Data Controller Binding Corporate Rules of the Telefonica Group

Online version

March 2023

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

DATA CONTROLLER BINDING CORPORATE RULES OF THE TELEFONICA GROUP

Table of Contents

Introduction 3
1. Scope 4
2. Key terms 4
3. Data Protection Safeguards 8
3.1. Transparency and fairness 9
3.2. Lawfulness of processing 10
3.3. Purpose limitation 11
3.4. Data minimization and accuracy 11
3.5. Limited storage periods 11
3.6. Special Categories of Personal Data 12
3.7. Children's Personal Data 12
3.8. Security 12
3.9. Restrictions on onward Transfers 14
3.10. Accountability 14
3.11. Data subjects' rights 15
4. Liability 17
4.1. Who can enforce the BCRs? 17
4.2. What entities are responsible within the Telefonica Group? 18
4.3. What are the rights of Third-Party Beneficiaries? 19
4.4. Who has the burden of proof? 19
5. BCRs complaint handling procedure 20
6. Updates, modifications, and termination of adherence to the BCRs 21
ANNEX on the List of Companies bound to the BCRs at the Initial Stage 22
ANNEX on the Categories of International Data Transfers (Data Controller) 27
ANNEX on the Management of Data Subjects rights Protocol 30
Which is the responsible corporate body? 30
How can Data Subjects rights be exercised? 30
What is the time frame for obtaining a response on a Data Subjects' rights request? 30
What if a request is rejected or if the Data Subject is dissatisfied with the response given? 31
Compliance record 31
ANNEX on the BCRs complaint handling procedure 32
Which is the corporate body in charge? 32
On what grounds can a complaint be filed? 32

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

How can a complaint be filed? 32
What is the time frame for obtaining a response on a complaint? 33
What if a complaint is admitted? 33
What if a complaint is declared inadmissible? 33
What if a complaint is rejected or if the Data Subject is dissatisfied with the response given? 34
Compliance record 34

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

Introduction

Telefonica Group is one of the world's leading telecommunications service providers with nearly 100 years of history, a presence in Spain in more than 80% of households and with more than 345 million accesses worldwide. We are mainly focused on Spain, the United Kingdom, Germany, and Latin America.

We are aware that connectivity is the main tool to access the current digital world, improve people's quality of life and generate wealth and in that regard, we believe networks account for the most powerful transformational platform. Our mission is to make our world more human connecting people's lives.

Considering the foregoing, one of the pillars of Telefonica's global strategy is the generation of trust in its end users by committing to the respect of privacy, security, and transparency. Therefore, we have implemented the present Binding Corporate Rules ("**BCRs**") in order to perform **International Data Transfers** among Telefonica's entities adhered to the BCRs (Telefonica, S.A. and each of its controlled undertakings, which are also bound by the BCRs in accordance with Annex on the List of Companies bound to the BCRs, **"Telefonica Group"** and each of the bound companies the "**Group Companies"**) and meet the highest data protection and privacy standards for **Data Subjects**.

These BCRs are adopted in accordance with the provisions of Regulation (UE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/CE (**"General Data Protection Regulation"** or **"GDPR"**). As such, they aim to establish appropriate safeguards that grant personal data being processed by the Telefonica Group (**"Personal Data"**) with a level of protection essentially equivalent to that granted by **European Data Protection Laws**, as required by **European Authorities**.

The BCRs apply to all Personal Data transferred by Group Companies located in the European Economic Area (**"EEA"**) that act as **Data Exporters** and as **Data Controllers** to Group Companies located out of the EEA that act as **Data Importers** and depending on the circumstances at hand act either as **Data Controllers** or as **Data Processors** of a Data Exporter. All Group Companies bound by the BCRs are listed on the Annex on the Categories of International Data Transfers.

The set of rules contained in the BCRs is binding for the Group Companies, listed in the Annex on the List of Companies bound to the BCRs, by the means of an Intra-group Agreement on the BCRs (**"Intra-group Agreement"**). By signing or adhering to the Intra-group Agreement, Group Companies undertake to respect and comply with all their provisions in all processing activities they are involved, directly or indirectly, and that fall into the scope of the BCRs.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

The BCRs are part of the Group's Global Privacy Policy. As such, the obligations they set forth by them and their mandatory nature have been informed to all individual parties under their scope, who have been granted access to them in advance. Specifically, they are binding on internal Data Processors used by Telefonica and on all employees of the Telefonica Group by virtue of the corresponding Data Processing Agreements (**"DPA"**), employment contracts, and the Group's internal policies, respectively.

In sum, the BCRs are aimed at establishing appropriate data protection safeguards that vest Personal Data processed by the Telefonica Group and transferred to countries out of the EEA with a level of protection essentially equivalent to that provided by European Data Protection Laws. They are of mandatory nature for all Group Companies, employees and individuals that work at them. In order to fulfil the purpose, standardized procedures and mechanisms are provided herein to guarantee uniformity in our Group's actions and to facilitate comprehension of the rules and their functioning for Data Subjects.

1. Scope

The BCRs will apply to all:

- Data Transfers from one Group Company to another, where both of them have fully adhered to the BCRs and are bound to them.
- Data Subjects whose personal data are transferred within the scope of the BCRs from an entity under the scope of application of Chapter V GDPR.

Onward transfers in the context of these BCRs will comply with the requirements set forth in section 3.9.

Further detail on the Group Companies within the scope of the BCRs and on their territorial scope of the BCRs is indicated in the corresponding Annexes to the BCRs.

2. Key terms

These Key terms must be understood as having the identical definitions provided for them in the GDPR. That said, some of the below definitions have been summarized or/and completed with examples for clarification purposes but in case of inconsistency, the definitions set out in Article 4 GDPR will prevail.

- **BCRs:** A transfer tool specifically provided in the General Data Protection Regulation and understood as an appropriate safeguard for the transfer of personal data out of the EEA. The BCRs have been approved by Data Protection Supervisory Authorities and are binding on all Group Companies of the Telefonica Group. Their goal is to set out a standardized internal framework that regulates the transfer of personal data to countries

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

out of the EEA while vesting personal data processed with a level of protection essentially equivalent to that ensured by the General Data Protection Regulation.

- **Data Controller:** The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Group Companies may act as data controllers when they decide on the purposes and means of the processing of personal data (e.g., when they process personal data from their employees for the performance and execution of an employment contract with them).

- **Data Exporter:** the natural or legal person bound by the BCRs that transfers personal data to a country out of the European Economic Area.

- **Data Importer:** the natural or legal person bound by the BCRs that acts as a recipient of personal data transferred from a country part of the European Economic Area.

- **Data Processor:** The natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

- **Data Subjects:** An identified or identifiable natural person to which the personal data being processed refer. For instance, Group Companies' employees may act as data subjects in the context of the processing activities of their personal data carried out by the Telefonica Group.

- **DPA:** A contract governing the processing of personal data by a Data Processor on behalf of a data controller. The drafting of such contract is mandatory under the General Data Protection Regulation. DPAs must be binding on both the data controller and the Data Processors, and set out the subject matter, duration, nature and purpose of the processing, the type of personal data, categories of data subjects and obligations of the data controller. In this regard, Group Companies have signed and executed DPAs with their internal or external providers in line with requirements set by the General Data Protection Regulation.

- **Due Diligence:** It accounts for an investigation, review or audit process aimed at verifying specific facts or details. Regarding data protection matters, this examination will be performed by Group Companies to check that service providers used as Data Processors provide sufficient guarantees and enable the enforcement and compliance with technical and organizational measures implemented by the Telefonica Group.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- **EEA:** It consists of the economic organization of states comprised by the Member States part of the European Union and the countries part of the European Free Trade Association.

- **EEA supervisory authority(ies):** Independent data protection authorities, established in the European Union's Member States or in one of the States that are party to the European Economic Area, who are in charge of monitoring compliance with the General Data Protection Regulation.

- **Competent Supervisory Authority:** EEA supervisory authority that, pursuant to applicable laws, results competent for the Data Exporter and for the Data Exporter's processing activities.

- **EEA competent courts:** The courts of the European Union's Member States that should be competent to rule on data protection infringements relating to complaints lodged by Data Subjects.

- **European Authorities:** These account for European Institutions generally considered (e.g., the European Commission, the European Parliament, the European Court of Justice, the European Council, etc).

- **European Data Protection Laws:** These should be understood as data protection regulations applicable in European Union's Member States, jointly considered with the General Data Protection Regulation.

- **General Data Protection Regulation (GDPR):** Accounts for the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).

- **Group Companies:** These account for all the companies within the Telefonica Group that are listed in the Annex on the List of Companies bound to the BCRs, and that are bound to the rules established by the BCRs.

- **International Data Transfer:** These account to transfers of personal data that are performed from the EEA to third countries that are not part of this organization.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- **Intra-group Agreement:** It refers to the corporate agreement that binds Group Companies to the BCRs, meaning that when signed, the companies must abide the rules set by the BCRs.

- **Local Privacy Leader:** It refers to the corporate body of the Telefonica Group in charge of monitoring compliance with data protection regulations and obligations locally (e.g., in a specific country in which the Telefonica Group operates).

- **Local Regulation:** It refers to any piece of legislation or regulations applicable within a specific territory covered in the geographic scope of these BCRs. Group Companies established in the territories covered in the geographic scope of these BCRs may be subject to several local regulations.

- **Network of DPO:** It refers to the group of Local Privacy Leaders (including the Global DPO) in charge of protecting the rights and freedoms of data subjects and with responsibility to monitor compliance with the BCRs.

- **Personal Data:** It refers to any information relating to a data subject, and particularly that allows for its identification either directly or indirectly. This can be done, for instance, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the data subject.

- **Personal Data Breach:** It refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

- **PIA:** It refers to a data protection impact assessment, which evaluates the risks that the processing poses for the fundamental rights and freedoms of data subjects. It is of mandatory conducting in certain circumstances provided in the GDPR.

- **Processing:** It should be understood as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- **Responsible Area:** It's the business area, according to the organizational structure of Telefónica, owner of the processing activity related to the relevant intragroup international transfer.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- **Responsible Business Communication Channel:** It's the communication channel put in place in the web site of Telefonica regarding consultation and complaints about any aspect related to Telefónica's Responsible Business Principles for example ethics, human rights, environment, privacy, health & safety, etc.

- **Requesting Authority:** A law enforcement or public authority from a country outside the EEA that requests a Telefonica Entity the disclosure of personal data.

- **Special Categories of Personal Data:** These refer to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- **Telefonica Group:** It should be understood as the Telefonica Group composed by Telefónica, S.A. and its subsidiaries bound to the BCRs.

- **Third Party Beneficiaries:** Natural and legal persons that benefit from the rights set forth in Section 4.3. of the BCRs.

3. Data Protection Safeguards

The Telefonica Group processes Personal Data only to the extent necessary to carry out its business with the highest quality standards. Group Companies are subject to data protection standards, rules and principles defined by European Data Protection Laws, which provide for a high level of protection of Personal Data. Consequently, in line with the Telefonica Group's privacy strategy aimed at generating trust in end users, we have established by virtue of these BCRs appropriate safeguards aimed at granting the Personal Data that fall within the scope of these BCRs with a level of protection essentially equivalent to that granted by European Data Protection Laws, as required by European Authorities.

The Telefonica Group first and foremost complies with applicable European Data Protection Laws, and ensures that the collection, storage, use, transfer, destruction, and all sort of Processing activities of Personal Data are carried out by the Group Companies in line with said laws. The present section describes the key principles of European Data Protection Laws that govern the Processing activities covered by these BCRs across the Telefonica Group. They are implemented not only by these BCRs, but also by the Group's Global Privacy Policy, as well as by procedures and techniques applied by us.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

3.1. Transparency and fairness

Personal Data will be processed lawfully, fairly and in a transparent manner in relation to the Data Subjects involved by Group Companies.

The Telefonica Group implements all necessary measures to guarantee that Data Subjects are provided with information that is easily accessible and understandable regarding their Personal Data being processed by Group Companies.

In this regard, our Global Privacy Policy as well as the privacy notices addressed to Data Subjects contain information on the following aspects:

- The identity and contact details of the Group Company acting as Data Controller, or the same information regarding its representative, where applicable.
- The contact details of the Global DPO and, where relevant, of the Local Privacy Leader.
- The purposes of the Processing of the Personal Data. In addition, where the Group Company intends to further process the Personal Data for a purpose other than that for which it was collected, it must provide the Data Subject with relevant information on that other purpose in advance.
- The legal basis for the Processing of the Personal Data, and the legitimate interests pursued by the Group Company or a third party when these serve as a legal basis for Processing.
- The categories of Personal Data concerned, where Personal Data is not obtained directly from the Data Subject.
- The recipients or categories of recipients of the Personal Data where applicable, and information on whether they are located within the EEA or out of the EEA.
- The source from which the Personal Data were obtained if it is not obtained directly from the Data Subject.
- The period for which the Personal Data will be stored, or the criteria used to determine such period.
- When the Personal Data is provided in order to enter into a contract or by a statutory or contractual requirement, the consequences of failure to provide such data.
- Information on Data Subjects' rights and the means to exercise them.
- The existence of automated decision-making, including profiling where applicable, as well as information on the logic involved and on the consequences of such kind of Processing.
- The right to lodge a complaint with the relevant EEA supervisory authority**.**
- The right to withdraw consent where consent serves as a legal basis for Processing.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

For the purpose of transparency, the main body of the BCRs, alongside Annexes on Management of Data Subjects rights Protocol and the BCRs complaint handling procedure, will be publicly available in Telefónica's Transparency Center for all categories of Data Subjects. To this end, the main body of the BCRs published at Telefónica's Transparency Center must include, at least:

- the description of the scope of the BCR-C;
- the Group's liability;
- the data protection principles;
- the lawfulness of the processing;
- security and personal data breach notifications;
- restrictions on onward transfers; and
- the rights of the data subjects.

In particular, employees may access the BCRs in the Group Companies' Intranet and will also be provided with them when carrying out the onboarding process. The Group Companies make employees aware of the consequences of non-compliance with the BCRs as they are part of the Global Privacy Policy. Likewise, Data Subjects benefitting from third party beneficiary rights will be able to access the BCRs online via Telefonica's website.

3.2. Lawfulness of processing

The Telefonica Group only processes Personal Data if it can rely on one of the legal bases set out by European Data Protection Laws.

Therefore, the Processing of Personal Data will only be carried out by any of the Group Companies, provided any of the circumstances below is satisfied:

- Data Subjects have given their consent for the Processing in a free and unambiguous manner for one or more specific purposes.
- The Processing of Personal Data is necessary for the performance of a contract to which the Data Subjects are party or in order to take steps at the request of the Data Subjects prior to entering into such contract.
- The Processing of Personal Data is necessary for compliance with a legal obligation to which a Group Company is subject.
- The Processing of Personal Data is carried out in order to perform a task in the public interest.
- The Processing of Personal Data is aimed at fulfilling the legitimate interests of any of the Group Companies. However, the Processing will not be carried out by Group Companies if the interests or fundamental rights and freedoms of Data Subjects override such legitimate interests.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- The Processing of Personal Data is necessary to protect the vital interests of Data Subjects or other natural persons.

Group Companies may also Process Personal Data where allowed by applicable Local Regulations from an EU Member State.

3.3. Purpose limitation

The Telefonica Group will only collect Personal Data for specific, explicit, and legitimate purposes in accordance with the legal bases provided in Section 3.2. Additionally, Personal Data will not be further processed by Group Companies in a way that is incompatible with the aforementioned purposes.

In order to guarantee compliance with the principle of purpose limitation, when considering whether Personal Data can be processed for a different purpose, the Group Companies will take into account the following aspects:

- Whether there is a connection between the original and the new purpose(s).
- Data Subjects' expectations regarding the processing of their Personal Data by the Telefonica Group.
- The nature of the Personal Data concerned, in particular whether special categories of personal data are processed, pursuant to Article 9 GDPR, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 GDPR.
- The consequences of the further Processing for Data Subjects.
- The safeguards implemented to protect Personal Data.

3.4. Data minimization and accuracy

Group Companies will only process Personal Data provided that it is adequate, relevant, and limited to what is necessary for the purposes of the Processing. The Telefonica Group's systems, equipment and procedures are designed to minimize the amount of Personal Data being processed.

Personal data will always be accurate and where necessary kept up to date. The Telefonica Group embeds the principle of accuracy into its internal policies by creating mechanisms for Data Subjects to communicate any changes in their Personal Data. As a result, any inaccurate Personal Data will be erased or rectified without undue delay.

3.5. Limited storage periods

Personal Data processed by the Telefonica Group will be stored in a form which permits identification of Data Subjects for no longer than what is necessary for the purposes for which they are being processed.

The Telefonica Group has implemented a data retention policy by virtue of its Conservation Domain that foresees the applicable legal retention periods in each Group Company's jurisdiction.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

Such retention periods have been established taking into account the purposes for which Personal Data are processed and the applicable statutory limitations. Retention periods will be recorded in the Record of Processing Activities.

3.6. Special Categories of Personal Data

Special Categories of Personal Data will only be processed by the Group Companies when they can rely on a legitimate legal basis in accordance with European Data Protection Laws and, additionally:

- When Data Subjects have given their explicit consent for the Processing for one or more specified purposes.
- When the Processing is necessary to protect the vital interests of Data Subjects or other natural persons whereby the Data Subjects are physically or legally incapable of giving their consent.
- When the Processing relates to Personal Data which have been manifestly made public by Data Subjects.
- When the Processing is necessary for carrying out obligations and exercising specific rights of the Group Company acting as Data Controller or of the Data Subjects in the field of employment and social security protection law and provided it is authorized by a law or a collective agreement.
- When the Processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity.

3.7. Children's Personal Data

Telefonica Group will not process children's Personal Data unless there is a legitimate reason and a legal basis that justifies such Processing.

The Telefonica Group expresses its commitment to the right to privacy of children, the protection of their Personal Data, and the promotion of the proper use of technology in accordance with applicable laws and regulations.

3.8. Security

The Telefonica Group is deeply committed to ensuring the security and confidentiality of Personal Data. Therefore, we only process Personal Data in a manner that ensures its appropriate security and protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage by using adequate technical and organizational measures. Whereby Personal Data cannot be processed in the aforementioned conditions by the Telefonica Group, the Telefonica Group will not process Personal Data.

Since the Telefonica Group deals with the operation of telecommunication networks, which are regarded as strategic infrastructures, we dedicate significant resources to the design of technical and organizational measures aimed at enhancing the security of Personal Data that flow through

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

such networks and between the Group Companies. Technical and organizational measures implemented are designed to ensure a level of security appropriate to the risk, having regard of the state of the art and the costs of implementation, nature, scope, context, and purposes of the Processing, as well as the risk of varying the likelihood and severity for the rights and freedoms of Data Subjects.

In view of the foregoing, Personal Data processed by Group Companies is always vested with a level of protection essentially equivalent to that granted by European Data Protection Laws, and in order to pursue such high privacy standards we:

- Pseudonymize or encrypt Personal Data where necessary.
- Install security controls in every equipment and system dealing with the Processing of Personal Data (e.g. access controls, transmission controls, memory controls, etc.).
- Make sure that in the event of physical or technical incident the access and availability to Personal Data by users is restored.
- Make sure our employees processing Personal Data are aware of the rules set out in these BCRs and of the security protocols installed, by the respective trainings plans and notices. Disciplinary sanctions will be applied for non-compliance with the rules and protocols mentioned.
- Evaluate and test the effectiveness of the technical and organizational measures implemented so as to improve or modify them appropriately.

When a **Personal Data Breach** takes place affecting the Personal Data covered by these BCRs, Group Companies will notify, without undue delay, Telefonica, S.A. and the Global DPO and competent Local Privacy Leader, if relevant. In addition, Competent Supervisory Authorities will be informed no later than 72 hours after the Group Company or Group Companies become aware of the Personal Data Breach. Where the Competent Supervisory Authorities are not notified within the aforementioned time frame, the delay will be justified accordingly. Data Subjects will be notified without undue delay of Personal Data Breaches that are likely to result in a high risk to their own rights and freedoms.

Personal Data Breaches will be managed in accordance with Incident management internal rules and data breach internal protocols, and facts, effects and remedial action taken in view of the Personal Data Breach will be documented. The corresponding documentation referring to these aspects will be put at the disposal of the Competent Supervisory Authorities upon their request.

When acting as Data Controller, the Telefonica Group contractually ensures that any provider acting under its authority and having access to Personal Data of Data Subjects can only process such data according to its instructions and, in any case, in a secure manner by adopting the necessary technical and organizational security measures and in full compliance with the applicable European Data Protection Laws and internal rules and procedures. Each agreement entered into by the Telefonica Group and its providers sets out the obligations foreseen in Article

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

28 GDPR and, in particular, the duty to notify without undue delay any Personal Data Breaches to the Telefonica entity acting as the signatory party, where the Personal Data Breach is likely to result in a high risk to their rights and freedoms. The Group Companies have internally implemented an appropriate protocol so that Telefonica SA becomes aware of the Personal Data Breach suffered by any supplier that provides services to them.

3.9. Restrictions on onward Transfers

The Telefonica Group will only perform onward International Data Transfers to third parties when these third parties acting as Personal Data recipients and located in a country out of the EEA are part of the Telefonica Group, have fully adhered to these BCRs and are capable of complying adequately with the principles and rules set herein.

When the Personal Data recipients are not bound by these BCRs the Telefonica Group will only perform data onward Transfers if:

- It has entered into written agreements with the Personal Data recipients that meet the requirements set forth in Article 28.3 GDPR provided they act as Data Processors prior to the onward Transfer taking place and,
- The European Commission has decided by an Adequacy Decision that the country out of the EEA, a territory, or one or more specified sectors within that country in question ensure an adequate level of protection or,
- Other appropriate safeguards are provided by the onward transfer recipients (e.g. Standard Data Protection Clauses adopted by the European Commission), and to the extent that such safeguards ensure enforceable rights and effective legal remedies afforded to Data Subjects or,
- The Transfer satisfies a condition specified as a derogation permitted by European Data Protection Laws.

By contrast, when an onward transfer recipient cannot ensure a level of protection substantially equivalent to that granted by European Data Protection Laws additional technical, contractual, and organizational measures will be put in place. If even when such measures are implemented the Processing does not adjust to European Data Protection Laws and standards, the Processing will not be carried out.

3.10. Accountability

The Group Companies acting as controller shall be responsible for and able to demonstrate compliance with the BCRs.

Group Companies embed the principles of privacy by design and by default in the development of their products and services so that, from its initial conception, such products and services incorporate the applicable Data Protection requirements. Both principles are key for achieving full compliance with the BCRs.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

In that respect, the Telefonica Group shall assume certain commitments regarding: (i) Data Protection Impact Assessment; (ii) agreements with third parties, and (iii) keeping register of processing activities.

3.11. Data subjects' rights

The Telefonica Group duly attends Data Subjects' requests to exercise their rights under EU Data Protection Laws.

When a Group Company acts as a Data Controller, we ensure that the Data subject can exercise its right to:

- **Information:** by being informed from the Data Controller about the collection, use and processing of its personal data, if obtained directly from the Data subject or from a Third-party, in accordance with the provisions of GDPR.
- **Access**: by obtaining from the Data Controller confirmation as to whether or not Personal Data concerning it are being processed, and where that is the case, access copies of such Personal Data.
- **Rectification**: by obtaining from the Data Controller the rectification of inaccurate Personal Data concerning it without undue delay. In this regard, Personal Data may be completed accordingly by the Data Subject by a supplementary statement.
- **Object:** to the processing of its Personal Data at any time on compelling legitimate grounds relating to its particular situation. The Data Controller will only carry out the Processing if it demonstrates compelling legitimate grounds which override the interests, rights, and freedoms of the Data Subject.
- **Erasure:** by obtaining from the Data Controller the erasure of its Personal Data without undue delay if one of the grounds provided in Article 17 (1) of the GDPR applies:

    a) The Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    b) The Data Subject withdraws consent on which the processing is based;

    c) Where there is no other legal ground for the processing;

    d) The Data Subject objects to the processing;

    e) The Personal Data have been unlawfully processed;

    f) The Personal Data must be erased for compliance with a legal obligation in Union or Member State law to which the Data Controller is subject;

    g) The Personal Data have been collected in relation to the offer of information society services.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

The Data Controller will only reject the Data Subject's request if any of the grounds provided in Article 17 (3) of the GDPR applies (e.g., for the establishment, exercise, or defence of legal claims).

- **Restrict processing**: by obtaining from the Data Controller restriction of Processing when one of the following grounds applies, in line with Article 18 (1) of the GDPR:
    - Where the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
    - Where the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
    - Where the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims.
    - Where the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

  Under such circumstances, Personal Data will only be processed, apart from storage, with the Data Subject's consent or for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of public interest.
- **Not to be subject to a decision based solely on automated processing, including profiling**, which produces legal effects concerning the Data Subject or that similarly and significantly affects it, unless permitted under the following circumstances, in line with Article 22 (2) of the GDPR:
    - Where such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller;
    - Where such decision is authorized by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
    - Where such decision is based on the data subject’s explicit consent.
- **Withdraw consent:** at any time in an easily done manner.

In any case, the Data Controller shall communicate any rectification, erasure or restriction of processing to each recipient (every entity to which the personal data have been transferred to), to whom the personal data concerning the Data Subject have been disclosed. The Data Controller shall also inform the Data Subject about those recipients, upon request.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

The Telefonica Group provides Data Subjects with clear and simple tools and procedures to guarantee and ensure the correct exercise of their rights according to the applicable European Data Protection Laws.

Group Companies facilitate the exercise of these rights within a one-month time frame, which can be extended to two further months and undertake to respond to requests, queries, and complaints as rapidly as possible within such periods. Data Subjects may exercise their rights at any time by contacting the Responsible Business Communication Channel at www.telefonica.com (subject matter Binding Corporate Rules of the Telefonica Group - BCRs).

Requests must comply with the following formal requirements:

- National identity card for confirming the Data Subject's identity, or any other mechanism providing similar identity assurance, where there are reasonable doubts concerning the Data Subject's identity.
- If applicable, the representation accreditation of the legal representative of the Data Subject.
- Indication of the specific right that the data subject wants seeks to exercise.

Once a request for the exercise of a Data Subjects' right is registered, the **Responsible Area** for the enforcement of the request will take appropriate actions to handle the request.

A response to the request will be given within a one-month time frame, which can be extended to two further months in view of the complexity and number of complaints the competent Responsible Area is managing at the time. When the time frame for responding to the request is extended, the Data Subject will be informed accordingly on such extension and on the specific reasons that justify it within the initial term of one month.

Data Subject will also be entitled to either lodge a complaint with the relevant EEA supervisory authorities or to file a claim before the competent EEA courts. These rights shall be exercised in accordance with Section 4.1.

Data Subjects requests may be rejected when they reiterate other previous and responded requests already filed by the same Data Subject in relation to the same facts.

Further information on how the Telefonica Group handles requests, queries and complaints related to the exercise of Data Subjects rights can be found in the Annex on the Management of Data Subjects rights Protocol.

4. Liability

4.1. Who can enforce the BCRs?

The BCRs are enforceable by

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- Group Companies in accordance with the Intra-group Agreement and the Telefonica Group's Global Privacy Policy;
- Employees of the Telefonica Group in accordance with their employment contract and the Telefonica Group's Global Privacy Policy.
- Providers in accordance with their respective contracts and the Telefonica Group's Global Privacy Policy;
- **Third Party Beneficiaries** in accordance with the terms set forth in Section 4.3.

against:

- Group Companies;
- Other parties bound by the BCRs.

Furthermore, Data Subjects are entitled to:

- Lodge a complaint with the relevant EEA supervisory authority of their choice between that of the Member State where they have their habitual residence or place of work, or that relating to where the alleged infringement of the BCRs has taken place**.**
- File a claim before the EEA competent court of their choice between that of the Member State where there is an establishment of the Telefonica Group or that relating to where they have their habitual residence (**EEA competent courts).**

Data subjects shall be entitled to be represented by a non-profit body organization or association which has been properly constituted in accordance with the law of a European Union Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of Data subjects' rights and freedoms with regard to the protection of their personal data. These organisms shall lodge complaints on the Data subjects' behalf to exercise the rights recognized in these BCRs and any other right whose Data subject applicable law may confer.

4.2. What entities are responsible within the Telefonica Group?

Both Data Exporter and Data Importer are jointly liable for any infringement of the BCRs with regards to a particular Data Transfer. However, either Data Exporter or Data Importer may be exempt from this liability if it provides sufficient evidence of the lack of responsibility for the event that caused the infringement.

Notwithstanding the above, Telefonica, S.A., as parent company of the Telefonica Group, accepts liability for any breaches of the BCRs by any Group Company not established in the EEA and agrees to:

- Take all necessary actions to remedy for the acts of the breaching Group Company.
- Pay the corresponding compensation for any material or non-material damages resulting from the breach of the Group Company.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

Telefonica, S.A, will only be exempted from the above obligations if it is proved that the Group Company is not responsible for the event giving rise to the damage.

Telefonica, S.A. shall accept the jurisdiction of the competent courts or Competent Supervisory Authorities in the EEA, as well as responsibility for violations of the BCRs and for remedies resulting from the exercise of rights by Data Subjects as if the violation had been caused by it in the Member State in which it is based.

For the purposes of the obligations provided, Telefonica, S.A. has accepted liability for the acts of the Group Companies and has adopted the appropriate measures to assume such liability.

Telefonica, S.A., the Data Exporter or the Data Importer have the right to redress to any of the parties involved in the relevant Data Transfer any damage arising from a faulty, willful or negligent infringement of the BCRs.

4.3. What are the rights of Third-Party Beneficiaries?

Third Parties may enforce the BCRs in order to fulfill:

- The principles set forth in Section 3.
- Any of the rights set forth in Section 3.11 and in Annex on the Management of Data Subjects' rights Protocol.
- Their transparency and easy access right to the BCRs in accordance with Section 3.1.
- Mechanisms provided in Section 9.1 for addressing conflicts of laws.
- The right to lodge a complaint through the internal complaint procedure set forth in Annex on the BCRs complaint handling procedure.
- The duty to cooperate with Competent Supervisory Authorities in accordance with Section 9.
- The rights to lodge a complaint with the relevant EEA supervisory authorities and to file a claim before the EEA competent court in accordance with Section 4.1.

Failure to comply with the above points will be subject to provisions set out in Section 4.2.

4.4. Who has the burden of proof?

Where individuals lodge a complaint alleging a violation of these BCRs that resulted in damages, and they can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the violation, the relevant Group Company, including Telefonica SA, will be responsible for proving that it is not liable for such violation or that no violation occurred.

In the event that the relevant Group Company succeeds at proving that the Group Company is not liable for the event causing the violation of the BCRs, it may discharge itself from any liability.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

5. BCRs complaint handling procedure

Data Subjects whose Personal Data are being processed by a Group Company are entitled to file a complaint against the Group Company or Companies in question in accordance with the Annex on the BCRs complaint handling procedure.

Data Subjects may file a complaint before the Global DPO or the Responsible Area for non-compliance with the BCRs against a Group Company when they believe such Group Company has not complied with the rules embedded in these BCRs and they can allege dissatisfaction in that regard.

Data Subjects may file a complaint for infringements of the BCRs within the statutory periods provided by applicable administrative and civil regulations. Such complaints will be subject to the relevant statutes of limitation, as set forth by applicable law to Data Subjects.

Complaints for infringements of the BCRs may be filed in writing by contacting the Responsible Business Communication Channel at www.telefonica.com (subject matter: *Binding Corporate Rules of the Telefonica Group - BCRs*). Other data protection complaints unrelated to the BCRs shall follow the channels and contact points already dedicated to this purpose by each Telefonica Entity.

Complaints must comply with the following formal aspects:

- Name, surname(s), and address of the Data Subject and, if applicable, of the duly accredited representative, national identity card or passport number, where applicable.
- Grounds of the complaint, with clear specification of the issues on which a response is requested.
- Group Company(ies), department or service where the facts giving rise to the complaint have taken place.
- The documentary evidence in its possession on which the complaint is based.

A respond to the complaint will be given within a one-month time frame, which can be extended to two further months in view of the complexity and number of complaints the competent Responsible Area is managing at the time. When the time frame for responding to the complaint is extended, the Data Subject will be informed accordingly on such extension and on the specific reasons that justify it. Additionally, the Data Subject will be informed on the approximate timing for obtaining a response.

Data Subject will also be entitled to either lodge a complaint with the relevant EEA supervisory authorities or to file a claim before the competent EEA courts. These rights shall be exercised in accordance with Section 4.1.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

6. Updates, modifications, and termination of adherence to the BCRs

These BCRs will be updated in order to reflect modifications in our regulatory framework, changes in the Telefonica Group structure or changes in our data protection and privacy practices.

When such modifications are introduced in the BCRs or Annexes, we commit to duly report them without undue delay to all Group Companies and to their employees, as well as to the Competent Supervisory Authorities upon its request, via the Lead Supervisory Authority. For this purpose, the Global DPO shall keep record of any updates in the BCRs, including the BCRs Member List. Additionally, Global DPO will make this information available for Data Subjects following the same transparency principles than those granted to the BCRs.

Updates to the BCRs or to the list of Group Companies will be made without having to reapply for an approval of a Supervisory Authority provided that:

- The network of DPOs keeps a fully updated list of the Group Companies and keeps track of and record any updates to the rules and provides the necessary information to the Data Subjects or Competent Supervisory Authorities upon request.
- No transfer is made to a newly adhered Telefonica Entity until it is effectively bound by the BCRs and can deliver compliance.
- Any changes to the BCRs and to the list of the Group Companies is reported once a year to the relevant Supervisory Authorities, via the Lead Supervisory Authority with a brief explanation of the reasons justifying the update.

Nonetheless, where a modification could potentially be detrimental to the level of protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character), it shall be previously communicated to the relevant Supervisory Authorities, via the Lead Supervisory Authority with a brief explanation of the reasons for this update. In this case, the Lead Supervisory Authority will also assess whether the changes made require a new approval.

A Group Company or any other third party bound by the BCRs that ceases to be bound to them may keep, return, or delete the Personal Data.

If the Data Exporter and the Data Importer agree that the Personal Data may be kept by the Data Importer, protection must be maintained in accordance with Articles 45 or 46 of the GDPR unless one of the derogations pursuant to Article 49 GDPR applies. However, if the Data Exporter and the Data Importer do not agree on the Data Importer keeping of the Personal Data, the Data Importer must delete or return the Personal Data and their copies at the choice of the Data Exporter.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

ANNEX on the
List of Companies bound to the BCRs at the Initial Stage

Exporters			
Country	**Group Company**	**VAT**	**Contact information**
Germany	Telefónica Germany Gmbh & Co. OHG	DE 811 889 638	Georg-Brauchle-Ring 50, 80992 München, Germany
	Telefónica Global Services Gmbh	DE 221 033 439	Adalperostraße 82-86, 85737 Ismaning, Germany
	Telefónica Global Roaming Gmbh	DE268569923	
	Telefonica Cybersecurity and Cloud Tech Deutschland Gmbh	DE347731744	
	Telefónica Global Solutions Germany Gmbh,	143/317/21426	Adalperostr 82-86, 85737, Isamaning, Múnich
Spain	Telefónica Iot & Big Data Tech S.A.	A78967577	Ronda de la Comunicacion (ed Oeste 1, 2º), S/N, Madrid, 28050, Madrid.
	Telefónica Tech S.L.	B78529724	
	Telefónica Cybersecurity & Cloud Tech S.L.	B-01636760	
	Telefónica Finanzas S.A.	A28639169	
	Telefónica Servicios Audiovisuales S.A.U.	A80568645	
	Telefónica de España, S.A.U.	A82018474	
	Telefónica, S.A.	A28015865	
	Telefónica Educación Digital S.L.U.	B82857053	
	Telefónica Global Solutions S.L.U.	B85627792	
	Telxius Telecom, S.A.	A86565926	

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	Telefónica Hispanoamérica S.A.	A86854684	
	Telxius Cable España, S.L.	B87449922	
	Teleinformática y Comunicaciones, S.A.	A78050481	Calle Marroquina, 43 - 1, Madrid, 28030, Madrid
	Telefónica Innovación Digital, S.L.	B83188953	
	Telefónica Compras Electrónicas S.L.U.	B85284594	
	Telefónica Gestión Integral de Edificios y Servicios S.L.U.	B86471802	
	Telefónica Soluciones de Informática y Comunicaciones de España, S.A.	A78053147	Ronda de la Comunicacion (ed Norte 2), S/N, Madrid, 28050, Madrid
	Telefónica Móviles España, S.A.U.	A78923125	Ronda de la Comunicación s/n, Distrito C, Edificio Sur 3, 2ª planta, (28050 Madrid)
	Telefónica Correduría de seguros y reaseguros compañía de mediación, S.A.	A80157795	Ronda de la Comunicación, S/N 28001 Madrid.
	Fonditel Pensiones, entidad gestora de fondos de pensiones, S.A.	A80416332	C. de Pedro Teixeira, 8, 28020 Madrid
	Fonditel Gestión, sociedad gestora de instituciones de inversión colectiva, S.A.	A83632638	
	Telefónica Servicios Integrales De Distribución, S.A.U.	A82261280	C. de Melchor Fernández Almagro, 105, 3, 28029 Madrid
	Telefónica Global Technology, S.A.	A82261231	C/ Gran Vía 28, 20813 – Madrid
	Telefónica Seguros Y Reaseguros Compañía Aseguradora, S.A U.	A05362645	Ronda de la Comunicación, S/N 28001 Madrid.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	Acens Technologies S.L.U.	B84948736	C. de San Rafael, 14, 28108 Alcobendas, Madrid.
	Telefónica Audiovisual Digital S.L.U.	B87613816	Avenida de los Artesanos, 6, tres Cantos, 28760, Madrid
	Telefónica Ingeniería De Seguridad S.A.	211406340011	C. de Ramón Gómez de la Serna, 109, Bajo Posterior, 28035 Madrid.
France	Telefonica Global Solutions France Ii, S.A.S.,	508 009 982 R.C.S. Nanterre	Tour First 1 Place des saisons Paris La Défense 1, 92400, Courbevoie Francia,
Holland	Telfisa Global BV	8174.04.612	Zuidplein 112, 1077 XV Amsterdam, Países Bajos.
Luxembourg	Nova Casiopea RE S.A.	B158616	23 Av. Monterey, 2163 Luxembourg, Luxemburgo

Importers			
Country	**Group Company**	**VAT**	**Contact information**
Argentina	Telefónica Global Solutions Argentina, S.A.,	AC.U.I.T 30-71516462-7	Avenida Independencia n.º 169, Planta Baja CP 1099, Buenos Aires Argentina
Brazil	Telefônica Brasil, S.A.	02.558.157/0001-62	Av. Engenheiro Luis Carlos Berrini 1376, 32.º andar, São Paulo, São Paulo, 04571-936, São Paulo
	T. On The Spot Soluçoes Digitais do Brasil Ltda	03865842000-02	Avenida Doutor Chucri Zaidan, 2460. Andar: 4; Lado B; Vila Sao Francisco (Zona Sul) Sao Paulo - Sp 04711-130
	Telefónica Corretora de Seguros Limitada	04.772.577/0001-72	Telefônica Corretora de Seguros Ltda, na Rua Geraldo Flausino Gomes, n.º 61, conjunto 12, Bairro Brooklin Novo, CEP. 04575-902, Cidade de São Paulo, Estado de São Paulo
	Telefônica Cibersegurança e Tecnología do Brasil Ltda	19.290.938/0001-11	Av Marcos Penteado de Ulhoa Rodrigues, 1690, 06543-001, Tambore, Santana de Parnaiba.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	Telefónica Cloud e Tecnologia do Brasil S.A.	35.473.014/0001-07	
	Terra Networks Brasil S.A.	91.088.328/0001-67	Avenida Engenheiro Luís Carlos Berrini, 1376, conjunto 131, Cidade Monções, São Paulo - SP, 04571-936
	Telefônica Infraestrutura e Segurança Ltda	03.441.668/0001-62	Rua Haddock Lobo, 337, 2.º andar, Cj. 21 e 7.º andar, Conjunto 71, Bairro Cerqueira Cesar, CEP 01414-001
	Telefónica Global Solutions Brasil Ltda,	14.314.117/0001-54	Avenida Doutor Chucri Zaidan n.º 1240, 13.º andar, sala 1.304, CEP 04711-130, São Paulo, São Paulo Brasil,
Chile	Telefónica Global Solutions Chile, S.P.A.	RUT:76540944-6	General Bustamante, 10 (piso 5), 7500000, Santiago, Comuna de Providencia. Chile
Colombia	Telefónica Global Solutions Colombia, S.A.S	NIF: 900940386-5	Calle 108 N.º 45 - 30 To 2 of 1601, 1014, Bogotá D.C. Colombia
Ecuador	Telefónica Global Solutions Ecuador Tgse S.A.	RUC: 1792646766001	Avenida Simón Bolívar 4. Centro Corporativo Ekopark. Torre 4. Oficina 2, 170124, Quito, Pichincha Ecuador,
Mexico	Pegaso PCS S.A. de C.V.	PPC980624U16	Prolongación Paseo de la Reforma 1200, Colonia Cruz Manca Cuajimalpa De Morelos, Ciudad De México, Código Postal 05349.
	Telefónica Global Solutions México, S.A. de C.V.,	RFC: BCR040422I1A	
Peru	Telefónica Global Solutions Perú S.A.C.	20601013011	Avenida La Paz N.º 1049, Miraflores, 15074, Lima, Miraflores Perú
United Kingdom	Telefónica Digital Limited	1707821788	Highdown House, Yeoman Way, Worthing, West Sussex, Reino Unido, BN99 3HH.
	Telefónica Tech UK & Ireland Limited	11243168	East House, Newpound Common, Wisborough Green, West Sussex, RH14 0AZ.
United States of America	Telefónica Global Solutions Usa, Inc.	52-2215332	Waterford Way Suite 300, 33126, Florida, Miami EE.UU.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	Telefónica Tech Inc.	85-3009229	800 Waterford Way Ste 300 Miami, FL, 33126 Estados Unidos.
Venezuela	T. Venezolana C.A.	J003439940	Avenida Francisco de Miranda, Caracas 1062, Miranda, Venezuela.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

ANNEX on the
Categories of International Data Transfers (Data Controller)

Categories of Data Subjects	**People** • Employees including Managers • Board Members and Directors • Candidates • Students and collaborators taking part in Projects concerning Telefonica. **Legal & Compliance** • Legal representatives • Contractors / Vendors • Individuals who reach out to the DPO inbox to submit a privacy request. **Operations / Marketing** • End users of Telefonica services • Clients **Security** • Visitors • Security Managers • Individuals affected by a potential cyber-incident. **Finance** • Investors, brokers, stakeholders.
Categories Personal Data transferred, and processing activities related	**People** • Employee's personal data: identity data (first and last name, ID); gender information; corporate email address, position within the organization, date of birth, CV / professional profile at Telefonica, including picture; position and role within Telefonica's organizational chart; performance data; information related to the employee's trajectory / seniority at Telefonica; qualification and training; payment related data, incl. bank account, credit card details, transactional details; identity data related to persons within the relevant facility, CCTV images which may feature persons within the relevant facility; country of origin, visited country. • Candidates' personal data: Personal identification data relating to candidates, including curricular and job position data. • Students and collaborators' personal data: Identification data (e.g., first and last name) and contact details. **Legal & Compliance** • Senior Managers and Board Members' personal data: Identification data (first and last name) and relatives' personal data position; within the organization. • Legal representatives' personal data: Identification data (name, surname, address for notification purposes, National Identification Number) scope of powers of representation. • Personal data processed in the context of the whistleblowing hotline: Identity data related to the claimant and potentially to the affected individuals; personal data contained in the business ethics claim, open text entry; in global-scope claims, an action plan may also be shared. • Personal data processed in the context of the DPO hotline: Identification data relating to data subjects who individually wish to exercise data protection rights or submit a privacy request; information around the privacy request in question;

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	identification data relating to individuals affected by a potential cyber-incident. **Operations / Marketing** • End users' personal data: CDRs, including incoming calls, outgoing calls, IMSI, TAPs, including inbound calls, outbound calls, IMSI; roaming related data; network information; users ID; IMSI and MSISDM of the devices related to the provision of IoT services; Personal data related to users of digital platforms and databases and personal data stored by users of cloud services in Telefonica systems. • Clients, Vendors and Contractors' personal data: identity data (first and last name, ID number); contact details; professional data, including employer and job position, payment related data, incl. bank account, credit card details, transactional details; financial risk and compliance related information. **Security** • Visitors' personal data: Identity data related to persons within the relevant facility, CCTV images which may feature persons within the relevant facility. • Individuals affected by a potential cyber-incident personal data: Data related to cybersecurity incidents and/or threads (e.g., IP addresses, usernames, passwords, etc.) **Finance** • Investors, brokers, stakeholders' personal data: Identification data (first and last name).
Purposes of processing as data controller	**People** • Administrative and organizational purposes, including HHRR management. • Recruiting services • Employee loyalty and wellbeing purposes. • Talent and HR Mobility initiatives • Training and awareness in global matters **Legal & Compliance** • Powers of attorney management to comply with legal obligations • Management of global (within the Group) providers repository: coordination and control purposes with respect to service providers contracting within the Group. • Ensuring compliance with Telefonica Responsible Business Code of Conduct and applicable legislation, including coordination, implementation and standardisation of compliance practices within the Group. • Monitoring of business ethics-related indicators within the Telefonica Group and drafting of non-financial information report. • Meet privacy requests of individuals around the Group, including for the exercise of their data protection rights as foreseen in Data subjects' applicable laws . **Operations** • Business operation and commercial contact. • Roaming services management • Provision of global supporting services. • Provision of IoT services. • Organization of the participation of start-up and small companies in innovation projects. • Provision of app development and operation services.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

	• Management of the incidents arising from the materials and products provided by third parties. **Finance** • Roaming services billing • Consolidation and service billing purposes • Internal communication and employee loyalty purposes. • Storage and processing payments and other financial transactions. **Security** • Security of Telefonica IT systems, Telefonica facilities and personnel. • Provision of cybersecurity services **Marketing** • Organization and arrangement of on-site events in different countries. • Encourage investment movements and enhance Telefonica's growth around the world. • Business development & commercial contact.

Categories of recipients of Personal Data	Group Companies located outside EEA

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

ANNEX on the

Management of Data Subjects rights Protocol

Data Subjects may request the Telefonica Group to exercise the rights that they are vested in accordance with European Data Protection Laws (see Section 3.11) by following the indications set out in the present protocol.

Which is the responsible corporate body?

The Global DPO is the responsible corporate body within the Telefonica Group for the Management of Data Subjects rights protocol.

That said, the corresponding Privacy Responsible Areas within each Group Company are responsible for the enforcement of the provisions of the present protocol.

How can Data Subjects rights be exercised?

Data Subjects may exercise their rights at any time by contacting (i) the dedicated email address "bcr.dpo@telefonica.com"; and/or (ii) the Responsible Business Communication Channel available at www.telefonica.com (subject matter Binding Corporate Rules of the Telefonica Group - BCRs).

Requests for the exercise of Data Subjects rights will be processed by the Global DPO and assigned to each Privacy Responsible Area accordingly for its further processing and enforcement.

Requests must comply with the following formal requirements:

- National identity card for confirming the Data Subject's identity or any other mechanism providing similar identity assurance where there are reasonable doubts concerning the Data Subject's identity.
- If applicable, the representation accreditation of the legal representative of the Data Subject.

The above formal requirements will be assessed by the Responsible Area in charge of enforcing the right that is exercised.

When the Privacy Responsible Area appreciates the absence of any of the formal requirements, it will communicate it to the Data Subject with the purpose of requesting the correction of the same. By contrast, when the Privacy Responsible Area appreciates the aforementioned formal requirements, it will proceed to register the request.

What is the time frame for obtaining a response on a Data Subjects' rights request?

Once a request for the exercise of a Data Subjects' right is registered, an area specifically in charge of its enforcement will be assigned (Execution Area). The Execution Area will take appropriate actions to carry out such enforcement (e.g. the modification of incomplete or

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

inaccurate Personal Data indicated in the request for the exercise of the right to rectification). Such actions will be adequately registered by the Privacy Responsible Area.

In addition, when Data Processors are required to cooperate in the enforcement of the corresponding Data Subjects' right, the responsible Group Company will forward the Data Subject's request to them.

A response to the request will be given within a one-month time frame, which can be extended to two further months in view of the complexity and number of complaints the competent Privacy Responsible Area is managing at the time. When the time frame for responding to the request is extended, the Data Subject will be informed accordingly on such extension and on the specific reasons that justify it within the term of one month.

The response will be notified to the Data Subject in writing or by electronic means, provided that these allow for the reading, printing and conservation of the same as expressly designated by the Data Subject and, in the absence of such indication, through the same means in which the request was filed.

Once the Data Subject has been notified, the date of the response and the means used will be registered in the management system.

What if a request is rejected or if the Data Subject is dissatisfied with the response given?

If a Data Subject does not agree with the rejection of its request as stated in the response received in the established time frame, or if it wishes to challenge the response given, it will be entitled to either lodge a complaint with the relevant EEA supervisory authorities or to file a claim before the competent EEA courts. These rights shall be exercised in accordance with Section 4.1.

Data Subjects requests may be rejected when they reiterate other previous and responded requests already filed by the same Data Subject in relation to the same facts.

Compliance record

The Global DPO will keep a record of all requests filed by Data Subjects and of the result of their enforcement and response.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

ANNEX on the
BCRs complaint handling procedure

Which is the corporate body in charge?

The Global DPO is the corporate body within the Telefonica Group in charge of the management of complaints for non-compliance with the BCRs procedure.

On what grounds can a complaint be filed?

Data Subjects may file a complaint before the Global DPO or the Responsible Area for non-compliance with the BCRs against a Group Company when they believe such Group Company has not complied with the rules embedded in these BCRs and they can allege dissatisfaction in that regard.

How can a complaint be filed?

Data Subjects may file a complaint, within the statutory periods provided by applicable administrative and civil regulations, for infringements of the BCRs. The complaint or request may be made against the Group Company they believe is in breach or, where the breach is likely to result from an act of a Group Company outside the EEA, the Data Subject is entitled to lodge the complaint or file a request directly to Telefonica S.A., Spain.

Complaints for infringements of the BCRs may be filed in writing by contacting (i) the dedicated email address “bcr.dpo@telefonica.com”; and/or (ii) the Responsible Business Communication Channel available at www.telefonica.com (subject matter Binding Corporate Rules of the Telefonica Group - BCRs). Other data protection complies unrelated to the BCRs shall follow the channels and contact points already dedicated to this purpose by each Telefonica Entity. Telefonica Entities shall collaborate with each other in managing the BCRs-related complaints when received through a channel other than the dedicated email address or the Responsible Business Communication Channel and provide the data subject with enough information in this regard.

Complaints must comply with the following formal aspects:

- Name, surname(s) and address of the Data Subject and, if applicable, of the duly accredited representative, national identity card or passport number, where there are reasonable doubts concerning the Data Subject's identity
- Grounds of the complaint, with clear specification of the issues on which a response is requested.
- Group Company(ies), department or service where the facts giving rise to the complaint have taken place.
- The documentary evidence in its possession on which the complaint is based.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

If the identity of the Data Subject cannot be sufficiently accredited, or if the facts giving rise to the complaint cannot be clearly established, the Data Subject may be requested to complete the documentation sent within ten calendar days. If the documentation is not completed as stated, the complaint procedure will be terminated and filed.

What is the time frame for obtaining a response on a complaint?

Once a complaint for non-compliance with the BCRs has been filed by a Data Subject, the Responsible Area within the Group will assess requirements for admission.

A response to the complaint will be given within a one-month time frame, which can be extended to two further months in view of the complexity and number of complaints the competent Responsible Area is managing at the time. When the time frame for responding to the complaint is extended, the Data Subject will be informed accordingly on such extension and on the specific reasons that justify it within the term of one month. Additionally, the Data Subject will be informed on the approximate timing for obtaining a response.

The response will be notified to the Data Subject in writing or by electronic means, provided that these allow for the reading, printing and conservation of the same as expressly designated by the Data Subject and, in the absence of such indication, through the same means in which the complaint was filed.

The response given to the Data Subject will be in any case reasoned, and it will include clear conclusions on the request raised in the complaint.

What if a complaint is admitted?

When a complaint has been admitted by the Responsible Area in charge, an acknowledgement of receipt will be sent to the Data Subject, indicating the date of receipt. In addition, the corresponding file will be opened and processed.

Where the complaint is admitted, Telefonica will proceed to investigate the facts and reasons that caused the complaint. Telefonica shall use the contractual and governance mechanisms provided for in the BCRs to correct the facts that caused the complaint, remedy their effects and avoid them in the future. The data subject will be informed of the steps adopted by Telefonica in this regard.

What if a complaint is declared inadmissible?

A complaint may be declared inadmissible when essential information for its processing is omitted, including cases in which the grounds for the complaint are not specified, and in particular:

- When the facts, grounds and request of the complaint do not refer to specific processing activities.
- When the complaint reiterates other previous and responded complaints already filed by the same Data Subject in relation to the same facts.
- When the time frame for the filing of the complaint has elapsed.

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

- Failure to comply with the formal aspects set out above.

When a complaint is declared inadmissible for any of the above reasons, the Data Subject will be notified and provided with a reasoned response and will be allowed to present its allegations in that respect, as indicated in the relevant notification. Notwithstanding the aforementioned, during the course of the procedure, the Responsible Area in charge may request from the Data Subjects and other corporate bodies as much information and clarifications as it deems necessary to provide a response.

When the Data Subject has presented its allegations and the reasons for declaration of inadmissibility remain, a final response will be notified to the Data Subject in that respect.

When the Responsible Area in charge becomes aware of the simultaneous processing of a complaint and an administrative, arbitration or judicial proceeding on the same matter, it shall refrain from processing the former.

In addition, a Data Subject may request the discontinuance of the complaint procedure, or the Group Company(ies) may rectify the situation with the Data Subject to its satisfaction, in which case it will document it and communicate it to the competent Responsible Area. Should the complaint procedure be terminated in any of the aforementioned events, it will be filed accordingly.

What if a complaint is rejected or if the Data Subject is dissatisfied with the response given?

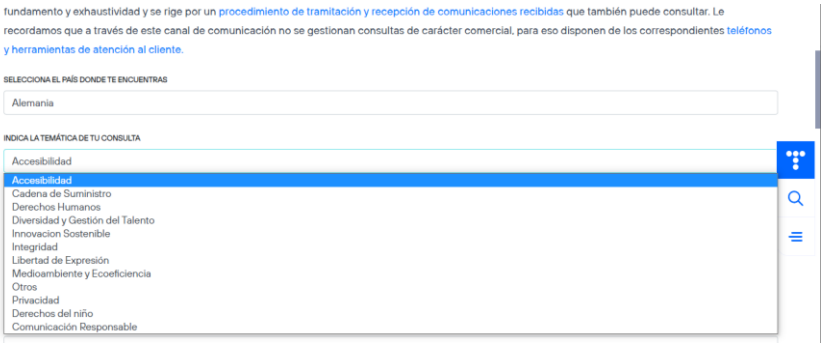
If a Data Subject does not agree with the rejection of its complaint as stated in the response given in the established time frame, or if it wishes to challenge the response given, it will still remain entitled to lodge a complaint with the relevant EEA supervisory authorities or to file a claim before the competent EEA courts. These rights shall be exercised in accordance with Section 4.1.

Compliance record

The Global DPO will keep a record of all complaints filed by Data Subjects and of the result of their enforcement and response.

In addition, an example of the complaints process tool is provided below.

You select the country and the cause of the claim.



***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.

www.telefonica.com

***Este documento está clasificado como PUBLICO por TELEFÓNICA.
***This document is classified as PUBLIC by TELEFÓNICA.