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

The SPANISH DATA PROTECTION AGENCY,

Pursuant to the request by MAPFRE S.A., on behalf of the MAPFRE Group, received on May 2022, for approval of their binding corporate rules for controller;

Having regard to Articles 47, 57 and 64 of 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); Having regard to the CJEU decision Data Protection Commissioner Maximillian Schrems and Facebook Ireland Ltd, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Having regard to 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 20 June 2023;

Makes the following observations:

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

2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the EU as to the protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any 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 in the case of the specific data transfer, including onward transfer situations. This assessment must be conducted in order to determine whether any legislation or practices of the third country applicable to the to-be-transferred data

may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR, taking into account the circumstances surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent Supervisory Authority and as such, they are not assessed by the competent Supervisory Authority as part of the approval process of the BCRs.

4. In any case, 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 these BCRs. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.

5. In accordance with the cooperation procedure as set out in the Working Document WP263 rev01[1], the Controller BCRs application of MAPFRE S.A was reviewed by the SPANISH DATA PROTECTION AGENCY, as the competent supervisory authority for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) 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.

6. The review concluded that the Controller BCRs of MAPFRE GROUP comply with the requirements set out by Article 47(1) of the GDPR as well as the 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 20 June 2023 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 entering in an Internal Procedure.

   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 (Section 5.3 of BCR);

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

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

a) The structure and contact details of the group of undertakings and each of its members are described in the Application form that was provided as part of the file review and in Annex I of BCR;

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in Section 3.2 and Annex VI of BCR;

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in the Application form and in Section 3 of BCR ;

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, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules are detailed in Section 4 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 in accordance with Article 22 of the GDPR, 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 which are set forth in Section 5 of the BCR;

f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in Section 11;

g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of Article 47.2 of the GDPR are provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in Section 5.1 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 monitoring the compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in Section 9.1 and Annex V of the BCR;

i) the complaint procedures are specified in Section 6 of the BCR;

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the binding corporate rules are detailed in Sections 7.2 and 7.3 of the BCR. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to the board of the audited Group Company, and the board of directors of the parent company) and are available upon request to the competent supervisory authority;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authorities are specified in Section 8 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 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) above are specified in sections 7.2 and 7.3 and Annex IV of the BCR;

m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules are described in Section 9.2 of the BCR;

n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (Section 7.1 of the BCR).

7. The EDPB provided its opinion 5/2024 in accordance with Article 64(1)(f) of the GDPR. The Spanish Data Protection Agency took utmost account of this opinion.

DECIDES AS FOLLOWING:

1. The **Spanish Data Protection Agency** approves the Controller BCRs of MAPFRE GROUP as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2) (b) and Article 47(1) and (2) GDPR. For the avoidance of doubt, the SPANISH DATA PROTECTION AGENCY recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which, an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
2. The approved BCRs will not require any specific authorization from the concerned SAs.
3. In accordance with Article 58(2)(j) GDPR, each concerned SAs 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 the Controller BCRs of MAPFRE GROUP are not respected.

ANNEX TO THE DRAFT DECISION

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

a. **Scope:** The purpose of the BCRs is to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when performing International Transfers of Personal Data between MAPFRE Group Companies established in the EEA and MAPFRE Group Companies established outside the EEA, importing such Personal Data in its capacity as Controller or Processor on behalf of Group company adhered to a controller BCR.

b. **EEA countries from which transfers are to be made**: Spain, Portugal, Italy, Germany, Malta, Ireland Belgium, France and Hungary (EEA countries).

c. **Third countries to which transfers are to be made**: United Kingdom, Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, U.S.A., Guatemala, México, Panamá, Paraguay, Perú, Puerto Rico, Dominican Republic, Uruguay, Turkey.

d. **Purposes of the transfer:** The purposes are detailed in Annex VI. They include the following: (i) human resources management, (ii) purchasing and provider management, (iii) contract and customer service/data subject management, (iv) benefits and claims management, and (v) auxiliary and internal advising functions.

e. **Categories of data subjects concerned by the transfer:** Those categories are specified in Annex VI. They included: employees, customers and customers representatives, third parties related to claims, event attendees, representatives and administrators, company directors, candidates, company representatives, and administrators, providers and providers representatives, internal and external auditors and users of social networks.

f. **Categories of personal data transferred**: Those categories are specified in Annex VI. They included: identification and contact information, professional contact information, economic, financial and insurance data, employment information, special data categories, social circumstances, academic and professional data, data related to transactions of goods and services, data related to personal characteristics and geolocation data.