SNI TEKNOLOJİ HİZMETLERİ A.Ş.

THE POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

I. Purpose

The purpose of this Policy on the Storage and Destruction of Personal Data ("Policy") is to establish a set of criteria and methods for determining the periods of processing for the personal data processed by **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** ("SNI"), and for the deletion, destruction or anonymization of personal data for which the processing period has ended and/or the processing of which no longer has any legal grounds.

This Policy also includes the technical and administrative measures taken to ensure data security as per Article 6 of the Regulation on the Deletion, Destruction or Anonymization of Personal Data that entered into force on October 28, 2017. This framework also incorporates the Regulation on the Registry of Data Controllers dated December 30, 2017, and the Guide on the Deletion, Destruction and Anonymization of Personal Data.

II. Scope

As per Article 7 of the Law No. 6698 on the Protection of Personal Data, this Policy covers the actions of **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** as the "data controller" with respect to deleting, destroying or anonymizing all personal data that is processed using fully/partially automatic methods or manually on the condition that the data is part of a data recording system, and that is stored electronically and/or physically in paper format, and for which the grounds for processing have ended.

III. Explanation as to the legal, technical or other reasons requiring the storage and destruction of personal data

In an effort to carry out business processes conducted by various departments in accordance with their job description and organize activities related to these processes, **SNI** processes personal data belonging to its employees, employee candidates, employee relatives, customers , customer business partners, customer employees, business partners, suppliers, visitors, and online visitors. The company then stores this personal data for certain periods of time as stipulated by regulations or determined by the relevant department within the scope of the purposes of processing personal data. This entire process is included in the Personal Data Processing Inventory. When relevant storage periods come to an end and

IV. The technical and administrative measures taken to store personal data safely and prevent it from being processed or accessed unlawfully

With regard to ensuring that the personal data that it processes is not accessed or processed illegally and is duly protected, **SNI** takes the following technical and administrative measures:

Anti-virus

All PCs and Servers at the **SNI**'s IT technologies infrastructure have a periodically updated antivirus application installed.

Firewall

The Data Centers and Disaster Recovery Centers housing **SNI**'s servers are protected by periodically updated firewall software, and these firewall applications control the internet connection of all employees and provide protection against viruses and similar threats.

VPN

Employees connect to workplace server systems via IP-SEC VPN and the traffic between the two points is encrypted.

Suppliers gain access to **SNI** servers and systems via the SSL-VPN defined on Firewalls. Each supplier has an SSL-VPN connection defined for them which they use to reach the systems that they must use or are authorized to access.

Network Configuration

SNI has configured the workplace network, limiting access to authorized persons.

User Definitions and Need to Know

SNI has limited employee access to **SNI** systems to the extent of their job descriptions, and swiftly updates systemic authorizations in case of a change of position of authority.

Information Security Threat and Incident Management

Incidents at **SNI** servers and firewalls are transmitted to the "Information Security Threat and Incident Management". This system issues warnings to relevant employees in the event of a security threat, and ensures that the threat is responded to in a swift manner.

Penetration Testing

Penetration testing is carried out by a supplier firm manually on **SNI** servers, computers, and a pilot workplace. The security vulnerabilities discovered as a result of this test are eliminated, and a verification test is conducted to ensure that these vulnerabilities have indeed been addressed. In addition, an automatic penetration test is carried out by the Information Security Threat and Incident Management system.

ISMS

At ISMS meetings held at **SNI**, the agenda items on the control form are reviewed by the IT Technologies Director and CFO on a monthly basis. An audit list - created in accordance with the Cobit standards and GV auditing standards - has been controlled periodically since **2014**.

Awareness Training

SNI regularly offers trainings to increase the awareness of its employees as to various information security breaches, and to minimize the impact of the human factor in information security violations. All employees have received the Cyber Security and Information Security training.

Clean Table & Clean Desk

Pursuant to **SNI** internal policy, all SNI employees are obligated to comply with the "clean table & clean desk" principle.

Other

Employees protect all fields that handle personal data on the website with SSL.

They use the method of pseudonymization in terms of all secondary data processing activities (Example: Ahmet Yılmaz "A... Y...").

They ensure that personal data in document format is preserved in locked containers and accessed only by authorized persons.

They prevent third parties from entering the workplace without authorization and ensure that third parties are always accompanied when visiting the workplace.

After the grounds for storing relevant data are no longer valid or the employee's ties to the company have been severed, the company ensures that the personal data located on personal devices provided by the company and in personal environments is deleted.

Personal data obtained and processed by third parties from which the company procures services is deleted from third-party systems at the end of such business relationships.

In the event that, despite **SNI** taking all measures for information security, personal data is damaged or obtained by unauthorized third parties as a result of attacks on **SNI**-run platforms or the **SNI** system, **SNI** shall notify you and the Personal Data Protection Board immediately, and take all necessary measures.

V. The technical and administrative measures taken to destroy personal data legally

SNI has created an in-house unit ("Technical Unit") in charge of destroying, in accordance with legal requirements, the personal data that **SNI** processes. The Technical Unit ensures that the personal data is deleted so that it can be processed by relevant users but not by anyone from any other department. Masking methods are used for electronically stored personal data to the extent that is necessary. For personal data in paper format, the process of deletion is carried out by obscuring the parts of the document containing personal data.

5.1. Deleting Personal Data

Deleting personal data refers to the process by which personal data can never be accessed or used again. The data controller is responsible for taking all necessary technical and administrative measures to ensure that deleted personal data becomes inaccessible to users and cannot be used again for any purpose.

5.1.1. The Process of Deleting Personal Data

The process that must be followed while deleting personal data is as follows:

- Identifying the personal data subject to erasure.
- Identifying the users of each fragment of personal data, using an authorization or control matrix or a similar system.
- Identifying the powers of the relevant users, including accessing, recovering, and re-using data.
- Deactivating and destroying the abovementioned powers of accessing, recovering, and re-using data.

In the event that any deleted personal data finds its way back on the system, deleting it immediately upon becoming aware of its existence on the system

5.1.2. Methods of Deleting Personal Data

a) Application-as-a-Service Cloud Solutions

Personal data found on a cloud system must be deleted using the delete command. While carrying out this procedure, it must be ensured that the user does not have the ability to retrieve any deleted data.

b) Personal Data in Paper Format

Personal data in paper format should be obscured. Obscuring is done by shredding the paper if possible, and if not, painting the paper in indelible ink and thereby making it irrevocably unintelligible, even with the application of any technology whatsoever.

c) Office Files Located at the Central Server

The file should be deleted with the delete command in the operating system, or it should be rendered inaccessible by removing the users' access to the index where the file or folder in question is located. While carrying out this procedure, it must be ensured that the user is not the system administrator.

d) Personal Data Located on Portable Media

Personal data located on portable media should be stored with encryption and deleted using software fit for use on this media.

e) Databases

The lines where personal data are found must be deleted with database commands (DELETE etc.). While carrying out this procedure, it must be ensured that the user is not the database administrator.

Personal data stored electronically or physically for which there are no grounds for processing is destroyed in accordance with the Guide on the Deletion, Destruction or Anonymization of Personal Data published by the Personal Data Protection Board and anonymized using the methods specified in this Guide. All actions that involve the deletion, destruction or anonymization of personal data carried out by the Technical Unit are recorded electronically with time-stamped logs. With respect to personal data in paper format, such actions are recorded with an official report which is preserved by the Technical Unit. Records as to the deletion, destruction or anonymization of personal data stored electronically or physically is preserved for three years. During the storage period, **SNI** uses the "deletion" method to make personal data inaccessible to all but the relevant department.

In the event that the storage period has ended and there are no other purposes for which to store personal data, the method of anonymization is used instead.

5.2. Destroying Personal Data

The destruction of personal data refers to the process by which personal data can never be accessed, retrieved or used again by any party. **SNI** is obligated to take all technical and administrative measures with regard to destroying personal data.

5.2.1. Methods of Destroying Personal Data

In order to destroy personal data, it is necessary to find all copies of the said data and destroy them using one or more of the methods listed below, depending on the system in which the data is located:

a) Local Systems

One or more of the methods outlined below can be used to destroy data found on local systems.

- **Physical Destruction:** Personal data on optical or magnetic media is destroyed by melting, burning, or grinding the media. Personal data is rendered inaccessible by melting, burning, or grinding optical or magnetic media. With respect to solid hard disks, if the method of overwriting or magnetization does not work, this media must also be physically destroyed.
- **Overwriting:** Refers to the process of writing random binary data (0s and 1s) at least for seven times on magnetic or rewritable optical media, thereby rendering old data irretrievable. This process is carried out using proprietary software.

b) Peripheral Systems: The methods of destruction that can be used depending on the type of medium/environment are found below:

- **Network devices (switch, router etc.):** The storage media found in these devices are fixed. The products often have a deleted command but offer no method to destroy data. Personal data must be destroyed using one or more of the methods listed in (a).
- **Flash-based media:** Personal data found on flash-based hard disks with interfaces such as ATA (SATA, PATA etc.) and SCSI (SCSI Express etc.) must be destroyed using the <block erase> command if it is supported, and if not, one or more of the methods mentioned in (a), or the method of destroying data recommended by the manufacturer must be used.

- **Mobile phones (SIM cards or fixed storage areas):** There is a delete command in smartphones; however, there is no command to destroy data. Personal data must be destroyed using one or more of the methods listed in (a).
- **Peripheral units such as printers whose data recording media are modular:** Confirming that all data storage media are taken out of the relevant devices, personal data must be destroyed by using one or more of the methods listed in (a).
- **Peripheral units such as printers whose data storage media are fixed:** There is a command to delete data in most such devices, but there isn't a command to destroy data. Personal data must be destroyed using one or more of the methods mentioned in (a).

c) Paper Format

Personal data on the said media must be destroyed by permanently destroying the media. While carrying out this procedure, the media must be shredded to pieces so small that they cannot be put back together by putting the media in a paper shredder, both horizontally and vertically, if possible.

Personal data transferred to an electronic environment by scanning a paper document must be destroyed using one of more of the methods listed in (a).

d) Cloud Environment

Personal data must be encrypted when stored or used on the said systems.

In addition to the environments mentioned above, the destruction of personal data on devices that need repair or have been sent for maintenance is carried out as follows.

- Destroying personal data found on a device using one or more of the methods mentioned in (a) before the said device is sent to third-party firms such as manufacturers, vendors, or service providers,
- In cases where it is not possible or appropriate to destroy data, removing and storing the data storage media, and sending other parts to third-party firms such as manufacturers, vendors, and service providers,
- Taking the necessary measures to ensure that the technicians who come in to do maintenance work or repairs on the equipment are not able to copy personal data and transfer it outside the company.

5.3. Anonymizing Personal Data

Anonymizing personal data refers to the process by which personal data can never be associated with an identified or identifiable person, even by cross-referencing it with other sources of data.

To verify that data is anonymized, it is necessary to ensure that data cannot be associated with an identified or identifiable person using any data storage methods, including the retrieval of the data by the data controller or recipient groups, and/or comparing the data with other data sources.

SNI takes all technical and administrative measures with regard to anonymizing personal data. **SNI** shall anonymize personal data using the methods specified in the Guide on the Deletion, Destruction and Anonymization of Personal Data.

VI. Titles, departments and job descriptions of those involved in the processes of storing and destroying personal data

SNI employs people working with the following titles, departments and job descriptions during the processes of storing and destroying data as per the Policy on the Storage and Destruction of Personal Data.

a) The "data owners" of all departments that process personal data within **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** Data owners can assign other employees from the same department to ensure that the personal data processing inventory of their own department is up to date, and to have the other employees follow the processes of storing and deleting personal data.

b) Technical Unit

VII. Table of Storage and Destruction Periods

The table of storage and destruction periods is included in the Personal Data Processing Inventory prepared for each department, and this Inventory, which is a living document and will be updated by relevant departments from time to time, is monitored and preserved by the Technical Unit.

VIII. Periodic destruction

SNI destroys personal data for which the storage period has ended and there are no other reasons or purposes for its processing within 6 months of the end of the storage period.

IX. The period of deleting and destroying data at the request of a Data Subject

When a data subject applies to **SNI** and requests the deletion or destruction of their personal data;

a) If there are no longer any grounds for processing the said personal data, **SNI** deletes, destroys or anonymizes the said data. **SNI** concludes deletion or destruction requests coming from data subjects within **"thirty days"**.

b) If there are no longer any grounds for processing personal data and the personal data subject to the request has been transmitted to third parties; **SNI** notifies the related third party of this situation and requests that the said personal data is deleted or destroyed.

If there are still grounds for processing the data, this request may be rejected by **SNI** based on Article 13 of the Law on the Protection of Personal Data, and the letter of rejection will be sent to the data subject within "thirty days" in writing or electronically.

X. Updates to be Made to the Policy on the Storage and Destruction of Personal Data

SNI submits any amendments or updates to be made to this policy to the CEO, and after receiving approval, publishes the revised articles with the date of revision and approval.

XI. Related Documents

The Policy on Corporate Information Security

SNI TEKNOLOJİ HİZMETLERİ A.Ş. The Inventory on Processing Personal Data, the Policy on the Protection of Personal Data and Privacy

The amendments made to this Policy are included in the table below.

DOCUMENT HISTORY		
Version	**Date of Publication**	**Definition of the Amendment**
v1	13.06.2017	Initial Publication
v2	08.01.2020	Optimization

TABLE OF STORAGE AND DESTRUCTION PERIODS

Process	Storage Period	Destruction Period
Personal Data Relating to Customers, Customer Employees and Business Partners	10 years after the legal relationship has ended; 3 years as per Law No. 6563 and relevant secondary regulations	The First Periodical Destruction After the Storage Period Has Ended
Personal Data Relating to Business Solution Partners / Suppliers	10 years after the legal relationship has ended	The First Periodical Destruction After the Storage Period Has Ended
CV and Professional Details Collected During Job Applications	2 years	The First Periodical Destruction After the Storage Period Has Ended
Call Center Audio Recordings	3 years	The First Periodical Destruction After the Storage Period Has Ended
Employee Email Archives	10 years after the legal relationship has ended	The First Periodical Destruction After the Storage Period Has Ended
Personal Data Relating to Online Visitors	10 years; 3 years as per Law No. 6563 and relevant secondary regulations	The First Periodical Destruction After the Storage Period Has Ended
Personal Data Relating to Potential Customers	1 year	The First Periodical Destruction After the Storage Period Has Ended
Personal Data Relating to Visitors (Camera Recordings)	3 years	The First Periodical Destruction After the Storage Period Has Ended
Personal Data Relating to Visitors / Online Visitors	2 years	The First Periodical Destruction After the Storage Period Has Ended
All Records as to Financial and Accounting Transactions	10 years	The First Periodical Destruction After the Storage Period Has Ended