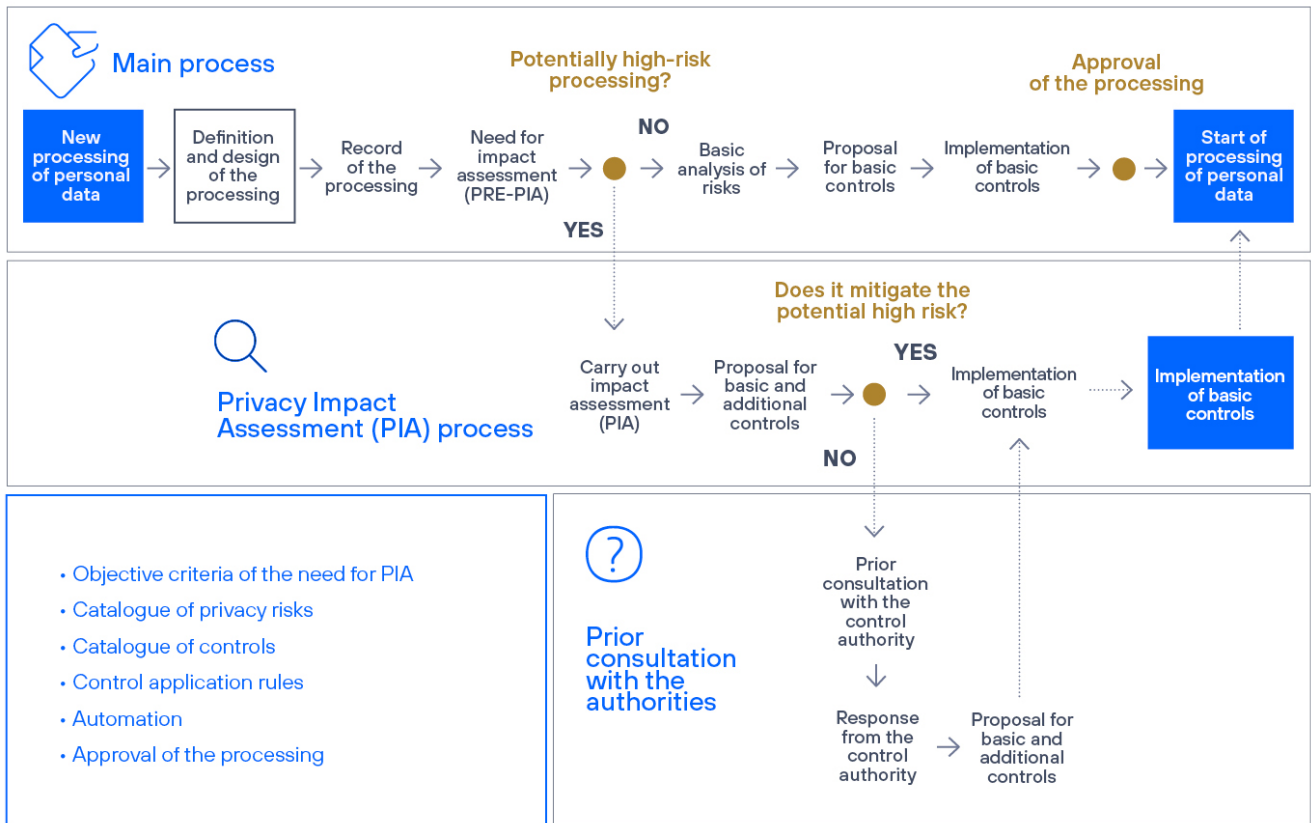
In general, Telefónica does not market or sell its customers' personal data. Telefónica may share aggregate analytical data that have been rendered anonymous, as described in the [Movistar Privacy Policy](#).

The practical application of Privacy by Design involves bearing the following in mind when defining or developing a product or service: the lawfulness and the legitimate grounds for the data processing; guarantees 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; **data minimisation**, in that any data used must be strictly

necessary to the purposes of the processing; commitment to the data subjects' rights; and storage period limitations, among other aspects.

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

**Privacy by design process**



**+** For further information, see 2.11. Sustainable offering and innovation

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

The DPF is the framework for Telefonica's global legal and privacy strategy with respect to the GDPR and the ePrivacy regulation on data processing platform products and systems.

The DPF adapts the guidelines on legal privacy compliance to a technological reality in order to standardise and conceptualise the functional and technical requirements governing the dynamics of privacy systems, and apply them automatically and digitally to the processing of personal data.

Digitalisation is implemented from the design stage and naturally enables us to build a dynamic and automatic privacy process between the customer and the systems that process personal data, and to comply with the GDPR.

We are implementing this digitalisation framework in the systems and platforms via which we process data, such as Kernel, Telefónica's big data platform. We made significant progress with the Digital Privacy Framework in Spain in 2022, and continued to do so in 2023 among our operators in jurisdictions that are more demanding when it comes to certain data protection requirements, for example, 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 a number of different initiatives to implement it:

### Global Privacy Centre

The Global Privacy Centre is a public benchmark for our privacy and security policies and processes. Our stakeholders can easily find all the information they need in the [Global Transparency Centre](#), where it is presented in a simple format by means of visual and graphic resources. Our objective for 2024 is to continue improving this centralised channel, among other things by linking all of our operators' Transparency Centres so that all relevant information is in one place.

### Operators' Privacy and Security Centres

The purpose of these centres is to enable both our customers and stakeholders to obtain information about the processing of their personal data in a simple, digital and understandable way. This includes:

- Information about the channels and avenues for exercising their rights.
- Security and confidentiality measures adopted for data processing.
- The privacy terms and conditions applicable to our products and services.
- Communication transparency reports.
- Our ethical principles regarding AI.
- **Child security and protection** matters specific to digital environments.

The Privacy and Security Centres are currently available on our operators' websites. They are updated regularly in accordance with regulations and stakeholder analysis.

### Telecommunications Transparency Report

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

For each request we follow a strict procedure, which is laid down in the Regulation on Requests by Competent Authorities. Doing so guarantees both the fulfilment of our obligations in terms of collaborating with these authorities and the protection of the fundamental rights of the people affected, in accordance with our human rights commitments.



For further information, see 2.14. Human rights

## Customer empowerment

As part of the principle of transparency, Telefónica provides customers with access to the data they generate when using our products and services. These data are collected in the Kernel "Personal Data Space" and are accessible through various channels.

The **Transparency Centre** allows all customers to set their data privacy and management preferences via their Personal Data Space. This feature is currently available to most 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, customers can manage the legitimate grounds for use of their data for certain purposes via the Privacy Permissions section. In addition, the Access and Download section provides practical examples of different types of data. These examples are presented in a user-friendly manner and in compliance with privacy criteria; customers also have the option of downloading a more detailed document.

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

We also prioritise **data minimisation**, ensuring that we obtain only the information necessary for our legitimate purposes. Furthermore, we have established **policies and incorporated guidelines on the storage and deletion of data in the Transparency Centres of the Group's operators**. Thus, we ensure that the data are stored only for the minimum periods necessary for the intended purposes and are deleted safely when they are no longer necessary (as soon as possible).

The Transparency Centres represent our first steps towards fulfilling our promise to give our customers tools with which to control and ensure the transparency of their data in accordance with applicable privacy regulations. For example, in Europe our data processing will be fully aligned with the GDPR.

## Query and complaint mechanisms

Users may submit queries and file complaints via:

- Letter, email or telephone.
- Electronic means such as the Mi Movistar app or their personal area of [www.movistar.es](http://www.movistar.es).
- The Customer Defence Service, a second-instance mechanism that reviews the decisions made in relation to customer queries/complaints submitted via the regular channels provided by Telefónica.

Telefónica has also implemented other query and complaint mediation systems:

### Queries Channel

We have a public channel on our website via which all our stakeholders can enquire or complain about anything related to the Responsible Business Principles. Throughout 2023, 10 communications on privacy and 2 on freedom of expression were processed, received a reply or, where applicable, received a solution.

### Voluntary mediation system with AUTOCONTROL

On the one hand, customers have at their disposal a mediation system that 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 Supervisión Authority (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 2023, 30 requests for mediation were processed.

On the other hand, in 2023 the AEPD approved the Code of Conduct on Data Processing in Advertising Activity, under which 45 complaints have been dealt with or submitted to mediation.

### 2.18.2.7. Progress in 2023

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

As a demonstration of our commitment and ongoing progress, we have been recognised as the leading telco in this respect among all the global telecommunications companies assessed by Ranking Digital Rights (RDR), in the last three editions of the RDR's index. This ranking

assesses corporate commitments, policies and practices that affect freedom of expression and customer privacy, including governance and oversight mechanisms.

## Binding Corporate Rules

Our Binding Corporate Rules (BCRs) are in the process of being formally approved by the relevant supervisory authorities. They are designed to permit the movement of data from inside the Telefónica Group in the European Economic Area (EEA) to countries outside the EEA in accordance with article 47 of the GDPR.

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

In addition, the BCRs will contribute greater legal security by facilitating alignment with the Group's organisational model.

In 2022 Telefónica began the process of approving its BCRs and during this period we took the following steps:

- Analysis of international intra-group transfers.
- Drafting of our BCRs.
- Designation of the AEPD as the lead supervisory authority, which shall be responsible for leading the process, as well as the supervisory authorities concerned, which shall co-review the approval procedure, following a proposal by Telefónica.
- Sending of the BCRs and complementary documentation to the lead authority and co-reviewer authorities for approval.
- Launch of the cooperation phase upon forwarding the BCRs to all the respective European supervisory authorities 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. We have therefore incorporated data protection agreements across the whole Telefónica Group and included specific supplier commitments pertaining to international transfers.

In 2023 a number of supplier monitoring procedures were introduced and educational materials were made available via tools created by Telefónica. Specifically, 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 the personal data managed by third parties, automated mechanisms were developed to optimise training initiatives.

## Telecommunications Transparency Report

In 2023 we recorded a total of 4,711,614 requests for customer information from competent authorities (lawful interception and access to metadata). Of these applications, we rejected 217,090, which was 95% of the requests dealt with. The number of accesses/customers affected was 4,784,392.

### 2.18.3. Security

#### 2.18.3.1. Vision

Security as a concept seeks to protect against potential damage to people and property and to guarantee the confidentiality, integrity and availability of a company's information assets. Ensuring network and data security is a major issue for Telefónica due to its significant impact on both our stakeholders and on the value of the Company. (See chapter 1.4. Materiality).



For further information, see 1.4. Materiality

At Telefónica, security is treated as a **broad concept** that includes physical and operational security (of people and goods), digital security (encompassing information security and cybersecurity), business continuity, prevention of fraud in the commercial portfolio of products and services, and supply chain security.

The increased number, complexity and types of threats make 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, and in doing so deliver a security management system that is aligned with international reference frameworks and standards such as **ISO 27001 and NIST (National Institute of Standards and Technology)**.

Our approach to security, including the list of certifications obtained by the companies of the Telefónica Group, is published in the [Security section of Telefónica's Global Transparency Centre](#).

#### 2.18.3.2. Targets

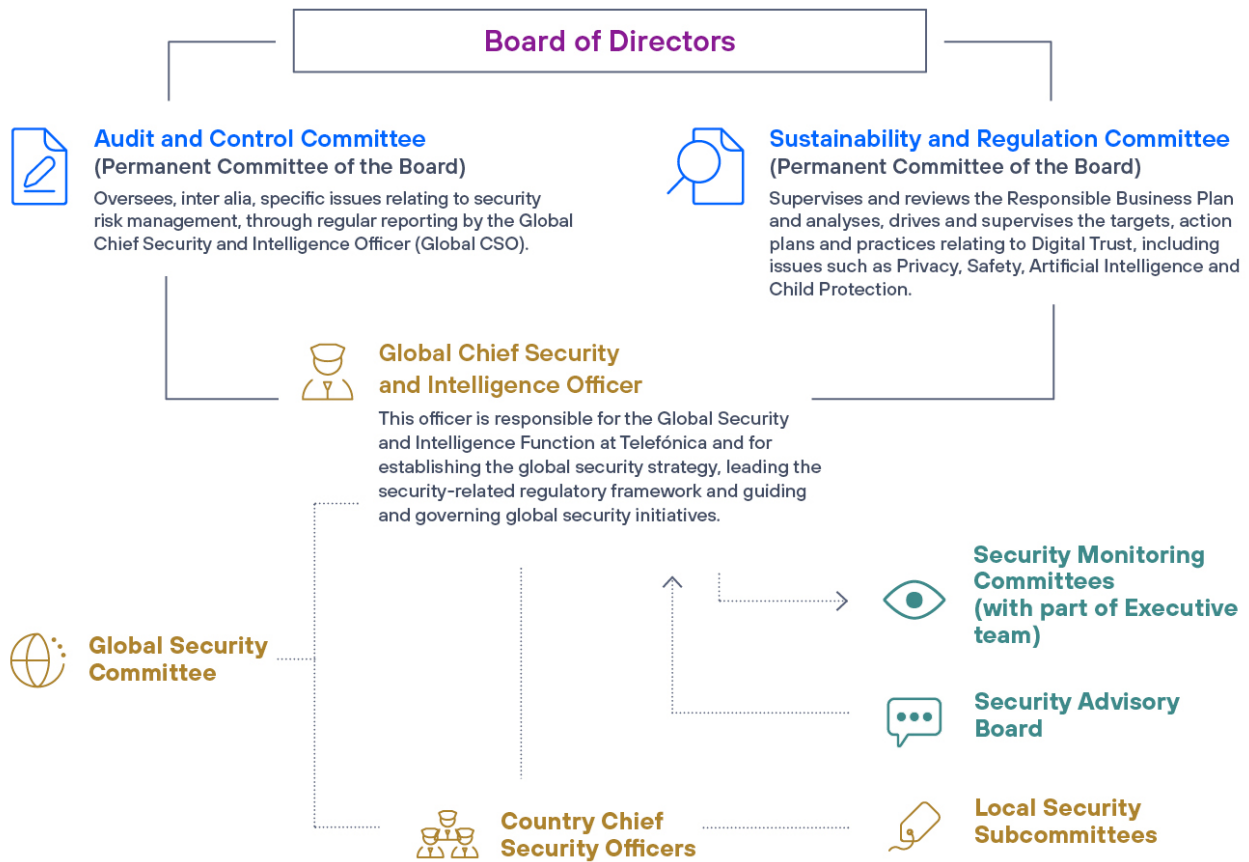
The short- and long-term targets we have set ourselves are:

- Continue our review of the global regulatory framework on security in order to simplify it and align it with new versions of international standards, such as ISO 27001.
- Move forward with deploying the Zero Trust<sup>1</sup> model to control IT system access and with implementing 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.

#### 2.18.3.3. Governance

The Global Security and Intelligence area is supported by the Company's management and reports to the Board of Directors through the Sustainability and Regulation Committee and the Audit and Control Committee. It also coordinates with the local security departments, as shown in the following diagram:

<sup>1</sup> Zero Trust is a security strategy applied to accessing information that 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 head of security at the Company is the **Global Chief Security and Intelligence Officer (the Global CSO)**. The Company's Board of Directors delegates the authority and responsibility for establishing the global security strategy to the Global CSO. **This Officer leads development and monitors implementation** of the policy framework and the global security initiatives. The Global CSO nominates a local security manager at each Telefónica Group company, which is then approved (or rejected) by the corresponding company's management bodies.

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

There are also local security sub-committees, which are chaired by the local CSOs. They help to define strategic initiatives and global guidelines and implement them in each Telefónica Group company.

The Global Security and Intelligence area also promotes and drives the Global Digital Security Committee, in which several members of the Company's Executive Committee and the Global Business Continuity Committee participate.

## The Global Security and Intelligence area reports to the Board of Directors through the Sustainability and Regulation Committee and the Audit and Control Committee.

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

### 2.18.3.4. Policies

At Telefónica we foster regulatory security policies that are mandatory for all Group companies. Our security policies also apply to members of the supply chain (suppliers, subcontractors, etc.). See section "Security in the Supply Chain".

[+](#) For further information, see Supply Chain Security

**Security regulations**



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

### 2.18.3.5. Impacts, risks and opportunities

Telecommunications companies around the world are facing a continuous increase in cybersecurity threats as businesses become increasingly digital and dependent on telecommunications, computer systems/networks and adopt cloud technology. At Telefónica we have an important role to play in mitigating and avoiding the impacts of these challenges, to ensure the security of the services we provide, as well as the privacy and confidentiality of our customers' data. In this way, we contribute to **creating a climate of digital trust, beneficial for both society and businesses.**

Conversely, information technology is a relevant element of our business, and we must minimise or avoid the adverse effects of potential cyber threats on the Company's assets. For these reasons, **cybersecurity risk** is included in Telefónica's risk map, which defines guidelines that facilitate uniform reporting, alignment with business objectives, and corporate risk tolerance criteria.



For further information, see 3. Risks

Additionally, through cybersecurity solutions, we combine the capabilities of cybersecurity and cloud technologies to build robust solutions that are tailored to the needs of businesses or organizations.



For further information, see 1.6.2. Global businesses

### 2.18.3.6. Action plan and commitments

At Telefónica we understand security as a broad concept, the goal of which is to protect our **assets, interests and strategic objectives**, ensure their integrity and protect them from potential threats that could damage their value, affect their confidentiality, reduce their effectiveness and/or alter their operability and availability.

**Comprehensive security** encompasses:

- Physical and operational security (of people and assets)
- Digital security
- Business continuity
- Fraud prevention
- Security in the supply chain
- Any other relevant area or function aimed at protecting the Company from potential damage or loss.

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

Our security provisions apply to all our supply chain partners, but focus especially on companies that manage the Telefónica Group's or its customers' data.

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

The most recent version of the Company's Global Strategic Security Plan, approved by the Global Security Committee on 27 September 2023, sets the goal of implementing the basic principles laid down in the Security Policy and identifies and prioritises the main lines of action.

#### Digital security. Cybersecurity

Digital security is a key part of our business. Its ultimate goal is to **ensure our resilience**, in other words, our ability to withstand and contain attacks so that our business is not affected or is affected to a degree that is tolerable.



Telefónica adopts technical and organisational measures laid down in its digital security strategy to manage cybersecurity risks.

- The organisational measures include cyber-intelligence processes, early vulnerability detection, access control management, system patching, security event monitoring and incident management, technological platform risk analysis, and security training and awareness raising.
- The technical measures include deployment of firewalls, cryptographic tools for storing and sending information, intrusion detection and prevention systems, monitoring connections to networks and cloud services, protection against DDoS (distributed denial-of-service) attacks, systems for detecting and blocking viruses and malware in servers and workstations, email protection and producing back-up copies to restore any information that becomes affected.

The control and protection mechanisms are applied both to third parties that attempt to obtain unauthorised access to Telefónica's systems and information, and to employees and collaborators. The aim is to **guarantee internal control over access to the Company's information and that of our customers**, and respect privacy legislation.

## Our technical and organisational measures for employees and third parties seek to ensure internal control over access to Company information and that of our customers.

The global area defines the strategy, while activities are coordinated by the various digital security units of the Group's companies. We align activities and share experiences at our annual meetings.

Particular emphasis is placed on the following aspects:

### Cyber intelligence and incident management

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

- **Anticipation** of any incidents that may affect us through **cyber-intelligence measures**. Our approach to cyber intelligence is proactive; we apply knowledge gained from external sources and technology to determine trends, progress, and potential adversaries and lines of attack against Telefónica.
- **Prevention** to ensure the protection of both facilities and assets, as well as our and our customers' data. We have internal expert teams (Red Teams) dedicated to searching for any digital security vulnerabilities.

These teams are coordinated by the global area and analyse the Company's networks and systems, scanning for weaknesses, performing manual testing (ethical hacking, also known as penetration testing) and requesting those responsible for the systems and networks to correct the security problems detected. We also have an open-access public mailbox for reporting any bugs or threats that could affect Telefónica's technological infrastructure. This mailbox can be found in the Global Privacy Centre/Security sections of Telefónica's global website and the websites of its operators. We also have a bug-bounty reward program managed by recognised industry leaders, through which we receive input from cybersecurity experts (ethical hackers) worldwide.

## We have a public mailbox for reporting weaknesses and threats, and a bug-bounty program for finding them.

- **Detection and response** via a network of 17 Incident Response Centres (Cybersecurity Incident Response Teams, CSIRTs). We also have the technical and human capabilities needed to respond effectively and quickly to any breach or incident in order to minimise attacks and their consequences.

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 countries to handle potential incidents.

In 2023, there were no relevant security incidents (relevant incidents are those that meet certain criteria at a global level which results in being considered relevant due to their economic, legal or service impact or to the impact on the fundamental rights of data subjects). Moreover, there were no incidents with sufficient material impact to be reported to the financial market supervisory authorities.

Lessons learned from incidents help us to improve the security of our processes and technological capabilities and platforms. One of the lessons learned was the need to reinforce anticipation through cyber-intelligence activities and continue to conduct cyber exercises, as described earlier, while reviewing the action protocols in order to become swifter in detecting and responding to them. Our analysis and learning have enabled us to customise awareness efforts, reinforcing particular aspects where they are dependent on the actions performed by the user and conducting simulations of phishing campaigns that are similar to the detected attack attempts or incidents (see section 2.19.4.2. Training and awareness raising). We also take into account the analysis of past incidents when establishing the strategic digital security projects in each cycle.



For further information, see 2.19. Responsible supply chain management

We follow 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, and the appropriate mitigation measures are established.

The Company has various **insurance programs and policies** 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, inter alia, a loss of revenue, loss of customers, extra costs or recovery costs for digital assets, and cover for Technological Errors and Omissions in the event of customer and third-party claims for damages 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 to the business. The aim is for the networks to be properly planned and deployed in accordance with applicable security requirements that minimise the risk of downtime, 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 (e.g. GSMA). Examples include 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 development of our network virtualisation platform (UNICA NEXT), network splitting and new radio access technologies, incorporate Security by Design.

## Physical and operational security

At Telefónica we make a continuous effort to improve our ability to physically protect infrastructure and assets. The following programs stand out in this regard:

- The interconnection of control centres to create a resilient network that increases 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 from 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:

- Risk analysis and management process.
- Commitment to innovation, including the development of proprietary technologies.
- Raising employee awareness.
- Security requirements imposed on our supply chain.

This approach ensures that security requirements are considered from the design stage of applications and systems, that controls against known bugs are incorporated and that there are no security weaknesses at source. The result is systems and applications that are more resistant to malicious attacks.

### Supply Chain Security

At Telefónica we impose security requirements on our suppliers and identify any risks associated with the provision of a service/product. We continue to develop **3PS+**, our tool for digitalising the security process in the supply chain. The security requirements are reviewed annually according to international regulatory updates and technology developments (5G, AI). The main features of 3PS+ are:

#### Supply chain security process



- **Prior to contracting**, the tool can be used to generate the security requirements for new procurement processes. It collates supplier responses and objectively assesses compliance levels and access to their proposed mitigation measures.
- **During service provision**, the tool can be used to monitor 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 completion of service provision**, the tool can be used to oversee the supplier's offboarding and mitigate or even prevent the most common security risks at service termination, such as 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, while Crisis Management allows us to successfully tackle any serious incident that affects the organisation.

In the event of a crisis, our priorities are to:

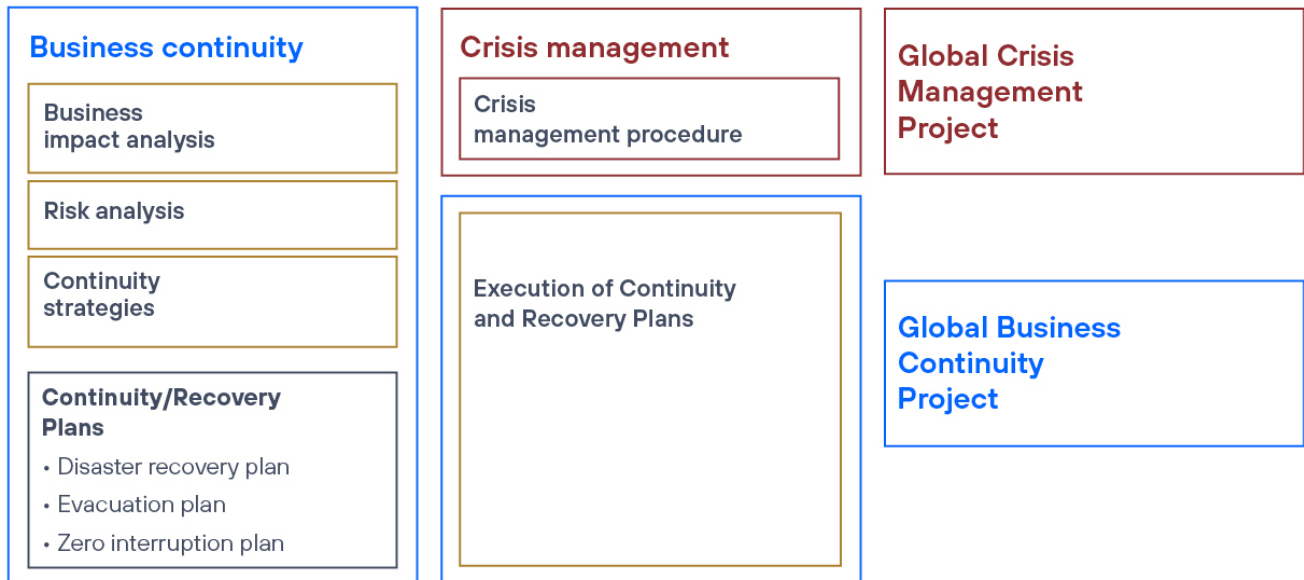
- **Protect people**, ensuring the well-being of employees and collaborators.
- **Provide the agreed services** to our customers, at the agreed availability and quality.
- **Protect and look after the interests** of our shareholders and institutional investors.
- **Comply with our regulatory and legal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

The business continuity function is set out in the [Global Security Policy](#). Further details are defined in the Global Business Continuity Regulation, as well as in various Company-wide and local documents maintained by 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.

Under the Crisis Management Plan, each area's processes are identified, scenarios that could interrupt them are detected, potential treatment plans are set out, the business continuity strategies to be applied are determined and, if necessary, business continuity plans listing the appropriate actions to be taken are generated.

### Global Crisis Management Plan



Our strategy revolves around strengthening our:

- **Strategic vision:** global threats require global action. Having a strategic vision of business continuity leads to global decision-making that results in greater resilience.
- **Effectiveness in crisis management:** we have a proven crisis management model, the definitions and procedures of which are common to the entire Company.
- **Coordination and collaboration:** the organisational model guarantees, aligns and promotes the development of business continuity equally across all business units.
- **Measurement standards:** these allow us to objectively and consistently measure various indicators to determine the Company's maturity from a business continuity perspective, as well as its level of resilience. This gives us the necessary information to be able to establish medium- and long-term goals.

All of the above is based on international standards such as ISO 22301 for business continuity management, ISO 22320 for emergency management and ISO 22361 for crisis management.

We also conduct several global and local exercises each year to check our business continuity mechanisms, simulate crisis scenarios and identify opportunities for improvement in the face of real incidents.

#### Governance model

The **Global Business Continuity Committee**, the highest governance body, defines the global strategy from the design stage, and prioritises and allocates the necessary resources.

The **local business continuity committees**, the bodies responsible for ensuring business continuity in each business unit, guarantee implementation of the strategic decisions made at a global level and report on the needs, achievements and maturity indicators that provide a comprehensive view of business continuity in the Company.

Both global and local committees prioritise and direct resources to 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 by the **Global Business Continuity Office (GBCO)**. The GBCO operates out of the Global Security and Intelligence Directorate, which is part of the Company's corporate area. It coordinates the LBCOs and passes on the various strategic decisions defined by the Global Business Continuity Committee.

### Global Business Continuity Program

Our Global Business Continuity Program seeks to improve our resilience. It is aligned with ISO standard 22301 and is made up of the following phases:

1. **Planning:** involves drawing up a Statement of Work (SoW) detailing the scope of business continuity and an annual activities plan.
2. **Implementation and operation:** includes deliverables aimed at establishing and documenting the business continuity mechanisms such as a Business Impact Analysis (BIA), which identifies major processes and services, risk analyses, continuity plans, return to normality plans, etc.

3. **Monitoring and evaluation:** involves assessing the effectiveness of the business continuity arrangements in place by testing them in realistic and bounded scenarios. Indicators are used to assess the performance, maturity level and implementation of the overall business continuity project.

4. **Maintenance and improvement:** encompasses lessons learned and opportunities for improvement identified as a result of business continuity testing and crisis simulation, the business continuity management continuous improvement process, training and awareness raising.

The Global Business Continuity Program seeks to strengthen our resilience; in other words, our ability to contain attacks and withstand them.

The LBCOs are responsible for ensuring and driving 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**

► **Business continuity management system**

◀ **Proactive phase** ◀ **Reactive phase**



**Business continuity maturity monitoring**

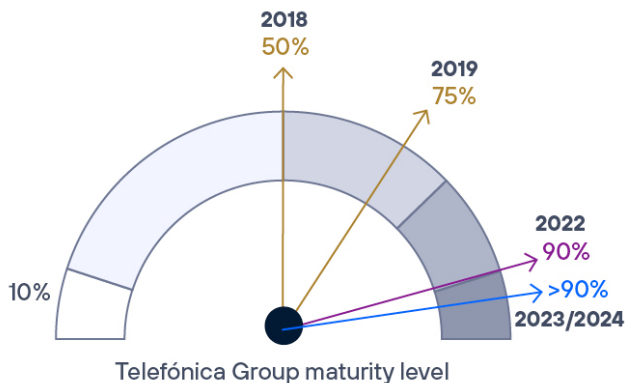
To ensure that LBCO execution of the management process is evaluated consistently across the board, we have established a definition of "maturity".

**Business continuity maturity model**



In recent years, we have achieved and maintained an “optimised” level of maturity, which means that we have established, tested and learned lessons about the defined business continuity mechanisms:

**Evolution of maturity**



**Crisis management**

The Global Crisis Management Project covers everything related to the successful coordination and handling by senior management of events that could have a major impact on the Company, and so have to be treated as a crisis.

Crisis management is structured in 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, media and channels involved in crisis management, as well as the relationship and responsibilities of the crisis committees.
3. The third layer groups together the procedures, plans and documentation necessary for managing crises.
4. The fourth layer defines the overarching Company architecture of warning systems, secure communication and the general digitalisation-related operations that support the activities of the different crisis committees.

## Layers of Crisis Management

	<b>Crisis</b>	<ul style="list-style-type: none"> <li>• Definition</li> <li>• Classification (Local, Regional, Global)</li> <li>• Overall strategy</li> </ul>
	<b>Crisis Committee</b>	<ul style="list-style-type: none"> <li>• Chairman</li> <li>• Members and boards</li> <li>• Media and channels</li> </ul>
	<b>Procedures</b>	<ul style="list-style-type: none"> <li>• Crisis response procedures</li> <li>• Business continuity drills/plans</li> <li>• Communication plans</li> </ul>
	<b>Architecture</b>	<ul style="list-style-type: none"> <li>• Warning system</li> <li>• Secure communication system</li> <li>• Crisis committee support system</li> </ul>

The Global Crisis Management Project also provides other mechanisms that are complementary to business continuity and enable us to manage incidents with an extensive impact on the Company.

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

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

We have different active warning, notification, management and coordination protocols and systems for the different types of crisis, all of which are known to everyone involved in the Global Crisis Management Project.

The main role in this management process is played by the members of the Crisis Committee, at both global and local level. Members can be divided into permanent members who participate in all activations of the Committee, ad hoc members who participate depending on the type of crisis, and those in working groups or task forces that support the permanent and ad hoc 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 at hand and the business continuity work done previously.
- Reliably transmit information about what has happened to customers, authorities, organisations and/or any other stakeholders.

Finally, we are obliged to conduct **tests and drills** to prepare for different scenarios that may potentially be harmful to the Company. **The drills are to 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 that supports crisis management activities.
- Evaluate coordination mechanisms.
- Prepare Crisis Committee members to act.



The events discussed by the Crisis Committee are outlined below:

### Events discussed by the Crisis committee

#### PERU (LOCAL) December 2022

<b>Description</b>	<b>Political instability and public demonstrations</b>
Type of crisis	Political-social
Impact	Services to customers were not impacted. However, there was damage to premises as a result of the demonstrations.
Actions	<p>The Crisis Committee was activated on 8 December 2022.</p> <p>Regular sessions were held, during which security measures were adopted 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. The Committee worked with government authorities to coordinate actions that would ensure continuity of the services.</p> <p>In addition, all travellers were advised to leave the country because of the risk to their safety. Those thinking about visiting the country were warned of the risk to their safety and required to undergo a consultation process to authorise their trip.</p> <p>Demonstrations continued until the end of March 2023. The affected regions were Puno, Cuzco, Huancavelica, Arequipa, Ica and Lima. Emergency plans and infrastructure and network reinforcement plans were activated.</p>

#### CHILE (LOCAL) February 2023

<b>Description</b>	<b>Contingency at Paine Data Centre</b>
Type of crisis	Operational continuity
Impact	Customer services were affected.
Actions	<p>The Crisis Committee was activated on 2 February 2023.</p> <p>A uninterruptible power supply (UPS) battery system failure occurred following a national grid power cut at the Paine Data Centre, which affected the centre's equipment and led to services being unavailable for brief instants until the back-up power generators became operational.</p> <p>The Committee held eight meetings, during which various action plans were established, the most significant being an agreement with the service provider on a plan of action for changing the batteries.</p> <p>The incident was deemed closed in mid-May, but the action plans developed as a result of the incident continue to be monitored.</p>

#### CHILE (LOCAL) February 2023

<b>Description</b>	<b>Wildfires</b>
Type of crisis	Natural disaster
Impact	Customer services were affected.
Actions	<p>The Crisis Committee was activated on 3 February 2023.</p> <p>High temperatures caused a number of fire outbreaks, prompting the declaration of a state of emergency as the fires grew out of control, spreading and affecting both rural and urban populated areas. As a result of the fires, 65 mobile sites were damaged, leading to customers' services being suspended and/or degraded. Customers' homes were also affected.</p> <p>The Committee held 23 sessions and established a number of action plans, issuing warnings to all employees with homes in the area affected by the fires and putting in place emergency commercial measures for all customers from the affected areas.</p> <p>The incident was deemed closed in March, but the action plans developed as a result of the incident continue to be monitored.</p>

**PERU (LOCAL) March 2023**

<b>Description</b>	<b>Cyclone Yaku</b>
Type of crisis	Weather event
Impact	Customer services were affected.
Actions	<p>The Crisis Committee was activated on 4 March 2023.</p> <p>Cyclone Yaku mainly affected Tumbes, Piura, Chiclayo, Lambayeque, La Libertad and Lima. It caused torrential rain, flooding and landslides. A number of different Company sites were affected by the cyclone, leading to multiple fibre optics outages and impacting services to customers.</p> <p>Among the action plans activated was the emergency and service monitoring plan, in line with which the NOC performed testing and premises were monitored for damage to infrastructure. Crews were also deployed to deal with emergencies and mitigate the impact on connectivity, making use of portable generators. Spare parts and power rectifiers were acquired and fuelling was ensured via external tanks. In addition, remote working was activated.</p> <p>The incident was closed on 20 March when the cyclone moved away from the country.</p>

**PERU (LOCAL) April 2023**

<b>Description</b>	<b>Coastal El Niño phenomenon</b>
Type of crisis	Weather event
Impact	Customer services were affected.
Actions	<p>The Crisis Committee was activated on 4 April 2023.</p> <p>The Coastal El Niño phenomenon is caused by the persistent presence of anomalously warming waters over several months. The 2023 phenomenon resulted in heavy rain, flooding and landslides, and mainly affected Tumbes, Piura, Chiclayo, Loreto, Lambayeque, Cajamarca, La Libertad, Ancash, Ica, Huancavelica and Lima.</p> <p>A number of Company sites were impacted, multiple fibre optics outages occurred and services to customers were affected. Plans similar to those for Cyclone Yaku were activated.</p> <p>Monitoring continued until September when the incident was deemed closed.</p>

**CHILE (LOCAL) August 2023**

<b>Description</b>	<b>Flooding</b>
Type of crisis	Weather event
Impact	Employee travel, facilities and the network were affected.
Actions	<p>The Crisis Committee was activated on 22 August 2023.</p> <p>Significant flooding in the central and southern areas of the country affected employees (due to travel issues), facilities and network infrastructure. The network infrastructure was mainly affected by power cuts, while facilities were impacted by water leakage issues.</p> <p>Two meetings were held, and mobile device deliveries had to be suspended as a result of the transport problems. Customers were kept informed regarding scheduled deliveries. However, the operations groups remained 100% active in order to deal with emergencies.</p> <p>The incident was closed the same month (August).</p>

**ECUADOR (LOCAL) October 2023**

<b>Description</b>	<b>Scheduled power cuts</b>
Type of crisis	Operational continuity
Impact	Customer services were affected.
Actions	The Crisis Committee was activated on 28 October 2023.
	As a result of a prolonged period of drought and low water levels, the national government decided to introduce rolling 3–4-hour blackouts throughout the country, by sector, province and city, every day from 06:00 until 18:00, until December or until there was no longer a need for them.
	Despite use of the UPS and electricity generators, several base stations were affected.

### 2.18.3.7. Progress in 2023

We made progress in our implementation of security measures for cloud environment governance.

We continued to integrate new capabilities into the proprietary cyber-defence solutions we have developed to enable us to anticipate, detect and respond more swiftly to cybersecurity threats

Our work of fostering training and awareness-raising among our employees continued, with the number of employees who received training increasing by 38.7%.

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

We satisfactorily activated the management process and the available resources to deal with global and local crises, which permitted us to maintain the service levels agreed with customers at all times and adapt the network capacity to changes in demand.

In 2023 there was continued improvement in, support for and broadening of the supply chain security initiative. We consolidated and evolved the **3PS+** tool, which makes it possible to digitalise the entire security risk management process in our purchasing.

### 2.18.4. Cross-cutting privacy and security issues

#### 2.18.4.1. Internal control

In order to address and comply with the legal provisions related to local **data protection and privacy** laws and regulations in the different countries, the 2023 Annual Plan allocated a total of 420 specific Internal Audit days to verifying certain aspects and identifying best practices in terms of data protection. In 2023 the work focused on reviewing the successful design and execution of controls over personal data processing in a sample of specific products and services, covering the control framework from the perspective of both the data controller and the data processor.

In addition, we continued with the review of certain aspects of the internal control structures at our European operators. The review took in data processing and the design and operation of the data deletion procedures in the systems that support data processing, in accordance with the specific scope under consideration.

In the rest of the countries affected by local data protection laws, the major aspects reviewed were the following: the application of security measures in the systems that process personal data; the control structures in place to ensure the quality of the personal data (pursuant to the definition of quality in current data protection legislation); the control activities covering management of user consent to the processing of their personal data; the legitimate basis for the data processing; handling the data subjects exercise of their rights; and management of international transfers.

In the Annual Plan, emphasis was placed on the **auditing of cybersecurity and security in networks and systems**, with a total of 5,657 days devoted to this work, which included reviewing the relevant aspects relating to new technologies, such as the control environment defined in public and private cloud deployments, as well as reviewing interactions with the on-premises infrastructure deployed, through audits to assess the internal network control environment.

Other noteworthy activities included are the cross audit review regarding the preparation of indicators for basic security processes used to calculate the digital security index (ISD) and the cross audit performed for reviewing the security setting status in network and data base elements using AOL Edge (an online auditing tool).

### 2.18.4.2. Training and awareness-raising

We ran privacy and security awareness-raising and training campaigns for employees and relevant third parties (subcontractors, service providers and similar).

For further information, see 2.19. Responsible supply chain management

With regard to employee training in 2023, 94,642 employees completed their training on privacy, data protection, security and cybersecurity, which represents an increase of 87% compared to the previous year. These courses amounted to a total of 75,821 training hours provided. Key topics addressed across the many different training initiatives included the basic principles of data protection and security, how to act in the event of a data breach, roles in processing, data subject rights and the importance of data processing agreements (DPAs).

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

- Phishing campaigns aimed at all Group employees, 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 and containing short messages to raise awareness about specific aspects.
- Gamification techniques, which include elements and dynamics that are typical of games and leisure activities, in order to foster motivation and reinforce behaviour in terms of information security and Company asset protection practices.

At Telefónica we are aware that information and communication technologies have caused a complete

revolution and are now a basic tool for children's growth and development. That is why we are committed to fostering the responsible use of technology. In order to fulfil this commitment, we develop numerous initiatives that promote a safer and healthier digital environment; in addition, we make the necessary resources available to our customers and society in general so that they can take advantage of the full potential offered by technology and best manage their digital identity.

For further information, see 2.12. Digital inclusion

### 2.18.4.3. Stakeholder relations

Telefónica actively participates in various international organisations and forums, most of which are multi-stakeholder bodies.

#### Internet Governance Forum in Spain

In 2023 we helped organised the Spanish edition of the Internet Governance Forum (IGF). This year, under the theme "Connecting rights, forging futures", we actively contributed to the debates on such different issues as fair contribution and the financing of telecommunications infrastructure by different players and network neutrality.

#### 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. Since 2022, Telefónica has been participating in the Committee on Artificial Intelligence (CAI) and its work to prepare a Convention on Artificial Intelligence, which is to become the first international treaty on AI within the framework of 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. 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. In 2023 Telefónica continued to participate actively, in collaboration with companies and governments, with the goal of enhancing security in an increasingly connected environment. Noteworthy aspects of Telefónica's contribution included its promotion of projects aimed at improving cybersecurity in the supply chain and relating to cooperation on transparency about weaknesses.

### **Organization for Economic Co-operation and Development (OECD)**

We are a member of Business at OECD (BAIC), Vice-Chair of its Committee on Digital Economy Policy and Vice-Chair of its Governance and Regulatory Policy Committee. Telefónica is an active participant, making substantial contributions to debates and reports on digital rights, data and privacy, cybersecurity and the updating of AI principles. We continued to participate in the OECD Working Party on AI Governance (AIGO) and the OECD Working Party on Data Governance and Privacy, as well as initiatives associated with the metaverse and privacy.

### **International Telecommunication Union (ITU)**

In 2023 we took part in the meeting of Study Group 3, which deals with regulations and public policies and designs tariffs. We were involved in the working group devoted to the metaverse, which debated issues such as digital identity standards on a global scale, recommended architectures and other aspects relating to security and privacy.

### **International Chamber of Commerce (ICC)**

Telefónica is Vice-Chair of the ICC Global Digital Economy Commission, in which capacity it aims to promote global development of the digital economy and growth, based on clear rules, and also to protect rights and promote best practices. The working groups focus on developing full connectivity, improving cybersecurity policies, creating opportunities through governance of the Internet, and security and protection in international data flows. Among other activities, in 2023 Telefónica participated in updating the cybersecurity briefs and initiated a proposal for improved protection of critical infrastructure and essential services. Through this organisation, contributions are being made to the United Nations treaty as well as to other bodies such as the Council of Europe, particularly as regards AI governance.

### **Global System for Mobile Communications (GSMA)**

We participate in the GSMA and in its working groups that address privacy, fraud and security issues.

### **ENISA Ad-Hoc Working Groups**

We participate in the working groups that the European Union Agency for Cybersecurity (ENISA) has created with different European operators and manufacturers, with the aim of defining security certification schemes with which all European Union countries are recommended to comply.

## 2.18.4.4. Main indicators

GRI 418-1

### Summary of key privacy and security indicators

	2022	2023
Number of attendees on data protection and cybersecurity training courses <sup>2</sup>	67,880	94,642
Number of hours of data protection and cybersecurity training	81,460	75,821
Number of procedures opened due to data protection issues	49	83
Number of fines for data protection issues	18	18
Sum of fines (euros) due to data protection issues	318,059	300,366
Number of confirmed fines due to data protection issues as a result of a security breach or incident (physical or cybersecurity) affecting the personal data of customers, employees or others.	0	0
Number of queries/complaints about data protection/privacy issues submitted through the Responsible Business Channel	32	10
Number of queries/complaints about freedom of expression issues submitted through the Responsible Business Channel	0	2
Number of days devoted to data protection and cybersecurity by Internal Audit	5,836	6,077
Cyber security incidents categorised as high severity (Num.)	2	0
Cyber security incidents categorised as high severity with impact on customers' personal data (Num.)	2	0
Number of customers affected by data breaches	23,958,088	0
Percentage of customers whose information is used for secondary purposes <sup>3</sup>	69%	72%

## Milestones

- 1 Leading telco in the latest edition of the Ranking Digital Rights index and the Digital Inclusion Benchmark.
- 2 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.
- 3 We enhanced our privacy and security training and awareness-raising programs for our employees and relevant third parties.

<sup>2</sup> An employee may have taken more than one privacy and/or security course.

<sup>3</sup> 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 (72%) demonstrates that the tools we make available to our customers are useful to them and that customers are exercising their rights effectively.

# 2.19. Responsible supply chain management

## Key points

### 100%

of suppliers are required to operate with stringent sustainability standards similar to our own.

### Proactive

engagement with key suppliers on specific issues, such as decent working conditions and reducing emissions in the supply chain.

### SBTi

In 2023 we requested our key suppliers to align and validate science-based decarbonisation targets by SBTi.

## 2.19.1. Vision

A very important part of the social and environmental impact of companies is directly related to their supply chain. This situation is even more significant for large companies working across different sectors. At Telefónica, we are aware of this and we assume ~~accept~~ our responsibility, making sustainability a key part of how we do business. In this way, collaborating with suppliers is of strategic value, as it facilitates alignment with our commitments to customers and to the rest of society.

Telefónica has set **ambitious sustainability targets** in relation to reducing CO<sub>2</sub> emissions, promoting decent working conditions and 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** on our common journey towards a **more sustainable economy**.

In order to build trusting relationships with our suppliers, we have developed robust policies and processes with a triple purpose:

- Firstly, **to manage the potential impacts** of Telefónica on society and the environment, through its commercial relationships.
- Secondly, **to jointly identify potential sustainability risks** common to our supply chain in order to address them effectively.

- Thirdly, **to collaborate proactively on key issues** (e.g. CO<sub>2</sub> emissions), **harnessing the opportunities**, in order to turn the ICT supply chain into a driver for sustainability.

This triple approach ensures that we are delivering to our customers the supply of **products and services** which not only have a **positive impact** on society and the planet, but which have also been **developed in a responsible manner**.

## 2.19.2. Governance

### GRI 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 Regulation Committee of the Board of Directors** supervises its implementation and monitors its goals.

The governance of this subject is complemented by:

- Monitoring and coordination of the Responsible Business Plan by the **Global Sustainability (ESG) Office**.
- The **management of our Due Diligence process in the supply chain**, by the managing areas such as Global Sustainability (ESG) Office, Procurement, Human Resources, Compliance and General Counsel, among others.

### 2.19.3. Policies

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

- [Supply Chain Sustainability Policy](#), which includes the **code of conduct for all our suppliers**. In it, we outline the minimum standards for sustainable business that any company aiming to be a supplier of the Telefónica Group must adhere to. Their compliance has a positive impact on the different workers in our supply chain. This policy was drawn up in accordance with international standards such as the United Nations (UN) Guiding Principles on Business and Human Rights and the Universal Declaration of Human Rights, the conventions of the International Labour Organization (ILO), the UN Convention on the Rights of the Child, the guidelines of the Organisation for Economic Co-operation and Development (OECD) and the criteria of the International Organization for Standardization (ISO).
- General conditions for the supply of goods and services, which apply to all supplies from our suppliers.
- Low Carbon Procurement Instruction: This is an internal regulation which promotes the application of **energy efficiency principles** on the main **purchases of products that require energy consumption (electricity and fuel)**. With this, we incorporate criteria to internalise the cost of energy and carbon through the Total Cost of Ownership (TCO) in our procurement processes favouring suppliers that offer equipment with a lower impact throughout its useful life.

The rest of the Company's policies reflect **our supply chain commitment** with regards to our relationships with commercial partners:

- [Human Rights Policy](#).
- [Global Privacy Policy](#).
- [Global Security Policy](#).
- [Occupational Health, Safety and Well-being Regulation](#).
- [Global Environmental Policy](#).

### 2.19.4. Impacts, risks and opportunities

Our actions and those of our suppliers (who are located in over 60 different countries) may give rise to **adverse impacts** on society and the environment. The most important of these relate to the labour conditions of those working in the supply chain and our suppliers' carbon emissions.

Having said this, companies can transform these potentially adverse impacts into **positive impacts** through a responsible management of the supply chain. For example, through the implementation of social criteria that seek to improve the quality of life of workers in the supply chain. Another example would be the reduction of our Scope 3 emissions by engaging with suppliers through programmes that support them in reducing their carbon footprint, or by including climate-change requirements as part of the procurement process.

Similarly, such responsible supply chain management also helps us to anticipate the **main sustainability risks** for the Company. Such risks include the possibility of business interruptions due to a failure to address ESG issues in the supply chain and/or the loss of our reputation owing to supplier-related controversies.



For further information, see 1.4. Materiality

We **work closely** with our suppliers, maintaining **ethical and fair business relationships** with them. As a result, we are able to create **efficiencies**, which are reflected, for example, in the reduction of costs in materials, energy and transport. We are also able to increase **labour productivity** by ensuring decent working conditions in our supply chain. Lastly, we are able to **innovate collectively** in the face of ever-changing markets to meet the growing demand for sustainable solutions in the transition to a more sustainable economy.



## 2.19.5. Action plan and commitments

### GRI 2-6

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 managed through the local procurement teams in each country, making it possible to anticipate demand and supervise the execution of contracts and supplier performance in the various areas (including social and environmental requirements).

- **Internal efficiency** through the optimisation of procurement processes and systems, by initiatives to simplify process and develop support systems.
- The **commitment to sustainability** present throughout the entire process and relationship with our suppliers and developed through our sustainable management model. This is in line with the objective to generate 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 that have a **high social and environmental impact** and are **significant** for **both the sector** and the **Company’s strategy**. In particular:

### Our commitments according to the main impacts on sustainability aspects in our supply chain

Aspect	Our commitments	Stakeholder affected	Further information on how we manage this:
Abolition of child/forced labour	To contribute to the abolition of child/forced labour through specific projects focused on the protection of children’s human rights (e.g. on-site audits of high-risk suppliers).	<ul style="list-style-type: none"> <li>• Employees of our suppliers</li> <li>• Society</li> </ul>	<b>2.14.</b> Human rights <b>2.19.5.1.</b> Risk management <b>2.19.6.1.</b> Risk management in 2023 <b>2.19.6.2.</b> Engagement in 2023
Working conditions	To promote decent working conditions among our suppliers, especially for those labour-intensive service suppliers (contractors and subcontractors).	<ul style="list-style-type: none"> <li>• Employees of our suppliers</li> </ul>	<b>2.19.5.1.</b> Risk management <b>2.19.6.1.</b> Risk management in 2023 <b>2.19.6.2.</b> Engagement in 2023
Occupational health and safety	To promote best practices in health and safety among our suppliers, with the common aim of achieving zero accidents.	<ul style="list-style-type: none"> <li>• Employees of our suppliers</li> </ul>	<b>2.19.6.1.</b> Risk management in 2023 <b>2.19.6.2.</b> Engagement in 2023
Conflict minerals	To strengthen control over the use of 3TG minerals (tin, tantalum, tungsten and gold) throughout our value chain.	<ul style="list-style-type: none"> <li>• Employees in our supply chain</li> </ul>	<b>2.19.6.2.</b> Engagement in 2023
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.	<ul style="list-style-type: none"> <li>• Society</li> </ul>	<b>2.3.</b> Circular economy
CO <sub>2</sub> emissions - Scope 3	To improve emissions management in our supply chain and increase engagement with our suppliers both globally and locally.	<ul style="list-style-type: none"> <li>• Society</li> </ul>	<b>2.2.</b> Energy and climate change <b>2.19.6.2.</b> Engagement in 2023
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.	<ul style="list-style-type: none"> <li>• Customers</li> </ul>	<b>2.18.</b> 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 a sustainable management of our supply chain.

Our suppliers can access all the information on our [Supplier Portal](#).

In line with international standards such as ISO 20400 and the OECD Due Diligence Guidelines 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**



**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.

**2.19.5.1. Risk management**

GRI 308-2, 407-1, 408-1, 409-1, 414-2

**Step 1. Minimum standards required**

We require 100% of our suppliers to conduct their business activities in line with ethical standards similar to ours, to ensure 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 standards for sustainable business that our suppliers must comply with (thus directly affecting their employees).
- Anti-corruption Policy (Certificate).

Prior acceptance of these minimum conditions means that awarded suppliers are assessed in relation to the social and environmental issues set out in our norms.

**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 potential high-risk suppliers

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

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

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

To this end, we take into account how the **risk level** of each aspect can vary, according to the sector of origin of each type of product or service supplied.

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

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

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

## Step 3. Performance assessment of our potential high-risk suppliers

We monitor the possible risks associated with our potential high-risk suppliers identified in the initial analysis. The procurement teams in the various countries can view the results directly on the purchasing platform:

**External assessment platform (IntegrityNext)** Conducts an external 360° **evaluation** of our main potential high-risk suppliers based on 15 **sustainability criteria** that cover ethical, social, environmental and supply chain management aspects.

These assessments allow us to identify any aspects that could be better managed by our suppliers and proactively work to avoid or minimise potential adverse impacts on human rights or the environment.

### Performance-based actions

Sustainability Performance	Action
<b>ADVANCED</b>	<ul style="list-style-type: none"> <li>Collaborate with the supplier to identify possible improvements or sharing of best practices.</li> </ul>
<b>PARTIAL</b>	<ul style="list-style-type: none"> <li>Request a commitment from the supplier to implement an improvement plan in the coming year, with the aim of improving its level of performance.</li> </ul>
<b>INSUFFICIENT</b>	<ul style="list-style-type: none"> <li>Preventive blocking of the supplier in the procurement system.</li> <li>Report and agree on an improvement plan with the supplier.</li> </ul>

### 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. With this tool, we can **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 cross-checking with Dow Jones Risk & Compliance** results in **adverse information** about the supplier, an **analysis of this information is conducted** 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 key 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 performed through the internal Allies Programme (for service suppliers) and the sectoral Joint Alliance for CSR (JAC)<sup>1</sup> initiative (for product manufacturers). Both types are performed by accredited auditing entities, applying the established protocol when required.

The audits include improvement plans agreed with 100% of the suppliers who do not comply with any of the aspects that may have a negative social or environmental impact. Suppliers make explicit commitments through the agreed improvement plans to remedy any adverse impacts that they have caused or contributed to.

We have annual local and corporate budgets to retain external auditors for the performance of the audits and subsequent monitoring of improvement plans, as well as the support of the local teams affected, depending on the aspects that are audited.

#### 2.19.5.2. 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 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 best practices, fostered through different initiatives and meetings with our suppliers.

One example is the management of 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 jointly establishing mechanisms for early detection and prevention of possible risks in our contractors and subcontractors (most of them in direct contact with our customers). To this end, we rely on a continual process of administrative and on-site audits of our Allies, with the aim of ensuring that minimum working and workplace health and safety conditions for their workers are provided - important in this type of labour-intensive services.

Another example is our participation in the Joint Alliance for CSR (JAC) industry initiative, together with 27 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 regions such as Asia, Latin America and Eastern Europe. To this end, we carry out on-site audits of both direct suppliers and tier 2 and 3, etc. In this context, improvement plans are implemented to rectify the non-conformities identified. Additionally, specific working groups are set up in JAC (climate change, human rights and circular economy), in which we go beyond the audits to implement best practices in our supply chains.

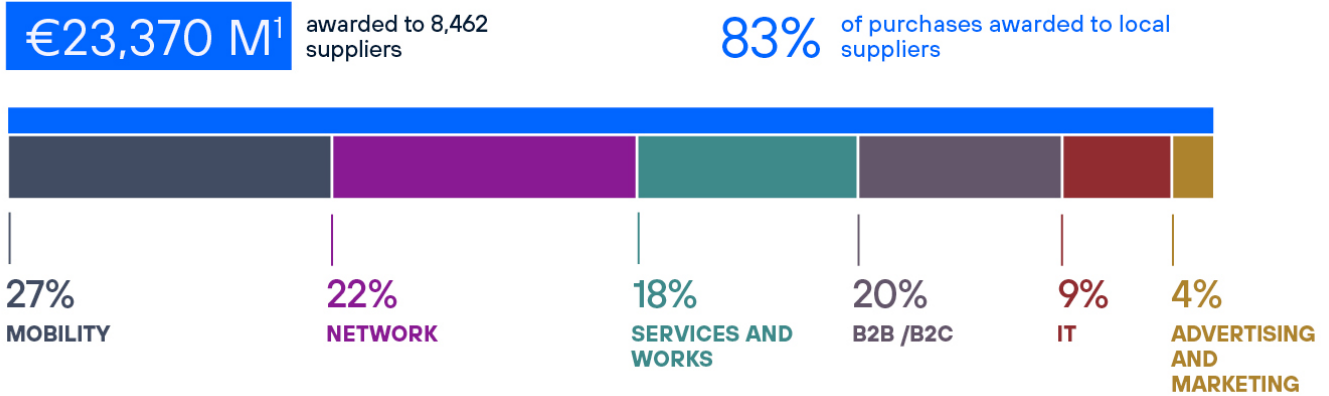
#### Targets

- 100% of potential high-risk suppliers assessed on sustainability matters via an external platform by the end of 2026.
- 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 the components or products they sell to us.
- Reduce CO<sub>2</sub> emissions in our value chain (Scope 3) by 56% by 2030 compared to 2016, and achieve net zero emissions by 2040.

<sup>1</sup> 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).

Impact of our business on society

Volume of purchases awarded %/Total



(1) Agreements negotiated in Procurement with impact in 2023.

2.19.6. Progress in 2023

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

2.19.6.1. Risk management in 2023

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

In 2023, we required 100% of our suppliers to accept the minimum standards set out in our Supply Chain Sustainability Policy (step 1).

Based on our global risk analysis of awarded suppliers contracts in 2023, we identified 687 suppliers that provide us with products or services classified as potentially high risk from a sustainability perspective. In 2023 we maintained our analysis methodology in order to focus on those suppliers with a significant impact on the business as well as on the Company’s strategy (step 2).

Of the suppliers identified, 72% have been externally assessed against sustainability criteria through the external IntegrityNext platform (including those that are currently in progress, pending analysis of the information provided). The IntegrityNext platform allows us to select the criteria to be included in each assessment according to the potential risk level they may pose to Telefónica as identified in our overall risk analysis (step 3).

According to the information available in the procurement system at the end of this reporting period, 5 suppliers were blocked in our database due to integrity/sanctions or sustainability risks or non-compliance. These represent 100% of the suppliers with identified risks – relating to either integrity/sanctions or sustainability issues (social or environmental reasons) – which had not yet remedied the situation or shown a commitment to implementing improvement plans to ensure compliance with our standards.

In addition, we complement our supplier risk management process with audits that allow us to verify suppliers’ level of compliance with the various sustainability requirements we ask of them, including respect for human rights.

In 2023 we conducted 18,324 administrative or on-site audits. According to the results obtained in these audits, at the end of the year we had 853 suppliers with improvement plans in place (representing 10% of all awarded suppliers in 2023), (step 4).

See breakdown of audits by topic in the table below.

**Details of the Annual Audit Plan**

Type of supplier	Region/ Country	Ongoing audits and improvement plans	Audited risk topics							Security, privacy and data protection	
			Ethics	Labour	Health and safety	Supply chain management	Human rights Child/ forced labour	Conflict minerals	Environment		
<b>ALLIES PROGRAM</b> Labour-intensive collaborator companies.	Spain and seven countries in Latin America <sup>2</sup>	LOCAL • 9,116 administrative audits. • 8,263 on-site audits. • 239 suppliers with improvement plans.		✓	✓			✓			
	Germany, Spain and eight countries in Latin America <sup>3</sup>	CORPORATE • 85 on-site audits. • 81 suppliers with improvement plans.	✓	✓	✓	✓	✓		✓	✓	
<b>JAC INITIATIVE</b> Manufacturing centres in the ICT sector.	64% in China and the rest in 13 countries <sup>4</sup>	• 91 on-site audits: 67% on Tier 2 or 3 suppliers. • 44 suppliers with improvement plans.	✓	✓	✓	✓	✓	✓	✓		
<b>OTHER LOCAL AUDITS</b> Due to risks associated with the product or service.	Brazil and Venezuela	• 180 administrative audits. • 166 suppliers with improvement plans.									
	Brazil, Ecuador, Mexico and Peru	• 9 on-site audits. • 9 suppliers with improvement plans.							✓		
	Brazil, Chile and Germany	• 392 on-site audits • 165 suppliers with improvement plans.			✓						
	Brazil, Colombia and Germany	• 172 on-site audits. • 142 suppliers with improvement plans.								✓	
	Germany	• 1 on-site audits. • 1 suppliers with improvement plans.	✓	✓	✓	✓	✓		✓		
	Chile	• 15 on-site audits. • 6 suppliers with improvement plans.		✓							
			<b>Social</b>						<b>Environmental</b>		
<b>Total audits per topic<sup>5</sup></b>			<b>17,963</b>						<b>366</b>		
<b>Suppliers with improvement plans</b>			<b>536</b>						<b>301</b>		

<sup>2</sup> Argentina, Brazil, Chile, Colombia, Mexico, Peru and Venezuela.

<sup>3</sup> Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru and Venezuela.

<sup>4</sup> Spain, France, India, Japan, Malaysia, Mexico, UK, Czech Republic, Romania, Sweden, Thailand, Taiwan and Vietnam.

<sup>5</sup> Total audit per topic do not tally with the total audits realised as some audits focus on other aspects (e.g. privacy) as opposed to social and environmental matters.

### Details of JAC audits (product manufacturers)

In total, 890 corrective action plans were proposed as a result of the 137 audits conducted under the JAC sector initiative in 2023, of which 91 corresponded to Telefónica's suppliers.

The following table provides additional information on the four audited topics that raised the most corrective action plans in this audit campaign.

Topic	Non-compliance	Corrective action	Status at the end of 2023
Health and Safety	Fire drills are not conducted on a regular basis for all factory employees, especially those on the night shift.	Adjustment of drill plans and schedules to ensure regular drills (e.g. extending the scope of the Drill Plan to all employees).	Closed
	Emergency lighting and emergency exit signs have not been properly installed.	Proper installation of emergency exit signs and fire exits and implementation of regular inspections of emergency signs and equipment (e.g. annual inspections of facilities, signs and equipment such as fire extinguishers).	Closed
Work schedule	The working-hour management and control system is not effective.	Establishment of systems to record, manage and monitor working hours, including overtime, with reliable and detailed records of workers' working hours.	Closed
	Workers' overtime hours exceed local legal requirements and their weekly working hours exceed 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.	Calculation of greenhouse gas emissions and implementation of measures to reduce them. For example, hiring a third party to define emissions reduction measures and targets.	Closed
	The factory does not have chemical labels for the hydrochloric acid containers in the chemical store or, if available, they are not written in the local language.	Affixing labels in the appropriate language on chemical containers.	Closed
Wages and compensation	Wage deductions are effected in exchange for receiving work clothes.	There are now no wage deductions for clothing, and personal protective equipment is offered free of charge to employees.	Closed
	Insufficient social security provided to workers.	Social security is now provided to all workers.	Closed

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

We closely monitor service providers' (including contractors') compliance with our standards. In 2023 the audit process covered each of our main markets – Brazil, Spain and Germany – and seven countries in Latin America (Argentina, Chile, Colombia, Ecuador, Mexico, Peru and Venezuela).

In 2023 we audited 85 labour-intensive suppliers. As in previous years, a high level of compliance was achieved: over 86% in the five topics audited (Responsible Business Principles, human resources, health and safety, environment, and security and data protection).

Looking at the average number of risks identified per topic in each of the countries, we found that **health and safety** was the topic with the highest number of risks, with these being concentrated around industrial hygiene and safety, emergency control, verification and planning.

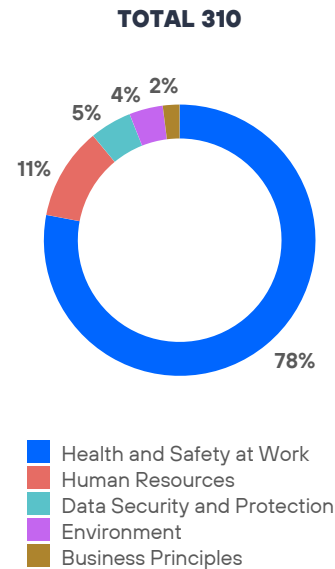
For **human resources**, the most common risks were detected primarily in relation to the recruitment process and personnel administration, training, workplace climate assessment and meeting the percentage target for staff with disabilities. For **environmental** processes, the most common risks concerned the environmental management system, waste management and noise. As for **security and data protection**, the most common risks related to failures to identify the personal data processing carried out by the supplier and specific training for their employees in this area.

Of the potential social or environmental<sup>6</sup> impacts of the risks identified, the most significant were as follows:

- The most significant **social impacts** were mainly related to industrial hygiene and safety, emergency control, planning, and the recruitment process and personnel administration (mainly due to the absence of certain clauses in contracts or lack of an equal pay policy).
- The **environmental impacts** were related to environmental management (due to the lack of a policy approved by the company's senior management) and the lack of preventive measures or monitoring of the level of environmental noise caused by supplier activities.

In this context, and although the results obtained generally reflect a good performance of our partners, improvement plans have been agreed with each of the audited suppliers to address the negative impacts identified.

### Breakdown of significant non-conformities



### 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 2023, **67% of the audits** we conducted were of **Tier 2 or 3 suppliers**.

### 2.19.6.2. Engagement in 2023

For another year running, we continued promoting new capabilities among our suppliers, in order to improve their performance on key sustainability-related issues.

### Supply chain emissions

In 2023, we implemented various supply chain decarbonisation engagement initiatives based on each supplier's contribution to our Scope 3 emissions:

- In collaboration with other telcos, we invited our most strategic suppliers to participate in the **Carbon Reduction Programme**, a project that promotes the decarbonisation of suppliers at product level, considering those products most sold to telcos.
- Suppliers accounting for around 90% of our supply chain emissions were invited by Telefónica to provide climate data through **CDP Supply Chain**, information used in the **Supplier Engagement Programme** initiative, to categorise suppliers by their level of climate maturity and provide training sessions to help them make improvements in this regard.


<sup>6</sup> Critical non-conformities identified during audits in each area are considered significant impacts, either social or environmental.



Additionally, top suppliers were requested to align and validate their emissions reduction targets with **the Science Based Target initiative (SBTi)**.

- All suppliers accepted Telefónica's **Supply Chain Sustainability Policy**, which includes emissions reduction requirements.

Other SME-specific engagement measures, such as the **SME Climate Hub** and **1.5C Supply Chain Leaders**, and sectoral level actions, such as our leadership of the climate change working group of the **JAC Initiative**, have also been fundamental to our supplier collaboration strategy.

 For further information, see 2.2. Energy and climate change

Telefónica has implemented a new climate requirement within its procurement process, requesting its key suppliers to provide science-based decarbonisation targets and validate them with SBTi.


### Labour conditions

**Under the JAC initiative**, we collected **direct feedback** from **10,342 employees** at 13 supplier factories through an **anonymous survey** conducted on their own mobile phones. This enabled us to analyse working conditions in more detail, especially those concerning the number of hours worked, rest periods, harassment, discrimination, treatment, relationship with their direct manager, overtime, the handling of chemical materials, etc.

In the new **Living Wage Working Group** of 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 scheme, we ensure that suppliers pay their employees a **fair and reasonable wage** that is high enough to maintain a **decent standard of living**.

### Human rights

In 2023, within the JAC initiative, we participated in the creation of a **new working group on Due Diligence** with the aim to ensure compliance with a set of minimum social and environmental standards throughout the ICT sector supply chain. This working group analysed the different national and international legal requirements (such as the proposed Directive on Corporate Due Diligence in Sustainability) and works on the identification and implementation of sectorial solutions to ensure compliance.

 For further information, see chapter 2.14. Human rights

### Responsible sourcing of minerals

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

#### 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 potentially high-risk suppliers

1. We identify suppliers with a potential high risk regarding minerals on the basis of our risk analysis methodology.
2. We assess performance based on the Conflict Minerals Reporting Templates (CMRTs) 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 are shared and stakeholder dialogue is 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 Whistleblowing and Queries Channel through which our stakeholders can submit enquiries and complaints about the sourcing of minerals.

## 5. Information

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

## Occupational Risk Prevention

In 2023, once again, we focused on fostering best practices regarding **safety, health and well-being** in our **supply chain**, placing particular **emphasis on contractors** who assist us in the deployment and maintenance of the network, which are where the main risks lie (work at height, electrical risk and confined spaces).

In 2023 we worked with our suppliers on a series of initiatives that took different forms depending on the situation in the different countries:

- Specific and direct **communication with our suppliers** via face-to-face sessions that addressed what needs to be done to prevent the risks inherent in each activity from causing accidents. For example, **in Colombia** we organised **two technical round tables** at which we shared best **practices** with our suppliers on how to manage tasks involving **exposure to electrical risk and effective road safety**. We showcased our new tool for reporting and monitoring accidents to the almost 100 people who participated in these round tables.
- Occupational health and safety **audits** specifically adapted to each country, in order to verify compliance with the established procedures and protocols to prevent risk and ensure employee safety at our 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 issues).
- **Follow-up** and monitoring of the corresponding indicators in order to analyse accident rate trends throughout the year.

Through dialogue with our suppliers, as well as verification and monitoring of compliance on their part, we can work to improve the level of safety and health of employees in our supply chain.

## Monitoring model at Telefónica Spain

As an ISO 45001-certified company, we have a monitoring model in place to prevent and mitigate potential risks related to the operations of our contractors. The model contains the following work processes:

### • Control of preventive documentation

Suppliers must prove, prior to the start of the activity, that they are aware of the risks and preventive measures detailed in the contracts signed. Their workers must have the necessary training and personal protective equipment to carry out the activity in question.

### • On-site audits

In 2023 a total of 7,618 supervision processes (unannounced on-site OHS audits) were carried out. At year end, 34 audited suppliers had improvement plans in place to address the deficiencies identified.

### • Safety monitoring

For those tasks that involve climbing heights or working in a confined space, we have initiated a new type of monitoring procedure to verify that the corresponding safety report has been completed. If the safety report has not been completed, the company is notified of this shortcoming and urged to take the necessary measures to remedy it. In 2023, 18,490 shortcomings were notified.

### • Ad hoc meetings

- Ad hoc meetings are convened to coordinate Telefónica and third-party business activities (58 and 18 companies respectively).
- Ad hoc meetings are also held with the heads of our partner companies to inform them about new documents relating to specific prevention measures (all companies in the field of installation and maintenance are present at these meetings).
- Furthermore, single-issue meetings are held with those companies who obtained the worst prevention indicators.

### • OHS+ Initiative

The OHS+ Initiative is an ongoing forum for dialogue, sharing practices, answering queries and offering proposals for improvement. Its aim is to identify levers that will lead to a reduction in the number, volume and severity of OHS incidents until there are zero incidents.

#### 2023 results:

Our accident frequency rate (in the workplace in Telefónica Spain) fell to 1.24. Our target of 0.9 by 2024 still stands.

### • Updating of regulations and approval of specific prevention measures

An example of the work done under this process is our approval of the plan to accelerate the replacement of poles in poor condition.

### Diversity

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

In this regard, we promote "**Mujeres en Red**", a collaborative project with our contractors that we run in **Colombia and Peru** to promote **employability and training for women** in technical positions in the telecommunications sector, championing **equal opportunities** in roles where women are underrepresented. By the end of 2023, more than 1,070 female technicians had been hired by our operational partners in both countries, and over 7,000 people (both technicians and administrative staff) had received training on topics such as "Unconscious Bias", "Female Empowerment" and "New Masculinities".

*Mujeres en Red* has established itself as a leading initiative in terms of **employability and equity**. As a result, it received the following **awards in 2023**: in Peru, the Par Ranking award (in the "Best Innovative Labour Practice" category), the Corresponsables International Award, the Scotiabank Equality Award and the Companies that Transform Peru prize; in Colombia, the Award for Good Practices in Sustainable Development towards SDG 5 of the Global Compact.

In addition, 2023 saw the **annual "Allies for Equity" event** held in both countries for the first time to recognise the work of the *Mujeres en Red* project, as well as that of the contractors and Telefónica employees involved in this initiative. As part of the ceremony, awards were presented in the following categories: *Mujeres en Red* Woman of the Year, Breaking Biases: Technical Ally for Diversity, Company Committed to Equity, and Leadership and Commitment.



For further information, see 2.7. Diversity and inclusion

### Training and communication

Under our procurement model, **ESG topics** are **incorporated into the regular training sessions given to our buyers** in various countries. Our buyers also receive **training on specific topics** such as low-carbon procurement. In addition, like the rest of the Company's employees, **a percentage of their annual variable remuneration is linked to sustainability indicators**.

In **Germany**, we started offering **employee and supplier training** as part of our approach to **human rights and sustainable supply chain management** in 2023.

Among other topics, the course explains the **requirements contained in the German Act on Corporate Due Diligence Obligations in Supply Chains** and raises awareness about respecting human rights in our own business areas and supply chain. Furthermore, **100% of the Executive Committee of Telefónica Germany** received training on the German Regulation.


In **Brazil**, we implemented a communication plan for **contract managers** in 2023, in order to improve the internal culture around **third-party management** throughout the life cycle of a supplier's relationship with Telefónica. This plan focused on our processes, procedures and guidelines and was aimed at **mitigating potential risks in the procurement of outsourced services**.

In addition to the training given to our buyers and internal contract managers, we continued to provide **supplier training** and maintained our supplier **communication channels** for another year running.

In 2023, we delivered 14,816 in-person courses and 57,028 online courses involving over 548,769 participants from partner companies in Latin America.


Our supplier training was delivered in-person and online, addressing the specific needs in each country and the most critical issues according to the service the suppliers provided.

At a global level, in 2023 we launched a project to share our main **integrity regulations** and the consequences of non-compliance with suppliers that have been awarded contracts with us, in twice-yearly sessions.

 For further information, see 2.16. Ethics and compliance

One of our targets for 2023 was to strengthen our relationship with suppliers in the area of **privacy and data protection**. One of the key measures taken to achieve this at global level was to provide suppliers with training on the proper processing of personal data. Through specialised content, we shared practical guidelines to ensure respect for key privacy principles and Group Telefónica policies when processing data.

In **Ecuador**, privacy guidelines issued by the local DPO's office were shared with third parties such as authorised distributors. These guidelines convey the importance of acting in accordance with the provisions of Ecuador's Organic Law on the Protection of Personal Data.

 For further information, see 2.18. Privacy and security

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

In 2023, our participation in initiatives such as **SME Climate HUB** and 1.5°C Supply Chain Leaders continued, with the aim of helping SMEs to measure their emissions and take specific action to reduce them and achieve their climate targets. For instance, in 2023, we invited some of our small and medium-sized suppliers to a SME-oriented event entitled "Decarbonisation of SMEs. Boosting the SME Climate Hub in Spain".

In **Brazil**, we participated in an SME training program to strengthen sustainable value chains in the country. This program is part of the **AL-INVEST Verde initiative**, organised in partnership with the Spanish Chamber of Commerce. Training is provided by the team at Fundação Getúlio Vargas and financed by the European Commission.

The aim is to support Brazilian SMEs in the transition towards a circular and low-carbon economy, thereby facilitating the implementation of sustainable production models. We invited **17 of our suppliers** to participate, all of them important SMEs for Telefónica Brazil with the potential to incorporate better sustainability practices in their businesses.

We also promoted continuous communication as a key lever for boosting supplier engagement through a number of channels, such as our allies' newsletter, the Allies' Portal and the Suppliers' Portal. The Suppliers' Portal contains all of our global policies, as well as specific local requirements.

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


## Supplier satisfaction survey

We continue to work hard to find out our suppliers' opinions and priorities. In 2023 we conducted a **survey** of our main suppliers to determine their **satisfaction levels** and identify what they view positively and what they think could be improved. Our questionnaire targeted approximately **6,800 suppliers and achieved a participation rate of 26%**.

Our scores have shown an upward trend over the last nine years, reaching an **average rating** of 8.33 in 2023 (on a scale of 0 to 10).

Last year, the **most highly rated** aspects were those related to Telefónica's reputation and suppliers' attitudes towards the Company, specifically, Telefónica's leadership and reputation in the telecommunications sector, the honesty and transparency of our buyers in ensuring equal opportunities for suppliers, and willingness to work with other companies in the Group. Although none of the aspects scored less than seven, the **lowest rated** were related to invoicing and the simplification of suppliers' relationships with Telefónica.

The survey also asked our suppliers to give us their views on how they could be impacted by the measures taken by Telefónica in relation to each of the main material issues in our materiality analysis.

 For further information, see 1.4. Materiality


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

### The 14th Telefónica Global Energy and Climate Change Workshop

Lasting three days and attended by around **250 participants**, this workshop provides the annual meeting point for the **leaders of the Company's energy transformation and our main partner companies**, and centres around innovation and digitalisation as the means to protect the planet, reduce energy consumption and lower the global carbon footprint.

During the workshop, multiple initiatives from our different markets were presented. Among other things, they focused on energy purchasing, emissions in the value chain, reducing fuel consumption and increasing renewable consumption.

We also announced our goal of achieving a 90% reduction in global operational emissions (Scopes 1 and 2) and a 56% reduction in emissions in the value chain, in time for finalisation of the 2030 Agenda for Sustainable Development.

 For further information, see 2.2. Energy and climate change

### Workshop on Responsible Supply Chain Performance in Brazil

This workshop was attended by **almost 250 people from 105 Telefónica supplier companies**. During the event, we shared general insights into our Responsible Business Principles, **integrity program, data security and privacy** issues and **workplace safety** management.

### Forum on Occupational Risk Prevention in Spain

We have been organising this conference since 2018, bringing together our main contractors, technological partners, employee representatives, the prevention services from our other operators, and other participants from leading prevention organisations (the Quirón Group, Audelco, ADEMI, etc.). During the conference, **we address issues related to prevention and health in a format designed to encourage participation** (presentations, round tables, etc.).

The fifth edition, held in 2023, involved **companies from contracts in relation to network deployment and maintenance**.

### ESG Event with our Allies in Colombia

Last November we held an event to discuss topics related to the **opportunities available to companies that incorporate environmental, social and governance issues**. The event was attended by **40 representatives from our main partners in Colombia**.

### Summary of key indicators

#### GRI 204-1

Indicators		2022	2023
Activity	Volume of purchases awarded	21,863M	23,370M
	Suppliers selected	8,526	8,462
	% purchases awarded locally	83%	83%
Ethics and Compliance	Potential high-risk suppliers regarding sustainability identified in internal risk analysis	768	687
	% of potential high-risk suppliers assessed on sustainability aspects through external assessment platform	72%	72%
	% Suppliers assessed through Dow Jones Risk & Compliance.	100%	100%
	Suppliers blocked due to integrity or sustainability sanctions, risks or non-compliance	6	5
	Total audits of suppliers	18,578	18,324
	Suppliers with improvement plans in place following audits	879	853

## Milestones

- ❶ We continued to minimise sustainability risks within the procurement process, requiring 100% of our suppliers to accept our sustainability standards as part of their contractual obligations.
- ❷ We improved our supplier assessment processes in order to be able to meet new requirements for supply chain due diligence.
- ❸ In collaboration with other telcos in the JAC initiative, we audited 137 companies in the ICT sector and surveyed 10,342 employees at 13 supplier factories in 2023, covering different levels of our supply chains.
- ❹ As part of our supply chain decarbonisation strategy, we requested our key suppliers to commit to emissions reduction targets validated by the Science Based Targets initiative.
- ❺ We strengthened our scope 3 supplier engagement by providing tailor-made capacity-building within the Supplier Engagement Programme and by working on reducing product-level emissions within the Carbon Reduction Programme.
- ❻ We reduced CO<sub>2</sub> emissions in our value chain by 31% compared to 2016. Emissions in our supply chain account for the largest proportion of our Scope 3 emissions (64%).