LPPD Personal Data Processing and Protection Policy

1.1. Introduction

As TTS ULUSLARARASI NAKLİYAT VE TİCARET ANONİM ŞİRKETİ ("Company"), we hereby present this Policy on Processing and Protection of Personal Data ("Policy") for your information in order to fulfill the obligation of disclosure within the scope of Article 10 of the Law in order to process and protect personal data in accordance with the Law No. 6698 on the Protection of Personal Data ("Law") and to inform you of all administrative and technical measures we take within the scope of processing and protection of personal data.

1.2. Purpose of the Policy

The main purpose of this Policy is to make explanations about the systems for the processing and protection of personal data in accordance with the law and the purpose of the Law, and in this context, to inform the persons whose personal data are processed by our Company, especially Company Business Partners, Employee Candidates, Visitors, Company Customers and Third Parties. In this way, it is aimed to ensure full compliance with the legislation in the processing and protection of personal data carried out by our Company and to protect all rights of personal data owners arising from the legislation on personal data.

1.3. Scope of the Policy and Personal Data Subjects

This Policy has been prepared for the persons whose personal data are processed by our Company, especially Company Business Partners, Employee Candidates, Visitors, Company Customers and Third Parties, by automatic or non-automatic means provided that they are part of any data recording system, and will be applied within the scope of these specified persons. This Policy shall in no way apply to legal entities and legal entity data.

Our Company informs the Personal Data Owners about the Law by publishing this Policy on its website. For the employees of our Company, the Personal Data Processing Policy for Employees will be applied. This Policy will not be applied if the data is not included in the scope of "Personal Data" within the scope specified below or if the Personal Data processing activity carried out by our Company is not carried out in the above-mentioned ways.

In this context, the personal data owners within the scope of this Policy are as follows:

Company Real Person Business Partner	:	Real persons with whom the Company has any kind of business relationship.
Stakeholder, Official, Employee of Company Business Partners	:	All real persons, including employees, Stakeholders and officials of real and legal persons (such as business partners, suppliers) with whom the Company has all kinds of business relations.
Company Official	:	They are the authorized real persons of the Company.

Employee Candidate	:	Real persons who have applied for a job to the Company by any means or who have opened their CV and related information to the Company's review.
Company Customer	:	Real persons who use or have used the products and services offered by the Company, regardless of whether they have any contractual relationship with the Company.
Visitor	:	All real persons who enter the physical premises owned by the Company for various purposes or visit the websites for any purpose.
Third Party	:	Other real persons who are not included in the scope of the Personal Data Protection and Processing Policy prepared for Company Employees and who are not included in any personal data owner category in this Policy.

1.4.Definitions

The terms used in this Policy shall have the meanings set out below:

Company/Our Company	:	It's TTS ULUSLARARASI NAKLİYAT VE TİCARET ANONİM ŞİRKETİ.
Personal Data(s)	:	Any information relating to an identified or identifiable natural person.
Sensitive Personal Data(s)	:	Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.
Processing of Personal Data	:	Any operation performed on Personal Data such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of Personal Data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system.
Personal Data Owner/Related Person	:	Company Stakeholders, Company Business Partners, Company Officials, Employee Candidates, Visitors, Company and Group Company Customers, Potential Customers, Third

		Parties and persons whose personal data are processed by the Company.
Data Recording System	:	It refers to the registration request where personal data is structured and processed according to certain criteria.
Data Controller	:	The natural or legal person who determines the purposes and methods of processing personal data and is responsible for the establishment and management of the data recording system.
Data Processor	:	A natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the data controller.
Open Consent	:	It is consent on a specific subject, based on information and expressed with free will.
Anonymization	:	It is the process of making the data previously associated with a person impossible to associate with an identified or identifiable natural person under any circumstances, even by matching it with other data.
Law	:	Law No. 6698 on the Protection of Personal Data.
PDP Board	:	Personal Data Protection Board.

1.5. Enforcement of the Policy

This Policy, which is issued and entered into force by the Company, is published on the Company's website (www.tts.com.tr) and made available to the relevant persons upon the request of the Personal Data Owners.

PROCESSING AND TRANSFER OF PERSONAL DATA

2.1. General Principles for Processing Personal Data

Personal Data is processed by the Company in accordance with the procedures and principles stipulated in the Law and this Policy. The Company acts in accordance with the following principles when processing Personal Data:

- Personal Data is processed in accordance with the relevant rules of law and the requirements of good faith.

- It is ensured that Personal Data is accurate and up-to-date. In this context, issues such as determining the sources from which the data is obtained, confirming its accuracy, and evaluating whether it needs to be updated are carefully considered.

- Personal Data is processed for specific, explicit and legitimate purposes. The legitimate purpose means that the Personal Data processed by the Company is related to and necessary for the business or service provided by the Company.

- Personal Data is related to the purpose in order to realize the purposes determined by the Company, and the processing of Personal Data that is not related to the realization of the purpose or is not needed is avoided. It limits the processed data only to what is necessary for the realization of the purpose. Personal Data processed within this scope are relevant, limited and proportionate to the purpose for which they are processed.

- If there is a period stipulated in the relevant legislation for the storage of data, it complies with these periods; otherwise, it retains Personal Data only for the period required for the purpose for which they are processed. In the event that there is no valid reason for further retention of Personal Data, such data shall be deleted, destroyed or anonymized.

2.2. Terms of Processing Personal Data

The Company does not process Personal Data without the explicit consent of the data subject. In the presence of one of the following conditions, Personal Data may be processed without the explicit consent of the data subject.

- The Company may process the Personal Data of Personal Data Owners in cases expressly stipulated in the laws even without explicit consent. For example; In accordance with Article 230 of the Tax Procedure Law, the explicit consent of the relevant person will not be sought in order to include the name of the relevant person on the invoice.

- Personal Data may be processed without explicit consent in order to protect the life or physical integrity of persons who are unable to disclose their consent due to actual impossibility or whose consent cannot be recognized as valid, or of another person. For example, in a situation where the person is unconscious or mentally ill and his/her consent is not valid, the Personal Data of the Personal Data Owner may be processed during medical intervention in order to protect his/her life or body integrity. In this context, data such as blood type, previous diseases and surgeries, medications used can be processed through the relevant health system.

- Provided that it is directly related to the establishment or performance of a contract by the Company, Personal Data of the parties to the contract may be processed. For example, the account number information of the creditor party may be obtained for the payment of the money pursuant to a contract concluded.

- The Company may process the Personal Data of Personal Data Owners if it is mandatory in order to fulfill its legal obligations as a data controller.

- The Company may process the Personal Data made public by the Personal Data Owners themselves, in other words, the Personal Data disclosed to the public in any way, since the legal benefit to be protected has disappeared.

- The Company may process the Personal Data of Personal Data Owners without seeking explicit consent in cases where data processing is mandatory for the exercise or protection of a legitimate right.

- The Company may process the Personal Data of Personal Data Owners in cases where the processing of Personal Data is mandatory for the provision of legitimate interests, provided that it does not harm the fundamental rights and freedoms of Personal Data Owners protected under the Law and Policy. The Company shows the necessary sensitivity to comply with the basic principles regarding the protection of Personal Data and to observe the balance of interests of Personal Data Owners.

2.3. Conditions for Processing Sensitive Personal Data

The Company does not process Special Categories of Personal Data without the explicit consent of the data subject. Personal Data relating to health and sexual life are processed by the Company only for the purposes of protecting public health, preventive medicine, medical diagnosis and treatment and care services, planning and management of health services and financing, without seeking the explicit consent of the person concerned under the conditions that we are under the obligation of confidentiality. The Company carries out the necessary procedures to take adequate measures determined by the Board in the processing of Special Categories of Personal Data.

2.4. Conditions for Transfer of Personal Data

Our Company may transfer Personal Data and Sensitive Personal Data of Personal Data Owners to third parties in accordance with the Law by establishing the necessary confidentiality conditions and taking security measures in line with the purposes of processing Personal Data. Our Company acts in accordance with the regulations stipulated in the Law during the transfer of Personal Data. In this context, in line with the legitimate and lawful Personal Data processing purposes of our Company, based on and limited to one or more of the following Personal Data processing conditions specified in Article 5 of the Law

Personal Data to third parties:

- If there is explicit consent of the Personal Data owner;

- If there is a clear regulation in the laws regarding the transfer of Personal Data, if it is mandatory for the protection of the life or physical integrity of the Personal Data owner or someone else, and

- If the Personal Data owner is unable to disclose his/her consent due to actual impossibility or if his/her consent is not legally valid,

- If it is necessary to transfer Personal Data belonging to the parties to the contract, provided that it is directly related to the establishment or performance of a contract,

- If Personal Data transfer is mandatory for our Company to fulfill its legal obligation,

- If the Personal Data has been made public by the Personal Data owner,

- If the transfer of Personal Data is mandatory for the establishment, exercise or protection of a right,

- Provided that it does not harm the fundamental rights and freedoms of the Personal Data owner, it may transfer Personal Data if it is mandatory for the legitimate interests of our Company.

2.5. Conditions for Transfer of Special Categories of Personal Data

The Company may transfer the Special Categories of Personal Data of the Personal Data Owner to third parties in the following cases in line with the legitimate and lawful Personal Data processing

purposes by taking due care, taking the necessary security measures and taking adequate measures stipulated by the PDP Board.

1. In case of explicit consent of the Personal Data Owner or

2. In the presence of the following conditions, without seeking the explicit consent of the Personal Data Owner;

- Personal Data of Special Nature other than the health and sexual life of the Personal Data Owner (race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, association, foundation or union membership, criminal conviction and security measures, and biometric and genetic data), in cases stipulated by law,

- Personal Data of Special Nature related to the health and sexual life of the Personal Data Owner only for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, by persons or authorized institutions and organizations under the obligation of confidentiality.

PURPOSES OF PROCESSING AND TRANSFER OF PERSONAL DATA, PERSONS TO WHOM PERSONAL DATA WILL BE TRANSFERRED

3.1. Purposes of Processing and Transferring Personal Data

Personal Data; in accordance with the law and the purpose of the Law,

- Managing Emergency Processes

- Execution of Information Security Processes

- Execution of Obligations Arising from Labor Contract and Legislation for Employees

- Execution of Fringe Benefits and Benefits Processes for Employees

- Conducting Audit and Ethical Activities

- Execution of Access Authorizations

- Execution of Activities in Compliance with the Legislation

- Ensuring Physical Space Security

- Execution of Finance and Accounting Affairs

- Follow-up and Execution of Legal Affairs

- Execution of Communication Activities

- Execution / Supervision of Business Activities

- Execution of Occupational Health and Safety Activities

- Execution of Logistics Activities

- Execution of Goods / Service Procurement Processes

- Execution of Goods / Services After Sales Support Services

- Execution of Goods / Service Sales Processes

- Execution of Goods / Services Production and Operation Processes

- Execution of Customer Relationship Management Processes

- Execution of Storage and Archive Activities

- Execution of Contract Processes

- Execution of Supply Chain Management Processes

- Execution of Marketing Processes of Products and Services,

- Execution of Data Controller Operations

- Providing Information to Authorized Persons, Institutions and Organizations,

- Managing Governance Activities

limited to the purposes of the Law within the scope of the personal data processing conditions specified in Articles 5 and 6 of the Law. In the event that the processing activity carried out for the aforementioned purposes does not meet any of the conditions stipulated under the Law, your explicit consent is obtained by the Company regarding the relevant processing process.

3.2. Persons to whom Personal Data will be Transferred

Personal Data may be shared with our business and solution partners, banks and third parties who perform technical, logistics and other similar operations on our behalf in order to ensure that the services provided to you are complete and flawless and only to the extent appropriate to the nature of the service. These third parties are the persons who are obliged to access the relevant information in order to provide the relevant services fully and perfectly.

Apart from these, your Personal Data may also be transferred -limited only to the relevant person or institution- in cases such as having to share data with other third parties in order to provide the service fully and flawlessly, being mandatory for the Company to fulfill its legal obligations, being expressly stipulated in the laws or having a judicial / administrative order issued in accordance with the law.

METHOD AND LEGAL REASON FOR COLLECTING PERSONAL DATA, DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA AND STORAGE PERIOD

4.1. Method and Legal Grounds for Collecting Personal Data

For the purpose of checking compliance with Article 1 regulating the purpose of the Law and Article 2 regulating the scope of the Law, Personal Data; in all kinds of verbal, written, electronic media; by technical and other methods, through various means such as company workplace, dealer, Company website, mobile application, in order to fulfill the responsibilities arising from the law within the framework of legislation, contract, request and optional legal reasons in order to fulfill the purposes set out in the Policy, it is collected and processed by the Company or data processors assigned by the Company.

4.2. Deletion, Destruction or Anonymization of Personal Data

Without prejudice to the provisions of other laws regarding the deletion, destruction or anonymization of Personal Data, the Company deletes, destroys or anonymizes Personal Data ex

officio or upon the request of the data owner in the event that the reasons requiring its processing disappear, although it has processed it in accordance with the provisions of this Law and other laws. With the deletion of Personal Data, this data is destroyed in such a way that it cannot be used and recovered in any way again. Accordingly, Personal Data shall be irreversibly deleted from the documents, files, CDs, diskettes, hard disks, etc. in which they are stored. Destruction of Personal Data, on the other hand, refers to the destruction of materials suitable for storing data such as documents, files, CDs, diskettes, hard disks, etc. in which the data is recorded in such a way that the information cannot be recovered and used again. Anonymization of data means making Personal Data impossible to be associated with an identified or identifiable natural person even if it is matched with other data.

4.3. Retention Period of Personal Data

The Company stores Personal Data for the period specified in this legislation, if stipulated in the legislation. If a period of time is not regulated in the legislation regarding how long personal data should be kept, Personal Data is processed for the period required to be processed in accordance with the practices and customs of the Company's practices and commercial life, depending on the activity carried out by the Company while processing that data, and then deleted, destroyed or anonymized.

If the purpose of processing personal data has ended and the retention periods determined by the relevant legislation and the Company have come to an end; personal data may only be stored for the purpose of constituting evidence in possible legal disputes or for the assertion or defense of the relevant right related to personal data. In the establishment of the periods here, the retention periods are determined based on the statute of limitations for the assertion of the right in question and the examples in the requests previously addressed to the Company on the same issues despite the expiration of the statute of limitations. In this case, the stored personal data is not accessed for any other purpose and access to the relevant personal data is provided only when it is required to be used in the relevant legal dispute. After the aforementioned period expires, personal data are deleted, destroyed or anonymized.

Detailed regulations regarding the Company's techniques for the storage, deletion, destruction and anonymization of Personal Data are included in the Company's Personal Data Retention and Destruction Policy.

ISSUES ON THE PROTECTION OF PERSONAL DATA

In accordance with Article 12 of the Law, the Company takes the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent unlawful processing of the Personal Data it processes, to prevent unlawful access to the data and to ensure the preservation of the data, and conducts or has the necessary audits carried out within this scope.

5.1. Ensuring the Security of Personal Data

5.1.1. Technical and Administrative Measures Taken to Ensure Lawful Processing of Personal Data

The Company takes technical and administrative measures to ensure that Personal Data is processed in accordance with the law, according to technological possibilities and implementation cost.

Technical Measures Taken to Ensure Lawful Processing of Personal Data

The main technical measures taken by the Company to ensure the lawful processing of Personal Data are listed below:

- Personal Data processing activities carried out within the Company are audited through technical systems established.

- The technical measures taken are periodically reported to the relevant person as required by the internal audit mechanism.

- Personnel knowledgeable in technical issues are employed/consulted.

Administrative Measures Taken to Ensure Lawful Processing of Personal Data

The main administrative measures taken by the Company to ensure that Personal Data is processed in accordance with the law are listed below:

- Employees are informed and trained on the law on the protection of Personal Data and the lawful processing of Personal Data.

- Personal Data processing activities carried out by the Company's business units; The requirements to be fulfilled in order to ensure that these activities comply with the Personal Data processing conditions required by the Law are determined specifically for each business unit and the detailed activity it carries out.

- In order to ensure the legal compliance requirements determined on a business unit basis, awareness is raised and implementation rules are determined for the relevant business units; the necessary administrative measures to ensure the supervision of these issues and the continuity of the implementation are implemented through internal policies and trainings.

- In the contracts and documents governing the legal relationship between the Company and the employees, records that impose the obligation not to process, disclose and use Personal Data, except for the Company's instructions and exceptions imposed by law, are included in the contracts and documents governing the legal relationship between the Company and the employees, and the obligations arising from the Law are fulfilled by raising employee awareness and conducting audits.

5.1.2. Technical and Administrative Measures Taken to Prevent Unlawful Access to Personal Data

The Company takes technical and administrative measures according to the nature of the data to be protected, technological possibilities and implementation cost in order to prevent imprudent or unauthorized disclosure, access, transfer or any other unlawful access to Personal Data.

Technical Measures Taken to Prevent Unlawful Access to Personal Data

The main technical measures taken by the Company to prevent unlawful access to Personal Data are listed below:

- Technical measures are taken in accordance with technological developments, and these measures are periodically updated and renewed.

- Access and authorization technical solutions are implemented in accordance with the legal compliance requirements determined on a business unit basis.

- Access authorizations are limited and authorizations are regularly reviewed.

- The technical measures taken are periodically reported to the relevant person as required by the internal audit mechanism, and the issues that pose a risk are re-evaluated and necessary technological solutions are produced.

- Software and hardware including virus protection systems and firewalls are installed.

- Personnel knowledgeable in technical matters are employed/consulted.

- Security scans are regularly performed to identify security vulnerabilities in applications where Personal Data is collected. It is ensured that the vulnerabilities found are closed.

Administrative Measures Taken to Prevent Unlawful Access to Personal Data

The main administrative measures taken by the Company to prevent unlawful access to Personal Data are listed below:

- Employees are trained on the technical measures to be taken to prevent unlawful access to Personal Data.

- Access and authorization processes for Personal Data are designed and implemented within the Company in accordance with the legal compliance requirements for processing Personal Data on a business unit basis.

- Employees are informed that they cannot disclose the Personal Data they have learned to anyone else in violation of the provisions of the Law and cannot use it for purposes other than processing, and that this obligation will continue after their resignation and necessary commitments are obtained from them in this direction.

- In the contracts concluded by the Company with the persons to whom Personal Data are transferred in accordance with the law; Provisions are added that the persons to whom Personal Data are transferred will take the necessary security measures to protect Personal Data and ensure that these measures are complied with in their own organizations.

5.1.3. Storage of Personal Data in Secure Environments

The Company takes the necessary technical and administrative measures according to the technological possibilities and the cost of implementation in order to store Personal Data in secure environments and to prevent its destruction, loss or alteration for unlawful purposes.

Technical Measures Taken to Store Personal Data in Secure Environments

The main technical measures taken by the Company to store Personal Data in secure environments are listed below:

- Systems in accordance with technological developments are used to store Personal Data in secure environments.

- Expert personnel are employed/consulted on technical issues.

- Technical security systems are established for storage areas, security tests and researches are carried out to identify security vulnerabilities on information systems, and existing or potential risk issues identified as a result of the tests and researches are eliminated.

- Backup programs are used in accordance with the law to ensure that Personal Data is stored securely.

- Access to the environments where Personal Data is kept is restricted and only authorized persons are allowed to access this data limited to the purpose for which the personal data is stored, and access to the data storage areas where Personal Data is stored is logged and inappropriate access or access attempts are instantly communicated to those concerned.

Administrative Measures Taken for Storing Personal Data in Secure Environments

The main administrative measures taken by the Company to store Personal Data in secure environments are listed below:

- Employees are trained to ensure that Personal Data is stored securely.

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

- In the event that an external service is obtained by the Company due to technical requirements for the storage of Personal Data, the contracts concluded with the relevant companies to which Personal Data is transferred in accordance with the law include provisions stating that the persons to whom Personal Data is transferred will take the necessary security measures to protect Personal Data and ensure that these measures are complied with in their own organizations.

5.1.4. Supervision of Measures Taken for the Protection of Personal Data

In accordance with Article 12 of the Law, the Company conducts or has the necessary audits performed within its organization. The results of these audits are reported to the relevant department within the scope of the internal functioning of the Company and necessary actions are taken to improve the measures taken.

5.1.5. Measures to Be Taken in Case of Unauthorized Disclosure of Personal Data

The Company operates a system that ensures that if the Personal Data processed in accordance with Article 12 of the Law is obtained by others illegally, this situation is notified to the relevant Personal Data Owner and the PDP Board as soon as possible. If deemed necessary by the PDP Board, this situation may be announced on the website of the PDP Board or by another method.

5.2. Observing the Legal Rights of Personal Data Subjects

The Company observes all legal rights of Personal Data Owners with the implementation of the Policy and the Law and takes all necessary measures to protect these rights. Detailed information on the rights of Personal Data Owners is provided in the sixth section of this Policy.

5.3. Protection of Special Categories of Personal Data

The Company shows utmost sensitivity to the protection of special quality Personal Data, which is determined as “special quality” by the Law and processed in accordance with the law. In this context, the technical and administrative measures taken by the Company for the protection of personal data are also implemented with the utmost care in terms of Special Categories of Personal Data and necessary audits are provided within the Company in this regard.

RIGHTS OF THE PERSONAL DATA OWNER, EXERCISE AND EVALUATION OF RIGHTS

6.1. Informing the Personal Data Owner

In accordance with Article 10 of the Law, the Company informs Personal Data Owners during the acquisition of Personal Data. In this context, if any, the identity of the Company representative, the purpose for which Personal Data will be processed, to whom and for what purpose the processed Personal Data can be transferred, the method and legal reason for collecting Personal Data and the rights of the Personal Data Owner.

6.2. Rights of the Personal Data Owner Pursuant to the PDP Law

Pursuant to Article 10 of the Law, the Company informs you of your rights; provides guidance on how to exercise such rights and carries out the necessary internal functioning, administrative and technical arrangements for all these. Pursuant to Article 11 of the Law, the Company shall notify the persons whose Personal Data is received;

- Learn whether Personal Data is being processed,

- Request information if their Personal Data has been processed,

- To learn the purpose of processing Personal Data and whether they are used in accordance with their purpose,

- To know the third parties to whom Personal Data is transferred domestically or abroad,

- To request correction of Personal Data in case of incomplete or incorrect processing,

- To request the deletion or destruction of Personal Data within the framework of the conditions stipulated in Article 7 of the Law,

- To request notification of the transactions made pursuant to subparagraphs (d) and (e) of Article 11 of the Law to third parties to whom personal data are transferred,

- To object to the emergence of a result to the detriment of the person himself/herself by analyzing the processed data exclusively through automated systems,

- In case of damage due to unlawful processing of Personal Data, to demand the compensation of the damage

that they have rights.

6.3. Cases where the Personal Data Owner Cannot Assert Their Rights

As the following cases are excluded from the scope of the Law pursuant to Article 28 of the Law, Personal Data Owners cannot assert their rights listed in Article (6.2.) of this Policy in the following cases:

- Processing of Personal Data by natural persons within the scope of activities related to themselves or their family members living in the same residence, provided that they are not disclosed to third parties and the obligations regarding data security are complied with.

- Processing of Personal Data for purposes such as research, planning and statistics by anonymizing it with official statistics.

- Processing of Personal Data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or does not constitute a crime.

- Processing of Personal Data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.

- Processing of Personal Data by judicial authorities or execution authorities in relation to investigation, prosecution, trial or execution procedures.

Pursuant to Article 28/2 of the Law; In the cases listed below, Personal Data Owners cannot assert their rights listed in Article (6.2.) of this Policy, except for the right to demand compensation for damages:

- Processing of Personal Data is necessary for the prevention of crime or criminal investigation.

- Processing of personal data made public by the Personal Data Owner himself/herself.

- Processing of Personal Data is necessary for the execution of supervisory or regulatory duties and disciplinary investigation or prosecution by authorized and authorized public institutions and organizations and professional organizations in the nature of public institutions based on the authority granted by law.

- Personal Data processing is necessary for the protection of the economic and financial interests of the State in relation to budget, tax and financial matters.

6.4. Exercise of Rights by the Personal Data Owner

Personal Data Owners will be able to submit their requests regarding their rights listed in Article (6.2.) of this Policy to the Company free of charge with the information and documents that will identify their identities and with the methods specified below or by filling out and signing the Application Form on our website www.tts.com.tr as determined by the KVK Board:

1. After the application form is filled in, a wet signed copy of the application form should be sent by hand or by registered mail to İstoç Auto and Trade Center, Askar Plaza, Floor: 2, No: 22-23 34214 Bağcılar-İSTANBUL,

2. After the application form is filled in and signed with your “secure electronic signature” within the scope of the Electronic Signature Law No. 5070, you can send it to our company .....kep.tr address,

3. Fill out the application form and send it to info@tts.com.tr.