SPANISH DATA PROTECTION AUTHORITY
DECISION APPROVING BINDING CORPORATE RULES OF TELEFÓNICA GROUP

1. Having regard to Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), the SPANISH SUPERVISORY AUTHORITY shall approve Binding Corporate Rules (BCRs) provided that they meet the requirements set out under this Article.

   Whereas:

2. In accordance with the cooperation procedure as set out in the Working Document WP263 rev01[1], the Controller BCRs application of TELEFÓNICA GROUP were reviewed by the SPANISH DATA PROTECTION AUTHORITY, as the competent supervisory authority (SA) for the BCRs (BCR Lead) and by two Supervisory authorities (SAs) acting as co-reviewers. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.

3. The review concluded that the Controller BCRs of TELEFÓNICA GROUP comply with the requirements set out by Article 47(1) of the GDPR as well as the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art.47 GDPR) of June 2023 (hereinafter "the Recommendations") and in particular that the aforementioned BCRs:

   i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCRs by the **introduction of the BCR and the Intragroup Agreement**.

   ii) Expressly confer enforceable third party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs in **Section 4.3 of BCR**.

   iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:

a) The structure and contact details of the group of undertakings and each of its members **(Annex on the List of companies bound to the BCR).**

[1] Endorsed by the EDPB on 25 May 2018.

b) The data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the categories of data subjects affected, and the identification of the third country or countries **(Annex on the Categories of International Data Transfers (Data Controller) of BCR).**

c) The legally binding nature of the BCRs, both internally and externally **(Introduction BCR and Intra-Group Agreement).**

d) The application of the general data protection principles, in particular, purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data and the measures aimed at guaranteeing data security and the requirements regarding subsequent transfers to bodies not bound by the binding corporate rules **(Section 3 of the BCR)**.

e) The rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules **(Section 3.11, 4.1 and 4.2 and in the Annex on the management of data subjects rights Protocol of the BCR).**

f) The acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the Group not established in the Union, as well as the exemption of the controller or the processor from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage **(Section 4.1, 4.2 and 4.4 of the BCR).**

g) The way in which information about binding corporate rules is provided to data subjects **(Section 6 of the BCR)**.

h) The tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of

undertakings, as well as monitoring training, complaint-handling and the claim procedures **(Section 6 of the BCR).**

i) The claim procedure **(Section 5 and in the Annex on the BCRs complaint handling procedure of the BCR).**

j) The mechanisms established within the group of undertakings to verify compliance with the binding corporate rules are detailed in **Section 7 of the BCR and Annex on the Audits on the BCRs Protocol**. Such mechanisms shall include data protection audits and systems for ensuring corrective actions to protect the rights of data subjects. The results of such verification must be reported to the Data Protection Officer, as well as to the Group Management, and shall be available upon request from the competent data protection authority**.**

k) The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority **(Section 10 of the BCR)**.

l) The cooperation mechanism put in place with the supervisory authority to ensure compliance by any member of the group of undertakings is specified in **Section 9.1 of the BCR**. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j). **(Annex on the Audits on the BCRs Protocol;**

m) The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules **(Section 9.3, including 9.3.1 and 9.3.2 of the BCR).**

n) The appropriate training in data protection for personnel who have permanent or regular access to personal data **(Section 8 and Annex on the BCRs Training Plan).**

4. The EDPB provided its opinion 2/2024 in accordance with Article 64(1)(f) of the GDPR. The SPANISH DATA PROTECTION AUTHORITY took utmost

account of this opinion and communicated to the Board that it will amend the draft decision accordingly.

DECIDES AS FOLLOWING:

5. The Controller BCRs of TELEFÓNICA GROUP provide appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and(2)(b) and Article 47(1) and (2) GDPR and hereby the SPANISH DATA PROTECTION AUTHORITY approves the Controller BCRs of TELEFÓNICA GROUP.

6. However, before making use of the BCRs, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination, including onward transfer situations. This assessment has to be conducted in order to determine if the guarantees provided by BCRs can be complied with in practice, in light of the circumstances of the possible impingement created by the third country legislation with the fundamental rights and the circumstances surrounding the transfer. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

7. Where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under this BCRs. Therefore, the data exporter is required to suspend or end the transfer of personal data.

8. The approved BCRs will not require any specific authorization from the concerned SAs.

9. In accordance with Article 58(2)(j) GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by Controller BCRs of TELEFÓNICA GROUP are not respected.

ANNEX TO THE DRAFT DECISION

The Controller BCRs of TELEFÓNICA GROUP that are hereby approved cover the following:

a. **Scope**: The BCR 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, and Onward Transfers.

b. **Purposes of the transfer** are detailed in the Annex on the Categories of International Data Transfers (Data Controller) of BCR. They include the following:

i. **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.

ii. **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 Telefónica 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 Telefónica 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.

iii. **Operations :** business operation and commercial contact; roaming services management; provision of global supporting services; provision of lo T services; organization of the participation of start-up and small companies in innovation projects; provision of app development and operation services; management of the incidents arising from the materials and products provided by third parties.

iv. **Finance :** roaming services billing; consolidation and service billing purposes; internal communication and employee loyalty purposes; storage and processing payments and other financial transactions.

v. **Security :** security of Telefónica IT systems, Telefónica facilities and personnel; provision of cybersecurity services.

vi. **Marketing :** organization and arrangement of on-site events in different countries; encourage investment movements and enhance Telefónica's growth around the world; business development & commercial contact.

c. **Categories of data subjects** concerned by the transfer are specified in the Annex on the Categories of International Data Transfers (Data Controller) of BCR. They included:

People (employees including managers, Board members and directors, candidates, students and collaborators taking part in Projects concerning Telefónica).

Legal & Compliance (legal representatives, contractors/vendors, individuals who reach out to the DPO inbox to submit a privacy request).
Operations/Marketing (end users of Telefónica services, clients). Security (visitors, security managers, individuals affected by a potential cyber-incident).
Finance (investors, brokers and stakeholders).

d. **Categories of personal data transferred**: those categories are specified in the Annex on the Categories of International Data Transfers (Data Controller) of BCR. They included:

   i. **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 Telefónica, including picture; position and role within Telefónica's organizational chart; performance data; information related to the employee's trajectory / seniority at Telefónica; 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.
   ii. **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; identification data relating to individuals affected by a potential cyber-incident.
   iii. **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 Telefónica 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.

iv. **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.).

v. **Finance :** investors, brokers, stakeholders' personal data: Identification data (first and last name).

RELEVANT DOCUMENTATION TO BE ATTACHED WHEN SUBMITTING THE DRAFT DECISION TO THE EDPB VIA IMI AS

1. The Recommendations and in particular that the aforementioned BCR is completed with corresponding sections in Controller BCRs of TELEFÓNICA GROUP showing that they meet all requirements.
2. The BCRs, their Annexes, the IGA and the Application Form.