MAPFRE GROUP BINDING CORPORATE RULES

INDEX

1. Introduction

MAPFRE is an independent Spanish business group that carries out insurance, reinsurance, financial, real estate and services activities in Spain and nearly 40 countries. Within the framework of the different business activities carried out by the MAPFRE Group, an organisational structure has been defined by business units, establishing the following:

- **Insurance Unit**: The insurance subsidiaries in each country carry out their activities with full capacity for local execution, applying the MAPFRE Group's global, regional and local policies.
- **Reinsurance Unit**: It carries out its reinsurance activity in two clearly differentiated areas, one for the marketing of reinsurance for insurance Companies and the other for the management of reinsurance for Group Companies, as defined in section 2, under the centralised management of MAPFRE RE.
- **Global Risks Unit**: For large companies, there is a specialised unit, MAPFRE GLOBAL RISKS, which offers solutions for large risks (aviation, energy, industry, construction, etc.), taking advantage of the experience and leading global international programmes for the most complex risks.
- **Assistance Unit**: It carries out its local activity under the centralised global management of MAPFRE ASSISTANCE **(MAWDY)**.

More information about the MAPFRE Group's business can be found on the corporate website: https://www.mapfre.com/en/our-business/

These activities are carried out through more than 250 companies grouped into divisions and the aforementioned operating units, which have broad management autonomy, under the coordination and supervision of the parent company's senior management bodies, which set the general guidelines and common policies to which the Group must adhere, and approve the objectives and strategic lines of the various units and companies, as well as the most important decisions and investments.

Within the framework of the aforementioned coordination and supervision, the Parent Company expresses its firm commitment and respect for the privacy of individuals and the protection of their personal data by specifying the minimum principles that the Group's Companies must comply with to ensure compliance with its values in application of personal data protection regulations.

As a result of the foregoing, MAPFRE has a centralised organisational and regulatory structure for the management and control of its actions in the area of privacy and personal data protection. This is complemented by a network of local resources in the

different regions and countries in which MAPFRE operates, which make it possible to adapt and make corporate models more flexible to the regulatory and security needs generated by the different social, economic and political environments in which MAPFRE operates.

Thus, MAPFRE has a Corporate Security Division as the management, planning and execution body of the Corporate Security Function, including in its scope the management and control of privacy and personal data protection. The peripheral structure outside Spain is led by Regional and Local Security Directors with functional dependence on the central structure of the Corporate Security Division for Security, Privacy activities.

This organisational structure and body of rules and regulations have been adapted, as has MAPFRE, to the legislation that has emerged in the countries where it operates. MAPFRE also collaborates with public institutions and sector forums, in order to facilitate the most efficient implementation of the different legislations in this area, as well as their proper compliance.

Special mention should be made of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter, "**GDPR**"), the reference standard for MAPFRE in the area of privacy. In particular, in order to regulate International Transfers of Personal Data between Group Companies (as defined in point 2 below), MAPFRE has decided to approve these Binding Corporate Rules (hereinafter "**BCRs**").

The BCRs will constitute a further adequacy guarantee, which MAPFRE Group Companies may use to carry out International Personal Data Transfers. The BCRs shall apply to International Transfers of Personal Data between MAPFRE Group Companies where such transfers are not covered by an adequacy decision enabling them or another safeguard or measure deemed more appropriate than the BCRs, as provided for in Chapter V of the GDPR.

The BCRs are intended to ensure an adequate level of protection in accordance with the GDPR for the purpose of securing International Transfers of Personal Data that are made from a Group Company domiciled in one EEA state to another Group Company established in another state outside the EEA.

2. Definitions

The Group companies to which the BCRs apply (hereinafter the "**Group Company(ies)**") shall interpret them in accordance with the GDPR, or the regulations in force from time to time, as well as with the terms defined below:

- **Binding Corporate Rules (BCRs):** the Personal Data protection policies undertaken by a Controller or Processor established in the territory of a Member State for

Transfers or a set of International Transfers of Personal Data to a Controller or Processor in one or more third countries, within a Corporate Group or a group of companies engaged in a joint economic activity.

Specifically, this document establishes the Binding Corporate Rules applicable to International Transfers of Personal Data between MAPFRE Group Companies that adhere to its contents and, in particular, those carried out by a Controller established in the EEA to a Controller or Processor established in a Third Country, including subsequent transfers of Personal Data carried out by the Data Importer to entities that are or are not part of the MAPFRE Group on the basis of the processing and categories of Personal Data covered by the BCRs.

- **Competent Supervisory Authority (ies)**: Supervisory Authority (-ies) located in the Member State where the Parent Company (Spain) is established, or where the Data Exporter is located, or in the Member State where the Data Subject has his habitual residence, and has presented the complaint that derives in the supervision action.
- **Consent of the Data Subject:** any freely given, specific, informed and unambiguous expression of will by which the Data Subject agrees, either by a statement or a clear affirmative action, to the Processing of Personal Data concerning him/her.
- **Corporate group:** a group consisting of a controlling undertaking and its controlled companies.
- **Data Controller or Controller:** the natural or legal person, public authority, service or other body which alone or jointly with others determines the purposes and means of the Processing; if Union or Member State law determines the purposes and means of the Processing, the Controller or the specific criteria for its nomination may be laid down by Union or Member State law.
- **Data Exporter:** Controller in the EEA who transfers the Personal Data to a Controller or Processor in a Third Country by its own means or through a Processor located in the EEA, who carries out the transfer on behalf of and for the account of the Controller established in the EEA.
- **Data Importer:** Controller or Processor in a Third Country that receives Personal Data from a Data Exporter pursuant to an International Transfer of Personal Data and that is adhered to the BCRs.
- **Data Processor or Processor:** the natural or legal person, public authority, service or other body processing Personal Data on behalf of the Controller.
- **Data Protection Officer or DPO:** professional responsible for ensuring compliance with privacy and data protection regulations, for being the point of contact with the corresponding Supervisory Authority and for advising the Controller or Data Processor on all matters relating to data protection regulations.
- **Data Subject:** identified or identifiable natural person. An identifiable natural person is any person whose identity can be established, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

- **Data Subprocessor or Subprocessor:** the natural or legal person, public authority, service or other body processing Personal Data on behalf of the Processor.
- **European Economic Area (hereinafter "EEA"):** the countries of the European Union together with Iceland, Liechtenstein and Norway.
- **European Union:** as at the date of publication of the BCRs, the European Union is the economic and political association comprising Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.
- **GDPR:** Regulation (EU) No. 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).
- **Group Companies Adhered to the BCRs:** Those MAPFRE Group companies located both inside and outside the EEA that have formalized their adhesion to the BCRs.
- **International Transfer(s) of Personal Data:** transfers of Personal Data to Third countries or international organisations are defined as the transmission of Personal Data by a Data Exporter (Data Controller) subject to the GDPR to a Data Importer (Data Controller or Processor) located in a Third country or international organisations not established in the EEA. These are therefore transfers of Personal Data that are or will be processed after transfer to a third country or international organisation.
- **MAPFRE Group:** "MAPFRE Group" shall be understood to mean MAPFRE, S.A. and its subsidiaries, in accordance with the terms of article 5 of Royal Legislative Decree 4/2015, of 23 October, approving the revised text of the Securities Market Act and article 42 of the Commercial Code. The MAPFRE Group may be referred to as the "Group" or "MAPFRE".
- **Member State:** refers to any of the States that make up the European Union (see definition of European Union for details of the States).
- **Parent Company:** MAPFRE, S.A., as parent company of the MAPFRE Group.
- **Personal Data Breach:** any breach of security resulting in the accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed.
- **Personal Data:** any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable natural person is any person whose identity can be established, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

- **Processing:** any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automatic 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.
- **Profiling:** any form of automated Processing of Personal Data consisting of using Personal Data to evaluate certain personal aspects of a natural person, in particular to analyse or predict aspects relating to that natural person's professional performance, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Recipient:** the natural or legal person, public authority, service or other body to whom Personal Data are disclosed, whether or not it is a Third Party. However, public authorities that may receive Personal Data in the framework of a specific investigation in accordance with Union or Member State law shall not be considered as Recipients; the Processing of such data by such public authorities shall be in accordance with the data protection rules applicable to the purposes of the Processing.
- **Responsible Companies:** MAPFRE Group companies that assume responsibility for compliance with the BCRs by Group Companies established outside the EEA and undertake to supervise such compliance.
- **Special Categories of Data:** all those Personal Data collected by MAPFRE that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, trade union membership, the Processing of genetic data, biometric data aimed at univocally identifying a natural person, data relating to health or data relating to the sex life or sexual orientation of a natural person.
- **Supervisory Authority(ies):** independent public authority established by a Member State to supervise the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons with regard to the Processing and to facilitate the free flow of Personal Data in the European Union. In the approval of BCRs, the main supervisory authority is the Spanish Data Protection Agency.
- **Third Country:** Any country that is not an EEA Member State.
- **Third Party:** natural or legal person, public authority, service or body other than the Data Subject, the Controller, the Processor and the persons authorised to process the Personal Data under the direct authority of the Controller or the Processor.
- **Union or Member State law:** the law of the European Union or the law of any of its Member States.

3. Scope of application of BCRs

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 a Group Company Adhered to the Data Controller BCRs.

The BCRs are legally binding and must be observed by all Group companies that adhere to them, as well as by all their employees.

The Parent Company together with the Group Company established outside the EEA shall, prior to the latter's adhesion to the BCRs, assess whether the level of protection required by European Union law is respected in the Third Country in order to assess whether the guarantees provided by the BCRs can be complied with in practice by the Group Company established outside the EEA.

For assessing the regulations and practices of the Third Country which may affect the compliance of the terms contained in the BCRs, including those that require disclosure of data and information to public authorities or authorize access by such authorities, the MAPFRE Group Companies will take due account about the specific circumstances of the International Data Transfer(s), and of any envisaged onward Transfers within the same Third Country or to another Third Country, and also the following aspects: i) purposes for which the Personal Data are transferred and processed; ii) type of entities involved in the Processing (the Data Importer and any further recipient of any onward transfer); iii) sector in which the International DataTransfer(s); iv) categories and format of Personal Data transferred; v) location of the Processing including storage and; vi) transmission channels used.

In case a Group Company outside the EEA and Adhered to the BCRs member ceases to be part of MAPFRE Group or to be adhered to the BCRs, it should be continuing to apply the BCRs requirements to the Processing of those Personal Data transferred to it by means of the BCRs unless, at the time of leaving the Group or ceasing to be adhered to the BCRs, that member will delete or return the entire amount of the Personal Data transferred to the Data Exporter.

The Parent Company together with the Group Companies Adhered to the BCRs, will monitor and document that any relevant necessary supplementary measures (technical, contractual, organizational) during the transfer and the Processing of the Personal Data in the country of destination are taken to comply with the BCRs in order to ensure a level of protection essentially equivalent to that provided for in the applicable EEA legislation, provided that local law or practice in the Third Country does not affect these supplementary measures in such a way as to impede their implementation and effectiveness. The Group Companies should make such documentation available to the Competent Supervisory Authorities upon request.

3.1. Geographical scope of application

The BCRs will apply to International Transfers of Personal Data by Group Companies established in the EEA to Group Companies established in Third Countries that do not provide the adequate level of protection required by the GDPR.
Specifically, the BCRs shall only apply to International Data Transfers of Personal Data carried out by a MAPFRE Group Company established in an EEA country exporting Personal Data in its capacity as Controller to a MAPFRE Group Company not established in an EEA country, importing such Personal Data in its capacity as Controller or Processor, provided that, as indicated above, the said International Data Transfers are not covered by an adequacy decision of the European Commission enabling such international transfer or another guarantee or measure deemed more appropriate than the BCRs, in accordance with the provisions of the GDPR.

ANNEX I identifies all Group Companies that are linked to the content of the BCRs, as well as their contact details.

3.2. Material scope of application

The BCRs are mandatory for Group Companies that have adhered to them through the procedure of linking them to the internal corporate policies and procedures existing in the MAPFRE Group.

In this regard, the BCRs provide coverage for the Processing of Personal Data involving an International Transfer of Personal Data that is intended for the purpose to the:

- **Human Resources Management:** to manage the Group's Human Resources tasks, including the management of the contractual relationship with employees, of candidate selection processes and of the internal international mobility of employees and candidates between the Group's Companies.
- **Purchasing and supplier management:** contractual and commercial management of professionals and suppliers.
- **Management of contracting and client and stakeholder service:** to provide support in the management of the subscription of certain products, as well as for the appropriate customer service through the *contact centre* and the management of social networks.
- **Claims and benefits management**: to carry out the proper management and technical control of benefits, as well as for the management of the claim itself and the management of benefits.
- **Ancillary and internal consultancy functions:** to carry out an adequate management of the services offered at corporate level.

In order to achieve the aforementioned purposes, the following categories of Personal Data of the indicated Data Subjects will be processed:

- **Suppliers, if they are natural persons:** (i) professional identification and contact details, (ii) economic, financial and insurance details, (iii) transactions of goods and services, (iv) employment details.
- **Supplier representatives:** (i) professional identification and contact details; (ii) employment details.
- **Internal and external auditors:** (i) professional identification and contact details, (ii) academic and professional details, (iii) employment details.
- **Employees:** (i) identification and contact details, (ii) professional contact details, (iii) economic, financial and insurance details, (iv) employment details, (v) transactions of goods and services, (vi) academic and professional details.
- **Candidates:** (i) identification and contact details, (ii) job details, (iii) academic and professional data and (iv) data relating to personal characteristics.
- **Directors:** (i) identification and contact details, (ii) employment details, (iii) academic and professional details.
- **Representatives and administrators:** (i) identification data, (ii) employment details, (iii) academic and professional data.
- **Clients:** (i) identification and contact data, (ii) economic, financial and insurance data, (iii) employment details, (iv) Special Categories of Data, (v) academic and professional data, (vi) data relating to transactions of goods and services, (vii) geolocation data, and (viii) data relating to personal characteristics and social circumstances.
- **Claims-related third parties:** (i) identification data, (ii) economic, financial and insurance data, (iii) personal characteristics, (iv) Special Categories of Data, (v) employment details, (vi) relating to transactions of goods and services, (vii) data relating to social circumstances, (viii) geolocation data.
- **Client representatives:** (i) identification data.
- **Event attendees:** (i) identification data, (ii) image, (iii) identification and professional contact data, (iv) personal characteristics, (v) special categories of data.
- **Social media users:** (i) identification and contact details.

The possible International Data Transfers of Personal Data associated to these categories are further described in ANNEX VI.

4. Substantive principles for the Processing of Personal Data

4.1. General principles in Processing

Without prejudice to compliance with the provisions of the BCRs, Group Companies will have to comply with their applicable local legislation on the protection of Personal Data. Furthermore, in order to ensure that the level of protection of natural persons guaranteed

by the GDPR is not undermined, the Group Companies shall respect the following data protection principles relating to the Processing of Personal Data:

- **Principle of lawfulness, fairness and transparency in relation to the Data Subject**: the Data Subject must be provided with the information specified in Section 5.1 of the BCRs. This information shall be provided in a concise, transparent, intelligible and easily accessible manner, using clear and plain language. Processing shall be carried out in accordance with the data protection regulations in force, i.e. in a lawful, fair and transparent manner in relation to the Data Subject.

  The Processing shall be lawful only if and to the extent that at least one of the following applies:

  - the Data Subject has given consent to the Processing of his or her Personal Data for one or more specific purposes;
  - Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
  - Processing is necessary for compliance with a legal obligation to which the Controller is subject;
  - Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
  - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
  - Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

- **Purpose limitation principle**: the Processing of Personal Data shall be for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.
- **Data minimisation principle**: Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle of accuracy:** the data shall be accurate and, if necessary, updated, and Group Companies shall take reasonable steps to ensure that Personal Data that are inaccurate with respect to the purposes for which they are processed are deleted or rectified without delay.
- **Principle of limitation of the storage period:** Personal Data shall be kept in a form that allows the identification of Data Subjects for no longer than is necessary for the purposes of the Processing of the Personal Data.
- **Principle of integrity and confidentiality:** Personal Data shall be processed in a manner that ensures adequate security, including protection against unauthorised or

unlawful Processing and against accidental loss, destruction or damage, by assessing the appropriate level of security account taken in particular the risks that are presented by Processing, implementing appropriate technical and organisational measures, including, inter alia as appropriate:.

- the pseudonymisation and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the Processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

Furthermore, in the event of a Personal Data Security Breach, the Group Companies shall notify without undue delay the Group Parent Company established in the EEA.

- **Principle of data protection by design and by default**: the Controller, having regard to the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing, as well as the likelihood of occurrence of risks of various kinds and severity that the Processing of Personal Data may entail, shall adopt, both at the time of determining the means and at the time of the Processing itself, appropriate technical and organisational measures, designed to effectively implement the data protection principles, as well as the necessary safeguards for the purposes of complying with the requirements of the GDPR and protecting the rights of Data Subjects. In addition, the Controller shall implement appropriate technical and organisational measures in order to ensure that, by default, only Personal Data that are necessary for each of the specific purposes of such Processing are processed and that the Personal Data are not accessible to an indefinite number of natural persons.

- **Proactive accountability principle:** Group Companies shall comply strictly with the content of the BCRs and shall be able to demonstrate this. For such purposes, the Group Companies shall keep a register of the Processing activities carried out, which shall be made available to the Competent Supervisory Authority, as well as analyse the risk of the Processing, and shall carry out a data protection impact assessment when a type of Processing is likely to entail a high risk to the rights and freedoms of natural persons.

  The Group Companies acting as Data Controllers will keep a record in writing (including electronic form) of the data Processing activities carried out under their responsibility. Said record must contain all the information indicated below:

  - The name and contact details of the Controller and the Data Protection Officer.
  - The purposes of the Processing.
  - A description of the categories of Data Subjects and the categories of Personal Data.

- The categories of recipients to whom the Personal Data was disclosed or will be disclosed, including recipients in Third Countries or international organizations.
- If applicable, the International Transfers of Personal Data and the documentation of adequate guarantees.
- Whenever possible, the retention periods for the deletion of the different categories of Personal Data.
- Where possible, a general description of the technical and organizational security measures.

The Group Companies acting as Data Processor, will keep a record in writing (including electronic form) of all categories of processing activities carried out on behalf of a Data Controller that contains:

- The name and contact details of the Processor or Processors and of each Controller on behalf of whom the Processor acts, and of the Data Protection Officer.
- The Processing categories carried out on behalf of each Data Controller.
- If applicable, the International Transfers of Personal Data and the documentation of adequate guarantees.
- Where possible, a general description of the technical and organizational security measures.

Where appropriate, where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the Controller should, prior to Processing, consult the Competent Supervisory Authority.

4.2. Processing of Special Categories of Data

In general, the Processing of Special Categories of Data is prohibited, provided that none of the following circumstances apply:

- The explicit consent of the data subject has been obtained.
- The Processing is carried out in fulfilment of obligations and the exercise of specific rights of the Data Controller or the Data Subject in the field of labour law, social security and social protection (e.g. in collective conventions of employees).
- Processing is necessary for the protection of the vital interests of the Data Subject or of another natural person, where the Data Subject is physically or legally incapable (e.g. the Data Subject has suffered a serious accident) of giving his or her Consent.
- The Processing relates to Personal Data that the Data Subject has manifestly made public.
- Processing is necessary for the formulation, exercise or defence of claims, or when the courts are acting in their judicial role.

- Processing is carried out for reasons of essential public interest, such as, for example, the prevention of epidemics.
- Processing is necessary for the purposes of preventive or occupational medicine, assessment of the worker's capacity to work, medical diagnosis, provision of health or social care or treatment, or management of health and social care systems and services (e.g. medical examinations in the field of occupational risk prevention) or under a contract with a health professional.

4.3. Contracting of Data Processors and Subprocessors

When a MAPFRE Group Company is going to carry out a Processing of Personal Data that requires the contracting of a Third Party located outside the EEA that has the status of Processor, it shall ensure that the transfer is regulated in such a way as to maintain adequate protection of the Personal Data processed in accordance with the criteria provided for by the GDPR.

The MAPFRE Group Company shall only choose a Processor that offers sufficient guarantees to implement measures to ensure that the Processing complies with the principles and requirements of the BCRs, as well as to ensure the protection of the rights of the Data Subjects covered by the GDPR.

A contract or other similar legal act shall be signed that binds the Processor with respect to the Controller and establishes the object, duration, nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, and the obligations and rights of the Controller and the Processor, respectively. The obligations of the Data Processor shall be, as a minimum, and must be expressly set out in the contract or in an assimilable legal act, the following:

- Process Personal Data only in accordance with documented instructions from the Controller, including with respect to Transfers of Personal Data to a Third Country or an international organisation, unless obliged to do so under European Union or Member State law applicable to the Controller. In such a case, the Controller shall inform the Data Controller of such a legal requirement prior to processing, unless such a law prohibits it for important reasons of public interest.
- Ensure that persons authorised to process Personal Data have undertaken to respect confidentiality or are subject to a confidentiality obligation of a statutory nature.
- Take all appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.
- Not to use another Processor - that is, a Subprocessor - without the prior written authorisation, specific or general, of the Controller. The same data protection obligations as those stipulated in the contract or similar legal act between the

Controller and the Processor shall be imposed on the said Subprocessor, by means of the formalisation of a contract or similar legal act, and, in particular, the granting of sufficient guarantees in relation to the application of technical and organizational measures appropriate to the nature of the Processing so that it is carried out in accordance with the provisions of the GDPR.

Before contracting or substitution of the Subprocessor, the Controller shall have the right to object to or terminate the Processing contract, given the case.

Notwithstanding the foregoing, the Data Processor will be held responsible by the Data Controller for compliance with the Data Protection obligations by the Subprocessor.

- To assist the Controller, taking into account the nature of the Processing, through appropriate technical and organisational measures, where possible, to enable the Controller to fulfil its obligation to respond to requests aimed at exercising the rights of Data Subjects set out in the GDPR and in these BCRs.
- Assist the Controller in ensuring compliance with data protection obligations relating to the security of processing, the management of Personal Data Security Breaches, and the conduct of data protection impact assessments.
- At the Controller's option, delete or return all Personal Data upon termination of the provision of the Processing services, and delete existing copies, unless the Personal Data are required to be retained by European Union or Member State law.
- Make available to the Controller all information necessary to demonstrate compliance with its data protection obligations, as well as to allow and contribute to audits, including inspections, by the Controller or another auditor authorised by the Controller.

4.4. Further transfers of Personal Data

The BCRs cover onward International Transfers of Personal Data made by a Data Importer to a Controller and/or a Processor established in another Third Country, whether it is a MAPFRE Group Company not adhered to the BCRs or a Third Party not part of the MAPFRE Group, provided that (i) such transfers are related to the processing and to the categories of Personal Data covered by the BCRs, and (ii) an adequate level of protection is ensured in accordance with the terms set out in the GDPR, in particular:

- The European Commission has decided that the Third Country, territory or one or more specific sectors within that Third Country to which the Personal Data are intended to be transferred, ensures an adequate level of protection. For this purpose, the European Commission publishes in the Official Journal of the European Union and on its website a list of third countries, territories and specific sectors in a third country for which it has decided that an adequate level of protection is ensured or, where appropriate, is no longer ensured.

- In the absence of an adequacy decision by the European Commission in the terms indicated in the previous point, the Data Importing Group Company would have provided adequate safeguards to carry out the International Transfer and the Data Subjects have enforceable rights and effective legal remedies. This safeguards may be provided by:

    - Standard data protection clauses adopted by the Commission.
    - Standard data protection clauses adopted by a Supervisory Authority and approved by the Commission.
    - An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the Controller or Processor in the Third country to apply the appropriate safeguards, including as regards Data Subjects' rights.
    - An approved certification mechanism together with binding and enforceable commitments of the Controller or Processor in the Third country to apply the appropriate safeguards, including as regards Data Subjects' rights.

- In the absence of the above measures, the International Transfer of Personal Data meets one of the following conditions:

    - The granting of the Data Subject's Consent explicitly to the proposed International Transfer of Personal Data, after having been informed of the possible risks of such a transfer due to the absence of an adequacy decision of the European Commission and of adequate guarantees.
    - The International Transfer of Personal Data is necessary for the conclusion or performance of a contract between the Data Subject and the Group Company concerned or for the performance of pre-contractual measures taken at the request of the Data Subject.
    - The International Transfer of Personal Data is necessary for important reasons of public interest, if public interest is recognised in the member State or European regulation.
    - The International Transfer of Personal Data is necessary for the formulation, exercise or defence of claims.
    - The International Transfer of Personal Data is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving his or her Consent.

5. Rights of the Data Subject

5.1. Transparency and information

In order to ensure transparent Processing, the Group Companies shall take appropriate measures to provide the Data Subject with information regarding the Processing of his or her Personal Data in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

Data subjects shall have the right to access the contents of the BCRs, which shall be published on the corporate website of the Parent Company. In addition, Data Subjects may request a copy of the BCRs from any Group Company.

When the Personal Data are obtained from the Data Subject, the Group Company collecting the Personal Data from the Data Subject as Data Controller, or the one collecting the Personal Data from the Data Subject as Data Processor on the instructions of the Data Controller, shall provide the following information to the Data Subject:

- The identity and contact details of the Controller and, where applicable, of his or her representative.
- The contact details of the Data Protection Officer, if applicable.
- The purposes of the Processing for which the Personal Data are intended and the legal basis for the Processing.
- When the Processing of Personal Data is based on the existence of legitimate interests, specification of such interests of the Controller or of a Third Party.
- The Recipients or categories of Recipients of the Personal Data, if applicable.
- Where applicable, the entity's intention to carry out an International Data Transfer to a third country, as well as its legal authorisation.
- The period for which the Personal Data will be kept or, where this is not possible, the criteria used to determine this period.
- The existence of the right to request from the Data Controller access to Personal Data relating to the Data Subject and their rectification or erasure, or the limitation of their Processing or to object to their Processing, as well as the right to data portability.
- Where the Processing of Personal Data is based on the Data Subject's Consent, the existence of the right to withdraw it at any time, without affecting the lawfulness of the Processing based on the Data Subject's Consent prior to its withdrawal.
- The right to lodge a complaint with a Supervisory Authority.
- Whether the provision of Personal Data is a legal or contractual requirement, or a necessary requirement for entering into a contract, and whether the Data Subject is obliged to provide the Personal Data and is informed of the possible consequences of not doing so.

- The existence of automated decisions, including Profiling and, where appropriate, meaningful information about the logic applied, as well as the significance and expected consequences of such Processing for the Data Subject.

Where the Personal Data have not been obtained from the Data Subject, the relevant Group Company shall provide the above information in addition to the categories of data concerned and the source of the data within a reasonable time after the Personal Data have been obtained, and at the latest within one month. If the data are to be used for communication with the Data Subject, at the latest at the time of the first communication to the Data Subject or, if it is intended to be communicated to another Recipient, at the latest at the time the Personal Data are communicated for the first time.

5.2. Rights of access, rectification, erasure, objection, limitation and portability

The Group Companies, through the implementation of the corresponding internal procedures, guarantee to the Data Subjects the exercise of the following rights regarding the Processing of their Personal Data:

- **Right of access**: to request confirmation as to whether or not Personal Data concerning him/her are being processed and, if so, to access them and the information related to their Processing.
- **Right to rectification**: to request the rectification of inaccurate or incomplete data.
- **Right to erasure**: to obtain without undue delay the erasure of data concerning him/her, the Data Controller being obliged to erase his/her Data when, among other reasons, they are no longer necessary for the purposes for which they were collected, in which case the Data Controller shall cease to process the Personal Data except for the exercise or defence of possible claims.
- **Right to restrict the Processing**: request the restriction of the Processing of your Personal Data when one of the following conditions is met: (i) the Data Subject contests the accuracy of the Personal Data, (ii) the Processing is unlawful and you request the restriction of its use and not the erasure of the data, (iii) the Controller no longer needs the Personal Data for the purposes of the Processing and (iv) the Data Subject has objected to the Processing of his/her data while we verify whether the legitimate reasons of the Controller prevail over those of the Data Subject. In this case, the Personal Data of the Data Subject may only be processed with his or her Consent, with the exception of their retention and their use for the exercise or defence of claims or for the protection of the rights of another natural or legal person or for reasons of substantial public interest of the European Union or of a particular Member State.
- **Right to object**: to object to the Personal Data concerning him/her being subject to Processing based on the fulfilment of a public interest or the satisfaction of legitimate interests of the Controller or a Third Party, including Profiling. The Controller shall cease processing the Data, except for the defence of possible claims or compelling

legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject.

- **Right to object to Automated individual decision-making, including profiling:** request not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- **Right of portability**: to receive the Personal Data concerning him/her that he/she has provided to the Controller in a structured, commonly used and machine-readable format, and to transmit it to another Controller where technically feasible when the Processing is based on Consent or on the performance of a contract and the Processing is carried out by automated means.

5.3. Third Party Beneficiary Rights

Without prejudice to any other administrative or judicial remedy, every Data Subject shall have the right to lodge a complaint with a Supervisory Authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the Data Subject considers that the processing of Personal Data relating to him or her infringes the BCRs.

In addition, and without prejudice to any administrative or non-judicial remedy that is applicable, including the right to lodge a complaint with the Supervisory Authority described above, each Data Subject shall have the right to an effective judicial remedy where he or she considers that his or her rights have been infringed as a result of the Processing of his or her personal data that infringes the BCRs.

Proceedings against a Controller shall be brought before the courts of the city of Madrid, Spain (being the Member State where the Parent Company has its corporate establishment). Alternatively, such proceedings may be brought before the courts of the Member State where the Data Subject has his or her habitual residence.

In particular, Data Subjects have the right to bring a claim before the competent jurisdiction and the right to obtain redress and, where appropriate, to receive compensation in case of a breach of the following:

- Data protection principles, lawfulness of processing, security and Personal Data breach notifications, restrictions on onward transfers (as per section 4.1 of the BCRs).
- Transparency and ease of access to BCRs (as per section 5.1 of the BCRs).
- Rights of information, access, rectification, erasure, restriction, objection to processing and the right not to be subject to decisions based solely on automated processing, including Profiling (as per section 5.2 of the BCRs).
- Third Party Beneficiary Rights (as per section 5.3 of the BCRs).

- National legislation preventing compliance with BCRs and obligations in case of government access requests (as per sections 3 and 9.2 of the BCRs).
- Right to complain through the internal complaint mechanism of the MAPFRE Group Companies (as per sections 5.4 and 6 of the BCRs).
- Obligations of cooperation with the Supervisory Authorities (as per section 9.4 of the BCRs).
- Liability and jurisdiction provisions (as per section 11 of the BCRs).
- Duty to inform the Data Subjects about any update of the BCR and of the list of Group Companies Adhered to the BCRs (as per section 8 of the BCRs).
- Right to judicial remedies, redress and compensation (as per section 11 of the BCRs).

5.4. Right to lodge a complaint

Data Subjects shall have the right to lodge claims or complaints relating to breaches of the BCRs by any of the Group Companies before the Competent Supervisory Authority and before the competent courts of the Member States in accordance with GDPR, and the right to obtain redress, and, where appropriate, compensation, following what is stated in section 5.3. Such claims shall be handled in accordance with the procedure set out in section 6 below.

The Data Subjects shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a 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 to lodge any complaint, to exercise the rights, and to exercise the right to receive compensation on his or her behalf where provided for by Member State law.

6. Complaint Handling Procedure

The Group Companies shall have an internal complaint handling process in place and which will ensure that, in the event of a dispute, Data Subjects residing in the European Union may lodge a complaint about any Processing of their Personal Data that they consider to be unlawful, inappropriate or otherwise incompatible with the BCRs. Data Subjects who wish to file a complaint with the MAPFRE Group for non-compliance with the provisions of the BCRs may do so simply, quickly and efficiently by sending their request in any format to MAPFRE, S.A., Carretera de Pozuelo, nº 52, 28222 Majadahonda, Madrid (Spain) or by e-mail to dpo.mapfre-bcr@mapfre.com.

The claim must be resolved and the Data Subject informed of the resolution without undue delay, and in any event within a maximum period of one month from its receipt at MAPFRE. This period may be extended by a further two months, if necessary, taking into account the complexity and number of requests, complaints and claims received. The relevant Group Company shall inform the Data Subject of any such extension within

one month of receipt of the complaint, stating the reasons for the delay, via the e-mail address mentioned in the previous section or via the alternative means indicated by the Data Subject in his complaint.

In the event that the Data Subject is not satisfied with the response of the Data Protection Officer or the lack thereof, he / she will have the right, in any case, to file a claim with the Competent Supervisory Authority or with the competent jurisdictional bodies, according to to the provisions of section 5.3 above. Likewise, the Data Subject will be informed about the consequences in the event that the claim is denied, there are delays in the response or it is justified and, therefore, it is admitted.

7. Mechanisms to ensure the effectiveness of BCRs

7.1 Training

In order to ensure that all MAPFRE Group employees are informed of the BCRs, their content and the Group's rules on Personal Data protection, the MAPFRE Group shall take all necessary measures to make the BCRs available to its employees and thus ensure that they are respected and complied with. The MAPFRE Group shall establish annual training plans to ensure appropriate and up-to-date regular dissemination and training in data protection matters, which shall guarantee, among other things, knowledge of the principles contained in the BCRs. Within these training plans, general actions aimed at all employees will be considered, as well as specific ones aimed to key groups that based on their functions and responsibilities have permanent or regular access to Personal Data and/or are involved in the collection of data or in the development of tools related to Personal Data Processing, including procedures of managing requests for access to Personal Data by public authorities.

The basic contents of the training will be established centrally by the Group´s Parent Company to the Group Companies and practical examples will be distributed, but the final development and implementation of the training and dissemination sessions will be carried out by each of the Group Companies subject to the BCRs in accordance with their local regulations and applicable local procedures.

7.2 Audits

In order to guarantee and review compliance with the BCRs, the MAPFRE Group has established an annual internal audit plan to carry out the corresponding assessments and audits according to the needs and findings detected from the MAPFRE Group Companies to ensure the correct application of its internal rules and, in turn, of the regulations in force on data protection. Initially, the audits will be carried out every two years, although this can be altered based on the level of risk of the Processing. A summary of the aforementioned plan is attached as **ANNEX II**. Specific or ad hoc audits

can be carried out upon request from the DPO or any other competent function in the organisation.

The scope of the audits covers the full scope of the BCRs and ensures the implementation of corrective measures, where appropriate. The audited Group Companies report the results of the audits to the Board of the audited Group Company, to the local Data Protection Officer, or failing that, to the local privacy team, and the Board of Directors of the Parent Company and to the MAPFRE Group's Data Protection Officer.

The MAPFRE Group shall make available to the Supervisory Authority the results of assessments or audits in relation to BCRs when required to do so.

7.3 Security breaches

The MAPFRE Group has procedures for the management of Personal Data security breaches, so that in the event of any breach affecting the security of Personal Data in any Group Company, the latter must follow the MAPFRE Group's internal procedures and notify the Group's Parent Company without undue delay so that, if necessary, the Competent Supervisory Authority could be notified not later than 72 hours after having become aware of it and, where appropriate, also the Data Subjects.

This notification shall be made whenever such a breach may pose a risk to the rights and freedoms of natural persons. Group Companies shall keep a record of Data Security Breaches and all related documentation comprising all the facts that took place relating to the Personal Data Breach, its effects and the remedial action taken, which shall be made available to the competent data protection supervisory authority upon request.

8. BCRs Update Procedure

The BCRs may be updated and modified in order to adapt them to regulatory changes in force or to the practices, procedures and organisation of the MAPFRE Group Companies as a whole or of any or some of its entities in particular, as well as to adjust them to the requirements imposed by the competent authorities in the field of data protection. For this purpose, a procedure for updating and amending the BCRs has been developed and is attached as **ANNEX III**.

Proposed amendments which may affect the level of protection offered by the BCRs, or which may significantly affect the BCRs (i.e. amendments which may affect their binding nature), shall be previuosly communicated without undue delay, to the Competent Supervisory Authority with a brief explanation of the reasons for the update, for validation from said Authority, and also to all the Group Companies Adhered to the BCRs.

Updates that do not affect the level of protection offered by the BCRs and do not significantly affect the BCRs, as well as the list of Group Companies Adhered to the BCR, shall be communicated to the Competent Supervisory Authority, with a brief

explanation of the reasons for the update, and also to all the Group Companies Adhered to the BCRs on an annual basis.

No new International Transfer of Personal Data to a new member linked to the BCRs shall take place until such new member has formally acceded to the amended BCRs and can deliver compliance.

9. Mutual assistance and cooperation with data protection authorities

9.1 Network of data protection officers or appropriate staff to monitor compliance with BCRs

Within the MAPFRE Group there is a corporate DPO, a Corporate Privacy and Data Protection Committee, as well as local DPOs or, failing that, local privacy teams. Data Subjects can contact directly for any enquiry about the Processing of their Personal Data through the defined channels (as per sections 6, 12 and ANNEX I). Further details of the governing bodies related to the MAPFRE Group's BCRs can be found in **ANNEX V**.

In this regard, the MAPFRE Group's corporate structure oversees privacy and data protection and leads, promotes and coordinates corporate initiatives for proper compliance with regulations in this area. In turn, the local structure makes it possible to adapt and make the corporate models more flexible to the specific needs and problems of each location, in order to meet the specific regulatory requirements on privacy, data protection and security generated by the different social, economic and political environments in which the MAPFRE Group operates.

Group Companies within the EEA Adhered to the BCRs who, in order to guarantee the compliance and effectiveness of the BCRs, identify the need to implement additional security measures to those already implemented in certain International Data Transfers, must inform the rest of the Group Companies Adhered to the BCRs of the assessment carried out and of its results. Said Group Companies Adhered to the BCRs shall apply the additional measures identified for the same type of International Data Transfer or, in case those measures could not be put in place, the International Data Transfers involved will be suspended or ended.

9.2 Relationship between BCRs and local legislation

The BCRs will only be used as a mechanism to carry out the International Transfers of Personal Data once it has been evaluated that the laws and practices applicable in the Third country of destination for the Processing of Personal Data respect the essence of fundamental rights and freedoms, do not exceed what is necessary and proportionate in

a democratic society, and do not prevent from complying with the obligations established in the BCRs.

Local law shall apply in preference to the content of the BCRs where such law requires a higher level of protection of Personal Data than that provided by the BCRs. In any case, the Personal Data will be processed in accordance with the fundamental principles set out in the GDPR detailed in point 4.1 above.

If a Group Company believes that local laws or regulations prevent it from complying with the BCRs, it shall notify the Parent Company and, in particular, to the Corporate DPO as soon as possible and, where possible, to the Data Subject. Subsequently, they will identify the appropriate measures (technical or organisational measures to ensure security and confidentiality) that should be adopted in order to enable them to fulfill the obligations resulting from their adhesion to the BCRs. If even so, the obligations established in the BCRs cannot be fulfilled, the Transfer or set of International Personal Data Transfers must be suspended; as well as all International Personal Data Transfers with respect to which the same evaluation and reasoning would lead to a similar result, until compliance is ensured or it is definitely suspended. The effects of the suspension are described in point 10 of the BCRs.

This includes any legally binding request for disclosure of Personal Data made by a public authority to a MAPFRE Group Company established outside the EEA that is likely to have a substantial adverse effect on the guarantees provided by the BCRs. In this case, the Corporate DPO shall be informed as soon as possible of the request received and, if necessary, shall inform the Responsible Companies and the Competent Supervisory Authority of the request, about the data requested, the body requesting the data and the legal basis for disclosure.

It will also be necessary to inform the Data Exporter and, where necessary the Data Subject, if the Data Importer becomes aware of any direct access by public authorities, in accordance with the laws of the country of destination, to Personal Data transferred pursuant to the BCRs; such notification will include all information available to the Data Importer.

In those specific cases where a local public authority prohibits the MAPFRE entity receiving the request from transmitting the notification to inform the Data Exporter or the Data Subject where necessary, the Group Company requested by the local public authorities undertakes to make every effort to obtain the right to waive this prohibition with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

The Data Importer will regularly provide the Data Exporter with all the relevant information on the requests received by public local authorities. If, according to the local law applicable in the country of the Data Importer, or meeting a direct requirement from the local public authority, the Data Importer can not provide partially or completely such

information to the Data Exporter, it shall, without undue delay, specifically inform the Data Exporter about this fact.

The Data Importer will preserve the information for as long as the personal data are subject to the safeguards provided by the BCRs, and shall make it available to the Competent Supervisory Authority upon request.

The Data Importer will review the legality of the request for disclosure of information submitted by the public local authority, in particular whether it is issued under the competence of the requesting authority, and will challenge the request if, given the case, after careful assessment, it concludes that there are reasonable grounds to consider that the request has not legal base under the local laws applicable of the country of the Data Importer -the laws of the country of destination- nor the applicable obligations under international law, nor based on the principles of international comity. The Data Importer will, under the same conditions, pursue possibilities of appeal.

In the event of challenging the request, the Data Importer will seek interim measures with the purpose of suspending the effects of the request until the competent judicial authority has decided over the lawfulness of such request. The Data Importer will not disclose the Personal Data requested to the requesting authority until required to do so under the applicable procedural rules. The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of the Data Importer -the laws of the country of destination- will make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authority upon request.

In the event that, despite having acted diligently, the requested Group Company is not in a position to inform the Competent Supervisory Authority, it shall, at least annually, provide the Competent Supervisory Authority with general information on the requests it has received (e.g. number of requests for disclosure, type of Personal Data requested, person making the request -to the extent possible- etc.).

In any case, the communication of Personal Data by the Group Company required by any local public authority will provide only the information that is legally required by the applicable local regulation, and cannot be disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

9.3. Applicable law and jurisdiction

9.3.1. Applicable Law

The BCRs shall be governed by Spanish law.

9.3.2. Conflicts between Data Importer and Data Exporter

Disputes arising between the Data Importer and the Data Exporter in connection with the BCRs shall be submitted for resolution to the competent court in the Data Exporter's country, unless otherwise provided by local law.

9.4 Relationship with the Supervisory Authorities

The Group Companies undertake to cooperate and assist each other, whenever necessary, in the event of any complaint from a Data Subject or the initiation of inspections or the receipt of requests or requests for information from the Supervisory Authorities, in accordance with the procedure set out in **ANNEX IV**.

They shall also cooperate with, assist and accept audits by the competent data protection authorities for the purpose of verifying compliance with the BCRs, respond diligently and appropriately to requests from the supervisory authority regarding the application or interpretation of the BCRs, cooperate with each other for this purpose where necessary and take into account the advice of the Supervisory Authorities and abide their decisions in relation to any issues related to the BCRs.

Any dispute related to the Competent Supervisory Authority exercise of supervision of compliance with the BCR will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural laws that deem applicable in such Member State. The Group Companies agree to submit themselves to the jurisdiction of such courts.

10. Non compliance of the BCRs

No International Data Transfer is made to a MAPFRE Group Company Adhered to the BCRs unless such Company is effectively bound by the BCRs and can deliver compliance with the obligations imposed by the BCRs.

If the Data Importer breaches the BCRs or it is unable to comply with the BCRs, it shall promptly inform the Data Exporter, who shall suspend the Transfer.

At the Data Exporter's choice, the Data Importer must immediately return or delete the entirety of the Personal Data that have been transferred under the BCRs in its entirety when:

- The Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under the BCRs,
- The Data Importer sustains a substantial or persistent breach of the BCRs clauses or
- Compliance with the BCRs is not restored within a reasonable time and in any event within one month of suspension.

The return or erasure of Personal Data will be extended to any copies of the Personal Data made by the Data Importer. The Data Importer shall certify, given the case, the deletion of the Personal data to the Data Exporter. Until the Personal Data is deleted or

returned, the Data Importer shall continue to ensure compliance with the BCRs. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer warrants that it will continue to ensure compliance with the BCRs and will only process the Personal Data to the extent and for as long as required under the applicable local law.

11. Responsibility

The Responsible Companies assume responsibility for compliance with the BCRs by Group Companies established outside the EEA and will monitor such compliance.

In this respect, the Responsible Companies listed below shall assume liability for any violation of the BCRs in the following cases:

- MAPFRE ASISTENCIA COMPAÑIA INTERNACIONAL DE SEGUROS Y REASEGUROS, S.A. ("**MAWDY**"): will assume responsibility for non compliance with the BCRs when the Data Exporting entity is an entity controlled[1] by MAWDY domiciled in the EEA.
- MAPFRE RE COMPAÑIA DE REASEGUROS, S.A. ("**MAPFRE RE**"): shall assume liability for non-compliance with the BCRs where the Data Exporting entity is an entity controlled by MAPFRE RE domiciled in the EEA.

Notwithstanding the foregoing, the Parent Company shall assume liability for non-compliance with the BCRs in the event that the non-compliance arises from a Group Company located in the EEA, but not controlled by MAWDY or MAPFRE RE.

As stated in paragraphs 9.3.2 and 9.4, the courts or any other judicial authorities in the EEA will be competent to enter in any case of a breach of the contents of the BCRs by Group Companies established outside the EEA to which the BCRs apply, and the

1 "**Control**" shall be presumed to exist when a company, which shall be deemed to be the parent company, is in any of the following situations in relation to another company, which shall be deemed to be a subsidiary:

a) holds a majority of the voting rights.

b) has the power to appoint or dismiss a majority of the members of the management body.

c) may dispose, by virtue of agreements concluded with third parties, of a majority of the voting rights.

d) has appointed with its votes the majority of the members of the management body who are in office at the time the consolidated accounts are to be drawn up and during the two immediately preceding financial years. In particular, this shall be presumed to be the case where the majority of the members of the board of directors of the controlled company are members of the board of directors or senior management of the parent company or of another company controlled by the latter.

affected Data Subject shall have the same rights as if the breach had occurred within the European Union. In view of the above, the Responsible Companies undertake the following commitments:

- They shall take the necessary measures to remedy breaches committed by Group Companies established outside the EEA to which the BCRs apply.
- They shall remedy and pay, where appropriate, compensation to the Data Subject for any material or immaterial damage caused by the breach of the BCRs by Group Companies established outside the EEA to which the BCRs apply, without prejudice to the possibility of passing on the amount of compensation internally, if practicable, to the Group Company located outside the EEA that caused the damage.

In this regard, the Responsible Companies acknowledge and assume that the burden of proof rests with them in respect of an alleged breach of the BCRs by Group Companies located outside the EEA, assuming that they will only be exonerated, in whole or in part, from such liability if they prove that the act giving rise to the damage is not attributable to the Group Company located outside the EEA.

12. MAPFRE Group structure and contact details

If you have any further questions, please contact our privacy office at the following address: dpo.mapfre-bcr@mapfre.com

13. Approval

This document has been approved on 23rd of April of 2024 by the Executive Committee of MAPFRE S.A.

Last Update Date April 29, 2025 (according to the MAPFRE Group BCR Modification/Update Procedure, described in ANNEX III)

ANNEX I. Territorial Scope of BCRs

The MAPFRE Group Companies will join the BCRs progressively and in phases, involving different countries and their respective entities according to the MAPFRE Group's business and strategic needs.

These BCRs will apply to International Transfers of Personal Data carried out by a MAPFRE Group Company established in an EEA country exporting Personal Data as a Controller to a MAPFRE Group Company not established in the EEA, importing the data as a Controller or Processor and to onward Transfers of Personal Data to a MAPFRE Group Companies not adhered to the BCRs or to Third Parties not part of the MAPFRE Group based on the categories of Personal Data and the Data Processing covered by the BCRs.

For any contact or query related to the MAPFRE Group's BCRs or the Group Companies Adhered to the BCRs, please contact the Corporate Data Protection Officer at the following email address: dpo.mapfre-bcr@mapfre.com

The MAPFRE Group Companies by country, which will join the BCRs in different phases, are described below:

MAPFRE GROUP COMPANIES IN EEA	
COUNTRY	**ADDRESS[2]**
SPAIN	**MAPFRE S. A.** CIF: A08055741 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid **MAPFRE ESPAÑA, S. A.** CIF: A28141935 Carretera de Pozuelo, 50 28222 Majadahonda, Madrid **MAPFRE VIDA S.A. DE SEGUROS Y REASEGUROS SOBRE LA**

[2] The reference made into brackets to ASISTENCIA and RE are related to the responsible entity for each company and that, where there is no reference into brackets, the responsible entity will be the Parent Company

MAPFRE GROUP COMPANIES IN EEA	
COUNTRY	**ADDRESS[2]**
	VIDA HUMANA CIF: A28229599 Carretera de Pozuelo, 50 28222 Majadahonda, Madrid **VERTI ASEGURADORA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.** CIF: A85078301 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid **MAPFRE RE, COMPAÑÍA DE REASEGUROS, S.A.** CIF: A78346558 Paseo de Recoletos, 25 28004, Madrid **MAPFRE GLOBAL RISKS, AGENCIA DE SUSCRIPCIÓN, S.A.U.** CIF: A28204006 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid **MAPFRE ASISTENCIA COMPAÑÍA INTERNACIONAL DE SEGUROS Y REASEGUROS, S.A. (MAWDY)** CIF: A79194148 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid **MAWDY, DIGITAL ASSISTANCE SERVICES, S.A. (MAWDY)** CIF: A79505350 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid **MAPFRE TECH, S. A.** CIF: A82178468 Carretera de Pozuelo, 52 28222 Majadahonda, Madrid
PORTUGAL	**MAPFRE SEGUROS GERAIS S.A.** Rua Doutor António Loureiro Borges, 9, Edifício Zenith – Miraflores 1495-131 Algés **MAPFRE PORTUGAL SEGUROS DE VIDA S.A.** Rua Doutor António Loureiro Borges, 9, Edifício Zenith – Miraflores 1495-131 Algés. **MAPFRE ASISTENCIA PORTUGAL (MAWDY)** Edificio Europa, Av. José Malhoa, 16 F, 7º, 1070-159 Lisbon **MAWDY SERVICES, S.A. (MAWDY)**

MAPFRE GROUP COMPANIES IN EEA	
COUNTRY	**ADDRESS[2]**
	Edificio Europa, Av. José Malhoa, 16 F, 7º, 1070-159 Lisbon **MAPFRE RE PORTUGAL (RE)** Rua Joshua Benoliel, 6 – 7º C 1250-133 Lisbon
GERMANY	**VERTI VERSICHERUNG AG** Rheinstraße 7A, 14513 Teltow **MAPFRE RE GERMANY (RE)** Alter Hof 5 80331 Munich
ITALY	**VERTI ASSICURIZIONI S.P.A.** Via A. Volta 16 20093 Cologno Monzese (MI) **MAPFRE ASISTENCIA ITALIA (MAWDY)** Strada Trossi, 66 – 13871 Verrone (BI) **MAWDY SERVICES, S.P.A. (MAWDY)** Strada Trossi, 66 – 13871 Verrone (BI) **MAPFRE RE ITALY (RE)** Vía Privata Mangili, 2 20121 Milan
MALTA	**MAPFRE MIDDLESEA P.L.C.** Middle Sea House, Triq San Publiju, Floriana FRN 1420 **MAPFRE M.S.V. LIFE P.L.C.** The Mall, Triq il – Mall, Floriana, FRN 1470 **MIDDLESEA ASSIST LIMITED (MAWDY)** 4D, Development House, Triq Sant' Anna, Floriana FRN 9010
IRELAND	**MAPFRE IRELAND ASSISTANCE (MAWDY)** Ireland Assist House 22-26 Prospect Hill, Galway **MAWDY SERVICES LIMITED (MAWDY)** Ireland Assist House 22-26 Prospect Hill, Galway

MAPFRE GROUP COMPANIES IN EEA	
COUNTRY	**ADDRESS[2]**
FRANCE	**MAPFRE RE FRANCE (RE)** Succursale de Paris 5 avenue de l´Opéra 3eme etage 75001 Paris
HUNGARY	**MAPFRE HUNGRY ASSISTANCE (MAWDY)** 1041 Budapest, István út 16. II. em.
BELGIUM	**MAPFRE RE BELGIUM (RE)** 45 Rue de Trèves P.O. Box 1 1040 Brussels

MAPFRE GROUP COMPANIES OUTSIDE EEA	
COUNTRY	**ADDRESS**
ARGENTINA	**MAPFRE ARGENTINA SEGUROS S.A.** Torre Bouchard Bouchard 547 – Piso 14 C1106ABG Buenos Aires **MAPFRE ARGENTINA SEGUROS DE VIDA S.A.** Avda. Juana Manso, 205 C 1107CBE Puerto Madero Buenos Aires **MAWDY, S.A.** Lavalle 344/346/348, PB y 3º Buenos Aires **MAPFRE RE ARGENTINA** Edificio Laminar Plaza. Pasaje Ingeniero Enrique Butty 240, piso 3º, oficina A CP 1001 CABA - Buenos Aires
BRAZIL	**MAPFRE SEGUROS GERAIS S.A.** Av. das Nações Unidas, 11.711 – Ed. MAPFRE – Brooklin – São Paulo/SP [state of São Paulo] **MAPFRE VIDA S.A.** Av. das Nações Unidas, 11.711 – Ed. MAPFRE – Brooklin – São Paulo/SP

MAPFRE GROUP COMPANIES OUTSIDE EEA	
COUNTRY	**ADDRESS**
	MAPFRE SAUDE LTDA Av. das Nações Unidas, 11.711 – Ed. MAPFRE – Brooklin – São Paulo/SP **MAPFRE RE DO BRASIL COMPAÑÍA DE REASEGUROS S.A.** Rua das Olimpiadas, 242, 5° VILA OLIMPIA SÃO PAULO – SP CEP 04551-000 **MAWDY LTDA.** Alameda Rio Negro, 503, 24º andar, Sala 2414 Bairro: Alphaville – City: Barueri- São Paulo
CHILE	**MAPFRE COMPAÑÍA DE SEGUROS GENERALES DE CHILE S.A.** Isidora Goyenechea 3520, Las Condes Santiago de Chile **MAPFRE COMPAÑIA DE SEGUROS DE VIDA DE CHILE, S.A.** Isidora Goyenechea 3520, Las Condes Santiago de Chile **MAWDY, S.A.** Av. Apoquindo 4499 – Piso 7 – Las Condes 7580575 Santiago de Chile
COLOMBIA	**MAPFRE SEGUROS GENERALES DE COLOMBIA, S.A.** Carrera, 14, nº 96-34 Santa Fé de Bogotá **MAPFRE COLOMBIA VIDA SEGUROS S.A** Carrera, 14, nº 96-34 Santa Fé de Bogotá **MAWDY, S.A.S.** Carrera, 14, nº 96-34 Santa Fé de Bogotá **MAPFRE RE COLOMBIA** Calle 72 nº 10-07 Oficina 502 Bogotá
COSTA RICA	**MAPFRE SEGUROS COSTA RICA, S.A** Torre Condal, piso 7, contiguo a Muñuz & Nanne San Pedro de Montes de Oca Province of San José
DOMINICAN REPUBLIC	**MAPFRE BHD SEGUROS, S.A.** Av. Abraham Lincoln nº 952 esq. José Amado Soler, Piantini, Santo Domingo

MAPFRE GROUP COMPANIES OUTSIDE EEA	
COUNTRY	**ADDRESS**
	MAWDY, S.A. Av. Tiradentes esq. Presidente Gonzalez – Edif. La Cumbre, 6º Piso – Ensanche NACO 10122 Santo Domingo
ECUADOR	**MAPFRE ATLAS COMPAÑÍA DE SEGUROS, S.A** Kennedy Norte, Justino Cornejo Entre Av. Fco. Orellana y Av. Luis Orrantia. Edificio Torre Atlas Guayaquil **MAWDY, S.A.** Av. 12 de Octubre y Luis Cordero Nº 24-562 – WTC Torre A Oficina 208 Quito, Ecuador
GUATEMALA	**MAPFRE SEGUROS GUATEMALA S.A.** 5a Avenida 5-55 Zona 14 Europlaza, Torre 4 Nivel 16 y PH. Guatemala City **MAWDY, S.A.** 8a Ave. 3-80 Zona 14 – Edificio La Rambla II, 5 nivel Of. 5-2, 10014, Guatemala City
MEXICO	**MAPFRE MÉXICO, S.A** Av. Revolución 507, San Pedro de los Pinos, 03800, Benito Juarez, Ciudad de México **MAWDY S.A. de C.V** Av. Revolución 507, San Pedro de los Pinos, 03800, Benito Juarez, Ciudad de México **MAPFRE RE MÉXICO** Av. Insurgentes Sur 1425 Piso 3 Insurgentes Mixcoac 03920, Benito Juarez, Ciudad de México
PANAMA	**MAPFRE PANAMÁ, S.A** Costa del Este, Edificio GMT, Panamá City **MAWDY, S.A.** Costa del Este, Torre GMT. Avenida la Rotonda, Diagonal a Business Park. Piso 1, Pánama City

MAPFRE GROUP COMPANIES OUTSIDE EEA	
COUNTRY	**ADDRESS**
PARAGUAY	**MAPFRE PARAGUAY COMPAÑÍA DE SEGUROS S.A.** Avda. Mcal López esq. Gral Aquino 910 Asunción **MAWDY, S.A.** Avda. Mariscal López 910 esquina Gral. Aquino Asunción
PERU	**MAPFRE PERÚ COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.** AV 28 de julio 873 Miraflores- Lima, Perú **MAPFRE PERU ENTIDAD PRESTADORA DE SALUD** AV 28 de julio 873 Miraflores- Lima
PUERTO RICO	**MAPFRE PAN AMERICAN INSURANCE COMPANY** Urb. Tres Monjitas Industrial 297 Avda.Carlos Chardón Hato Rey PO Box 70333, San Juan, 00936-8333 **MAPFRE LIFE INSURANCE COMPANY OF PUERTO RICO** Urb. Tres Monjitas Industrial 297 Avda.Carlos Chardón Hato Rey PO Box 70333, San Juan, 00936-8333
TURKEY	**MAPFRE SIGORTA AS** Yenişehir Mah. Irmak Cad. No:11. 34435 Salipazari Istanbul
UNITED KINGDOM	**MAPFRE RE UK (RE)** Dixon House 1st Floor 1 Lloyd's Avenue EC3N 3DQ London, UK
URUGUAY	**MAPFRE URUGUAY SEGUROS, S.A** Juncal 1385 Piso 1. Montevideo **URUGUAY ASISTENCIA, S.A. (MAWDY)** Plaza de Cagancha 1335 Of. 901 – Edificio Torre Libertad 11100 Montevideo
USA	**MAPFRE USA CORPORATION INC** 211 Main Street Webster. Massachussetts, MA 01570 **REINSURANCE MANAGAMENT INC.** 100 Campus Drive Florham Park, NJ 07932 1006 New Jersey, USA

MAPFRE GROUP COMPANIES OUTSIDE EEA	
COUNTRY	**ADDRESS**
	MAPFRE RE VERMONT CORPORATION 122 Cherry Tree Hill Road 05651 East Montpelier, Vermont

ANNEX II - Audit plan for the assessment of compliance with the BCRs in the MAPFRE Group

Audits to assess compliance with the BCRs shall be integrated into the MAPFRE Group's annual audit planning processes elaborated by the General Audit Department, and shall therefore be taken into consideration in the preparation of the Annual Internal Audit Plan, identifying and planning at all times, in coordination with the Corporate Security Division, which entities will be subject to these audits.

The management and assurance of regulatory compliance with regard to privacy and data protection in the MAPFRE Group has been approached through the following three independent lines of defence:

- The Corporate Areas, in application of the internal regulatory body on privacy and data protection, as the first line of defence.
- The Corporate Security Division, as the management, planning and execution body of the Corporate Security Function, as the second line of defence.
- MAPFRE's General Audit Department, carrying out the Group's internal audit functions, as the third and last line of defence.

The audits of the BCRs may be carried out internally or externally. In the case of external audits, the General Purchasing Standards and Procedures will be followed, wich is the contracting management process common to all MAPFRE Group Companies.

All suppliers of the MAPFRE Group must be previously approved, which enables the suppliers of goods and services to participate in the tender processes, and in the event of being awarded, to establish a commercial relationship with MAPFRE.

The contracting of the external audit service will follow the standard tender and award process. For this, a technical document will be drawn up detailing the specifications, conditions and needs of the service so that suppliers can issue their offers in the most precise way that, in any case, it must contain the criteria that will be used to carry out their technical evaluation, as well as the weight of each one of them.

These criteria may vary from one type of contract to another, but normally the knowledge, experience, proposed solution, planning, dedicated team, results in similar projects, methodology, financial offer, etc. will be taken into account. In this way, the suppliers will know at the time of making the proposals the parameters that will be evaluated in their offers.

In accordance with the MAPFRE Group's audit plan for assessing compliance with the BCRs, compliance with the MAPFRE Group's obligations in relation to the following areas will be assessed:

- The updating of the geographical and material scope of application of the BCRs.
- The binding nature of the BCRs, both internally and externally.
- The effective application of general data protection principles.

- The proper management of Data Subjects' rights.
- The acceptance by MAPFRE Group Companies established in the European Union of liability for any breach or non-compliance with the BCRs.
- Adequate compliance with the duty to inform Data Subjects.
- The proper performance of the functions attributed to privacy governance in the Group Companies Adhered to the BCRs.
- The proper functioning of complaint handling procedures.
- The proper functioning of the articulated mechanisms to ensure the verification of compliance with the BCRs.
- The correct functioning of the procedures for updating and amending BCRs.
- The adequacy of cooperation mechanisms with the competent Supervisory Authorities.
- The mechanisms for detecting and informing the competent supervisory authority of those legal requirements applicable in a third country to an institution adhering to the BCRs that may have an adverse effect on the guarantees established in the BCRs.
- The existence of appropriate training programs.

The scope of the audits, will consider the reviewing of the following aspects:

- Applications / IT systems,
- Databases that process Personal Data,
- Review of contracts with Data Processors / Controllers outside the MAPFRE Group.
- Decisions taken as a result of mandatory requirements under national laws that conflict with the BCR

Compliance with the objectives and requirements of each audit will be assessed by the MAPFRE Group's Audit General Management, determining and applying, where appropriate, the corresponding corrective actions. In addition, both the Group Company affected and the Corporate DPO and the Privacy and Data Protection Department shall be informed, so that the observed facts can be monitored and rectified,, if necessary, and reflected in the status of said entity.

In the event that the result of the audit conducted shows deficiencies in compliance with any of the aspects included in its scope, the Business Area of the Corporate Security Division will, in coordination with the Corporate Security Division, plan and implement the corresponding corrective measures that will have to be carried out in order to ensure the level of assurance offered by the BCRs.

ANNEX III. Procedure for modifying / updating the MAPFRE Group's BCRs

Due to the changing nature of large corporations and their evolution, it will periodically be necessary to amend or update the Binding Corporate Rules approved by the Supervisory Authority.

The changes made to the BCRs for this purpose must be duly registered and communicated to the Spanish Data Protection Agency so that it may be aware of them, in accordance with the procedure detailed below, depending on the nature of the changes made:

Modifications to the MAPFRE Group's BCRs

An **amendment to the BCRs** shall mean any change made to the BCRs which:

(i) affects the level of protection of the rights and freedoms of Data Subjects; or

(ii) implies an alteration in its binding nature.

(iii) is motivated to adapt the BCRs to changes in local legislation affecting the level of protection of the BCRs or the linking of Group Companies Adhered to the BCRs;

(iv) arises from changes in the corporate structure of the MAPFRE Group, in particular, in the Group's privacy and data protection governance bodies.

In any of the above cases, the area of the Group company that promotes the modification of the BCRs must inform the local Privacy and Data Protection Committee of the proposed modification, which, in turn, in accordance with the Group's internal procedures, shall forward it together with the necessary information to the Corporate Privacy and Data Protection Committee for its analysis and approval, if applicable.

Subsequently, it will be the Corporate DPO who will transfer the modifications made to the Spanish Data Protection Agency without undue delay, with a brief explanation of the reasons for the modification. Such amendments shall not enter into force, and therefore cannot be implemented, until validated by the Supervisory Authority.

MAPFRE Group BCRs Update

An **update to the BCRs** shall mean any change made to the BCRs which

(i) does not affect the level of protection of the rights and freedoms of Data Subjects; or

(ii) does not alter its binding nature.

By way of example, the modification of the list of Group Companies Adhered to the BCRs, the change in the wording of the sections or annexes of the BCRs, the clarification of their material scope or of the categories of Personal Data transfers covered, the inclusion of certain processing operations linked to the purposes already indicated, among others, shall be considered an update of the BCRs.

The Corporate DPO shall be responsible for communicating any updates to the BCRs to the Spanish Data Protection Agency on an annual basis. Likewise, in the event of receiving a request in this respect, the reasons justifying such updates must be communicated to the Spanish Data Protection Agency or to the Data Subjects.

Procedure for recording modifications and updates

The Parent Company shall keep a record of updates and amendments to the BCRs and shall have a duly updated list of Group Companies adhering to the BCRs.

This register shall be at the disposal of the Corporate DPO who shall be responsible for submitting it to the Competent Supervisory Authority when appropriate. Likewise, the Corporate DPO shall also be responsible for notifying the updating or modification of the BCRs to all Group Companies.

As regards information to the Data Subjects, such duty shall be fulfilled by publishing the updated/amended BCRs on the corporate website of the Parent Company in any case.

ANNEX IV. Procedure for Communication with the Supervisory Authority on BCRs

MAPFRE Group Companies shall respond diligently and appropriately to requests from Supervisory Authorities in relation to any matter relating to the application or interpretation of the BCRs, with the Corporate DPO taking the lead in any interaction with such authorities. Therefore, all Group Companies shall cooperate with each other when necessary in order to be able to respond as soon as possible to any request received to this effect.

Furthermore, as provided for in the BCRs, Group Companies shall cooperate with, assist and accept audits by the competent Supervisory Authorities in relation to compliance with the BCRs.

The following scenarios are envisaged in relation to the MAPFRE Group's reporting to the Supervisory Authority:

- **Communications related to updating or modifying BCRs**

  The MAPFRE Group, through the Corporate DPO, will inform the Spanish Data Protection Agency of the updates (annually) and/or modifications that may be applicable through the channels provided for such purposes.

- **Conflicts with local legislation**

  In the event of conflict or contradiction between the BCRs regulation and the applicable local regulations, the Corporate DPO shall be responsible for transferring, in the event that this is determined internally, the solution deemed most appropriate and in accordance with the GDPR to the competent supervisory authority to resolve the conflict.

  This also includes any legally binding request for disclosure of personal data submitted by a law enforcement or state security agency to a MAPFRE Group Company established outside the EEA.

- **Audit**

  In the event that the Competent Supervisory Authority deems it necessary, it may request from the Parent Company the results of the audits carried out to verify compliance with the BCRs by the Group Companies Adhered to the BCRs. Such information shall be provided in accordance with the procedure established in the Protocol of Communication with the Supervisory Authority of the MAPFRE Group.

- **Claims**

  In the event that the Data Subject lodges a complaint with the Competent Supervisory Authority regarding the correct application of the BCRs, the procedure described in the text of the BCRs shall be followed.

ANNEX V. Governing bodies: functions at the level of the BCRs

The functions of the most relevant governing bodies involved in the preparation and compliance with the BCRs in the MAPFRE Group are described below.

Corporate DPO

The Corporate DPO will be responsible for overseeing the execution and ensuring compliance with the BCRs and shall directly report to the highest management level.. In particular, it undertakes the following tasks:

- Coordinate the implementation, as well as supervise the execution and ensure compliance with the BCRs.
- Report, if required to do so, on the proper implementation of and compliance with the BCRs. The DPO can inform the highest management level if any questions or problems arise during the performance of their duties.
- Submit BCRs to the competent supervisory authority for approval and coordinate the resolution of any queries that may arise.
- Notify and/or process updates or amendments to the BCRs with the Competent Supervisory Authority.
- Notify the Supervisory Authority of any conflicts between regulations applicable in third countries and the approved BCRs, in order to promote the most appropriate solution.
- Act as the main interlocutor for cooperation with the Supervisory Authorities, when required to do so.

Corporate Privacy and Data Protection Committee

The Corporate Privacy and Data Protection Committee shall provide support to MAPFRE Group Companies, in particular in the event of changes or amendments to local legislation, which may entail an update of the BCRs. In particular, it undertakes the following tasks:

- Ensure that any BCRs compliance issues are brought to the attention of the Corporate DPO or appropriate body, and that corrective measures are determined and implemented within a reasonable timeframe.
- Provide support to MAPFRE Group Companies / Corporate DPO in cases of conflict between local regulatory compliance and BCRs compliance. In particular, in the event of changes or amendments to local legislation that may entail an update of the MAPFRE Group's BCRs.
- Assist in the resolution of possible complaints related to the implementation of the BCRs.
- Promote awareness and knowledge of the implications of BCRs among the business units; and the training of MAPFRE Group employees on BCRs and

on data protection legislation.

Local DPO / CSO Privacy and Data Protection Officer

The Local DPO / CSO Privacy and Data Protection Officer shall support the Corporate DPO and the Corporate Privacy and Data Protection Committee in those situations in which they are required by such bodies, as well as ensure the proper implementation of the BCRs in his or her entity. In particular, it undertakes the following tasks:

- Ensure effective compliance with the BCRs.
- Coordinate the implementation of the BCRs in its field of action.
- Inform and support the Corporate DPO and the Corporate Privacy and Data Protection Committee in those situations in which they are required by said bodies.
- Notify the Corporate DPO and the Corporate Privacy and Data Protection Committee of any changes in local legislation that have an impact on the BCRs.
- Respond to queries from employees, clients and other third parties regarding compliance with the BCRs.
- Promote the training of MAPFRE Group Companies´ employees in data protection matters and, specifically, ensure that they are aware of the content and binding nature of the BCRs.
- Implement the complaints handling procedure and, as appropriate, handle any Data Subjects' complaints related to the application of the BCRs.
- Facilitate, cooperate and assist in the execution of BCRs compliance audits.
- Cooperate in the dialogue with the local Supervisory Authorities.

ANNEX VI. International Data Transfers within the MAPFRE Group

Given the global scope of MAPFRE and its implementation at an international level as a Business Group, with a presence in more than 30 countries, the management of MAPFRE's business implies the possibility of carrying out International Data Transfers from the EU Companies towards all countries outside the EU.

Purpose of Processing	Data Subjects	Personal Data	Countries
Human Resources Management: To manage the Group's Human Resources tasks, including the management of the contractual relationship with employees, of candidate selection processes and of the internal international mobility of employees and candidates between the Group's Companies.	Internal and external auditors Employees Candidates Directors Representatives and administrators	Identification and contact details Professional identification and contact details Economic, financial and insurance details Employment details Transactions of goods and services Academic and professional details Data relating to personal characteristics	Origin: MAPFRE Companies in the EEA adhered to BCRs Destination: MAPFRE Companies adhered to BCRs outside of the EEA
Purchasing and supplier management: Contractual and commercial management of professionals and suppliers.	Suppliers, if they are natural persons Supplier representatives	Professional identification and contact details Economic, financial and insurance details Transactions of goods and services Employment details	Origin: MAPFRE Companies in the EEA adhered to BCRs Destination: MAPFRE Companies adhered to BCRs outside of the EEA
Management of contracting and client and stakeholder service: To provide support in the management of the subscription of certain products, as well as for the appropriate customer service through the *contact centre* and the management of social networks.	Clients Client representatives Social media users	Identification and contact data Economic, financial and insurance data Employment details Special Categories of Data Academic and professional data Data relating to transactions of goods and services Geolocation data Data relating to personal characteristics and social circumstances	Origin: MAPFRE Companies in the EEA adhered to BCRs Destination: MAPFRE Companies adhered to BCRs outside of the EEA

Purpose of Processing	Data Subjects	Personal Data	Countries
Claims and benefits management: To carry out the proper management and technical control of benefits, as well as for the management of the claim itself and the management of benefits.	Clients Client representatives Claims-related third parties	Identification and contact data Economic, financial and insurance data Employment details Special Categories of Data Academic and professional data Data relating to transactions of goods and services Geolocation data Data relating to personal characteristics and social circumstances	Origin: MAPFRE Companies in the EEA adhered to BCRs Destination: MAPFRE Companies adhered to BCRs outside of the EEA
Ancillary and internal consultancy functions: To carry out an adequate management of the services offered at corporate level.	Internal and external auditors Employees Candidates Directors Representatives and administrators Event attendees Social media users	Identification and contact details Professional identification and contact details Economic, financial and insurance details Employment details Transactions of goods and services Academic and professional details Data relating to personal characteristics	Origin: MAPFRE Companies in the EEA adhered to BCRs Destination: MAPFRE Companies adhered to BCRs outside of the EEA