The Policy on the Protection of Personal Data and Privacy

Within the scope of this Policy on the Protection of Personal Data and Privacy, **SNI TEKNOLOJİ HİZMETLERİ A.Ş.** shall be referred to as (“SNI”), and the Law No. 6698 on the Protection of Personal Data shall be referred to as the "Law".

SNI, fulfills its responsibilities arising from the Law, including those related to the processing, deletion, destruction, and anonymization of personal data, informing the data subject, and ensuring data security.

Prepared in compliance with the Law, this Policy on the Protection of Personal Data and Privacy has been made available to real persons whose personal data is being processed (data subjects).

1. The Scope and Purpose of the Policy on the Protection of Personal Data and Privacy

This Policy on the Protection of Personal Data and Privacy specifies the following:

Within the scope of **SNI's** activities;

- The manner in which personal data is collected and its legal rationale,
- Which groups have their personal data processed (data subject categorization),
- Which categories the processed data belongs to (data categories) and sample data types,
- Which purposes the relevant personal data is being used for,
- The technical and administrative measures taken to ensure the safety of personal data,
- To whom and for what purpose personal data can be transferred,
- Details relating to the sharing of personal data with public institutions and official organizations,
- The period for which personal data may be stored,
- The rights of data subjects over their own data and how they can exercise these rights.

a. The Manner in Which Personal Data is Collected and its Legal Rationale

In compliance with the personal data processing conditions stipulated in the Law and in accordance with the legal grounds specified in this Policy on the Protection of Personal Data and Privacy, **SNI** collects personal data in auditory, electronic or written form via workplaces, call centers, websites, social media accounts, email, mail, CCTV, field visits, cookies, fax, notifications from administrative and legal authorities, and other means of communication.

b. Data Subject Categorization

SNI categorizes data subjects - whose personal data is processed - as follows, and this categorization may be further expanded in light of the processes or legal reasons specified in this policy.

i. Former Employees / Retirees

ii. Employee Relative

iii. Customer / Customer Employees / Customer Business Partners

iv. Online Customer

v. Visitor

vi. Online Visitor

vii. Business Solution Partner / Supplier

c. Data Categories and Sample Data Types

No	Data Subject	Data Category	Data Type
1.	**Employee / Former Employee / Retiree**	**ID information**	Name-Last Name, Gender, Turkish Identification Number, Turkish ID information, (Certificate no, serial no, family serial no etc), Date of Birth Place of Birth, Marital Status, Passport Number
		Contact Information	Address (home), email, phone / cellphone number, email Archive
		Financial Information	Bank Account Details, Salary Details, Debt Balance, IBAN Number, Payment Details
		Employee Details	Employment Start / End Date and Time, Department, Title, Payroll Details, Leave Status, Compensation Details, Appointment Details
		Personnel and Professional Details	Insurance Details, Education, Graduation Military Service Status, Job Experience, Hobbies, Job Interviews and Assessments, Personality Inventory, Employment Start / End Records, Performance Evaluations, MLA Details, Retirement Details, References

		Information on Legal Transactions and Compliance	Contracts, Lawsuit Files, Power of Attorney
		Personal Data of a Special Nature	Signature, Disability Status, Criminal Record, Medical Report
		Fringe Benefits	Bonus Details, Meal Cards and Vehicle Allocation Details, Private Health Insurance Details
		Family Members and Relatives	Name-Last Name, Relationship, Profession, Education, Date of Birth Cellphone Number, Gender
		Other	Photo, CCTV, Log Records, Device Mac Address
2.	**Employee Relative**	**ID information**	Name-Last Name, Gender, Turkish Identification Number, Turkish ID information, (Certificate no, serial no, family serial no etc), Date of Birth Place of Birth, Marital Status, Passport Number, Driver's License
		Contact Information	Address (home), email, phone / cellphone number
		Financial Information	Income Details
		Personnel and Professional Details	Relationship, Profession, Education, Date of Birth, Cellphone Number Gender, Affiliated Organization, Graduation
3.	**Customer / Customer Employees / Customer Business Partners**	**ID information**	Name-Last Name, Gender, Turkish Identification Number, Turkish ID information, (Certificate no, serial no, family serial no etc), Date of Birth Place of Birth, Passport Number
		Contact Information	Address (home/work), email, phone / cellphone number
		Financial Information	Bank Account Details, Financial Activities, IBAN Number, Payment Details

		Customer Details	Customer Number, Customer Business Relationship Start / End Date and Rationale, Customer Requests, Customer Satisfaction Details, Product Complaints and Requests, Affiliated Organization, Database of Customer and/or Customer Business Partners
		Information on Legal Transactions and Compliance	Official Minutes (Police etc.), Power of Attorney, Signature Circular
		Personal Data of a Special Nature	Biometric Data
		Safety of Transaction	Call Center Recordings
		Marketing	Product Preferences, Customer Survey Results
		Other	CCTV
4.	**Online Visitors**	**ID information**	Name-Last Name
		Contact Information	Address (home/work), email, phone / cellphone number
		Financial Information	Bank Account Details, Payment Details
		Customer Details	Customer Number, Customer Business Relationship Start / End Date and Rationale, Affiliated Organization, Customer Requests, Customer Satisfaction Details, Product Complaints and Requests, Website Use Habits, Search Details, Customer Orders and Records, Database of Customer and/or Customer Business Partners
		Safety of Transaction	Password, Membership No., Cellphone Number
		Marketing	Product Preferences, Customer Survey Results

5.	**Visitor**	**ID information**	Name-Last Name, Turkish Identification Number, Passport Number
		Contact Information	Email, phone / cellphone number
		Safety of Transaction	5651 Logs
		Other	License Plate, CCTV
6.	**Online Visitors**	**Safety of Transaction**	Password, Membership No., Cellphone Number
		Legal Proceedings	IP Address
7.	**Business Solution Partner / Supplier**	**ID information**	Name-Last Name, Gender, Turkish Identification Number, Turkish ID information, (Certificate no, serial no, family serial no etc), Date of Birth Place of Birth, Professional IDs
		Contact Information	Address (home/work), email, phone / cellphone number
		Financial Information	Bank Account Details, Financial Activities, IBAN Number, Payment Details, Letter of Guarantee Copies/Photocopies
		CV and Professional Details	Education, Military Service Status, Sector Details, Affiliated Organization, Employment Start/End Date, Title, Insurance Details
		Information on Legal Transactions and Compliance	Signature Circular, Activity Details, Power of Attorney
		Personal Data of a Special Nature	Criminal Record, Signature, Medical Details
		Other	License Plate, CCTV, Photo

d. Our Purposes for Processing Personal Data

Personal data is used by **SNI** for the following purposes;

- For relevant business units to carry out necessary studies and related business processes for the company's business activities
- Conducting Analyses on the Effectiveness/Efficiency and/or Suitability of Business Practices, Planning and/or Execution of Business Activities
- Ensuring Business Continuity, Planning and Executing the Company's Commercial Activities
- Planning and Executing the Company's Logistical Activities
- Planning and Executing the Company's Corporate Communication Activities
- Planning and Executing the Company's Supplier Chain Management Activities
- Planning and Executing the Company's Information Security Processes
- Conducting the Company's Financial and Accounting Activities
- Planning and Executing the Company's Operational Activities
- Planning and Executing the Company's External and Internal Training Activities
- Managing the Company's Relationship with Business Partners and/or Suppliers
- Planning and Executing Sales Management Efforts for Products and/or Services
- Planning and Executing the Company's Aftersales Support Service Activities
- Planning and Executing the Company's Customer Relations Management Processes
- Following Customer Requests and/or Complaints
- Planning and Executing the Company's Market Research Efforts for the Sales and Marketing of its Products and Services
- Planning and Executing Marketing Management Efforts for Products and/or Services
- Planning and Executing the Company's Customer Satisfaction Activities
- Following Legal Matters and Fulfilling Legal Obligations
- Planning and Executing Necessary Operational Activities for Ensuring that Company Activities are Conducted as per Company Policies and/or Relevant Regulations
- Notifying Authorized Organizations pursuant to Regulations
- Planning and Executing the Company's Auditing Activities
- Ensuring the Security of the Company's Sites and/or Facilities
- Ensuring the Security of the Company's Operations
- Ensuring the Security of the Company's Sites and Movables

- Ensuring the Security of the Company's Fixed Assets and/or Resources
- Creating Visitor Records
- Planning Human Resources Processes; Conducting, Auditing, and Enhancing Business Activities
- Managing Employee Satisfaction and Loyalty Processes
- Managing Processes Related to Performance Measurement, Talent / Career Development Activities
- Managing Employee Emergency Management Processes
- Conducting Financial and Accounting Activities
- Managing Activities Related to Workplace Safety and Security
- Ensuring Data Safety, Fighting Crime, Monitoring and Auditing Internet Traffic for the Purposes of Detecting Unlawful Use and Misuse

e. Technical and Administrative Measures Taken to Ensure the Safety of Personal Data

SNI guarantees that it shall take all necessary technical and administrative measures and display due diligence in order to ensure the privacy, integrity and security of your personal data. In that regard, it takes necessary measures to prevent misuse and unlawful processing of personal data, unauthorized access to data, as well as the disclosure, modification or destruction of data.

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 (classroom or online) 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 personal environments is deleted.

Personal data obtained and processed through cookies belonging to third parties from which the company procures services or using other means is deleted from third-party systems at the end of such business relationships.

In the even 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.

f. To Whom and for What Purpose Personal Data Can Be Transferred

SNI transmits personal data only for the purposes specified in this Policy on the Protection of Personal Data and Privacy and in accordance with Articles 8-9 of the Law to domestic and international third parties.

In that regard, personal data transfers are carried out via reliable environments and channels provided by the relevant third party. Depending on the content and scope of the services procured from third parties; pseudonymous data is transferred in all cases where there is no need for the transfer of the per-

Personal data subject to the abovementioned domestic or international transfer is protected not only through the technical measures designed to ensure their security, but also through legal means in accordance with the provisions compatible with the Law that are included in our agreements, taking into account the opposing party in the legal relationship is the data controller or the data processor.

No	Data Subject	To Whom and for What Purpose Can Personal Data Be Transferred?
1.	**Employee / Former Employee / Retiree**	Sharing personal data with a lawyer in order to conduct the necessary actions in the case of a legal dispute; Sharing personal data within the scope of reporting and statistical studies; Sharing data with suppliers that will store it physically and electronically; Sharing data with the Teknocity management and the customers that will conduct field visits; Sharing data with the customers relating to professional competence within the context of business relations
2.	**Customer / Customer Employees / Customer Business Partners**	Sharing contact information with SMS or email Supplier in order to ensure that SMS or emails are sent to users to provide them with commercial and promotional content as per the Electronic Commerce Law; Sharing personal data with a Call Center in order to resolve customer requests and complaints; Sharing personal data with a lawyer in order to conduct the necessary actions in the case of a legal dispute; Sharing with a shipping company information relating to the person to whom purchased goods and related documents will be delivered; Sharing personal data within the scope of reporting and statistical studies; Sharing data with suppliers that will store it physically and electronically; Sharing personal data with third parties in order to contact customers in line with their likes and preferences.
3.	**Business Solution Partner / Supplier**	Sharing ID information with the Teknocity management in the event of an event that will be held at **SNI** premises; Sharing data with suppliers that will store it physically and electronically;

Sharing financial information with banks so that payment obligations arising from an existing business relationship can be fulfilled.

g. Details Relating to the Sharing of Personal Data with Public Institutions and Official Organizations

No	Data Subject	To Whom and for What Purpose Can Personal Data Be Transferred?
1.	**Employee / Former Employee / Retiree**	Sharing personal data with SSI during audits conducted by SSI and the Ministry of Health; Notifying relevant authorities such as the Prosecutor's Office of unlawful incidents that take place at the workplace; Sharing log records with public authorities and sharing camera recordings with official bodies such as the Prosecutor's Office and courts upon their request.
2.	**Customer / Personal Data Relating to Online Visitors** **Customer / Customer Employees / Customer Business Partners**	Sharing personal data with SSI during audits conducted by SSI and the Ministry of Health; Notifying relevant authorities such as the Prosecutor's Office of unlawful incidents that take place at the workplace; and sharing invoices and collection statements with Ministry of Finance representatives during Tax audits.
3.	**Visitor / Personal Data Relating to Online Visitors** **Visitor**	Sharing with public authorities entitled by law to request this information (in cases where SNI has a legal and administrative obligation to offer information, including - but not limited to - cases such as fight against crime, countering threats against the state and public order or similar situations) traffic data such as personal data or browsing data obtained over visits or memberships on the **SNI** website or on various websites made using the Wi-Fi connection offered by the company; Sharing log records with public authorities; sharing camera recordings with official bodies such as the Prosecutor's Office and courts upon their request.

4.	**Business Solution Partner / Supplier**	Sharing with Registry of Commerce Directorates and the notary accounting records created within the scope of relationships developed with Business Sharing personal data with relevant public authorities and the notary so that the accounting team can carry out the legally required notifications; and sharing invoices and collection statements with Ministry of Finance representatives during Tax audits.

h. The Period for Which Personal Data May Be Stored

SNI TEKNOLOJİ HİZMETLERİ A.Ş. stores the personal data it processes for certain periods of time as specified by relevant regulations or as necessary for the fulfillment of the purposes for data processing, in full compliance with the Law. You can access the Policy on the Storage and Destruction of Personal Data on **https://snitechnology.net/kvkk**. The abovementioned periods of time are as fol-

Data Type	**Storage Period**	**Legal Reason**
Personal Data Relating to Customers, Their Employees and Business Partners Customer	10 years after the legal relationship has ended 3 years as per Law No. 6563 and relevant secondary regulations	Law No. 6563, Law No. 6102, Law No. 6098, Law No. 213, Law No. 6502
Personal Data Relating to Business Solution Partners / Suppliers	10 years after the legal relationship has ended	Law No. 6102, Law No. 6098, Law No. 213
CV and Professional Details Collected During Job Applications	2 years	Contacting Former Candidates About New Positions
Call Center Audio Recordings	3 years	Law No. 6563 and relevant secondary regulations

Employee Email Archives	1 year after the legal relationship has ended	Ensuring the Continuity of Business Relationships
Personal Data Relating to Online Visitors	10 years; 3 years as per Law No. 6563 and relevant secondary regulations	Law No. 6563, Law No. 6102, Law No. 6098, Law No. 213, Law No. 6502
Personal Data Relating to Potential Customers	1 year	Conducting Retrospective Analysis
Personal Data Relating to Visitors (Camera Recordings)	3 years	Ensuring the Security of Facilities
Visitor / Personal Data Relating to Online Visitors	2 years	Law No. 5651
All Records as to Financial and Accounting Transactions	10 years	Law No. 6098

The Rights of Data Subjects over Their Own Data and How They Can Exercise These Rights

The following are the rights that data subjects have as stipulated by Article 11 of the Law:

(1) Learn whether your personal data is processed or not,

(2) Request information if your personal data is processed,

(3) Learn the purpose of your data processing and whether this data is used for intended purposes,

(4) Know the third parties to whom your personal data is transferred at home or abroad,

(5) Request the rectification of the incomplete or inaccurate data, if any,

(6) Request the erasure or destruction of your personal data under the conditions laid down in Article 7 of the Law,

(7) Request notification of the operations carried out in compliance with Articles 5-6 to third parties to whom your personal data has been transferred,

(8) Object to the processing, exclusively by automatic means, of your personal data, which leads to an unfavorable consequence for the data subject,

(9) Request compensation for the damage arising from the unlawful processing of your personal data.

In order to exercise your rights over your personal data, you can use the "Contact Form" you can find on the **SNI** website, the **SNI** official email address (**kvkk@snitechnology.net**) and the customer hot-line of **+90 212 438 04 73** to make the necessary changes, updates and/or deletions on your data and communicate any other requests.

2. Conditions Governing the Deletion, Destruction, and Anonymization of Personal Data

SNI stores personal data collected during business processes via physical and electronic means including via websites and email for a period of time specified in Article 7 and 17 of the Law and Article 138 of the Turkish Penal Code, and/or for a period of time as needed for fulfilling the purpose of processing the said data. When such periods come to an end, the data shall be deleted, destroyed or anonymized in accordance with the Regulation on Deletion, Destruction or Anonymization of Personal Data and the Guide on Deletion, Destruction, and Anonymization of Personal Data.

The deletion of personal data by **SNI** refers to the process by which personal data can never be accessed or used again by relevant users.

The destruction of personal data by **SNI** refers to the process by which personal data can never be accessed, retrieved or used again by any party.

The anonymization of personal data by **SNI** 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.

SNI explains in detail the methods of deletion, destruction and anonymization that it uses and the technical and administrative measures that it takes with respect to its Policy on the Storage and Destruction of Personal Data, prepared in accordance with the Regulation on the Deletion, Destruction or Anonymization of Personal Data. You can access the Policy on the Storage and Destruction of Personal Data on **https://snitechnology.net/kvkk**. The period of time specified for the periodic destruction of personal data specified in the Regulation on the Deletion, Destruction or Anonymization of Personal Data and the Policy on the Storage and Destruction of Personal Data is 6 months.

3. Amendments to the Policy on the Protection of Personal Data and Privacy

SNI may make amendments to this Policy on the Protection of Personal Data and Privacy at any time. These amendments and changes shall take effect immediately upon the publication of the amended Policy on the Protection of Personal Data and Privacy. You shall be duly notified of the amendments to this Policy on the Protection of Personal Data and Privacy.