LPPD Personal Data Retention and Destruction Policy

PURPOSE OF THE DESTRUCTION POLICY

Our destruction policy has been prepared in order to determine the procedures and principles to be applied by the Company regarding the deletion, destruction or anonymization of personal data in accordance with the Personal Data Protection Law No. 6698 and other legislation in accordance with the Personal Data Protection Law No. 6698 and other legislation of the personal data we hold as data controller as TTS ULUSLARARASI NAKLİYAT VE TİCARET ANONİM ŞİRKETİ ("Company").

In this context, the personal data of our employees, employee candidates, customers and all natural persons who have personal data with the Company for any reason are managed in accordance with the laws within the framework of the Personal Data Processing and Protection Policy and this Personal Data Storage and Destruction Policy.

A.1. DEFINITIONS

Direct identifiers	Identifiers that, on their own, directly reveal, expose and make distinguishable the person with whom they are in relationship,
Indirect identifiers	Identifiers that, in combination with other identifiers, reveal, disclose and make distinguishable the person with whom they are associated,
Related person	The real person whose personal data is processed,
Extermination	Deletion, destruction or anonymization of personal data,
Law	Law No. 6698 on the Protection of Personal Data published in the Official Gazette dated 07.04.2016 and numbered 29677,
Regulation	Regulation on Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28.10.2017 and numbered 30224
Board	Personal Data Protection Board
Recording media	Any medium containing personal data that is fully or partially automated or processed by non-automated means, provided that it is part of any data recording system,
Personal Data Processing and Protection Policy	The policy determining the procedures and principles regarding the management of personal data held by the Company, which can be accessed from the web address "www.tts.com.tr",
Data recording system	A recording system where personal data is structured and processed according to certain criteria,

ENVIRONMENTS AND SAFETY MEASURES

B.1. MEDIA WHERE PERSONAL DATA IS STORED

Personal data stored by the Company are kept in a recording medium suitable for the nature of the relevant data and our legal obligations.

The recording media used for the storage of personal data are generally listed below. However, some data may be kept in a different environment than the environments shown here due to their special qualities or our legal obligations. In any case, the Company acts in the capacity of data controller and processes and protects personal data in accordance with the Law, the Personal Data Processing and Protection Policy and this Personal Data Storage and Destruction Policy.

Printed media	These are environments where data are kept by printing on paper or microfilms.
Local digital environments	Servers, hard or portable disks, optical disks and other digital media within the Company.
Cloud environments	These are the environments where internet-based systems encrypted with cryptographic methods are used, which are not within the Company, but are in the use of the Company.

B.2. ENSURING THE SAFETY OF ENVIRONMENTS

The Company takes all necessary technical and administrative measures in accordance with the nature of the relevant personal data and the environment in which it is kept in order to store personal data securely and to prevent unlawful processing and access. The measures taken include, but are not limited to, the following administrative and technical measures to the extent appropriate to the nature of the relevant personal data and the environment in which it is kept.

B.2.1. Technical Measures

The Company takes the following technical measures in all environments where personal data is stored in accordance with the nature of the relevant data and the environment in which the data is stored:

- Only up-to-date and secure systems in accordance with technological developments are used in the environments where personal data are kept.

- Security systems are used for the environments where personal data are kept.

- Security tests and researches are carried out to identify security vulnerabilities on information systems, and existing or potential risks identified as a result of the tests and researches are eliminated.

- Access to the environments where personal data are kept is restricted and only authorized persons are allowed to access these data limited to the purpose of storing personal data and all accesses are recorded.

B.2.2. Administrative Measures

The Company takes the following administrative measures in all environments where personal data is stored in accordance with the nature of the relevant data and the environment in which the data is stored:

- Efforts are made to raise awareness and raise awareness of all Company employees who have access to personal data on information security, personal data and privacy.

- Legal and technical consultancy services are obtained to follow developments in the field of information security, privacy and protection of personal data and to take necessary actions.

- In the event that personal data is transferred to third parties due to technical or legal requirements, protocols are signed with the relevant third parties for the protection of personal data, and all necessary care is taken to ensure that the relevant third parties comply with their obligations under these protocols.

B.2.3. Internal Audit

Pursuant to Article 12 of the Law, the Company conducts internal audits regarding the implementation of the provisions of the Law and the provisions of this Personal Data Storage and Destruction Policy and Personal Data Processing and Protection Policy. If deficiencies or defects regarding the implementation of these provisions are detected as a result of internal audits, these deficiencies or defects shall be corrected immediately. In the event that it is understood that personal data under the responsibility of the Company is obtained by others illegally during the audit or otherwise, the Company shall notify the relevant person and the Board as soon as possible.

SECTION: DESTRUCTION OF PERSONAL DATA

C.1. REASONS FOR STORAGE AND DISPOSAL

C.1.1. Reasons for Storage

Personal data kept within the Company are stored for the purposes and reasons specified herein in accordance with the Law and our Personal Data Policy (you can access the relevant policy from the web address “www.tts.com.tr”).

C.1.2. Reasons for Disposal

Personal data within the Company shall be deleted, destroyed or anonymized ex officio in accordance with this destruction policy upon the request of the person concerned or in the event that the reasons listed in Articles 5 and 6 of the Law disappear.

The reasons listed in Articles 5 and 6 of the Law are as follows:

1. It is expressly provided for in the law

2. It is necessary for the protection of the life or physical integrity of the person who is unable to disclose his consent due to actual impossibility or whose consent is not legally valid, or of another person

3. It is necessary to process personal data of the parties to a contract, provided that it is directly related to the conclusion or performance of the contract

4. It is mandatory for the data controller to fulfill its legal obligation

5. It has been made public by the person concerned

6. Data processing is mandatory for the establishment, exercise or protection of a right

7. Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject

C.2. METHODS OF DISPOSAL

The Company deletes, destroys or anonymizes the personal data that it stores in accordance with the Law and other legislation and the Personal Data Processing and Protection Policy, upon the request of the data subject or ex officio within the periods specified in this Personal Data Retention and Destruction Policy, if the reasons requiring the processing of the data disappear.

The most commonly used deletion, destruction and anonymization techniques used by the Company are listed below:

C.2.1.1 Disposal Methods

Disposal Methods for Personal Data Stored in Printed Media	
Blackout	Personal data in printed media are erased using the blackout method. The blackout process is performed by cutting out the personal data on the relevant document, where possible, and making it invisible by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.
Disposal Methods for Personal Data Stored in Cloud and Local Digital Environment	
Secure deletion from software	Personal data stored in the cloud or in local digital environments is deleted by digital command in a way that cannot be recovered. Data deleted in this way cannot be accessed again.

C.2.1.2 Destruction Methods

Destruction Methods for Personal Data Stored in Printed Media	
Physical destruction	Documents kept in printed form are destroyed by document shredders in such a way that they cannot be reassembled.
Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri	
Physical destruction	The process of physically destroying optical and magnetic media containing personal data, such as melting, burning or pulverizing them. Data is rendered inaccessible by melting, burning, pulverizing, or passing optical or magnetic media through a metal grinder.

De-magnetization (degauss)	It is the process of exposing magnetic media to a high magnetic field and distorting the data on it in an unreadable way.
Overwriting	Random data consisting of 0s and 1s are written at least seven times on magnetic media and rewritable optical media, preventing old data from being read and recovered.
Destruction Methods for Personal Data Stored in the Cloud	
Secure deletion from software	Personal data stored in the cloud is deleted by digital command in such a way that it cannot be recovered, and all copies of the encryption keys necessary to make the personal data usable are destroyed when the cloud computing service relationship ends. Data deleted in this way cannot be accessed again.

C.2.1.3. Anonymization Methods

Anonymization is the process of making personal data impossible to associate with an identified or identifiable natural person under any circumstances, even by matching it with other data.

Removing variables	It is the removal of one or more of the direct identifiers that are included in the personal data of the person concerned and that can be used to identify the person concerned in any way. This method can be used to anonymize personal data, or it can be used to delete personal data if there is information in the personal data that is not suitable for the purpose of data processing.
Regional hiding	It is the process of deleting the information that may be distinctive for the data that is an exception in the data table where personal data are collectively anonymized.
Generalization	It is the process of bringing together personal data belonging to many people and turning them into statistical data by removing their distinctive information.
Lower and upper limit coding / Global coding	For a given variable, ranges for that variable are defined and categorized. If the variable does not contain a numeric value, then data close to each other within the variable is categorized. Values within the same category are merged.
Micro-assembly	With this method, all records in the dataset are first arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Then, the value of each subset for the specified variable is averaged and the value of that variable of the subset is replaced with the average value. In this way, the indirect

	identifiers in the data are distorted, making it difficult to associate the data with the relevant person.
Data hashing and corruption	Direct or indirect identifiers in personal data are mixed or distorted with other values, severing their relationship with the person concerned and making them lose their identifying characteristics.

In order to anonymize personal data, the Company uses one or more of these anonymization methods depending on the nature of the relevant data.

C.3. STORAGE AND DISPOSAL PERIODS

C.3.1. Retention Periods

DATA OWNER	DATA CATEGORY	DATA RETENTION PERIOD
Employee, Intern, Employee Family Member, Supplier Employee Supplier Official, Product or Service Recipient	Identity	10 years
Employee, Intern, Employee Family Member, Supplier Employee Supplier Official, Product or Service Recipient	Contact	10 years
Employee	Location	1 month
Employee, Intern,	Personnel	10 years
Employee, Shareholder Partner, Intern, Supplier Employee, Supplier Official, Product or Service Recipient	Legal Action	10 years
Supplier Employee, Supplier Official, Product and Service Recipient	Customer Transaction	10 years
Employee, Visitor	Physical Space Security	1 year
Employee, Intern,	Process Security	3 years
Employee, Supplier Employee, Supplier Official, Product or Service Recipient	Finance	10 years
Employee	Professional Experience	10 years
Product or Service Recipient	Marketing	Until the first extermination period
Employee, Intern, Visitor	Audio and Visual Recordings	10 years
Employee	Health Information	15 years
Employee, Product or Service Recipient	Bank Account Information	10 years
Employee	Family Member and Relative Information	10 years

* In the event that a longer period is stipulated in the legislation or a longer period is stipulated for statute of limitations, forfeiture period, retention periods, etc. in accordance with the legislation, the periods in the provisions of the legislation are accepted as the maximum retention period.

C.3.2. Destruction Periods

The Company deletes, destroys or anonymizes personal data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymize the personal data for which it is responsible in accordance with the Law, relevant legislation, Personal Data Processing and Protection Policy and this Personal Data Storage and Destruction Policy arises.

When the person concerned applies to the Company pursuant to Article 13 of the Law and requests the deletion or destruction of his personal data;

1. If all of the conditions for processing personal data have disappeared; The Company deletes, destroys or anonymizes the personal data subject to the request within 30 (thirty) days from the day it receives the request, explaining the reason for it, with the appropriate destruction method. In order for the Company to be deemed to have received the request, the person concerned must have made the request in accordance with the Personal Data Processing and Protection Policy. In any case, the Company shall inform the relevant person about the transaction.

2. If all the conditions for processing personal data have not disappeared, this request may be rejected by the Company by explaining the reason in accordance with the third paragraph of Article 13 of the Law and the rejection response shall be notified to the data subject in writing or electronically within thirty days at the latest.

C.4. PERIODIC DESTRUCTION

In the event that all of the conditions for processing personal data specified in the Law disappear; The Company deletes, destroys or anonymizes the personal data whose processing conditions have disappeared by a process to be carried out ex officio at recurring intervals specified in this Personal Data Storage and Destruction Policy.

Periodic destruction processes repeat every 6 (six) months.

C.5. SUPERVISION OF THE LAWFULNESS OF DESTRUCTION

The Company performs its ex officio destruction operations both upon request and in periodic destruction processes in accordance with the Law, other legislation, the Personal Data Processing and Protection Policy and this Personal Data Storage and Destruction Policy. The Company takes a number of administrative and technical measures to ensure that the destruction processes are carried out in accordance with these regulations.

C.5.1. Technical Measures

- The Company maintains technical tools and equipment suitable for each destruction method specified in this policy.

- The Company ensures the security of the place where destruction operations are carried out.

- The Company keeps access records of the persons performing the destruction process.

- The Company employs competent and experienced personnel to perform the destruction process or receives services from competent third parties when necessary.

C.5.2. Administrative Measures

- The Company works to raise awareness and raise awareness of its employees who will carry out the destruction process on information security, personal data and privacy.

- The Company receives legal and technical consultancy services in order to follow developments in the field of information security, privacy, protection of personal data and secure destruction techniques and to take necessary actions.

- In cases where the Company outsources the destruction process to third parties due to technical or legal requirements, the Company signs protocols with the relevant third parties for the protection of personal data and takes all necessary care to ensure that the relevant third parties comply with their obligations in these protocols.

- The Company regularly audits whether the destruction operations are carried out in accordance with the law and the conditions and obligations specified in this Personal Data Storage and Destruction Policy, and takes the necessary actions.

- The Company records all transactions regarding the deletion, destruction and anonymization of personal data and keeps such records for at least three years, excluding other legal obligations.

SECTION: PERSONAL DATA COMMITTEE

The Company establishes a Personal Data Committee within its organization. The Personal Data Committee is authorized and tasked with taking the necessary actions and supervising the processes for the storage and processing of the data of the data subjects in accordance with the law, the Personal Data Processing and Protection Policy and the Personal Data Storage and Destruction Policy.

The Personal Data Committee consists of three people: a manager, an administrative expert and a technical expert. The titles and job descriptions of the Company employees assigned to the Personal Data Committee are given below:

Title	**Task Description**
Personal Data Committee Manager	It is obliged to direct all kinds of planning, analysis, research, risk identification studies in the projects carried out in the process of compliance with the Law; to manage the processes to be carried out in accordance with the Law, Personal Data Processing and

	Protection Policy and Personal Data Storage and Destruction Policy and to resolve the requests received by the relevant persons.
PDP Specialist (Technical and Administrative)	It is responsible for examining the requests of the data subjects and reporting them to the Personal Data Committee Manager for evaluation; carrying out the transactions regarding the requests of the data subjects evaluated and decided by the Personal Data Committee Manager in accordance with the decision of the Personal Data Committee Manager; auditing the storage and destruction processes and reporting these audits to the Personal Data Committee Manager; carrying out the storage and destruction processes.

SECTION: UPDATE AND COMPLIANCE

The Company reserves the right to make changes to the Personal Data Processing and Protection Policy or this Personal Data Storage and Destruction Policy due to amendments to the Law, in accordance with the decisions of the Authority or in line with developments in the sector or in the field of informatics.

Amendments to this Personal Data Storage and Destruction Policy are immediately incorporated into the text and explanations regarding the amendments are explained at the end of the policy.