POLICY ON STORAGE AND DESTRUCTION OF PERSONAL DATA

CONTENTS

1 OBJECTIVE

As per their social and legal responsibilities, MAPFRE Sigorta A.Ş. and MAPFRE Yaşam Sigorta A.Ş. ("**MAPFRE**") undertake to act in line with the regulations concerning the protection, processing and destruction of personal data. This Policy on Storage and Destruction of Personal Data ("**Policy**") binds every department at every level in MAPFRE within the context of the effective legislation, and is based on nationally accepted basic principles regarding the destruction of personal data. It lays out the framework and principles regarding the execution of the destruction works required as per the respective legislation.

In the Personal Data Protection Law ("**Law**"), Article 7, Subsection 3, it is stipulated that the "Procedures and principles regarding the deletion, removal or anonymization of personal data are laid out in regulations". A Regulation on Deletion, Removal or Anonymization of Personal Data ("**Regulation**") was prepared by the Personal Data Protection Committee ("**Committee**") as per this clause and Article 22, Subsection 1, Subclause (e) of the Law, and this was published in the Official Gazette dated 28 October 2017 and numbered 30224.

Based on the regulation above, the aim of this Policy is to designate the procedures and principles regarding the Regulation-compliant deletion, removal or anonymization of the personal data, which MAPFRE collects during its routine operations.

2 SCOPE

This Policy concerns the personal data, which belong to the personnel employed with MAPFRE, personnel candidates, visitors, the third parties we collaborate with (including but not limited to agencies and brokers) and these third parties' personnel and which are processed through the ways that are automatic in full or part or that are not automated but a part of any data recording system, and this Policy is further related to the storage and destruction of such data.

3 DEFINITIONS

Law/KVKK	Personal Data Protection Law
Committee/Institution	Personal Data Protection Committee/Personal Data Protection Institution
Personal Data	All information related to the known or identifiable natural persons.
Anonymization	The process of taking personal data to a level where they can in no way be associated with any known or identifiable natural person, even by means of matching up with other data.
Deletion of Personal Data	Deletion of personal data is the process of making personal data inaccessible and non-reusable by any means for the Related Users.

Removal of Personal Data	Removal of personal data is the process of making personal data inaccessible, non-recoverable and non-reusable by any means by any person.
Destruction of Personal Data	Deletion, removal or anonymization of personal data.
Processing of Personal Data	All kinds of data transactions such as obtaining, recording, storing, maintaining, altering, re-organizing, disclosing, transferring, taking over, making obtainable, classifying or preventing the usage of personal data through the ways that are automatic in full or part or that are not automated but a part of any data recording system.
Related Person	Owners of personal data as defined in the Personal Data Protection Law No. 6698.
Related Users	Except for the persons or units in charge of the technical storage, protection and backing up of data, the persons who process personal data within the data controller functioning or in accordance with the authorization and instruction of the data controller

4 ADMINISTRATIVE AND TECHNICAL MEASURES

As per the Regulation, this Policy must include, as a minimum, the information regarding the technical and administrative measures taken to lawfully destroy Personal Data. Therefore, the technical and administrative measures set by MAPFRE for the purpose of ensuring the processing of Personal Data in line with the Personal Data Processing principles are laid out below. Furthermore, new technical and administrative measures will be also taken as new requirements emerge in this area.

- The Board of Directors shall establish a Personal Data Committee, with the final responsibility in terms of effective compliance to the legislation regarding the protection of Personal Data falling on the Board of Directors;
- An Information Security Policy shall be prepared;
- The Internal Audit department shall periodically audit the compliance with the KVKK obligations;
- Limitations shall be set for access authorization;
- Data minimization shall be ensured;
- Data storing periods shall be determined;
- Awareness shall be created through meetings/training sessions MAPFRE is holding/will hold with all the business units;
- Personnel shall be given training regarding the matters to be taken into consideration in complying with the Law;
- MAPFRE business and operational processes shall be adjusted so that they comply with the Law;
- The cases which involve data inventory and data processing shall be determined;

- Personal Data Protection clauses shall be added to agreements signed with all third parties (primarily agencies and brokers) and personnel;
- MAPFRE website shall be ensured to provide the necessary guidance for receiving the applications of the related persons with regards to their personal data;
- Processes concerning the system security shall be improved; etc.

5 PRACTICE

MAPFRE maintains personal data only as long as the time period stipulated in the related legislation or required by the purpose of their processing. In this context, the organization firstly determines whether a limit is set in the related legislation in terms of how long personal data can be stored and, if there is a designated time period, the organization complies with such period of time. If there is no designated time period, personal data are stored as long as required by the purpose of their processing. In case the designated time period expires or the reasons requiring data processing no longer exist, personal data are deleted, removed or anonymized in line with the MAPFRE Policy unless there is a legal reason requiring that the data be further processed. All processes undertaken with regard to the deletion, removal and anonymization of personal data are recorded and such records, without prejudice to other legal liabilities, are kept for a period of minimum 3 (three) years.

Deletion of personal data

Deletion of personal data is the process of making personal data inaccessible and non-reusable by any means.

MAPFRE shall take certain technical and administrative measures so that the related business unit (related user) within its organization is prevented from processing the related personal data following the expiration of the purpose and storage time required for the processing of personal data. The related personal data will not be deleted, removed or anonymized before the expiration of the processing purposes and storage times for the other business units within MAPFRE regarding the same personal data.

If the deletion of personal data will also result in an inability to access and use other data in the system, which do not need to be deleted, such personal data shall then be deemed as deleted when they are

a) Anonymized and archived, or

b) Closed to access by any other organizations, institutions or persons and made only accessible by authorized persons by way of taking all the necessary technical and administrative measures.

Removal of personal data

Removal of personal data is the process of making personal data inaccessible, non-recoverable and non-reusable by any means by any person.

MAPFRE is liable to take any and all technical and administrative measures required for the removal of personal data.

Anonymization of personal data

Anonymization of personal data is the process of taking personal data to a level where they can in no way be associated with any known or identifiable natural person, even by means of

matching up with other data. For personal data to have been properly anonymized by MAPFRE, they should be made unable to be linked to a known or identifiable natural person even by the use of techniques such as retrieval and matching such data with other data, applicable for the recording medium and the related field of activity, by the data controller, receivers or receiver groups. MAPFRE is liable to take any and all technical and administrative measures required for the anonymization of personal data.

6 STORAGE AND DESTRUCTION TERMS

Liabilities laid out by legal regulations are taken into consideration in defining the term, during which personal data can be stored. Besides legal regulations, the purposes of processing personal data are taken into account when specifying the term of storage. In case the purpose of data processing no longer exists, data are deleted, removed or anonymized unless there is another legal reason or grounds which stipulate storing of the data.

If the purpose to process personal data no longer exists and the time periods set by the related legislation and MAPFRE have also expired, personal data can only be stored for the purposes of providing evidence in possible future legal disputes, claiming rights regarding personal data or establishing the necessary defense. For the establishment of such periods, the timeout periods for the claiming of rights and the examples specifying the demands previously addressed to MAPFRE in the same subjects despite the timeout periods having been surpassed are taken as the basis to designate the terms in which personal data can be stored. These terms are indicated in the below table. After these terms expire, personal data are deleted, removed or anonymized.

In terms of storing such personal data, if the time period stipulated in the legislation expires or if there is no time stipulated in the related legislation concerning the storing of such data, the said data are deleted, removed or anonymized by the data controller in 6-month periods.

MAPFRE chooses the most appropriate method for the deletion, removal or anonymization of personal data, unless the institution decides otherwise.

When a related person applies to MAPFRE and demands that their personal data be deleted or removed, the demand shall be evaluated according to whether the conditions that permit processing of personal data still exist. If the conditions for personal data processing disappeared in full, MAPFRE shall delete, remove or anonymize the personal data as so demanded. If such conditions have not disappeared in full, the demand shall be rejected with a statement explaining the justification of the rejection. In all cases such demands shall be concluded and reported to the related person in 30 days.

Details of Data Types	**Storage term commencement date**	**Storage term**
Personal data collected from prospective customers who have no insurance policies with MAPFRE (Offer requests)	Data processing date	2 years

Data collected during phone calls for general communication with clients	Termination of business operations with MAPFRE	2 years
Phone conversation records related to prospective clients	Date of communication	2 years
Award/drawing competitions where personal data are recorded	Date of drawing	10 years
Data collected in scope of agreements	Termination of business operations with MAPFRE	15 years
Data collected regarding Insurance Agencies, Brokers, etc.	Termination of agreement	6 years
Visiting data records taken by security officers	Data processing date	1 year
Security CCTV footage from MAPFRE buildings	Data processing date	3 months
Personal data collected from job applicants	Data processing date	1 year
Personal data from personnel, collected over the course of business relationship	Employment termination date	40 years
Data collected from non-personnel staff such as trainees, interns	Employment termination date	1 year
Personal data collected during exhibitions, non-marketing activities and training courses	Data processing date	15 years

7 RESPONSIBILITIES

The final responsibility concerning the collection or processing of Personal Data for insurance business activities, the establishment of guidelines consistent with this Policy and fulfillment of liabilities in terms of legislation and agreement lays on the MAPFRE Management Committee.
At MAPFRE, personal data processing management is based on MAPFRE's "Triple Lines of Defense" model.

First Line of Defense: All business units are responsible to take the necessary measures in their own operations to process, store and destroy personal data in line with KVKK.

Second Line of Defense: The Legal and Compliance Directorate is responsible to coordinate the KVKK compliance processes and ensure that the necessary measures are taken to process, store and destroy personal data. In addition, a Personal Data Committee has been established upon the decision of the Board of Directors to act as the data controller within the scope of the Law. The committee's principal responsibility is to monitor and coordinate the liabilities of the organization as per the Law and the related legislation and ensure the necessary measures are taken accordingly.

The Security and Environment Department is responsible to conduct the legislation-compliant operations with regards to data security.

Third Line of Defense: At MAPFRE, the Internal Audit Directorate is responsible to audit the first and second lines of defense, where efforts are made towards compliance with the KVKK legislation.

8 APPROVAL AND ENFORCEMENT

This Policy was approved by the MAPFRE Executive Committee on 18.12.2018. It will be effective and binding as of this date.