POLICY

PERSONAL DATA RETENTION, PROCESSING and DESTRUCTION POLICY

PT.HM.02

04.12.2020

Revision No: 00

Owner : UW, Sales, Legal and Reinsurance Assistant General Manager

---

Validation : Board of Directors

LAST EDITED		
Rev. No	**Date of Revision**	**Revision Details**
00	04.12.2020	• The definition of the Data Governance Committee created with the Data Governance Project has been added. • Our 15-year retention period determined by the management has been revised in Article 6.9 in order to be compatible after Verbis entries. • The governance structure for the protection of personal data, the roles and responsibilities of the data governance organization are included in Article 6.10. •In agreement with IT, the environments have been simplified and converted to a more general version in Article 6.3.

1.0 OBJECTIVE

This Personal Data Retention, Processing and Destruction Policy (**"Policy"**) is drafted and entered into force for non-disclosure of all Personal Data (see definitions below) and in order to comply with the Personal Data Protection Law no. 6698 (hereinafter referred to as **"PDPL"**) effective in Turkey and secondary legislation drafted based thereon and decision taken by the Personal Data Protection Board (collectively referred to as **"Data Protection Legislation"** in this document.) during the course of business and operations related to personal data processing, retention and destruction activities which are being conducted by Aksigorta Anonim Şirketi ("**Aksigorta**") and/or its behalf.

2.0 SCOPE

This Policy is drafted to regulate personal data processing activities which are performed on personal data, wholly or partially by automated means or non-automated means form part of a data filing system by Aksigorta and/or on its behalf related to all natural persons and applies to anyone engaged in personal data processing activities on behalf of Aksigorta.

3.0 REFERENCES AND ANNEXES

YK.HM.07. Aksigorta Personal Data Protection and Processing Regulation

PR.HM.10 Aksigorta Security Incident Response Procedure

PR.HM.11 Aksigorta Application Response Policy Procedure

Annex-1 Personal Data Protection Privacy Notice

Annex-2 Data Privacy Notice to Suppliers

Annex-3 Privacy Notice Regarding Processing of Personal Data of Aksigorta Employees and Aksigorta Employee Personal Data Protection and Processing Explicit Consent

Annex-4 Personal Data Privacy Commitment

Turkish Code of Obligations No. 6098

Social Insurance and General Health Insurance Law No. 5510

Law on Regulation of Publications on The Internet and Combating Crimes Committed by Means of Such Publications No.5651

Occupational Health and Safety Law No. 6361

Catastrophe Insurance Law No. 6305

Commercial Code No. 6102

Labor Law No. 4857

Highway Code No. 2918

Law on Consumer Protection No. 6502

Regulation on Health and Safety Measures to Be Taken in Workplace Buildings and Integral Parts

4.0 DEFINITIONS

The following terms set out in this Policy have the meanings as follows:

Agent: A real person that maintains a contractual relationship with Aksigorta and acquires to engage in and conduct insurance contracts on behalf of on a permanent basis at a certain place or within a

certain region as a profession and who carries out the preparatory works before the conclusion of the contract and assists for the application of contract and payment of indemnity.

Explicit Consent: Consent to a specific matter, based on informing and given by free will.

Brokerage: A real person that assists in the implementation of the contract and carries out the preparatory works before the conclusion of the contract or assists for the application of contract and collection of indemnity, by representing those who wish to conduct an insurance or reinsurance contract and acting in a completely impartial and independent manner in the selection of insurance companies with which these contracts are to be made and taking into account the rights and interests of persons seeking insurance coverage.

Data Governance: is a set of methods that enable end-to-end management of data within the organization. Data Governance aims to ensure accurate, consistent and timely decision-making by including policies, processes, standards, technologies and people.

Data Governance Committee: The Data Governance Committee was established to effectively manage Aksigorta's growing data ecosystem. The Committee consists of Information Technology teams and core members from the Compliance department. It includes different members from business units of which teams managing data within the scope of business processes. The Committee aims to create a data-driven culture that maximizes data value, reduces costs, improves security and quality, and reduces risk. It constructs the data life-cycle process, defines appropriate strategies to support and improve data quality, and aims to ensure that data is complete and valid to support analytics. It monitors the security of Aksigorta data in accordance with the relevant legal regulations and policies.

Employee: Real persons employed at Aksigorta based on an employment agreement.

Prospective Employee: Real persons that have made their Curriculum Vitae and relevant information accessible to Aksigorta either by a Job Application or by other means.

Personal Data: It means any information related to the data subject, such as name, address, phone number, e-mail address or similar credentials.

Personal Data Processing: Any kind of transaction made as regards Data such as; manual collection, record keeping, storage, preservation, amendment, re-arrangement, disclosure, transfer, take-over, transformation to acquirable state, categorization or prevention to the usage of Personal Data, provided that Personal Data are parts of a Data Record System that is wholly or partially automatic.

Client/ Prospective Client: Real persons whose personal data is obtained due to business relationships within the scope of activities carried out by Aksigorta, regardless of whether there is any contractual relationship.

Special Categories Of Personal Data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data.

Third Persons: Other real persons including but not limited to the supplier, the injured party, family members, etc. whose personal data is processed within the scope of this Policy, despite not being defined herein**.**

Data Processor: A real person or legal entity that processes personal data by the authority granted by the data controller on behalf of the data controller.

Data Subject or Relevant Person: An identified or identifiable real person to whom the data belongs.

Visitors: Real persons entered into the physical facilities of Aksigorta for various reasons or real persons that visited the website of Aksigorta.

5.0 RESPONSIBILITIES AND DISTRIBUTIONS OF TASK

All business units, employees, persons engaged in data processing activities on behalf of Aksigorta support the implementation of technical and administrative measures set out in this Policy and Aksigorta Regulation on Personal Data Protection and Processing, aimed at ensuring data security in all data processing media, ensuring the lawful processing of personal data with continuous supervision, such as training and awareness of persons, employees, agents, business partners engaged in data processing activities, and working in cooperation with responsible units.

The matters for which those involved in the personal data retention and destruction process are responsible are as follows.

a) It is the responsibility of the Data Governance Committee to review and approve this Policy and all revisions and amendments made to this Policy. The Data Governance Committee is also responsible for developing the Policy and providing the necessary training and guidance to those who process data on behalf of Aksigorta on the interpretation of the Policy. The Data Governance Committee also audits compliance with this Policy and provides the necessary support to comply.
b) Data Governance Committee is responsible for controlling the periodic destruction processes set out in article 6.9., maintaining the specified data during the relevant storage periods, supervision of these periods, and destruction of the data of which storage period has expired.
c) The periodic destruction process of Aksigorta, of which supervision is the responsibility of the Data Governance Committee, has been determined as 6 months. The task of the Corporate Legal and Compliance Department is to examine, approve the Policy and all changes made to the Policy, and to provide legal advice in line with the Data Protection Legislation.
d) With the support of the CEO and the Corporate Legal and Compliance Department, the task that it will carry out is to examine and approve requests for deviations and exceptions from the Policy.

6.0 AKSİGORTA PERSONAL DATA RETENTION AND PROCESSING ACTIVITIES

The personal data of relevant persons, Personal Data of which details are stated in Aksigorta Regulation on Personal Data Protection and Processing are collected, processed and retained and destructed during business activities pursuant to procedures stipulated in Aksigorta Regulation on Personal Data Protection and Processing.

In this context, detailed descriptions of retention and destruction are given below.

6.1 EXPLANATIONS ON RETENTION

The concept of “processing of personal data” is defined under Article 3 of the PDPL, the requirement of "being related, limited and extended to the purpose and stored for the period stipulated in the relevant legislation or required for the purpose for which they are processed” for the personal data is stated under Article 4 of the PDPL, “conditions for processing personal data” are listed under Article 5 and 6.

Accordingly, personal data is in accordance with the relevant legislation or processing purposes within the framework of Aksigorta business activities and 6.9 of this policy. it is stored for the periods specified in the article.

6.1.1 Legal Basis for Retention

Aksigorta stores personal data processed within the framework of business activities in accordance with the periods stipulated in the relevant legislation. In this context, as per the following, personal data;

- Turkish Code of Obligations No. 6098
- Social Insurance and General Health Insurance Law No. 5510
- Law on Regulation of Publications On The Internet And Combating Crimes Committed By Means Of Such Publications No. 5651
- Occupational Health and Safety Law No. 6361
- Catastrophe Insurance Law No. 6305
- Commercial Code No. 6102
- Labor Law No. 4857
- Highway Code No. 2918
- Law on Consumer Protection No. 6502
- Regulation on Health and Safety Measures to Be Taken In Workplace Buildings And Integral Parts

including but not limited to secondary regulations in force, personal data is retained and processed during the retention periods stipulated in accordance with the legislation and administrative regulations that Aksigorta shall comply with.

6.1.2 Processing Purposes Requiring Retention

Personal data is retained for the purposes detailed in Aksigorta Regulation on Personal Data Protection and Processing and listed below:

- Ensuring the security of the institution,
- Ability to conduct statistical studies,
- Execution of advertising and campaign processes,
- Execution of sales and marketing processes,
- Execution of human resources processes,
- Execution of processes related to supporting service providers within the scope of performing works and transactions within the scope of signed insurance agreements, calculation of insurance compensation, making payments and recourse follow-up to the insured and beneficiary,
- Conducting transactions related to the collection of premium payments,
- Execution of processes related to suppliers,
- Execution of related processes within the scope of agency application and agency agreements,
- Creating policy proposals, organizing policies, submitting policy renewal proposals and performing policy cancellation operations,
- Providing contact with real/legal persons who have business relations with Aksigorta,
- Execution of finance and accounting works,
- Drafting legal reports,
- Managing processes related to call centers,
- Managing risk assessment processes,
- The burden of proof in future legal disputes,

- Conclusion of an insurance agreement and conclusion of agreements between real person brokers, agents and actuaries and Aksigorta, which are affiliated with in order to provide the necessary services in case of damage, and mutual performance of services,
- Providing assistance services,
- Conducting communication activities,
- Calculation of insurance compensation, payment to the insured or beneficiary and application follow-up,
- Following-up of uncertain damage files,
- Preparation of damage file and settlement of payment as a result of damage,
- Drafting claims adjusters' and appraisal reports and following-up claims adjuster's performance,
- Execution of reinsurance and coinsurance processes,
- Making recourse claims to insurance companies and third parties and following-up these claims,
- Assessment and response of recourse claims submitted by insurance companies and third parties,
- Drafting and following-up of visitor records,
- Evaluation of customer requests and complaints,
- Conducting customer satisfaction surveys and interviews,
- Execution of marketing, advertising and campaign processes,
- Execution and follow-up of legal works and transactions,
- Providing information to authorized institutions and organizations in accordance with the obligations arising out of the relevant legislation,
- Planning and conducting internal audit activities necessary to ensure that the activities are carried out in accordance with Aksigorta procedures and relevant legislation,
- Realization of processes arising out of company law,

Managing risk assessment processes in accordance with Insurance Legislation.

6.2 REASONS FOR DESTRUCTION

In case of;

- Amendment in or abolishment of the provisions of the relevant legislation that are the basis for its processing,
- Elimination of purpose that requires processing or retention,
- The relevant person withdraws his/her explicit consent, if the processing of personal data occurs only based on explicit consent,
- According to Article 11 of the Law, Aksigorta accepts his/her application for the deletion and destruction of his/her personal data within the framework of the rights of the relevant person,
- A complaint is filed before the Personal Data Protection Board and this request is approved by the Personal Data Protection Board, if Aksigorta rejects the application of the relevant person regarding his/her request for deletion, destruction, or anonymization of personal data, Aksigorta's response is inadequate or no answer is given within the stipulated period under the PDPL;
- In cases where the maximum period requiring the retention of personal data has expired and there are no conditions that justify the retention of personal data for a longer period of time,

the personal data is deleted, destroyed or anonymized by Aksigorta ex-officio or upon the request of the relevant person.

6.3 RECORDING ENVIRONMENTS

Personal data is stored by Aksigorta in accordance with the law and securely in the media listed in Table 1.

Table 1: Personal data storage media

Electronic media	Non-electronic media
a) Insurance applications software (a) OLTP system (b) DWH (c) CRM (d) Data Science Applications (e) Big Data b) Data storage areas 1. Database 2. Document management system 3. Mail media 4. File Server - Shared folder	(1) Data storage areas Manual data recording media (a) Forms, (b) Documents

6.4 PERSONAL DAYA PROCESSING CONDITIONS

In order for personal data to be processed and used in accordance with this policy and the Aksigorta Regulation on Personal Data Protection and Processing, it is necessary to **inform** about the processing activities of the Data Subject, request permission for the processing of personal data, and **obtain the explicit consent** of the Data Subject.

For this purpose, consent forms and privacy notices approved by the Corporate Legal and Compliance Department shall be used.

However**, if one of the exceptions listed below is involved, the requirement to** obtain explicit consent from the Data Subject **shall not be applied**:

a) It is expressly provided for by the laws.

b) It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.

c) The processing of personal data belonging to the parties to the contract is necessary, provided that it is directly related to the establishment or execution of the contract.

d) It is necessary for compliance with a legal obligation to which the data controller is subject.

e) Personal data have been made public by the relevant person himself/herself.

f) Data processing is necessary for the establishment, exercise, or protection of any right.

g) Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

6.4.1 Obligation to Inform of Aksigorta As Data Controller

As stated in Article 6.4 of this Policy, even though the Data Controller is not always required to obtain explicit consent from the Data Subject for the processing of personal data, Aksigorta is always obliged to provide information to the Data Subjects on the following issues:

- The identity of the Data Controller and its representative, if any,
- the purpose of the processing personal data,
- To whom and for what purpose the processed personal data may be transferred,
- The method and legal basis of the collection of personal data,
- Other rights of the Data Subject listed in Article 6.6 of this Policy.

Obligation to inform can be fulfilled by using the Annex-1 Personal Data Protection Privacy Notice.

From time to time, Aksigorta may need the personal data of its suppliers' officials for the purposes of conducting business processes and providing communication. In this case, it is possible for the relevant Aksigorta officials to send Annex-2 Data Privacy Notice to Suppliers in order to ensure that Aksigorta's obligation to inform is fulfilled against the said supplier employees.

6.4.2 Rules to Be Followed in The Processing of Special Category Data

Unless it is required for the purpose to exercise certain rights and fulfill certain obligations arising out of labor laws and legislation and except the cases which are allowed or authorized as authorized in accordance with the applicable miscellaneous legislation, Data Protection Legislation in particular, before processing special categories of personal data, explicit permission and consent of the relevant person shall be necessarily and always obtained.

6.4.3 Rules for Processing Personal Data of Employees

In order for personal data, including Special Categories of Personal Data belonging to employees, to be processed in accordance with the Labor Law and other relevant legislation or for other purposes determined by Aksigorta, the obligation to inform and obtain explicit consent must be fulfilled by having the persons currently employed by Aksigorta sign the Annex-3 Privacy Notice Regarding Processing Of Personal Data Of Aksigorta Employees and Aksigorta A.Ş Employee Personal Data Protection and Processing Explicit Consent.

6.4.4 Principles to Be Followed in The Processing And Use Of Personal Data Belonging To Clients For Marketing Purposes

In order to collect and process clients' personal data for the purpose of marketing directly or indirectly, the Data Subject client's explicit consent shall be obtained prior to the collection of personal data. In addition, the opportunity to withdraw the consent for commercial communication shall be provided to Data Subjects both during the consent to be received and in each communication.

6.4.5 Issues That Employees Who Process Personal Data as Part of Their Duties Are Expected to Pay Special Attention

People who process personal data on behalf of Aksigorta as part of their duties and during the performance of their duties are expected to adhere to the following as well as the items set out in the Policy:

- Personal Data must be processed in accordance with Data Protection Legislation, by legitimate means and fairly.
- Personal Data must only be processed for permitted and disclosed legal purposes.
- For a purpose that is not disclosed to the Data Subject or that is illegitimate, it is absolutely necessary not to process and retain data.

- Personal Data must be adequate for the purpose of processing, related and linked to this purpose, and not in excessive amounts or numbers compared to the purpose of processing.
- Personal Data must be true and accurate and updated as needed.

Personal Data processed and used for any purpose should not be kept or retained for longer than the period required for that purpose.

6.4.6 Rules That Employees Who Process Special Category Data as Part of Their Duties Must Follow

Employees who process Special Category Data on behalf of Aksigorta as part of their duties and during the performance of their duties, are required to sign Annex-4 Data Privacy Commitment in accordance with Data Protection Legislation along with adhering to the other articles of this Policy and the items mentioned in Article 6.4.

6.4.7 Rules to Be Followed When Transferring Personal Data

Cross border transfer of personal data may be performed without the express consent of the relevant person only if one of the exceptions mentioned in Article 6.4 applies. For cross border transfer of Personal Data, the conditions set out under the Data Protection Legislation must be met and, if necessary, the explicit permission and consent of the relevant person must be obtained. In this context:

a) Personal Data will not be transferred to any third party except under the conditions set out in accordance with the Data Protection Legislation.

b) Personal Data will not be transferred to a country other than 'Countries Where There is Sufficient Protection', which will be determined and announced by the Personal Data Protection Board, unless the Relevant Person has given explicit consent.

c) Personal Data may only be transferred to a country other than 'Countries Where There is Sufficient Protection' if and only if the relevant Data Subject has given explicit permission and consent to this transfer.

6.5 TECHNICAL AND ADMINISTIRATIVE MEASURES

Technical and administrative measures are adopted by Aksigorta for the retention of personal data in a secure manner, prevention of unlawful processing of and access to them and destruction of personal data in accordance with the law, under the scope of the adequate measures defined and proclaimed under the Personal Data Protection Law and by the Personal Data Protection Board.

6.5.1 Technical Measures

Technical measures taken concerning the personal data being processed by Aksigorta are listed below:

- Network security and application security are provided.
- A closed system network is used for personal data transfers through the network.
- Key management is implemented.
- Security measures within the scope of procurement, development and maintenance of information technology systems are adopted.
- The security of personal data stored in the cloud is ensured.
- Access logs are kept regularly.
- Data masking measures are applied when necessary.
- Up-to-date antivirus systems are used.
- Firewalls are used.

- User account management and authority control system are implemented, and they are followed up.
- Log records are kept without user intervention.
- Current risks and threats have been identified.
- If special categories of personal data are to be sent via e-mail, they are definitely sent as encrypted and by using a KEP or corporate mail account.
- Up-to-date encryption/cryptographic keys are used and managed by different departments for special categories of personal data.
- Intrusion detection and prevention systems are used.
- Infiltration test is performed.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is performed.
- If remote access to data is required, a two-stage authentication mechanism is used.
- While data is transferred between servers in different physical environments, data transfer is carried out by setting up a VPN between servers or by the sFTP method.
- Personal data of special categories that are transferred from portable memory, CD, DVD media are transferred with encryption.
- Data loss prevention software is used.
- Data classification software is used.

6.5.2 Administrative Measures

Administrative measures taken regarding the personal data being processed by Aksigorta are listed below:

- There are disciplinary regulations for employees that include data security provisions.
- Training and awareness activities on data security are carried out for employees at regular intervals.
- An authorization matrix for employees has been created.
- Non-disclosure commitments are made.
- The authorizations of employees whose duties have changed or who left their jobs in this field are cancelled.
- The agreements that are executed include data security provisions.
- Additional security measures are taken for personal data transferred via paper, and the relevant documents are sent in the format of a document with a degree of confidentiality.
- Personal data security policies and procedures are established.
- Personal data security issues are quickly reported.
- Personal data security is monitored.
- Necessary security measures are taken regarding entries to and exits from physical environments containing personal data.
- The security of physical environments that contain personal data against external risks (fire,flood, etc.) is ensured.
- Environments containing personal data are secured.
- Personal data is reduced as much as possible.
- Personal data is backed up and the security of the backed up personal data is also ensured.
- Periodic and / or random internal audits are carried out and procured.
- Current risks and threats have been identified.

- Protocols and procedures for special quality personal data security are established and implemented.
- Data processing service providers are periodically audited regarding data security.

The awareness of data processing service providers regarding data security is ensured.

6.6 RIGHTS OF DATA SUBJECTS

Data subjects whose personal data is being processed by Aksigorta may apply to Aksigorta and submit requests related to him/her, with respect to the below mentioned matters.

a) To learn whether personal data is processed or not,

b) To request information about personal data if it is being processed,

c) To learn the purpose of personal data processing and whether they are used in accordance with their purpose,

d) To learn the third parties to which personal data is transferred (domestic or cross border transfer),

e) To request their personal data to be corrected if they are incomplete or incorrectly processed,

f) Request the deletion or destruction of personal data in accordance with the conditions set out in the Data Protection Legislation,

g) Request that actions made under paragraphs (e) and (f) be notified to third parties to whom personal data is transferred,

h) To object a consequence unfavorable for him as a result of the analysis of the data being processed exclusively via automated systems,

i) To claim damages and request compensation if she/he incurs damages due to unlawful personal data processing.

In cases where Personal Data is collected directly as part of efforts in marketing, the Data Subject may object to the transfer to third parties or the use with marketing purposes of the Personal Data that belongs to him or to request to be informed before that Personal Data is given to third parties or used with marketing purposes.

The evaluation of and response to these applications of the relevant persons should be carried out as referred to Aksigorta Application Response Policy.

6.7 SECURITY CONDITIONS

Aksigorta takes all reasonable security measures, including the following, to protect Personal Data against accidental or unlawful destruction, loss, falsification, unauthorized disclosure or unauthorized access risks (Security Incident).

- Limiting access to Personal Data only to people who are required to access this information during the performance of their duties.
- If appropriate, using password-protected electronic files.
- Regularly storing files containing Personal Data and restricting physical access to these files as necessary and appropriate.
- Immediately notifying the supervisor and information security when the employee becomes aware of events and situations such as unauthorized access to Personal Data or improper use of Personal Data.

- Obtaining explicit consent from the relevant data subject and fulfilling the obligation to inform in accordance with Data Protection Legislation before using Personal Data for a purpose other than its initial stated purpose.

The security conditions and technical measures taken to protect Personal Data are periodically reviewed and evaluated by the Data Governance Committee. In this way, it is determined whether additional security measures or procedures are needed to protect personal data.

In the event of the occurrence of any Security Incident, the steps to be followed by Aksigorta are specified in the 'Cyber Security Incident Response Plan' included in the PR BT 12 Incident Management Procedure annex.

6.8 PERSONAL DATA DESTRUCTION TECHNIQUES

At the end of the period set out in the relevant legislation or the retention period required for the purpose for which they are processed, personal data is destroyed by Aksigorta in accordance with the provisions of the relevant legislation ex-officio (periodic destruction periods) or at the request of the relevant person.

6.8.1 Deletion of Personal Data

Personal data is deleted using the methods given in Table-1.

Table 1: Deletion of Personal Data

Data Recording Environment	**Explanation**
Personal Data Contained In Systems	For those among the personal data contained in systems, whose period within which they are required to be retained has expired, the deletion is performed by the removal of the access permission of the relevant users by the system administrator.
Personal Data Contained In Electronic Media	Those among the personal data contained in electronic media, whose period within which they are required to be retained has expired, are rendered completely inaccessible and unreusable for other relevant users, except for the database administrator.
Personal Data Contained In Physical Environment	Those among the personal data contained in physical environment, whose period within which they are required to be retained has expired, are rendered completely inaccessible and unreusable for other relevant users. In addition, the obscuration process is also applied by crossing out/painting/erasing so that it cannot be read.
Personal Data Contained In Portable Media	Those among the personal data contained in stored in Flash-based storage environments, whose period within which they are required to be retained has expired, is stored in secure environments with encryption keys, by the encryption carried out by the system administrator and authorization of the system administrator to access them.

6.8.2 Destruction of Personal Data

Table 2: Destruction of Personal Data

Personal Data Contained In Physical Environment	Those among the personal data contained on paper, whose period within which they are required to be retained has expired, are irrevocably destroyed by paper shredders.
Personal Data Contained In Optical / Magnetic Media	The process of physical destruction, such as melting, burning or pulverizing, is applied to those among the personal data contained in optical media and magnetic media, whose period within which they are required to be retained has expired. In addition, the data is rendered unreadable by passing magnetic media through a special device and exposing it to a high-value magnetic field.

6.8.3 Anonymization of Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person under any circumstances, even if it is paired with other data. In order for personal data to be anonymized; personal data must be rendered impossible to associate with an identified or identifiable natural person even with the use of techniques appropriate in regards to the storage media and the relevant field of activity such as the retracing of data by the data controller or third persons and/or by matching the data with other.

Anonymization is carried out systematically and within certain rule sets with the technological tool obtained within the scope of technical measures.

6.9 STORAGE AND DESTRUCTION PERIODS BY DATA TYPES

The Data Governance Committee is responsible for storing the data mentioned in the table below during the relevant storage periods.

The period of periodic destruction concerning Aksigorta, for which the Data Governance Committee is responsible for monitoring, has been set as 6 months. The Data Governance Committee is responsible and authorized, concerning the performance of destruction in accordance with these periods and making the reminders necessary for the destruction of personal data whose period of storage has expired.

Table 3: Personal data retention and destruction periods

DATA TYPE	STORAGE PERIOD	DESTRUCTION PERIOD
Customer Records	**For 15 years following the termination of the contractual relationship**	At the first periodic destruction period after the end of the retention period
Employee Records	**For 15 years following their leave from work**	At the first periodic destruction period after the end of the retention period
Personal and Judicial Record Information of Employees	**For 10 years following their leave from work**	At the first periodic destruction period after the end of the retention period
Records of Prospective Employees	**For 2 years following the application**	At the first periodic destruction period after the end of the retention period

Records Regarding Business Partners and Employees	**For 15 years following the termination of the business relationship**	At the first periodic destruction period after the end of the retention period
Accounting and Finance Records	**15 years**	At the first periodic destruction period after the end of the retention period
Internal Documents and Records	**15 years**	At the first periodic destruction period after the end of the retention period
Audio and Video Recordings	**6 months**	At the first periodic destruction period after the end of the retention period

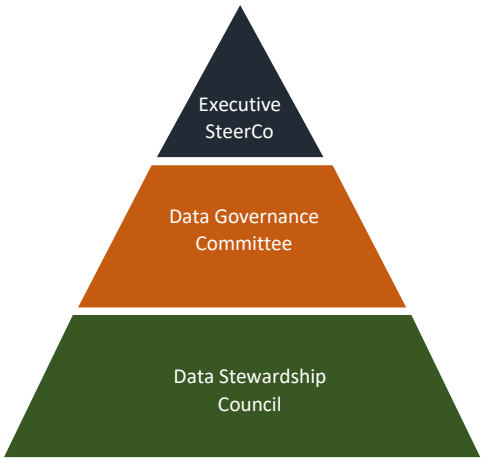
6.10 INTERNAL GOVERNANCE STRUCTURE RELATED TO PERSONAL DATA

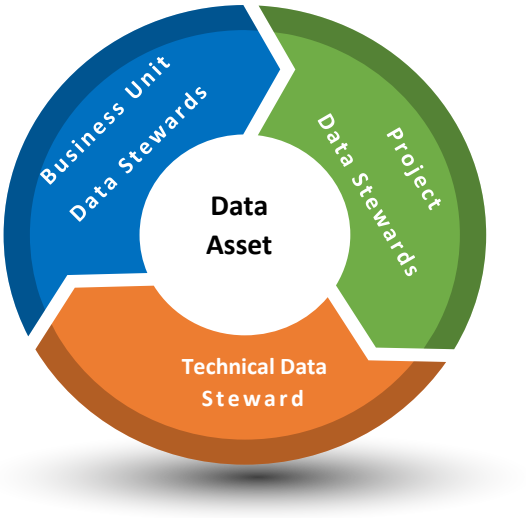
Monitoring and managing the actions necessary for compliance with the law within the Company is one of the main goals of the PDP Aksigorta Data Governance Committee. The main tasks of this Committee within the scope of PDPL compliance are;

- Preparing policies and procedures for the protection and processing of personal data and taking the necessary actions to enact these,
- Carrying out the distribution of tasks necessary for the implementation of policies and procedures and following up on the performance of the relevant actions,
- Ensuring that the necessary actions are taken to solve the questions and problems that may arise related to the implementation of the law and/or policy and procedure,
- Taking the necessary actions to solve data subject applications if necessary,
- Handling relationships with the Personal Data Protection Authority.

Data Governance Organization

The data governance organization structure is presented in the pyramid.





Roles	Responsibilities
Executive SteerCo	• It is composed by General Manager, ALT, Corporate Law and Compliance Department Manager, IT Governance and Service Management Manager, Digital, Financial and Enterprise Practices Department Manager, Information Security Unit Manager. • It is chaired by the CEO. • It approves the Data Governance Strategy and policies. • It provides sponsorship and senior management support in Data Governance. • It solves problems that cannot be resolved by the Data Governance Committee.
Data Governance Committe	Its main members are Corporate Law and Compliance Department Manager, IT Governance and Service Management Manager, Digital, Financial and Enterprise Practices Department Manager, Information Security Unit Manager. • The lower members; consist of Technical Governance Department Manager, Strategy, Transformation and Digital Channels Department Manager, Marketing Group Manager, Accounting Division Manager, Performance, Remuneration and Organizational Development Department Manager, Corporate Law and Compliance Department, Data Analytics and Performance Management Division Manager, Bank Channel Management Group Manager. • It is the cross-functional team that determines decisions about data governance and policies. • It solves problems that the Data stewardship council cannot solve. • It has the responsibility to appoint and replace data stewards that play a key role in Data Governance processes. • The Data Governance Committee meets periodically every 2 months to discuss the situation in Data governance processes and to adopt the necessary decisions for operation.
Data Stewardship Council	It consists of Technical, Business Unit and project data officials appointed by the data Committee. It is the operational owner of data assets and manages decisions related to data life cycle and flow.
Data Stewards	• They are appointed by the Data Governance Committee. • The data steward is appointed from those who have knowledge and experience in the field for which he is responsible. • Data managers are responsible for the data assets assigned to them. They are responsible for the collection, processing and protection of these assets and resolution of problems related to the data.
Business Unit Data Steward	• It is the key role responsible for the quality, meaning and use of data. • He has knowledge and experience in a specific business area (damages, bancassurance, collection, etc.).

	• He defines the need, use and storage of data from the standpoint of the business unit. • He updates the data inventory and data dictionary on the system if necessary. • He processes business data quality policies.
Project Data Steward	• He is responsible for accurate identification of data assets and processing needs in projects. They are mostly assigned from IT analyst teams. • He has knowledge/experience in data analysis, dependency, usage and integration. • He works with the business unit data steward, acts as a bridge between the technical data steward and the business unit data steward.
Technical Data Steward	• He has technical knowledge and experience in matters such as ETL, database, data storage, data engineering and data security. • He is the owner of the technical projection of the data asset. • He processes technical data quality policies.
Data Controller	• The natural or legal person who determines the purposes and means of data processing and who is responsible for the establishment and management of the data recording system.
Data Owner	• Data Owners are authorized by a Data Manager. • He implements effective local protocols to direct proper use of assets. Access to and use of corporate data is usually managed by the appropriate Data Owner. • He is responsible for the classification of data. • In accordance with the Data Classification Standard, Data Owners are responsible for ensuring that the data complies with legal regulations, for conducting the activities of regulation, change and operational work.