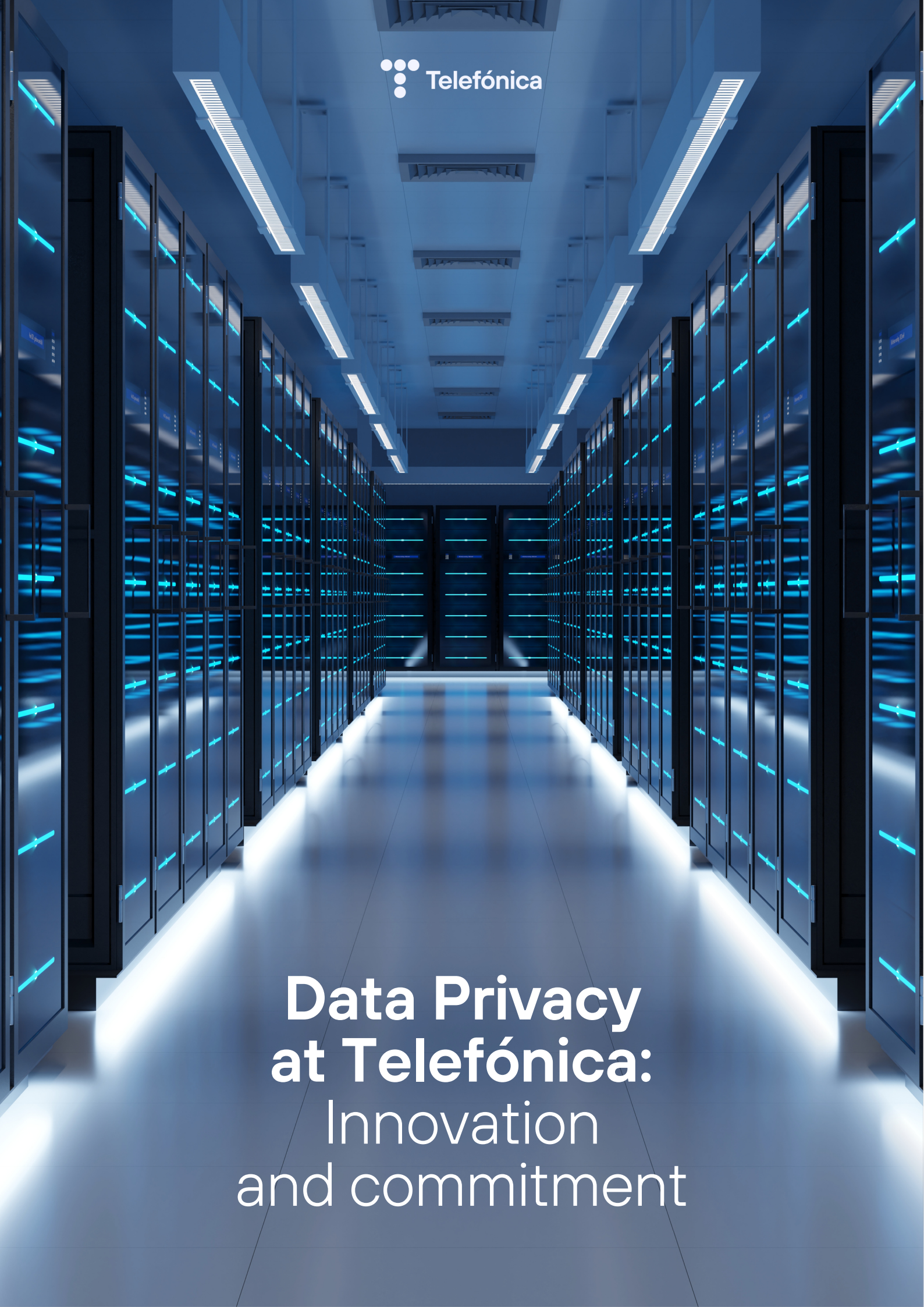


Data Privacy at Telefónica: Innovation and commitment

Contents

1 Vision and principles

Technology enhances people's quality of life and creates wealth, provided that privacy is upheld, and the highest standards of security are maintained throughout the processing of personal information and data.

We are committed to ensuring our customers feel confident when using our products and services, knowing that we always respect their rights and offer them choices regarding the use of their personal information. To build lasting relationships based on trust, we prioritise privacy at every stage of our interactions. Our approach is built on the following core principles:

- Protection: protect our customers' personal data through robust policies and processes.
- Empowerment: individuals should have full control over their personal data. This means giving them access to their information, as well as insights into the associated risks and benefits of managing it.
- Design: we prioritise privacy from the very beginning, embedding it into the foundation of our products and services. This ensures that privacy is maintained at every stage of development and throughout the lifecycle of our offerings.
- 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". Also, we are committed to transparency by providing users with clear, intuitive tools to manage their data, backed by the technological infrastructure required to uphold the highest standards of privacy.

Guided by our Responsible Business Principles, we ensure that this commitment is embedded across all our operations. These principles establish a shared framework for ethical conduct, uniting all companies within the Group under a common approach to safeguarding privacy and compliance.

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

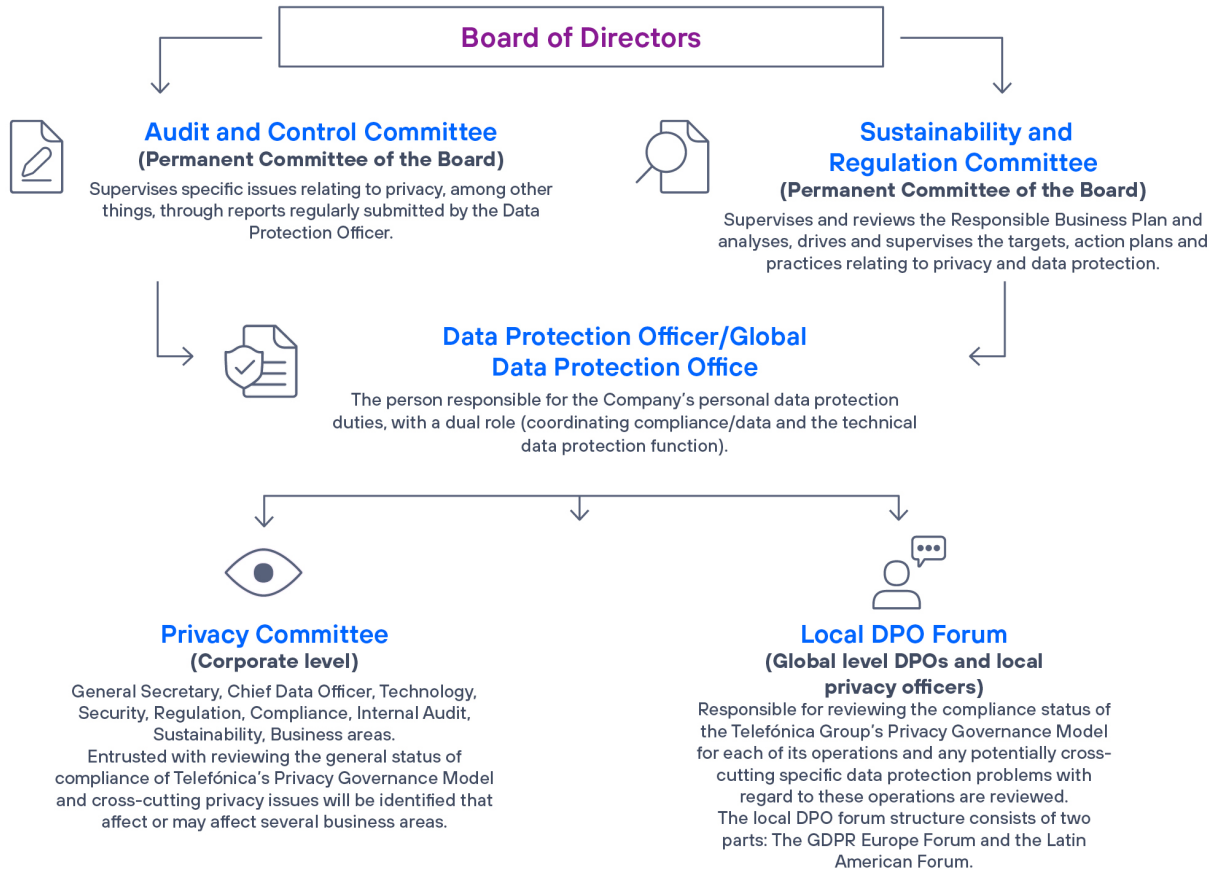
2 Governance

At Telefónica, we have implemented a comprehensive governance framework to manage personal data protection effectively and align it seamlessly with the Group's strategic priorities. This approach ensures a consistent, transparent, and unified standard of data protection across all our operations globally.

The Group's Data Protection Officer (DPO) plays a pivotal role in overseeing privacy compliance efforts. 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.
- Driving and managing the records of processing activities.
- 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 Privacy Committee and through the Local DPO Forum Structure. The Local DPO Forum is divided into two regional groups: one for the Latin America region and another for Europe. These forums enable collaboration and the exchange of best practices among data protection officers from different countries and regions, facilitating the alignment of strategies and policies to ensure regulatory compliance and privacy protection. gatherings help align efforts and ensure that privacy measures are effectively integrated throughout the organisation.



At Telefónica, we have implemented a comprehensive governance framework to manage personal data protection effectively

The Board of Directors is involved in this governance structure. Each year, the DPO presents a detailed report to the Board through the Audit and Control Committee, which provides oversight for data protection activities. Moreover, the Sustainability and Regulation Committee oversees the implementation of the Global Responsible Business Plan, ensuring that privacy goals are met. Updates on this plan are regularly tracked by the Global Sustainability Office, which keeps the Board informed about progress and key developments.

This governance model underscores Telefónica's unwavering commitment to safeguarding privacy and achieving the highest levels of accountability in how we manage and protect data.

3 Policies

At Telefónica, data protection is not just a priority but a structural commitment that is materialised through a robust framework of policies and procedures. These policies are designed to ensure that our privacy management is aligned with the highest international standards and applicable local regulations.

Privacy regulations

Global Privacy Policy

Corporate Rule

Approved by the Board of Directors of Telefonica, 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 framework applicable to our different actives in the field of data protection.

Regulation on Requests by Competent Authorities

Corporate Rule

Approved by the Ethics and Sustainability Direction of Telefónica S.A.

↓

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

3.1. Privacy Policies

Three regulatory pillars support our approach to privacy:

→ Global Privacy Policy

This policy, approved by the Board of Directors, establishes the guiding principles that ensure transparent, secure, and ethical data handling across all Group companies. It focuses on key values such as legality, transparency, and respect for the rights of data subjects. The global privacy policy is available to all interested parties in Spanish, Portuguese and in English.

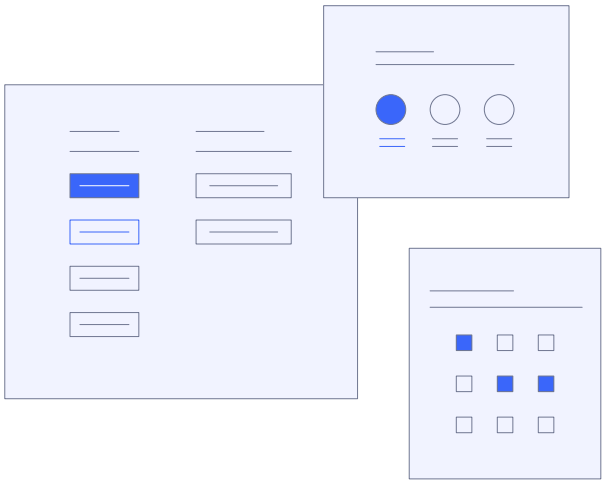
→ Data Protection Governance Model Regulation

Approved by the DPO Office, establishes the operational, strategic, and organizational governance model for managing privacy across the Group. This regulation defines how privacy is effectively governed, outlining the roles, responsibilities, and processes for implementing privacy strategies throughout the organization.

→ Regulation on Requests from Competent Authorities

Approved by Ethics and Sustainability Department, this regulation sets the minimum principles and guidelines that must be followed in internal procedures across each Group company, Business Unit, and Operational Business to fulfill the duty of collaboration with authorities regarding our customers' data.

All this information is accessible to Data subjects through our Global Transparency Center, available on our website.



3.2. Operational Domains: The Core of Our Internal Management

Operational Domains play a crucial role in the effective implementation of our data protection policies, serving as a comprehensive set of internal procedures established by the Telefónica Group DPO Office. These domains are regularly updated to reflect the latest legislative changes and evolving data protection requirements. The most recent update, which took place in November 2023, marked an important milestone by expanding the scope of the Operational Domains to encompass all data protection jurisdictions within the Telefónica Group. This extension ensures that our data protection practices are harmonised across all regions, reinforcing our commitment to compliance and privacy protection across the Group.

The Operational Domains regulate the following aspects:

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

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

Framework to follow for planning and conducting regular audits to verify compliance with established privacy policies and procedures. This framework outlines the processes, responsibilities, and criteria for performing thorough audits across all areas related to personal data protection.

Training and awareness

Coordination of employee training on 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. This domain outline the steps to be followed when a data subject submits a request to exercise any of these rights, ensuring that all requests are handled in a timely, transparent, and compliant manner.

Data retention and erasure

We follow the "Data minimisation" 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.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

Binding Corporate Rules

Governance model and obligations for exporters and importers of intragroup transfers of personal data coming from the application of Binding Corporate Rules as described in the next section below.

3.3. Binding Corporate Rules (BCRs)

The Binding Corporate Rules (BCRs) have been approved by Spanish Data protection Authority following the cooperation procedure between European Data Protection Authorities to regulate the international flow of data within the organization, in compliance with Article 47 of the GDPR. These rules allow the transfer of personal data from the European Economic Area (EEA) to countries outside it, in an efficient and secure manner.

The implementation of the BCRs contributes to ensuring compliance with European regulations across all Telefónica companies, enabling more efficient management of personal data, regardless of the location of the receiving subsidiaries. Additionally, the BCRs provide greater legal security and facilitate alignment with the Group's organizational model.

Since its approval in March, throughout 2024, we have focused on the following aspects:

- Abidance of affiliated entities to BCRs.
- Update of the Global Privacy Policy
- Inclusion of BCRs references and clauses of BCRs in contracts with new employees and suppliers.
- Training employees on privacy principles and BCRs.
- Creation of a dedicated inbox inside the Queries channel, as well as an email inbox for requests related to BCRs.
- Maintaining a record of processing activities for all processing operations related to BCRs, exporters and importers.
- Setting up a specific audit plan to assess the proper implementation of BCRs.
- As of the date of this report, more than 99% of group entities linked to the initial list have adhered to the BCRs.

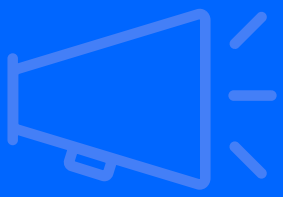
The implementation of the BCRs contributes to ensuring compliance with European regulations across all Telefónica companies

3.4. Monitoring practices

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.
- Training and awareness: 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.

4 Risk management



At Telefónica, we adopt a risk management-oriented approach as a fundamental pillar to ensure privacy and data protection across all our activities. Our main objective is to reduce risk exposure and enhance digital trust by implementing continuously evolving processes and policies.

Privacy risk management holds a prominent position in our corporate strategy. This approach involves proactive and thorough identification of associated risks, as well as applicable regulatory requirements, ensuring both risk mitigation and compliance with prevailing regulations.

A detailed record of data processing activities is maintained in an internal platform specifically developed for privacy management. For each processing activity, a privacy risk assessment is conducted to evaluate its potential impact and establish the necessary measures and controls to mitigate risks. Through this evaluation, risks are identified, controls are implemented, and continuous monitoring is carried out, ensuring effective management of the privacy impacts on customers.

Additionally, we apply a proactive accountability model based on critical and ongoing self-assessment of regulatory compliance. This model enables us to develop strategies that integrate privacy throughout the entire data lifecycle, from its collection and processing to rights management and data retention or deletion.

In this way, Telefónica reaffirms its commitment to incorporating privacy as a core value in all its products and services, strengthening users' digital trust and adapting to the challenges of an ever-changing technological environment.

5 Privacy by Design (PbD)

One of Telefónica's strategic pillars is **Privacy by Design**, a principle embedded in our internal regulations. This principle requires the entire organization to consider two key aspects during the design phase of products and services:

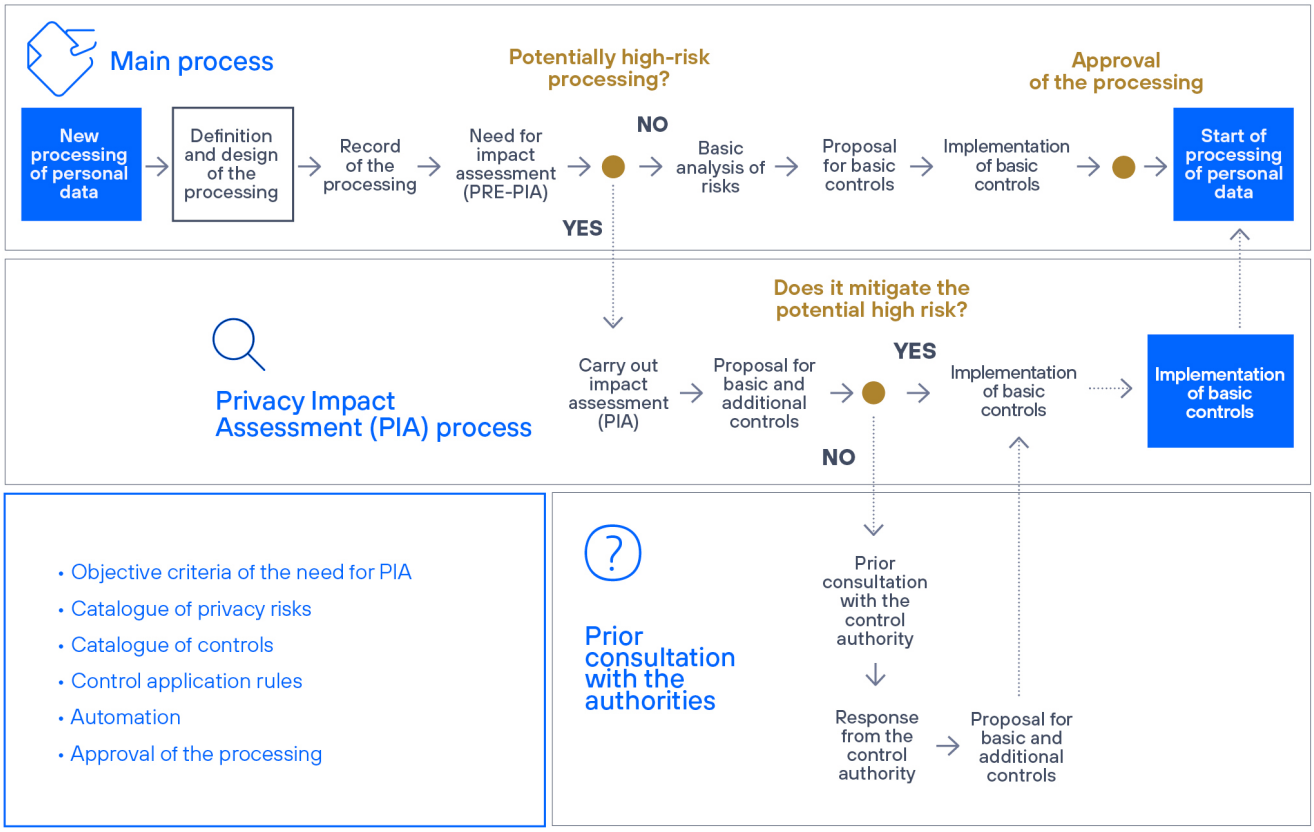
1. Apply legal and security measures to protect privacy from the earliest stages of any project.
2. Take into account all business processes and practices involved in data processing that may impact personal data.

We have created **Privacy by Design guidelines** that provide a set of standards, norms, and processes aligned with our **Global Privacy Policy.** These guidelines are designed to ensure that the rights and freedoms of data subjects are respected from the outset of any project or data processing activity.

These guidelines serve as reference documents for Telefónica professionals responsible for developing and implementing products and services, as well as for internal use cases involving personal data. Furthermore, product managers are supported by privacy and security specialists in each company or business unit within the Group to ensure that all legal and security requirements are considered from the design stage.

We adopt a **proactive risk management and accountability approach,** conducting critical and ongoing self-assessments to comply with privacy regulations throughout the entire data lifecycle for each product or service: data collection, processing, exercising of rights, retention, and deletion.

By applying the principle of **Privacy by Design,** we ensure that at all stages of product or service development, aspects such as the lawfulness of data processing, appropriate security measures based on potential risks, transparency of privacy policies, data minimization (collecting only data strictly necessary for processing), commitment to data subjects' rights, and data retention limitation are considered.



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

Digital Privacy Framework (DPF)

In today's landscape—where digital privacy is a critical pillar for user trust— **Digital Privacy Framework** (DPF) ensures compliance with the General Data Protection Regulation (GDPR) and ePrivacy directives while reinforcing our ability to scale secure and trustworthy technology solutions to data processing platforms and systems.

DPF translates legal privacy requirements into standardised functional and technical specifications, implemented in a fully automated, digital manner across our data processing platforms (such as Telefonica´s Kernel).

This approach allows Telefónica to take a proactive stance on regulatory compliance, embedding **privacy-by-design** principles across its AI initiatives.

Following its successful deployment in Spain in 2022, the rollout continued in following years to include key markets such as Germany and Brazil.

The DPF positions Telefónica at the forefront of privacy-driven digital transformation, delivering

long-term value in a market where data governance is increasingly critical.

Open Gateway

Open Gateway, an initiative in the telecommunications sector led by the GSMA, transforms telecom networks into developer-ready platforms, unlocking the full potential of the network. These capabilities are exposed through global APIs, designed with "privacy by design," including privacy management by Telefónica, ensuring control over the management of personal data with respect to authorities and our customers. This strengthens our promise to protect and give control of data and privacy to our end customers.

Retention Management in Kernel

Telefónica has continued to adapt to the challenges and opportunities presented by handling large volumes of data (Big Data). Our data retention policies in Big Data environments have been automated this year within our Kernel platform, evolving to ensure regulatory compliance, operational efficiency, and protection of our users' privacy.

With this automation, retention periods specified by our legal teams can be set within the systems, ensuring the secure deletion of data at the end of the retention period.

We ensure compliance with GDPR regulations while freeing up products from managing the data lifecycle, making this a 100% automated process.

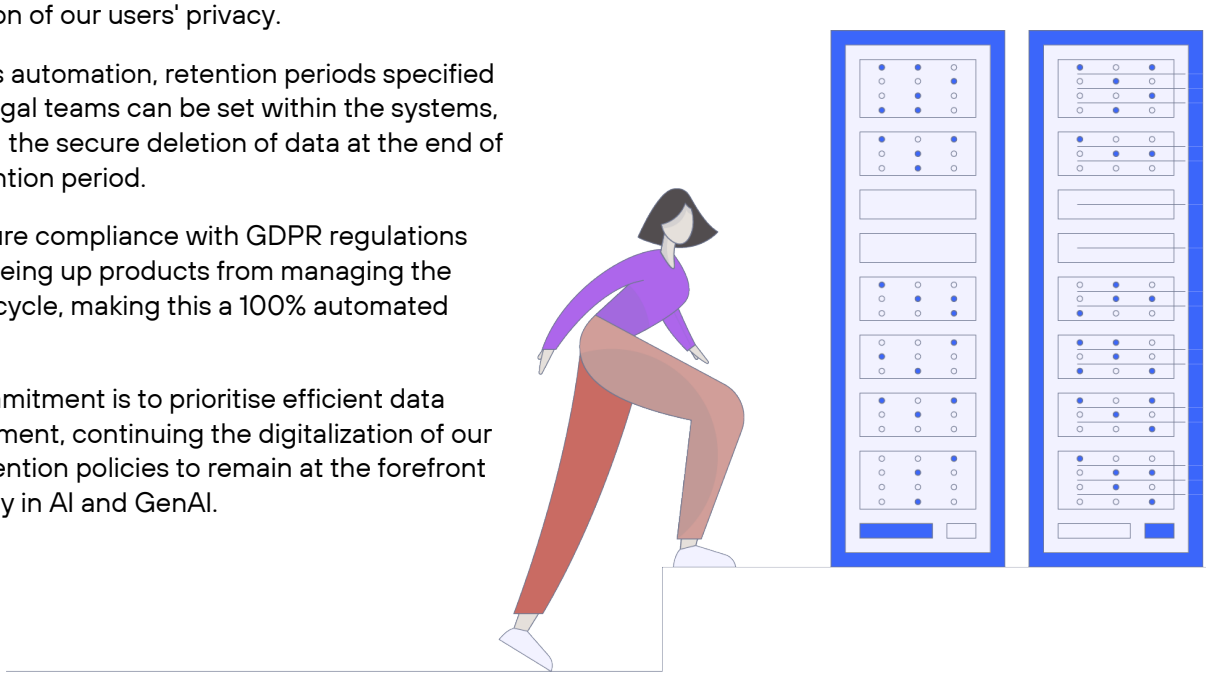
Our commitment is to prioritise efficient data management, continuing the digitalization of our data retention policies to remain at the forefront of privacy in AI and GenAI.

Privacy Management in Kernel

Kernel has revolutionised digital privacy management with its innovative ePrivacy capabilities, setting a new industry standard. Unlike traditional approaches that focus on device-level privacy, Kernel has implemented a customer-centric privacy management system, marking a significant advancement in protecting digitized personal data.

The distinctive advantages of this centralised privacy capability include consistency across devices and simplified control, allowing customers to manage their privacy preferences from a single point.

Our commitment is to prioritise efficient data management



6 Transparency

At Telefónica, we prioritise making privacy more understandable and human-centered. Transparency is a key element of our strategy, and we have launched several initiatives to make it a reality.

Global Privacy Center

Our Global Privacy Center serves as a public reference point for our privacy and security policies, offering clear and accessible information through visual tools. In 2025, we aim to improve this center by linking it to the Transparency Centers of our operators, centralising all relevant data.

Operators' Privacy and Security Centers

The Operators' Privacy and Security Centers provide customers and stakeholders with easy-to-understand digital information on how their personal data is handled. These centers offer guidance on exercising data protection rights, security measures, privacy terms, transparency reports, ethical principles for AI, and child protection online. They are regularly updated to stay compliant with regulations.

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

Telecommunications Transparency Report

Additionally, we publish an annual Telecommunications Transparency Report that details the requests we receive from authorities, such as legal interception, metadata access, content restrictions, and service suspensions. We adhere to a strict process to balance our cooperation with authorities while safeguarding the fundamental rights of individuals, in line with our human rights commitment.

7 Customer empowerment

We developed and implemented the Transparency Center ("Personal Data Space") in 2021 which is a centralised platform that allows our customers to access, manage, and control the information they generate by using our products and services, as well as those of our partners. This initiative reflects our commitment to business transparency and respect for the privacy of our users.

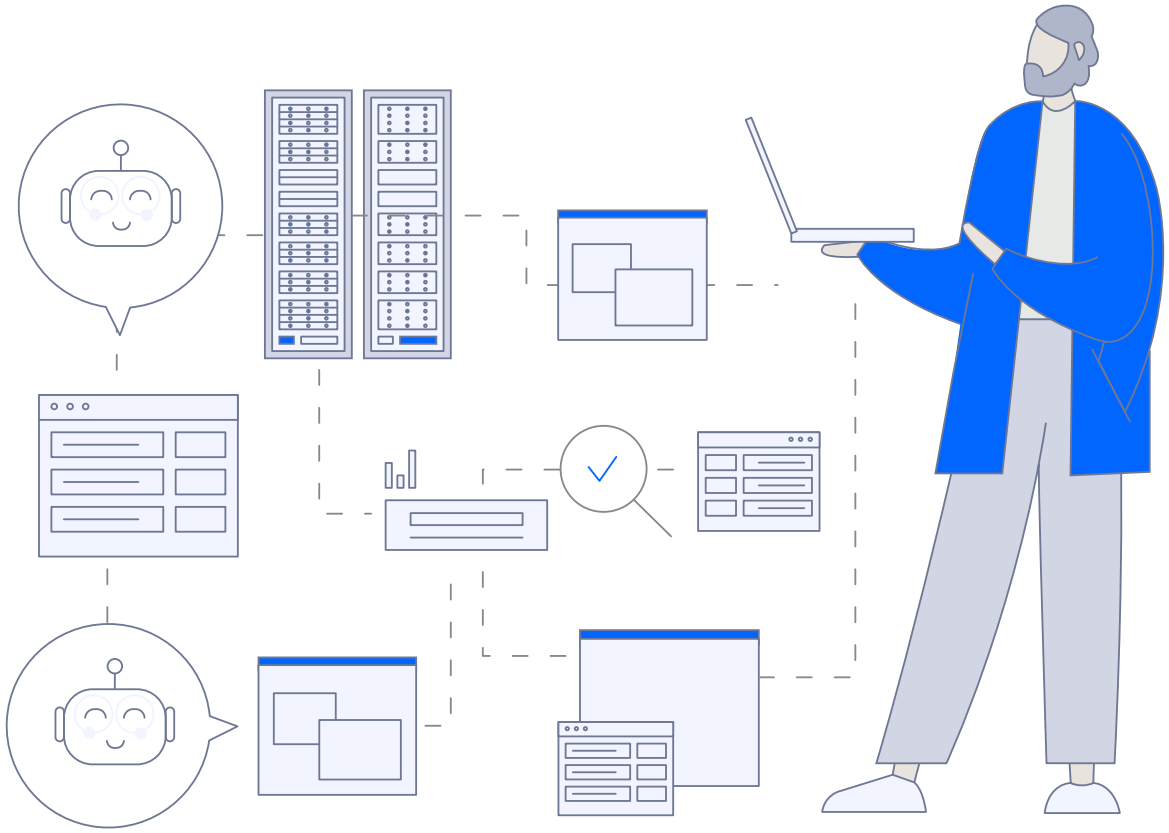
Key features of the Transparency Center include multichannel accessibility: mobile app, web, TV, and customer service centers. It provides users with the ability to view and control all collected data, categorized by product or service type.

Through the **Privacy Permissions** section in the Transparency Center, customers can manage the legal bases authorizing the use of their data for specific purposes. Additionally, in the **Access and Download** section, we offer user-friendly visualisations of different types of data, respecting privacy criteria, with the option to download a more detailed document.

The implementation of this initiative has had a positive impact on several aspects of our business, such as increased customer trust and excellence in regulatory compliance (GDPR and ePrivacy).

This initiative reaffirms our commitment to business transparency and the protection of our customers' data, positioning Telefónica as a leader in ethical and responsible practices within our industry.

The Transparency Center is designed to build user trust, using clear language to explain the purpose and nature of data processing within Telefónica. We also prioritise data minimization, ensuring that only necessary information is collected for legitimate purposes. Furthermore, we have implemented policies and guidelines for data retention and deletion within the Transparency Centers of the Group's operators, ensuring that data is retained only as long as strictly necessary and securely deleted when no longer needed.



The Transparency Center empowers customers with control and visibility over their personal data

Through the Transparency Center, we take the first steps to fulfill our promise of empowering our customers by granting them control and transparency over their data, always in compliance with applicable regulations, such as GDPR in Europe.

To ensure transparency and accountability in the use of personal data, we track the number of unique users whose information is utilized for **secondary purposes.** During 2024, the percentage of unique users whose data was used for secondary purposes is 73 %. This reflects our ongoing efforts to monitor and regulate how personal data is accessed and processed for non-essential activities such as marketing campaigns. We are committed to providing our customers with full visibility into how their personal data is used and ensuring that any secondary uses of data are done in compliance with applicable privacy laws and with user consent.

Query and raise concerns mechanisms

Data subjects may submit queries and raise concerns about Data Privacy via:

- Letter, email, or phone call through the data protection mailboxes made available to consumers in our legal notices and privacy policies.
- Personalised attention through contact mailboxes with the Data Protection Officers of Telefónica's operations.
- Electronic means such as the Mi Movistar app or their personal area of www.movistar.es.
- The Customer Defense Service, a second-instance mechanism that reviews the decisions made in relation to customer queries/complaints submitted via the regular channels provided by Telefónica.
- Dispute resolution under the Telecom Operators Code of Conduct in Spain, enabling customers to efficiently and promptly address data protection-related claims with telecommunications companies, allowing customers to resolve and quickly address claims related to data protection issues with telecommunications companies.
- Adherence to the AUTOCONTROL Code of Conduct for the "Processing of Data in Advertising Activities," approved by the AEPD, which provides a pathway for resolving data protection and advertising-related complaints from citizens in a more efficient manner. Furthermore, under the **Code of Conduct on Data Processing in Advertising Activities,** approved by the AEPD, 57 complaints or mediations were handled in 2024.

Telefónica has also implemented other mediation systems for queries and complaints. One of them is the **Queries Channel,** available on our website, where all interested parties can submit queries related to the Responsible Business Principles. . In 2024, 5 communications regarding privacy, 1 concerning privacy-BCRs, and 0 about freedom of expression were processed.

9 Management of our supply chain

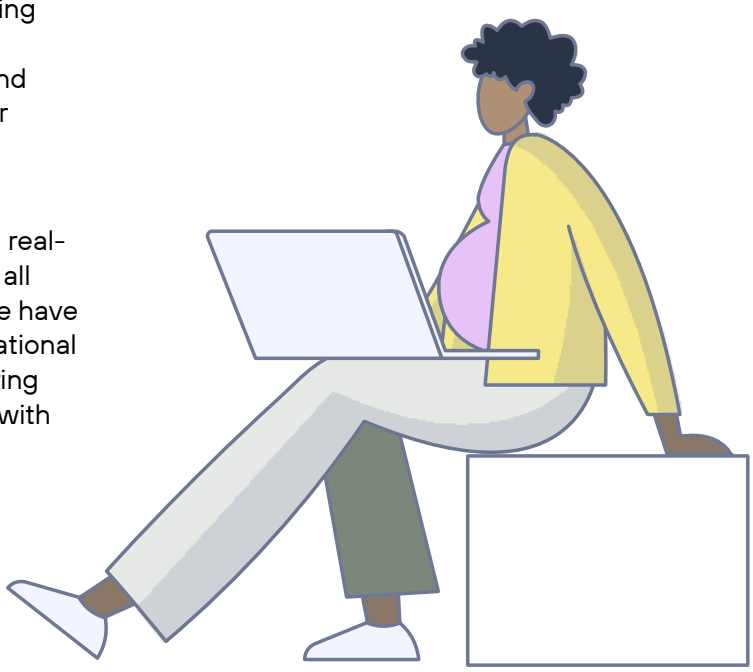
One of Telefónica's priorities in ensuring privacy is successful management of the supply chain in relation to the processing of personal data by third-party contractors. We have therefore incorporated data protection agreements across the whole Telefónica Group and included specific supplier commitments pertaining to international transfers.

Throughout 2024, we have continued to implement supplier monitoring procedures and have kept providing educational materials through tools created by the company. Specifically, we have maintained and enhanced automated control measures to ensure the proper processing of personal data before, during, and after the provision of services by the supplier. Additionally, to ensure the protection of personal data managed by third parties, we have developed automated mechanisms to optimize training initiatives, ensuring that our suppliers continue to comply with established data protection standards.

10 Digital Transformation

Digital transformation in privacy has been crucial in adapting our operations to the growing regulatory demands and enhancing data protection. As part of this process, we have developed an internal platform that centralizes all privacy compliance activities, from managing consents, tracking data breach incidents, managing internal Telefónica perimeter, and report KPIs related to privacy, among other functionalities.

This platform not only streamlines internal processes but also provides an integrated, real-time view of the compliance status across all areas of the organisation. With this tool, we have been able to automate tasks, reduce operational risks, and facilitate decision-making, ensuring more efficient protection and compliance with current regulations.



11 Training and awareness

At Telefónica, we recognise the importance of training and raising awareness about data protection and privacy, both for our employees and relevant third parties. To this end, we offer specific privacy courses covering our entire corporate footprint, complemented by training materials aimed at key suppliers from a privacy perspective. Specifically, we offer the following courses to our employees

- **Privacy awareness course:** This is an online training launched by the DPO Office. The first version was created in 2018 with the aim of training employees on the requirements of the European General Data Protection Regulation. It was reviewed, and in 2024 an updated version of the course was distributed, aiming to raise awareness of privacy concepts and how to apply them in daily functions. The update aims to provide employees with a more practical and tailored training, adapted to the internal procedures implemented to comply with the regulation's requirements.
- **Privacy principles and BCRs course:** This course aims to inform employees about privacy principles and explain what Binding Corporate Rules (BCRs) are. These rules enable the international transfer of personal data between Group companies and entail a series of obligations, as well as rights and guarantees for employees. The course has been developed in Spanish, English, Portuguese, and German, to be distributed across the entire Telefónica Group footprint, stemming from Telefónica's commitment to European authorities.
- **Global privacy policy course:** The course was reinforced, primarily in the HISPAM region, during 2023 and continued to be assigned to employees in 2024. It is also accessible to other employees in companies across Europe (except Germany) to raise awareness of Telefónica's commitment to privacy and data protection.

We deliver annually updated training on data protection and cybersecurity, expanding the scope of our formative contend to ensure alignment with the company's privacy policies and regulatory requirements.

In addition to training employees in privacy matters, we are committed to providing specialised training for our privacy experts. Our privacy-focused lawyers and teams undergo specific training programs and certifications to ensure they achieve the highest level of excellence and remain up-to-date with the latest developments in the field.

We have also introduced the 5Stars Awards to recognise and reward employees who demonstrate the highest level of awareness and commitment to privacy. These awards are designed to highlight individuals who consistently prioritise privacy in their daily work, setting an example for others and contributing to a culture of privacy excellence within the company.

This training effort reinforces our commitment to safeguarding data privacy by fostering a culture of responsibility and awareness across all levels of our organization.

Telefónica delivers training to employees of privacy and cybersecurity training, fostering a culture of data protection