Coface Sigorta A.S.

ADMINISTRATION OF SPECIAL CATEGORIES OF PERSONAL DATA POLICY

TABLE OF CONTENTS

A. SCOPE

1. This Special Categories of Personal Data Management Policy (“the Policy”) covers all departments, employees and third parties involved in any process that processes the personal data within the structure of Coface Sigorta A.S. (“the Company”).
2. This Policy shall identify the rules of the Company for the security of the Special Categories of Personal Data and shall cover all activities that will ensure - management in this area and shall be applied in every step in order to maintain it.
3. This Policy shall not be applied about the data, which is not special categories of personal data.
4. In the case that the new legislation is established or the relevant legislation is updated in relation to the subject matter, the Company shall update its policy so as to be compatible with the relevant legislation and shall comply with the legislation requirements.
5. In the cases where the Company is convinced that there is a legal obstacle in the application of this Policy-, the Company can redetermine this Policy by consulting with the Law Department and the Top Management about the steps that it will apply, if it considers necessary.

B. DEFINITIONS

Law	Personal Data Protection Law no.6698
Regulation	Regulation on Deletion, Destruction, and Anonymization of Personal Data
Relevant Decision	Decision, dated 31.01.2018 and no 2018/10, of the Personal Data Protection Board in relation to "the Adequate Measures must be taken by the Data Controllers in the processing of the Special Categories of Personal Data".
Board	Personal Data Protection Board.
Recording environment	Name given to all kinds of environments where the personal data is processed by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system.
Personal data	Any information relating to an identified or identifiable natural person, thus allowing the identification of a person as it involves concrete contents characterizing the person’s physical, economic, cultural, social or psychological identity or is linked with any register such as ID, tax or insurance number.
Personal data processing inventory	Inventory that establishes and details the personal data processing activities which the Data Controllers carry out depending on their work processes, by correlating them with the personal data processing purposes, the data category, the receiver group to which the personal data is transferred and the data subject. The inventory, which is created and detailed by the data controllers by way of the association of the personal data processing activities that are carried out thereby with the purposes of processing of personal data, the data categories, the recipient groups and the groups of persons, being the subject matter of the data.
Special Categories of Personal Data	The Special Categories of Personal Data specified in this law is the data bearing the risk of causing discrimination about the owners in case they are processed.

Registry	Data Controllers Registry kept by the Presidency (VERBIS).
Filing system	Any recording system through which personal data are processed by structuring according to specific criteria
Data Controller	Natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system.
Recipient Group	The group of natural persons or legal entities, to whom the personal data are transferred by the data controller;
Concerned User	Any person, who processes personal data as a part of the data controller's organization or in accordance with the powers delegated and instructions placed by the data controller, except for any person or unit, who or which is responsible for the storage, protection and back-up, technically, of data;

The definitions in the Personal Data Protection Policy and the PDP Privacy Policy, Transfer of Personal Data Policy and the Data Storage and Disposal Policy established within the structure of the Company are valid also for this Policy.

C. PURPOSE AND SCOPE

This Policy shall ensure that "the Special Categories of Personal Data Processing Requirements" set forth in the Regulation issued pursuant to the article 6 of the Law are applied about the real or legal persons who are responsible and shall determine the principles required to be complied with by the Company and the third persons who are contractually authorized by the Company.

Pursuant to the Decision dated 31.01.2018 of the Personal Data Protection Board, which was published on the Official Gazette dated 07.03.2018, the Company, as a Data Controller who has the obligation to be registered in the registry, is obliged to keep the Special Categories of Personal Data under its responsibility in compliance with the personal data processing inventory, to identify the rules for the security of this data, to prepare a Policy to apply in order to maintain it by covering all activities the management of which it will ensure and to act in compliance with this Policy.

The following principles shall be valid in storing and disposing of the personal data:

a) The general principles in the article 4 of the Law shall be complied with.

b) The Company agrees that the preparation of this Policy will not mean that the personal data has been deleted, destructed or made anonymous in compliance with the Regulation, the Law and the relevant legislation alone.

c) The Company agrees, declares and commits that it will act in compliance with the security measures set forth in the Article 12 of the Law, the provisions set forth in the relevant legislation, the decisions to be taken by the Personal Data Protection Board, the Administrative and Technical Measures set forth in the Data Security Guide and the Policy while storing, destructing or making anonymous the personal data.

d) The Company commits that it will ensure compliance with the tools, programs and processed to be applied depending on this Policy during deleting, destructing or making anonymous the personal data processes by the methods which are wholly or partially automatic or by the methods which are not automatic, provided that they will be a part of any recording system.

D. RECORDING ENVIRONMENTS

The Company agrees, with this Policy, to include the personal data in the environments including personal data and listed below and in the other environments that might arise in addition to these into the scope of the Policy.

a) Computers/servers used in the name of the Company
b) Network devices,
c) Shared/non-shared disc drivers used for storing data on the network,
d) Mobile phones and all storage areas inside them,
e) Paper,
f) Micro voucher,
g) Peripherals such as printer, finger print reader,
h) Magnetic tapes,
i) Optic discs,
j) Flash memories.

E. SPECIAL CATEGORIES OF PERSONAL DATA

a. General Principles for the Special Categories of Personal Data Processing

The Company takes all kinds of technical and administrative measures in relation to the storage of the personal data in a safe manner and the prevention of the processing and achievement of the personal data in contrary to the law.

The Company commits that it will not process the personal data in contrary to the format specified in the Law.

As long as there are no exemptions for the processing of special categories of personal data in Article 6 § 3 of the Law;

a) It is forbidden for the Company to keep the special categories of personal data without obtaining the explicit consent of the data subject except for the exceptions specified in the Law
b) It is prohibited to process sensitive personal data without obtaining the explicit consent of the data subject except for the exceptions specified in the Law.
c) In the cases where the Company keeps the special quality personal data, the Company processes the personal data if the explicit consent is obtained within the knowledge of the Company's Law Department and the Company PDPL Committee by adhering to the legislation related to the data.

b. Special Categories of Personal Data Processed by the Company

Special categories of personal data, other than personal data relating to health and sexual life, relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, foundation or union membership, criminal conviction and security measures, and biometric and genetic data may be processed without obtaining the explicit consent of the data subject if processing is permitted by any law.

Personal data relating to health and sexual life may only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations.

Personal data is processed via the explicit consent obtained from the data subject within the structure of the Company and this data is processed only within the framework of the controls specified in the **"General Principles for the Processing of the Special Categories of Personal Data"** section of this Policy. Personal data varies and differentiates depending on the type and quality of the relation between the Company and the data subject, communication channels used and mentioned purpose information. This data is specified in the Personal Data Processing Inventory.

c. Processing Purposes of the Special Categories of Personal Data

Personal data can be processed within the scope of the purposes specified in the Personal Data Processing Inventory and can be stored as long as these purposes and the relevant legal periods stipulate.

d. Transfer of the Special Categories of Personal Data

The Company makes domestic and foreign data transfer within the framework of the purposes exemplified in the "**Processing Purposes of the Special Categories of Personal Data**" section of this Policy and pursuant to the Articles 8 and 9 of the PDPL and the personal data can be processed and stored in the server and electronic environments used within this scope. The parties to which the data transfer is made and the purposes of the data transfer are specified in detail in the Personal Data Processing Inventory prepared by the Company. The quality of these transfers made and the parties with whom the personal data is shared vary depending on the type and quality of the relation between the Data Subject and the Company, the purpose of the transfer and the relevant legal basis and within this scope, the measures identified in the PDP Privacy Policy by the Company, the application principles and procedures and the actions to be taken within this framework are valid.

If the Company will transfer the Special Categories of Personal Data pursuant to the Decision dated 31.01.2018 of the Personal Data Protection Board, which was published on the Official Gazette dated 07.03.2018;

- If the data is required to be transferred by e-mail, it is transferred with the encrypted corporate e-mail address or by using the registered email (KEP) account.
- If the data is required to be transferred by environments such as portable flash memory, CD, DVD, it should be encoded by cryptographic methods and the cryptographic key is kept in a different environment.
- The transfer is made between the servers in different physical environments, the data transfer is made by establishing VPN between the servers or by the SFTP method.
- If the data is required to be transfer via paper environment, necessary precautions should be taken against risks such as theft, loss of documents or unauthorized viewing and the documentation is sent in the form of confidentiality documents .

e. Elimination of the Data Processing Requirements

The Company is responsible for the up-to-dateness of the Special Categories of Personal Data processing requirements and it shares this responsibility with all of its employees.

In the cases where the data processing requirements are eliminated, the employees may not continue to process data. The Company is obliged to eliminate the environments where the requirements have been eliminated in compliance with this Policy upon the request of the relevant work units or the PDPL Committee/Working Group.

The Company agrees that the Special Categories of Personal Data processing requirements are eliminated in the relevant cases which are listed below as examples and which are specified also in the Regulation:

a) The purpose requiring the processing of the personal data is eliminated,
b) The processing of the personal data is contrary to the law or honesty rule,
c) In cases where the processing of the personal data is performed only based on the explicit consent requirements, the relevant person withdraws his consent.

Within this scope, the measures identified in the Personal Data Storage and Disposal Policy by the Company, the application principles and procedures and the actions to be taken within this framework are valid.

f. Security of the Special Categories of Personal Data

In the processing of the special categories of personal data, it is also necessary for the adequate measures determined by the Board. They were determined as follows pursuant to the Decision dated 31.01.2018 of the Personal Data Protection Board, which was published on the Official Gazette dated 07.03.2018.

- The employees involved in the processes in which the Special Categories of Personal Data is processed are regularly given training on the special categories of personal data security with the Law, the sub-legislation and all kinds of decisions and guides that the Board will publish, The confidentiality agreements are made between the mentioned employees and the Data Controllers,
- The authorization scope and duration of the users having the authorization to access to the data are clearly identified,
- The authorization controls are made periodically,
- The authorizations of the employees whose duty has been changed or who has quitted the job should be immediately removed and within this scope, the inventory that was allocated to him by the Data Controller should be taken back. In this case, the compliance of the Company with the principles established in accordance with the procedure regarding the update of the approved inventory is valid.

If the environments where the Special Categories of Personal Data is processed, maintained and/or accessed are electronic environment;

- The data is maintained by using cryptographic methods,
- The cryptographic keys are kept in safe and different environments,
- The audit trails of all actions and process records performed on the data are kept and the security of the mentioned audit trails is ensured,
- The security updates of the environments where the data is available are continuously followed up and it is ensured that the necessary security tests are regularly performed/had performed, the test results are recorded and the action plans regarding the findings are created,
- If the data is achieved via any software, it is ensured that the user authorizations suitable for this software are made, the security tests of this software are regularly performed/had performed, the test results are recorded and the action plans regarding the findings are created,
- If remote access to the data is necessary, at least two-grade identity verification system is provided.

If the environments where the Special Categories of Personal Data is processed, maintained and/or accessed are physical environment:

- It is ensured that the adequate security measures (against electricity leakage, fire, flood, theft and similar situations) have been taken according to the quality of the environment where the Special Categories of Personal Data is available,
- The physical security of these environments is ensured to prevent unauthorized entries and exits.

F. POLICY ENFORCEMENT AND UPDATES

This Policy shall come into force on the date when it is approved by the Board of Directors of the Company. The amendments to be made in the policy and the works necessary for putting these amendments into force shall be carried out by the Law, Audit and PDPL Working Group and the amendments shall come into force after the approval of the Board of Directors of the Company.

However, the Company reserves its right to review this Policy in line with the amendments in the legislation, the change in a technical standard referred to, the processes of and/or the decisions to be taken by the Personal Data Protection Board and the court decisions and to update, amend or abolish the Policy and to establish a new Policy in the necessary cases.

The Company shall share the updated Policy with its employees by e-mail and submit it to the access of its employees over the corporate intranet in such a manner that the amendments that the Company made on the Policy can be examined.

The Policy is reviewed and updated ordinarily once a year. The authorization to take decision regarding the abolishment of the Policy belongs to the Board of Directors of the Company.

G. ENFORCEMENT DATE OF THE POLICY

This Policy came into force on DATE.