# PERSONAL DATA PROTECTION AND DESTRUCTION POLICY

The Policy on Protection and Destruction of Personal Data has been prepared by the Starch Industrialists Association (SIA) under three (3) main headings. These are as follows;

-Personal Data Protection and Processing Policy

-Policy for the Protection and Processing of Sensitive Personal Data

-Storage and Destruction Directive

**OBJECTIVE:**

The Personal Data Storage and Destruction Policy has been prepared in order to determine the procedures and principles of the operations and transactions on the storage and destruction activities carried out by SIA.

**SCOPE**

The Personal Data Protection and Destruction Policy is within the scope of the protection of the personal data of SIA customers, employees, visitors, the companies / stakeholders which are in cooperation with SIA and their customers/ employees or other third parties.

This policy is applied in all recording environments owned or managed by SIA, in activities related to the processing, protection, storage and destruction of personal data. The procedures and method regarding the processing, protection, storage and destruction of personal data and sensitive personal data are arranged under three main headings.

## (A) POLICY OF PROTECTION AND PROCESSING OF PERSONAL DATA

**1) OBJECTIVE**

**1.1)** The Personal Data Protection and Processing Policy has been prepared in order to determine the procedures and principles of the operations and transactions on the protection and processing activities carried out by SIA.

**1.2)** SIA has adopted the principle of processing and protecting personal data of SIA employees, employee candidates, service providers, visitors and other third parties in accordance with the relevant laws and regulations in line with the objectives set in the association's charter. (Turkish Constitution, international conventions, Personal Data Protection Law No. 6698). In addition, SIA has made it a priority to give the rights of the relevant persons.

**2) SCOPE and CHANGES**

**2.1)** This Personal Data Protection and Processing Policy (PDP Policy") prepared by NİSAD has been prepared in accordance with the Personal Data Protection Law No. 6698.

**2.2)** Personal data of SIA customers, employees, visitors, companies / stakeholders in cooperation with SIA and their customers / employees are covered by the PDP policy. In addition, personal data of other third parties automatically obtained are covered by the PDP

Policy. This policy is also applied to all registration activities in which personal data owned or managed by SIA are processed.

**2.3)** Data obtained with the consent of individuals or other data that are allowed to be used legally is used in order to increase the quality of the services provided by SIA and to improve the quality policy.

Some data are de-personalized and anonymized. Anonymized data are the data used for statistical purposes. It is not included in the PDP Law and PDP Policy.

**3) BASIC PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA**

**3.1) Compliance with the law and the rules of honesty:** SIA questions the source of the data they collect or receive from other companies and SIA attaches importance to the fact that these are obtained in accordance with the law and in accordance with the rules of honesty.

**3.2) Accuracy and Up-to-dataness**: SIA attaches great importance to the accuracy of all the data it collects and receives. When there is a change in any personal data and this situation is transmitted to SIA, the said data updated by SIA.

**3.3) Use of data for specific, explicit and legitimate purposes:** SIA uses some data in a limited way with the permission of relevant persons and organizations. Before the usage, SIA clearly states that how the information will be used and for what purpose. Data can be used only for business purpose. It can't be used or processed for any other reason.

**3.4) Limited use and Conformity to purpose:** SIA only uses the data for the purposes for which they are obtained and to the extent required by the service given.

**3.5) Storage period of data in accordance with the relevant legislation and its purpose:** SIA retains the data obtained from the contracts for the period specified in Law No. 6698 (in case of any dispute/ due to the requirements of commercial and tax law)

However, when these purposes disappear, the data are deleted or anonymized. SIA deletes or destroys the relevant data according to the Personal Data Deletion Directive.

We must emphasize this; These principles that we have listed above apply both to data obtained with consent and to data obtained through other legal means.

**4) MAXIMUM SAVING PRINCIPLE**

According to this principle called the principle of maximum savings or thrift principle;

**4.1)** The data reaching SIA is only processed into the system as necessary.

**4.2)** Therefore, what data we collect is determined by the purpose. Unnecessary data are not collected.

**4.3)** Other data received to SIA are also transferred to SIA's information systems. Excess information is not saved in the system; it is deleted or anonymized. These data can be used for statistical purposes.

**5) PRIVACY POLICY**

**5.1)** The data of employees or other persons at SIA are confidential. No one may use, copy, reproduce, transfer to others or use this data for purposes other than commercial purposes. it can't be used unlawfully.

**5.2) PROCESS SECURITY**

SIA takes all necessary technical and administrative measures to protect all personal data it has and to prevent unauthorized access to this information.

In this context, SIA ensures that the software complies with the standards and carefully chooses the other institutions it cooperates with. SIA always abides by the PDP Policy and security measures are improved.

**6) STORAGE AND DESTRUCTION OF PERSONAL DATA**

**6.1)** These personal data are deleted, destroyed or anonymized by NİSAD automatically or at the request of the person concerned, when the retention period expires which is determined by the law, when the judicial processes or other requirements are over,

**6.2)** "Storage and Destruction Directive" has been prepared to determine the procedure for the storage and destruction of personal data. The Storage and Destruction Directive is an integral part of this PDP Policy.

**7) ACCURACY AND UP-TO-DATANESS:**

**7.1)** The data acquired by SIA are processed without changing the declaration of the relevant persons.

**7.2)** SIA is not obliged to verify the accuracy of data declared by customers or persons contacting SIA.

This research is not legally possible and is also incompatible with SIA's working principles.

**7.3)** The data declared are considered correct. The principle of accuracy and up-to-dataness of personal data are adopted by SIA. SIA updates the personal data with the information obtained from an official document, and also SIA updates the personal data when it receives special request from the person concerned. SIA takes the necessary precautions for these kind of situations.

**8) PRIVACY AND DATA SECURITY**

**8.1)** Personal data are confidential and SIA abides by this privacy.

**8.2)** Personal data can only be accessed by authorized persons within SIA. All necessary technical and administrative measures are taken to protect the personal data collected by SIA and to prevent unauthorized access.

**8.3)** In this context, it is ensured that the software complies with the standards, the third parties are carefully selected and the PDP Policy is needed to be applied within SIA.

**8.4)** SIA requests companies and stakeholders with whom SIA legally shares personal data, to protect this data.

**9) DATA PROCESSING PURPOSES**

Personal data are processed by SIA within the scope of personal data processing conditions specified in Articles 5 and 6 of the PDP Law and in line with the purposes stated below.

**(a)**Benefiting of third parties from the products and services offered by SIA, and performing after-sales support services.

**(b)** Increasing the quality of the product / service offered by SIA, and customizing and improving the service provided according to the needs, tastes and usage habits of the customers.

**(c)** Planning and implementing human resources policies in the most efficient way

**(d)** Correct planning and execution of commercial partnerships and strategies,

**(e)** Ensuring the legal, commercial and physical security of SIA and its business partners.

**(f)** Ensuring SIA institutional functioning

**(g)** Ensuring the highest level of data security, creating databases, improving the services offered on SIA's website, communicating with those who conveyed their requests and complaints to SIA, eliminating errors on SIA's website

**(h)** Determining SIA's commercial and business strategies.

**10) CUSTOMER DATA and BUSINESS-SOLUTION PARTNERS DATA**

**10.1) Collection and Processing of Contract Data**

If a contract has been signed with customers, the personal data included in this contract can be used without the customer's consent. However, this use is carried out for the purpose of the contract only. Data are used to provide better service in line with the requirements of the service offered. Customers are re-contacted when data needs to be updated.

**10.2) Business and Solution Partners Data**

SIA prioritizes compliance with the law when sharing data with its business and solution partners. it is shared with a data privacy commitment as much as the required by the service. The parties which are shared data are absolutely required to provide data security.

**(a) Data Processing for The Purpose of Advertisement**

Electronic messages for advertising purposes can only be sent to those who are asked their permission in advance in accordance with the 'Law on the Regulation of E-Commerce' and the Regulation on 'Commercial Communication and Commercial Electronic Messages'. The approval of the person to whom the advertisement will be sent must clearly be obtained.

All commercial electronic messages in the following purposes needs to be approved before sent.

- Promoting the company's goods and service

-Marketing

-Promoting your business

-Increasing popularity with the events such as congratulations and wishes

This approval can be obtained in writing through any electronic communication tool or in person. The details that must be included in the approval are as follows; affirmative declaration of the recipient's acceptance of commercial electronic messages, name and surname and electronic contact address

**(b) Legal Obligation of SIA**

Personal data may be processed without approval, if clearly stated in the relevant legislation or if there is any legal obligation determined by the legislation. The type and scope of data processing must be necessary for the legally permitted data processing activity and must comply with the relevant legal provisions.

**(c) SIA's Data Processing**

Personal data may be processed in line with the service and legitimate purposes offered by SIA. However, the data cannot be used for illegal purposes in any way.

**(e) Data Processed by Automated Systems**

SIA complies with laws and secondary legislation regarding data processed through automated systems.

**(f) User Information and Internet.**

The relevant persons are informed with a privacy statement in the events that personal data is collected, processed and used in SIA's websites or other systems and applications. If necessary, information about cookies is also provided. People are informed about the activities on the internet pages. Personal data are processed in accordance with the law.

**10.3) Employee Data**

**(a) Processing of Data within the Frame of Business**

Personal data of the employees are processed as necessary in terms of the implementation of the employment contract and the availability of side rights. However, SIA ensures the confidentiality and security of data belonging to its employees.

**(b) Processing for Legal Obligations**

Personal data may be processed without approval by SIA, if clearly stated in the relevant legislation or if there is any legal obligation determined by the legislation. This point is limited to the obligations arising from the law.

**(c) Processing for the Benefit of Employees**

SIA may process personal data without obtaining a consent for the transactions in the interest of its employees, such as fringe benefits.

**(d) Data Processed by Automated Systems**

Employee data processed through automated systems can be used in internal promotions and performance evaluations. Employees have the right to object to the result against them and they do so by following the procedures within SIA. Employees' objections are also evaluated within SIA.

**(e) Telecommunications and Internet**

Computer, phone, e-mail and other applications allocated to employees by SIA are allocated to employees only for business purposes. Employees are not allowed to use any of these devices for their private purposes and communication. SIA can check and control all data on these devices. Employees guarantee that no other data or information is kept on computers, phones or other tools allocated to them from the moment they start working.

**11) SENSITIVE PERSONAL DATA PROCESSING**

**11.1)** According to the Law, data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and membership, association, foundation or union membership, health, sexual life, criminal conviction, security measures, biometric and genetic data are personal data of special nature.

**11.2)** In the processing of sensitive personal data, SIA takes the necessary measures determined by the board as well as gaining the consent of the relevant person. Special quality personal data can be processed without the consent of the person only in cases permitted by the Law. It is processed in a limited and legal frame.

**11.3)** A separate policy has been determined for the security of sensitive personal data. Sensitive Personal Data Protection and Processing Policy is an integral part of the PDP Policy.

**12) DOMESTIC AND INTERNATIONAL TRANSFER OF PERSONAL DATA**

**12.1)** Personal data may be shared with the main shareholder as well as business and solution partners in order to perform the services offered by SIA.

**12.2)** SIA may outsource personal data from its suppliers, as well as transfer data to its suppliers, as required by the service offered.

**12.3)** SIA has the authority to transfer personal data domestically and internationally within the conditions determined by the Board in accordance with the other conditions in the Law.

**13) RIGHTS OF THE PERSONAL DATA SUBJECT SPECIFIED IN ARTICLE 11 OF THE PDP LAW**

**13.1)** In line with the PDPL, SIA accepts that it must obtain the consent of the relevant person before processing the data. SIA also agrees that after the data use, the person concerned has the right to comment and intervene about this use.

**13.2)** People whose personal data are processed have the following rights according to Article 11 of the Law.

**13.3)** In order to facilitate the use of these rights, an application form has also been prepared by SIA and presented on its website (http://www.nisad.org.tr/)

**13.4)** People whose personal data are processed have the following rights. For these rights, the person concerned must contact the authority and inform his / her request (the person authorized by SIA and announced on the website).

-Being informed whether their personal data is processed,

- Requesting information about the use if their personal data is processed

- Being informed about the purpose of processing their personal data and whether it is used appropriately for the purpose

- Being informed about the third parties to whom their personal data are transferred domestically or abroad

-Requesting the deletion or destruction of personal data in the event that the reasons for processing disappears, although it has been processed in accordance with the provisions of PDPL and other related laws. (Article 7 of the PDPL)

- Requesting a notification of the transaction/deletion/destruction made within this scope to third parties to whom personal data have been transferred

- The objection right in case of an adverse result obtained about the relevant person if the processed data is analysed by automatic systems.

- Requesting the compensation of any damage if the person concerned is damaged in the event that personal data is processed illegally.

**13.5)** On the other hand,

-People do not have any right on anonymized data in SIA.

-SIA may share personal data with relevant institutions and organizations in case of a legal situation or a legal request of any government authority, in accordance with the employment contract.

**13.6)** Personal data subjects may submit their requests regarding the above-mentioned rights to SIA. For this, the person concerned must complete the application form on SIA's official website and send this form to SIA's address by registered mail. The form must have an original signature of the applicant. ID photocopy (for ID card, only the front side copy) must be attached to the form.

Applications are answered as soon as possible, depending on the content of the application, or within 30 days of receipt at SIA. Applications (excluding applications made online) must be made by registered mail. In addition, applications are personal, no application can be made on behalf of another person, otherwise this application is not replied. SIA may request some information or documents from the applicants regarding the application.

**14) INSPECTION**

SIA carries out the necessary internal and external inspections for the protection of personal data.

**15) NOTIFICATION OF VIOLATIONS**

SIA takes immediate action in the event of a breach of personal data. It minimizes the damage of the person concerned and compensates the damage.

If personal data is got by unauthorized persons, SIA immediately notify the Personal Data Protection Board about it.

Applications are made in accordance with the procedures specified on the official website for the notification of violations. Click for PDPL Application and Information Request form.

**16) UPDATE**

The changes made in this Policy are shown in the chart below.

| Policy Update | Date | Changes |
|---|---|---|

## (B) POLICY OF PROTECTION AND PROCESSING OF SPECIAL CATEGORY PERSONAL DATA

**1) OBJECTIVE**

The purpose of the Policy for the Protection and Processing of Sensitive Personal Data is to fulfil the legal obligations of 'the Decision of Adequate Measures to be Taken by Data Controllers' and to exhibit the technical and administrative measures taken in the processing of sensitive personal data. (In accordance with the provisions of the Law numbered 6698, and also in accordance with the provisions of the Personal Data Protection Board dated 31/01/2018 and numbered 2018/10 on Processing Sensitive Personal Data)

**2) DEFINITIONS AND ABBREVIATIONS**

| | |
|---|---|
| Explicit Consent: | Consent that is based on information and expressed with free will regarding a specific subject. |
| Destruction: | Deletion or anonymization of personal data. |
| Law: | Law No.6698 on Protection of Personal Data |
| Personal data: | All kinds of information regarding an identified or identifiable natural person. |
| Anonymization of personal data: | It is the transformation of personal data into a form that cannot be associated with an identified or identifiable natural person, even if the data is matched with other data. |
| Processing of personal data: | All kinds of processes of personal data obtained with the way either fully or partially automatic or non-automatic (provided that it is a part of any data recording system). Such as obtaining, recording, storing, preserving, changing, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing access. |
| Deletion of personal data: | The process of making personal data inaccessible and unavailable in any way for the relevant users. |
| Destruction of personal data: | It is the process of making personal data inaccessible, unrecoverable and unavailable by anyone. |
| Board: | Personal Data Protection Board |
| Policy: | Policy of Protection and Processing of Special Category Personal Data |
| SIA: | Starch Manufacturers Association |
| Data Subject: | Real person whose personal data is processed |
| Data controller: | Natural or legal person who determines the purposes and means of processing personal data and who is responsible for the establishment and management of the data recording system. |

**3) SENSITIVE PERSONAL DATA PROCESSING**

Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and membership, association, foundation or union membership, health, sexual life, criminal conviction, security measures, biometric and genetic data are sensitive personal data.

**3.1)** SIA complies with the Law and other legislative provisions in the processing of sensitive personal data. Sensitive personal data are processed in accordance with the following principles:

-Complying with the law and honesty rules

- Accuracy and up-to-dateness

- Being connected, limited, and measured with the purpose data are processed for.

- Processing for specific, explicit and legitimate purposes.

- Being kept for the period determined by the legislation or being kept for the period required for the purpose for which they are processed

**3.2)** Sensitive personal data except health and sexual life are processed by SIA in cases it is allowed by the data subject or the law.

**3.3)** Data on health and sexual life are processed in cases the explicit consent of the data subject is obtained or for the purpose of protecting public health, carrying out medical diagnosis, treatment and care services, preventive medicine, and some regulations in the health service.

**3.4)** The provisions of the Regulation on Processing Personal Health Data and Ensuring Privacy are obeyed in the processing of health data. (It was published in the Official Gazette dated October 20, 2016 and numbered 29863 and entered into force.)

**4) TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO PROTECT SENSITIVE PERSONAL DATA**

SIA processes sensitive personal data in accordance with the Law and the relevant legislation and SIA takes all kinds of measures to ensure the security of these data. The measures taken in this context are listed below:

**4.1) Administrative Measures**

**(a)** SIA provides regular training to employees on the processing of sensitive personal data.

**(b)** SIA concludes confidentiality agreements with its employees to ensure data security.

**(c)** Authority scopes and durations of users who are authorized to access data are clearly defined and periodic authorization checks are carried out.

**(d)** Employees who change their jobs or leave their jobs are immediately denied access to personal data. In this context, SIA immediately gets back the inventories allocated to employees.

**4.2) Technical Measures**

**(a) Technical Measures Taken in Terms of Sensitive Personal Data Stored and / or Accessed in Electronic Environment**

**i)** Sensitive personal data are stored using cryptographic methods.

**ii)** Cryptographic keys are kept in secure and different environments.

**iii)** Transaction records of all transactions performed on sensitive personal data are securely logged.

**iv)** Security updates of the environments where sensitive personal data are kept, are constantly monitored. Necessary security tests are carried out regularly and test results are recorded.

**v)** Users are specially authorized for the software of sensitive personal data. The security of these soft wares are regularly tested and the test results are recorded.

**vi)** In cases where private personal data is accessed remotely, at least two-step verification system is used.

**(b) Technical Measures Taken in Terms of Sensitive Personal Data Stored and / or Accessed in Physical Environment**

**i)** Adequate security measures are taken depending on the situation of the environment in which special personal data are kept

**ii)** Physical security of these environments is ensured and unauthorized access are prevented.

**5) TRANSFER OF SPECIAL PERSONAL DATA**

SIA transfers private personal data within the framework of the data processing conditions in Articles 8 and 9 of the Law.

In order to ensure data security, the following rules are applied by SIA in data transfer and periodic audits are carried out within this scope.

**5.1) Transfer by E-Mail**

In cases where sensitive personal data are transferred via e-mail, encrypted transfer is made using a corporate e-mail address or a Registered Electronic Mail (REP) account.

**5.2) Transfer Through Devices Such as Removable Memory, CD, DVD**

In cases where sensitive personal data are transferred via removable memory, CD, DVD, etc., encryption is applied with cryptographic methods and the cryptographic key is kept in a different environment

**5.3) Transfer Between Servers in Different Physical Environments**

In the transfer of sensitive personal data between servers in different physical environments, data transfer is carried out by setting up a VPN between servers or using the sFTP method.

**5.4) Documental Transfer of Physical Environments**

If it is necessary to transfer sensitive personal data with documents, necessary precautions are taken against risks such as theft, loss or being copied by unauthorized persons, and the document is sent in the "confidential documents" format.

**6) STORAGE AND DESTRUCTION OF SENSITIVE PERSONAL DATA**

**6.1)** Storage: Sensitive personal data are stored by SIA in accordance with the law, legislation and the decisions published by the Board (Decision of Adequate Precautions to be Taken by Data Controllers in the Processing of Sensitive Personal Data) in the following cases:

**(a)** Obtaining the explicit consent of the data subject

**(b)** The storage of sensitive personal data stipulated by law, except health and sexual life,

**(c)** Storage of health and sexual life data for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and finance.

**6.2) Destruction:** Sensitive personal data stored by SIA in accordance with the law and other legislation are deleted, destroyed or anonymized, either ex officio or upon the request of the data subject, in the event of the following reasons:

**(a)** Storage activities carried out with the consent of the data subject, the data in question is destroyed or deleted when the data subject withdraws his/her explicit consent.

**(b)** Data are destroyed in cases where the purpose of storing sensitive personal data is completed or disappeared for any other reason.

**(c)** Data are deleted in case the provisions of the legislation on the storage of sensitive personal data are changed or abolished.

**(d)** When all the processing conditions in Article 6 of the Law are eliminated, the relevant data is deleted.

**(e)** When a request for the destruction of personal data submitted to SIA with an official manner and when the request is accepted by SIA, the relevant data is destroyed

**(f)**The relevant person may complain about the situation to the board in cases where the request for the destruction of his/her sensitive personal data is rejected by SIA, the response is insufficient, the request is not responded on time. If this complaint is deemed appropriate by the board, the relevant data is destroyed.

**7) UPDATE**

The policy updates / changes made in this frame are shown in the table below.

| **Policy Update** | **Date** | **Changes** |
|---|---|---|

**(C) PERSONAL DATA STORAGE AND DESTRUCTION DIRECTIVE**

**1) OBJECTIVE**

Purpose of preparing personal data storage and destruction directive;

- Fulfilling the legal obligations stipulated in the Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017 and numbered 30224;

- Keeping personal data within the legal entity and announcing the regular destruction periods;

-Determining the titles, units and job descriptions of persons involved in the processes of storing and destroying personal data, and fulfilling other obligations.

The Personal Data Storage and Destruction Directive ("Directive") was prepared by the Starch Industrialists Association (SIA) with the title of data controller in accordance with SIA personal data processing inventory.

**2) DEFINITIONS**

| | |
|---|---|
| Consent: | Consent that is based on information and expressed with free will regarding a specific subject |
| Relevant User: | Person who process personal data in line with the authorization and instructions received from the data controller or the data controller (except the person or unit responsible for the technical storage, protection and backup of the data) |
| Destruction: | Deletion or anonymization of personal data. |
| Law: | Law No.6698 on Protection of Personal Data |
| Recording Medias | Any medias personal data processed in fully or partially in the automatic or non-automatic ways. (provided that it is a part of any data recording system) |
| Personal data | All kinds of information regarding an identified or identifiable natural person. |
| Personal Data Processing invertory | It is the inventory that the data controllers work on it. the data controller works on the inventory by detailing the following topics; the purposes of processing personal data and the maximum period required for this, the data category, the recipient group, the international data transfer and the measures taken for its security etc.. |

| | |
|---|---|
| Anonymization of personal data | It is the transformation of personal data into a form that cannot be associated with an identified or identifiable natural person, even if the data is matched with other data. |
| Processing of personal data | All kinds of processes of personal data obtained with the way either fully or partially automatic or non-automatic (provided that it is a part of any data recording system). Such as obtaining, recording, storing, preserving, changing, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing access. |
| Deletion of personal data | The process of making personal data inaccessible and unavailable in any way for the relevant users. |
| Destruction of personal data | It is the process of making personal data inaccessible, unrecoverable and unavailable by anyone. |
| Board | Personal Data Protection Board |
| Periodic destruction | The process of deletion, destruction or anonymization ex officio at repetitive intervals in the event that all the conditions for the processing of personal data are eliminated. (as specified in the personal data retention and destruction policy) |
| Registry | Data Controllers Registry under the control of the Personal Data Protection Authority |
| SIA | Starch Manufacturers Association |
| Data recording system | A recording system in which personal data are structured and processed according to certain criteria. |
| Data Subject | Real person whose personal data is processed |
| Data controller | Natural or legal person who determines the purposes and means of processing personal data and who is responsible for the establishment and management of the data recording system. |
| Directive | SIA Personal Data Storage and Destruction Directive |
| Regulation | Regulation on Deletion, Destruction or Anonymization of Personal Data |

**3) RECORDING MEDIA**

Personal data is stored by SIA in the following secure physical and electronic environments in accordance with the Law and other legislation:

**3.1) Physical Recording Media**

-Unit Cabinets

-Archive

**3.2) Electronic Recording Media**

-Servers (backup, e-mail, database, web, file sharing, etc.)

-Software (office software, portal, EDMS, VERBİS.)

- Information security devices (firewall, intrusion detection and blocking, log file, antivirus, etc.)

-Personal computers (Desktop, laptop)

-Mobile devices

-Optical discs (CD, DVD, etc.)

Removable sticks (USB, Memory Card etc.)

-Printer, scanner, copier

**3.3) Non-electronic recording media**

-Paper

-Manual data recording systems (survey forms, visitor entry book)

-Written, printed visual media

**4) REASONS REQUIRING THE STORAGE AND DESTRUCTION OF PERSONAL DATA**

**4.1) Reasons Requiring the Storage of Personal Data**

Personal data are stored for the following legal reasons for the purposes of SIA to fulfil its legal obligations, to maintain connection with customers, suppliers, employees and other business partners, and to conduct business activities:

**(a)** -6698 numbered Personal Data Protection Law,

-Law on broadcasts regulation made on the Internet and Combating Crimes Committed Through These Broadcasts, numbered 5651,

- Turkish Code of Obligations No. 6098,

- It is kept for the retention periods stipulated in the Labour Law numbered 4857 and other secondary regulations in force pursuant to these laws.

**(b)**The explicit consent of the data subject is obtained

**(c)**The storage of personal data is clearly stipulated in the legislation to which SIA subjects to

**(d)** It is necessary to store personal data belonging to one of the contracting parties, provided that it is directly related to the making or execution of the contracts

**(e)** Storage of personal data is mandatory for SIA to fulfil its legal obligations

**(f)** It is necessary to store personal data in order to give, exercise or protect a right.

**(g)** Personal data reported by the data subjects themselves must be stored in the line with the reporting purposes.

**(h)** Provided that it does not harm the fundamental rights and freedoms of data subject, it is necessary to store personal data for the legitimate interests of SIA.

**4.2) Reasons Requiring the Destruction of Personal Data**

Personal data stored legally and securely by SIA are deleted, destroyed or anonymized, either ex officio or on the request of the data subject, in the event of the following reasons:

**(a)** Storage activities carried out with the consent of the data subject, the data in question are destroyed when the data subject withdraws his explicit consent.

**(b)** Data are destroyed in cases where the purpose of storing personal data is completed or disappeared for any other reason.

**(c)** Data are deleted in case the provisions of the legislation on the storage of personal data are changed or abolished.

**(d)** When all the processing conditions in Article 6 of the Law are eliminated, the relevant data is deleted.

**(e)** When requests for the destruction of personal data submitted to SIA in accordance with its procedures are accepted by SIA, the relevant data is destroyed.

**(f)**The relevant person may complain about the situation to the board in cases where the request for the destruction of his/her personal data is rejected by SIA, the response is insufficient, the request is not responded on time. If this complaint is deemed appropriate by the board, the relevant data is destroyed.

**5) REASONS REQUIRING THE STORAGE AND DISTRUCTION OF SENSITIVE PERSONAL DATA**

**5.1)** Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and membership, association, foundation or union membership, health, sexual life, criminal conviction, security measures, biometric and genetic data are within the scope of sensitive personal data.

**5.2)** The measures taken by SIA for the protection and processing of sensitive personal data in accordance with the law are regulated in the Policy of SIA's Sensitive Personal Data Protection and Processing.

**5.3)** Storage: Sensitive personal data are stored by SIA for the following reasons in accordance with the Law No. 6698 and other legislation and the Adequate Precautions to be Taken by the Data Controllers in the Processing of Sensitive Personal Data published by the Board

**(a)** Obtaining the explicit consent of the data subject

**(b)** The storage of sensitive personal data stipulated by law, except health and sexual life,

**(c)** Storage of health and sexual life data for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning/ managing/financing of health services.

**5.4) Destruction:** Sensitive personal data are stored by SIA in accordance with Law No. 6698 and other legislation and the Decision published by the Board (the decision of Adequate Measures to be Taken by Data Controllers in the Processing of Sensitive Personal Data). These data are deleted, destroyed anonymized either ex officio or on the request of the data subject, in the event of the following reasons:

**(a)** Sensitive Data storage activities carried out with the consent of the data subject, the data in question is destroyed when the data subject withdraws his/her explicit consent.

**(b)** Sensitive Personal Data are destroyed in cases where the purpose of storing sensitive personal data is completed or disappeared for any other reason.

**(c)** Data are deleted in case the provisions of the legislation on the storage of sensitive personal data are changed or removed.

**(d)** When all the processing conditions in Article 6 of the Law are eliminated, the relevant data is deleted.

**(e)** When a request for the destruction of sensitive personal data submitted to SIA with an official manner and when the request is accepted by SIA, the relevant data is destroyed.

**(f)**The relevant person may complain about the situation to the board in cases where the request for the destruction of his/her sensitive personal data is rejected by SIA, the response is insufficient, the request is not responded on time. If this complaint is deemed appropriate by the board, the relevant data is destroyed.

**6) MEASURES TAKEN TO ENSURE DATA SECURITY**

All administrative and technical measures taken by SIA for the safe storage of personal data, prevention of unlawful process/access, and legal destruction of data, are listed below:

**6.1) Administrative Measures**

Administrative measures taken by SIA are as follows:

**(a)** SIA determines personal data security policies and procedures in accordance with the Law and other legislation. It conducts regular audits for the implementation of the Law and the determined policies within its legal entity.

**(b)** SIA employs personnel experienced in the protection of personal data. SIA also organizes personal data protection law training and conducts awareness activities for its staff.

**(c)** Confidentiality agreements are made with the employees in activities carried out by the Agency.

**(d)** Disciplinary procedure has been prepared by SIA for employees who do not comply with security policies and procedures.

**(e)** Employees who will work in personal data processing activities should first be given the necessary explanation and detailed information by the institution. Periodic and random inspections are carried out within the institution.

**(f)** SIA makes a data sharing agreement with the persons to whom personal data is transferred and SIA ensures data security.

**(g)** SIA gives only authorized personnel access to stored personal data within the legal entity.

**(h)** In the event that personal data are illegally seized by third parties, SIA immediately reports it to the data subject and the Board.

### 6.2) Technical Measures

The measures taken by SIA are as follows.

**(a)** Necessary internal controls are made within the scope of the systems installed.

**(b)** SIA conducts risk assessments and business impact analysis processes of information technologies within the scope of established systems.

**(c)** SIA ensures that the technical infrastructure is provided to prevent or detect data leakage and also SIA ensures that the relevant matrices are created.

**(d)** SIA regularly checks this system for data outflows leakages

**(e)** SIA audits and controls the access rights of employees in information technologies to personal data.

**(f)** SIA ensures that once personal data is destroyed, this process cannot be taken back

**(g)** In accordance with Article 12 of the Law, all kinds of digital media where personal data are stored are protected by encrypted or cryptographic methods to provide information security.

## 7) STORAGE OF RECORDS

All transactions regarding the deletion, destruction and anonymization of personal data are recorded and these records are kept for at least three years, excluding other legal obligations.

## 8) STORAGE AND DESTRUCTION PERIODS

Personal data are stored for the period stipulated in the legislation or stored for the period required for the purpose of the processing. The data are stored in the line with 'the general principles in article 4 of the Law'. The storage periods determined within this scope are given in the table below.

| Data Category | Storage Period | Destruction Period |
|---|---|---|
| CCTV Recordings | 30 days | Automatic destruction at the end of the storage period |
| Employee Personal File and Payroll Data | 15 years | Within 6 months following the expiry of the retention period |
| Employee Candidate Resumes | 1 year | Within 6 months after the expiry of the storage period |
| Information Contained in Contract, Invoice, Legal Declaration, Commercial Ledger and Business Correspondence | 10 years | Within 6 months after the expiry of the storage period |
| SIA Managers and Board Members Data | 10 years | Within 6 months after the expiry of the storage period |

**9) DESTRUCTION PERIODS**

SIA deletes, destroys or anonymizes personal data in the first period of destruction following the expiration of the storage period specified in the Policy and the emergence of the obligation of destruction. Periodic destruction is carried out twice a year, at 6-month intervals, in April-October.

**10) TITLES, UNITS AND TASK DESCRIPTIONS OF OFFICIAL / RESPONSIBLE PERSONNEL IN STORAGE and DESTRUCTION PROCESS**

The title, unit and task descriptions of SIA personnel participating in personal data storage and destruction processes are as shown in the table below.

| Unit | Title | Task Description |
|---|---|---|
| Human Resources Department | Director Of Human Resources | Ensuring the implementation of the Policy within the Department |
| Financial Affairs Department | Finance Director | Ensuring the implementation of the Policy within the Department |
| Information Technologies Department | Information Technology Manager | Ensuring the implementation of the Policy within the Department and to carry out the necessary destruction activities in the systems of SIA within the scope of periodic destruction periods |

**11) UPDATING**

The changes made in this Directive are shown in the table below.

| Policy | Update Date | Changes |
| --- | --- | --- |