

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	1/23


### Policy on Storage, Destruction and Anonymization of Personal Data

Document Details	
<b>Document Title:</b>	Policy on Storage, Destruction and Anonymization of Personal Data
<b>Document Content:</b>	The objective of this policy is to establish the rules in relation to the procedures for storage, destruction and anonymization of Personal Data
<b>Reference / Justification</b>	Law on the Protection of Personal Data No. 6698 Regulation on the Erasure, Destruction or Anonymization of Personal Data
<b>Approved By</b>	Executive Board of Üniteks Tekstil Gıda Motorlu Araçlar Sanayi ve Ticaret A.Ş.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	2/23

## Contents

<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA.....</b>	<b>3</b>
<b>I. SCOPE.....</b>	<b>3</b>
<b>II. DEFINITIONS.....</b>	<b>3</b>
<b>III. PURPOSE AND SCOPE .....</b>	<b>6</b>
<b>IV. RECORDING MEDIUMS .....</b>	<b>6</b>
<b>V. CIRCUMSTANCES WHICH REQUIRE STORAGE AND DESTRUCTION OF PERSONAL DATA .....</b>	<b>7</b>
<b>VI. MEASURES FOR THE STORAGE, PROCESSING AND DESTRUCTION OF PERSONAL DATA .....</b>	<b>9</b>
<b>VII. UNAUTHORIZED DISCLOSURE OF PERSONAL DATA .....</b>	<b>11</b>
<b>VIII. DESTRUCTION OF PERSONAL DATA .....</b>	<b>12</b>
<b>IX. DESTRUCTION METHODS AND PROCEDURES OF PERSONAL DATA .....</b>	<b>14</b>
<b>X. STORAGE AND DESTRUCTION DURATION .....</b>	<b>20</b>
<b>XI. INFORMATION OF PEOPLE TO TAKE PART IN THE STORAGE AND DESTRUCTION PROCESSES .....</b>	<b>21</b>
<b>XII. CHANGES TO BE IMPLEMENTED IN THE POLICY.....</b>	<b>22</b>
<b>XIII. EFFECTIVE DATE OF POLICY .....</b>	<b>23</b>

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	3/23

## Policy on Storage, Destruction and Anonymization of Personal Data

### I. SCOPE

- 1.1.** This Policy on Storage, Destruction and Anonymization of Personal Data (“**Policy**”) covers all departments, employees and 3rd parties involved in any process which Üniteks Tekstil Gıda Motorlu Araçlar Sanayi ve Ticaret A.Ş. (“**Üniteks**”) processes Personal Data.
- 1.2.** This Policy will be applied to all destruction operations, which ÜNITEKS will perform to all Personal Data, and will be implemented as a result of any destruction needs.
- 1.3.** This Policy will not be applied for data which is not Personal Data.
- 1.4.** In case that the new regulations are issued relating to the subject or of the modification of current relevant regulations, ÜNITEKS will adhere to the requirements of the regulations by updating the Policy accordingly.
- 1.5.** In case that a legal obstacle for this Policy to be implemented by ÜNITEKS is deemed to exist, ÜNITEKS will be able to re-determine the steps to be implemented, if deemed necessary.

### II. DEFINITIONS

“**Explicit Consent**” is the consent in relation to a specific topic based on informing and given with free will.


“**Recipient Group**” means the group of natural persons or legal entities, to whom the personal data are transferred by the data controller,

“**Anonymization**” refers to rendering it impossible for personal data to be associated in any manner with a real person identity of whom is identified or identifiable, even if they are matched with other data.

“**Anonymous Data**” Modified personal data in terms of the nature of personal data in such manner that they can no longer be associated to an identified or identifiable natural person even by way of matching with other data.

“**Destruction**” means the deletion, destruction or anonymization of personal data;

“**Concerned User**” means any natural person or legal entity, who processes personal data as a part of the data controller's organization or in accordance with the powers delegated and

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	4/23

instructions placed by the data controller, except for any person or unit, who or which is responsible for the storage, protection and back-up, technically, of data;

“**LPDP**” is the Law on Personal Data Protection No. 6698.

“**Recording Media**” means any medium, where the personal data are processed fully or partially automatically or through non-automatic means as a part of any data recording system

“**Personal Data**” is any kind of information about an identified or identifiable real person (in the context of this Policy, it will also include the “Special Categories of Personal Data,” under the condition that it is in line with the expression “Personal Data.”)

“**Processing Personal Data**” means any transaction performed on the data, such as obtaining, recording, storage, preservation, alteration, reorganization, disclosure, transfer, takeover, making obtainable, classifying the personal data or blocking the usage of it, by fully or partly automatic means, or by non-automatic means provided that they are part of a data recording system.

“**Committee**” refers to the committee responsible for the implementation of this Policy and the PPD Procedures to be applied in accordance with the Policy.

“**Board**” refers to the Personal Data Protection Board.


“**Authority**” refers to the Personal Data Protection Authority

“**PPD Regulations**” refers to the Law on Personal Data Protection No. 6698 and other regulation in relation to the protection of Personal Data, binding decisions, principle deliberations, provisions, directives and applicable international agreements regarding data protection and all other kinds of regulations given by regulatory and supervisory authorities, courts and other official authorities.

“**PDP Procedures**” refers to the procedures which determine the obligations which the Company employees, the Committee and Data Controller Representative need to adhere to in the context of this Policy.

“**Registry**” is the Data Controllers Registry kept by the Presidency.

“**Policy**” is the Personal Data storage and destruction policy which ÜNITEKS bases its process of determining the maximum duration required for purpose of processing of Personal Data and the process of erasure, destruction and anonymization.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	5/23

“**Special Categories of Personal Data**” refers to the data in relation to race, ethnic origin, political opinion, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, imprisonment and security measures and biometric and genetic data are special categories of personal data.

“**Deletion**” Deletion of Personal Data in a way that it becomes inaccessible or unusable by the related users.

“**Data Inventory**” Inventory including information such as the Personal Data Processing procedures and methods in terms of the Company’s Personal Data Processing operations, Personal Data Processing purposes, data category, third parties to whom Personal Data is transferred to, maximum period for processing personal data determined in line with the data subject group, precautions to be taken for transfer of data to abroad or regarding data security etc.

“**Data Recording System**” The recording system where the Personal Data are recorded and processed according to certain criteria.

“**Data Subject**” all real persons processed by a Personal Data Company or in the name of the Company.

“**Data Controller**” The real or legal persons who processes Personal Data by determining the Personal Data Processing purposes and processing methods, builds and manages the data recording system.

“**Contact Person**” refers to the real person who is assigned by the Data Controller in the course of the registration for the communication to be established with the Authority regarding the PPD Regulations.

“**Data Controller Representative**” refers to the person who is president of Committee which is responsible for the implementation of the Company's data protection policies and being compliance with the PPD Regulations in accordance with Articles 367 and 371 of the Turkish Commercial Code, and is assigned by board of directors.

“**Regulation**” It refers to Regulation on Deletion, Destruction or Anonymization of Personal Data.

“**Destruction**” means destruction of personal data in an irreversible and inaccessible and unusable manner

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	6/23

The definitions found in the Protection and Privacy of Personal Data Policy are valid for this Policy.

### III. PURPOSE AND SCOPE

**3.1.** This Policy will be implemented in relation to the real or legal persons responsible for the erasure, destruction or anonymization of Personal Data included in the Regulation issued in accordance with the 7th article and will specify the principles which should be complied by ÜNITEKS and the third parties rendered contractually responsible towards ÜNITEKS.

**3.2.** Pursuant to the Regulation, ÜNITEKS, as a Data Controller with the responsibility to enregister, is obligated to prepare a Policy to store, and when necessary, to erase, destroy or anonymize the Personal Data under its responsibility in accordance with the Personal Data Processing Inventory, as well as acting in accordance with this Policy. In this respect, ÜNITEKS has prepared this Policy with the purpose of carrying out listed obligations.

**3.3.** The following principles will be valid for the storage and destruction of Personal Data:


**3.3.1.** Adherence to the general principles in the article 4 of the Law and the principles in the article 7 of the Regulation.

**3.3.2.** ÜNITEKS accepts that having solely drawn up this Policy does not necessarily mean that the Personal Data have been erased, destroyed or anonymized in accordance with the Regulation, Law and relevant regulations.

**3.3.3.** ÜNITEKS accepts, declares and warrants that when storing or erasing, destroying or anonymizing Personal Data, it will act in adherence to the security measures indicated in the article 12 of the Law, the provisions indicated in the relevant regulations, the decisions to be taken by the Personal Data Protection Board and the Policy.

### IV. RECORDING MEDIUMS

**4.1.** ÜNITEKS agrees to include the Personal Data contained in the mediums listed below as well as the Personal Data contained in other mediums which may emerge in addition thereto, in its Policy.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	7/23

- 4.1.1. Computers/servers used in the name of ÜNITEKS
- 4.1.2. Network devices
- 4.1.3. Shared/unshared disc drivers used in the network for data storage
- 4.1.4. Cloud systems
- 4.1.5. Mobile phones and its all storage areas
- 4.1.6. Paper
- 4.1.7. Microfiche
- 4.1.8. Peripheral units such as printers, fingerprint scanner
- 4.1.9. Magnetic bands
- 4.1.10. Optic discs
- 4.1.11. Flash drives

## **V. CIRCUMSTANCES WHICH REQUIRE STORAGE AND DESTRUCTION OF PERSONAL DATA**

In the event that a violation within the scope indicated below has taken place, it shall be accepted as a Potential Security violation incident and action shall be taken by ÜNITEKS. ÜNITEKS shall take all technical and administrative measures to ensure secure storage of Personal Data and for prevention of unlawful processing of and access to Personal Data.

### **5.1. Circumstances which Require Personal Data to be Stored**

ÜNITEKS is obligated to store Personal Data pursuant to the regulations when; (i) it is prescribed clearly in laws, , (ii) it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.(iii) it is required to process the personal data of the contracting parties, provided that it is related to the conclusion or execution of a contract,(iv) it is required in order to carry out a legal obligation (v) it is essential to process the data in order to establish, use or protect a right (vi) it is required for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the Data Subject. ÜNITEKS is also entitled to store Personal Data upon; (i) obtaining explicit consent, (ii) there are exceptions indicated in articles 5(2) and 6(3).

### **5.2. Circumstances which Require Personal Data to be Destroyed**

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	8/23

### 5.2.1. Unlawfulness

ÜNITEKS warrants that it will not process Personal Data in an unlawful manner.

As long as the exceptions defined in the provisions of article 5 and 6 of the Law with regard to processing Personal Data and special categories of Personal Data are in question.

- a. ÜNITEKS does not store the Personal Data of people who have not given explicit consent apart from the exceptions indicated in the Law
- b. In case that ÜNITEKS stores special categories of Personal Data, it processes the data in accordance with the relevant regulation with the knowledge of the LPDP Committee. In this respect, within the framework of the article6(4) of the Law, measures determined or to be determined by the Board shall be taken.

### 5.2.2. Removal of Data Processing Conditions


ÜNITEKS is responsible for updating the data processing conditions and shares this responsibility with all its employees.

In the event that the data processing conditions have completely been removed, employees cannot continue to process data. ÜNITEKS Information Technology Department is responsible for erasing, destroying or anonymizing Personal Data, the conditions of which have been removed, in accordance with this Policy.

ÜNITEKS agrees that data processing conditions are removed in the circumstances listed below and those indicated in the Regulation:

- a. Modification or repeal of the provisions of related legislation which constitute the basis of processing Personal Data,
- b. Not being agreement executed between parties, being the agreement invalid, automatic termination of the agreement, termination or renouncement of the agreement,
- c. Being the purpose of processing Personal Data no longer valid,
- d. Being the processing of Personal Data illegal or against integrity rules,
- e. In case that Personal Data is only processed based on the explicit consent, withdrawing the consent by the related person,



	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	9/23

- f. Duly made application by the related person in relation to the processing of the Personal Data within the framework of the rights in the (e) and (f) sub clause of the article 11 of the Law,
- g. Making a complaint to the Board and being it deemed appropriate by the Board in case that Data Controller rejects the request of the related person to erase or destroy the Personal Data, its response is considered unsatisfactory or it does not respond within the period of time prescribed in Law,
- h. In case of exceeding the maximum duration of Personal Data storage, not existing any requirement which justifies keeping the Personal Data for a longer period of time.


## **VI. MEASURES FOR THE STORAGE, PROCESSING AND DESTRUCTION OF PERSONAL DATA**

For the Personal Data to be stored, processed and accessed in adherence to the law, ÜNİTEKS takes technical and administrative measures according to the characteristic of the data to be protected, the technological possibilities and implementation costs.

### **6.1. Technical Measures**

The main technical measures taken by ÜNİTEKS in order to prevent the illegal storage, processing and access to Personal Data are listed below:

- 6.1.1.** Technical measures in line with developments in technology are taken, and these measures are updated and renewed periodically.
- 6.1.2.** In accordance with requirements of legal conformity determined on a work unit basis, an authorization matrix has been constructed, a personal account management system has been installed and an encryption system has been activated.
- 6.1.3.** In this respect; software and hardware consisting of virus protection systems and firewalls are installed, logs are kept, regular back-ups are done.
- 6.1.4.** Necessary software and hardware are installed to ensure network security, authority checks and penetration tests are carried out every 6 months. In this context, firewalls and intrusion identification and prevention systems are installed.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	10/23

**6.1.5.** Technical measures are periodically reported to the ÜNITEKS LPDP Committee as required by the internal auditing mechanism, factors that are identified as risks are evaluated again and necessary technological solutions are generated.

**6.1.6.** Data for which there is no explicit consent and which do not qualify as legal exceptions are used by being masked.

**6.1.7.** Personnel with technical knowledge are recruited and these people are made permanent members of the ÜNITEKS's LPDP Committee.

## **6.2. Administrative Measures**


The main administrative measures taken by ÜNITEKS in order to prevent the illegal storage, processing and access to Personal Data are listed below:

**6.2.1.** ÜNITEKS has informed its employees and provided them with necessary training regarding the Personal Data Protection regulations. In the framework of the training, roles and responsibilities were explained to employees and they were informed the principle of “everything is prohibited unless it is permitted” is implemented, rather than the principle of “anything that is not prohibited is permitted.” Confidentiality agreements are signed for Personal Data Protection and necessary warrants have been obtained from employees that they will not disclose the Personal Data they obtained to others in breach of relevant legislative provisions and that this liability will continue after the end of their employment. In this framework; the provisions in accordance with the Law have been added to Employment Contracts and discipline regulations. The disciplinary procedures to be implemented in the events which these warrants and other obligations of confidentiality are not adhered to during in-house organizations have been prepared.

**6.2.2.** ÜNITEKS warrants to inform their employees every 6 months and that they will keep the information up to date.

**6.2.3.** ÜNITEKS have completed the necessary preparations to be able to submit notifications to the Information System of Data Controllers Registry.

**6.2.4.** In accordance with the work unit based legality requirements, Personal Data access and authorization procedures within the Company have been designed and are being implemented.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	11/23

- 6.2.5.** Provisions are inserted to the agreements ÜNITEKS concludes with parties to whom Personal Data is transferred: that parties whom the Personal Data transferred to will take necessary security measures for the protection of the Personal Data and that they will ensure adherence to these measures in their own organizations.
- 6.2.6.** Necessary arrangements have been implemented in the scope of this Policy in terms of Access, Information Security, Use, Storage and Destruction.
- 6.2.7.** The Personal Data Processing Inventory has been prepared and necessary provisions have been included in the agreements related to processing, preservation and transfer of Personal Data,
- 6.2.8.** Necessary Preparations for Internal Periodic and/or Random Auditing have been completed. Necessary measures have been taken to conduct Risk Analyses.
- 6.2.9.** Corporate communication procedures and briefing processes in the event of violation has been indicated in this Policy.

### **6.3. The Auditing of Measures Taken in Relation to the Protection of Personal Data**


ÜNITEKS carries out necessary audits in accordance with the article 12 of LPDP through the ÜNITEKS LPDP Committee created within the company or has another entity carry out. The results of these audits are reported to the relevant department within the Company's internal operations and necessary operations are carried out to improve measures taken.

## **VII. UNAUTHORIZED DISCLOSURE OF PERSONAL DATA**

ÜNITEKS has regulated the procedure to be followed in the event of the violation of Data security regulations indicated in the relevant legislations and this Policy, within the context of this Policy.

### **7.1. Violations within ÜNITEKS**

In the event a ÜNITEKS employee detects a violation or is faced with a possible violation, he/she shall communicate the situation to the relevant department supervisor and shall inform the department supervisor of how he/she noticed the violation and where it originated from. The department supervisor shall take the first measures to stop the violation if it is still continuing and if ended, to determine the extent of the violation, and shall inform the ÜNITEKS LPDP Committee director of the situation. The president shall obtain support from the IT department

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	12/23

in order to take measures against the violation and shall contact the legal department. The president shall gather the ÜNITEKS LPDP Committee within 24 hours as of the violation being identified; shall share reports of the extent, scope and outcomes of the violation with the Executive Board.

## 7.2. Violations in Third Parties

The ÜNITEKS LPDP Committee President, in the event a third party working with ÜNITEKS detects a violation or is faced with a possible violation, contacts the legal department and, if necessary, the IT department within 12 hours as of the violation being identified. The president gathers the ÜNITEKS LPDP Committee within 24 hours as of the report of the violation; shall share the reports of the extent, scope and outcomes of the violation obtained from the other party with the Executive Board and the Committee.


## VIII. DESTRUCTION OF PERSONAL DATA

The destruction of Personal Data can be carried out in three different ways: erasure, destruction or anonymization of data. The purpose of the destruction process is to ensure that it would be impossible to identify the real person with the remaining data. ÜNITEKS shall take all possible technical and administrative measures to ensure the legal erasure, destruction and anonymization of Personal Data.

### 8.1. Erasure of Personal Data

The erasure of Personal Data processed with completely or partly automatic means is the process which transforms Personal Data in question into a state which cannot be accessed or used again in any way by Related Users.

The Data Controller shall explain how the conditions indicated in the article 7(3) of the Regulation for Personal Data in the related policy and procedures to be regarded as erased. The erasure of Personal Data processed with non-automatic means and constitute as part of any Data Recording System; the process carried out by means of anonymizing unneeded hardcopy Personal Data, transferred on to an electronic media by means of scanning or without digitizing, is done in instances which ÜNITEKS has processed the data completely or partly automatic means; and ÜNITEKS, in the events which they have delete the Personal Data, transforms the data into a state which they cannot be accessed or used again. ÜNITEKS guarantees that as they

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	13/23

are carrying out this process, none of the data can be accessed or used again by a user. This guarantee is the responsibility of ÜNITEKS.

The erasure methods mentioned are dependent on the Regulation and when necessary, updates are the responsibility of ÜNITEKS.

## **8.2. Destruction of Personal Data**

The process of destruction will be carried out in the instances which ÜNITEKS has processed the data in a physical data record media and ÜNITEKS is obligated to transform this data into state which they cannot be accessed, cannot be used again or be re-generated.


During these processes, ÜNITEKS employees and relevant departments are obliged to notify the ÜNITEKS LPDP Committee of the data to be destroyed, and ÜNITEKS will take all necessary technical and administrative measures thereupon.

## **8.3. Anonymization of Personal Data**

The anonymization process, in the event ÜNITEKS has processed the Personal Data by completely or partly automatic means, is to render such Personal Data impossible to be associated with a real person identified or identifiable, even if they are matched with other data.

The anonymization of Personal Data is the duty of the data owner work unit within ÜNITEKS. The data owner work unit of can obtain support from different departments within ÜNITEKS for the destruction of the data, provided that the supervision will be carried out by them.

ÜNITEKS, during the process of anonymization, may use the methods indicated within this Policy. In the event the correctness of the method to be applied is doubted, ÜNITEKS must consult the LPDP Committee.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	14/23

## IX. DESTRUCTION METHODS AND PROCEDURES OF PERSONAL DATA

For the destruction of Personal Data, ÜNITEKS shall determine all methods which can be used during the destruction process in this Policy. The data owner work unit is responsible for determining and implementing the suitable method for the suitable condition as indicated in this Policy.

### 9.1. Erasure

During the process of erasure of Personal Data , ÜNITEKS employees carry out the erasure process by selecting a suitable method from those listed below:

#### a. Cloud Systems

Data found in the cloud system is erased by issuing a command to erase data. ÜNITEKS, while carrying out the process mentioned, shall ensure that the Relevant User is not authorized to retrieve the data erased from the cloud system.

#### b. Personal Data Stored in Hardcopy

Personal Data stored in hardcopy are erased by means of blacking out. The process of blacking out is carried out by either cutting out the Personal Data on the relevant document if possible, or transforming it into a state which makes them invisible to Relevant Users by means of permanent ink in a manner, ensuring it is irreversible and cannot be deciphered via technological solutions.

#### c. Office Files Stored in the Central Server

The file is deleted by the delete command within the processing system or access to the file or the index where the file is, is removed. While the process mentioned is being carried out, it is ensured that the Relevant User is not the system manager at the same time.

#### d. Personal Data Stored in Mobile Media

Personal Data in flash storage medium are stored cryptically and deleted via appropriate software for such medium

#### e. Databases

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	15/23

Related rows where the Personal Data is found is deleted with database commands (DELETE, etc.). While the process mentioned is being carried out, it is ensured that the Relevant User is not the database manager at the same time.

## 9.2. Destruction

During the destruction process of Personal Data, ÜNITEKS employees shall carry out the destruction process by selecting the appropriate method from those listed below:

### a. Overwriting

Is the process of transforming old data into an illegible state by writing random data consisting of 0s and 1s at least 8 times, with magnetic media and rewritable optical media software.

### b. Magnetizing

Is the process of transforming data into an illegible state by causing magnetic media to undergo physical transformation in a high-order magnetic field.

### c. Physical Destruction

Is the physical destruction process carried out by optical media or magnetic media to melt, pulverize, grind and the like. May be applied in instances which magnetizing or overwriting methods are unsuccessful.

### d. Cloud Systems


Is the destruction process of all copies of the encryption keys of Personal Data following the implementation of the destruction notification of the Personal Data stored in cloud systems by the contractual service provider.

### e. Destruction of Personal Data Found in Peripheral Systems

Is the destruction process of internal units if applicable, if not, by implementing overwriting, magnetizing or physical destruction of all devices storing Personal Data found in systems such as the printer, fingerprint scanner, and entrance turnstiles. It is obligatory for these processes to be applied prior to the back-up, maintenance and similar processes of these devices.

### f. Destruction of Personal Data as Hardcopy and in Microfiche Media

As Personal Data found in such media are permanently and physically written, the main media is destroyed. As this process is being carried out, the media is divided into small pieces with paper destruction or shredding machines into incomprehensible dimensions,

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	16/23

horizontal and vertically if possible, in a manner which they cannot be pieced together again.

Personal Data transmitted from original format to an electronic media by means of scanning are destroyed with one or more of the methods listed above, depending on the electronic media they are found in.

### 9.3. Anonymization

As a result of anonymization, the data obtained renders impossible the identification of the real person or their identifiable quality within a group or crowd, in a manner which cannot be associated with the real person.

In the event that ÜNITEKS decides to anonymize a Personal Data rather than erase or destroy it, it shall fulfil the following conditions:

- a. To render it impossible for the anonymity to be reversed by means of matching one anonymized data set with another.
- b. To render it impossible for more than one value to form a meaningful whole in a manner which can turn an entry into a singular state.
- c. To render it impossible for the values in the anonymized data set to connect and produce an estimate or result.

Due to the risks stated above, ÜNITEKS carries out regular checks on the anonymized data sets and makes sure the anonymity is protected.

When the anonymizing methods indicated below are applied, ÜNITEKS takes into account the quality of the data, the size, its tendency to be found in physical media, its variety, the benefit to be gained / purpose of processing, the processing frequency, the security of the party it will be transferred to, the meaningfulness of the effort to be spent on anonymizing it, the magnitude of the harm which may emerge if the anonymization is ruined, the area of influence, the distributional/collectivism rate, checking the Users' authority to access related data, the construction of an attack which will ruin the anonymization and the possibility of the effort to be spent to be meaningful.



	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	17/23

Having anonymized a data, ÜNITEKS checks whether the data known to be found within the institutions and organizations the Personal Data has been transferred to has the quality of rendering a person identifiable again, or again in case that public information is used.

During the process of anonymizing Personal Data, ÜNITEKS employees select a suitable method from the list below and carry out the anonymization process:

### 9.3.1. Anonymization Methods Which Do Not Render Value Irregularity

With methods which do not render value irregularity, a modification or an addition, subtraction of the values of the data set are not applied; instead, modifications are made to the complete row located in the set.

#### a. Removing the Variables

The anonymization method which involves completely removing one or more of the variables by means of deleting them completely from the table. In such an instance, the whole column is removed from the table.

#### b. Removing Entries

With this method, anonymization is strengthened with the removal of a row composed of a singularity in the data set and the possibility of generating predictions in relation to the data set is reduced.

#### c. Sectional Concealment

The aim of the sectional concealment method is to render the data set more secure and to reduce its risk of predictability. If the combination created by the value belonging to a specific record is producing a rare situation and this situation has a high potential of causing the person to become identifiable, the value creating the exceptional situation is changed to “unknown.

#### d. Generalization

Is the process of converting the related Personal Data from a specific value to a more general value. The new values obtained as a result of generalization presents total values or statistics belonging to a group which renders it impossible to access one person.

#### e. Upper and Lower Limit Coding

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	18/23

Upper and lower limit coding method is created by connecting the remaining values within the group created by the category which is defined for a certain variable. Generally, the upper and lower values of a variable are brought together and these values are defined anew.

**f. Global Coding**

Global coding is a grouping method used in instances which upper and lower coding is not applicable, in data sets which do not include numeric values or have values which cannot be sorted numerically. It is generally used in instances which it eases the process of classifying certain values and generate predictions and estimations. By creating a new, common group for the selected values, all the entries in the data set are changed with this new definition.

**g. Sampling**


In the sampling method, instead of the whole data set, a sub set taken from the set is announced or shared. This way, as it is not possible for it to be known whether a person who is known to be part of the whole data set is part of the shared sub set sample, the risk of on-point predictions to be generated about that person is reduced. Basic statistical methods are used to determine the sub set to be sampled.

**9.3.2. Anonymization Methods Which Render Value Irregularity**

Different from methods which render value irregularity and those mentioned above, distortions are created in the values of the data set by changing present values. In this case, as the values carried by entries are changing, the benefit desired to be gained from the data set must be calculated correctly. Even if the values in the data set are changing, by ensuring the total statistics are not distorted, the data can still be taken advantage of.

**a. Micro Integration**

With this method, all the values in the data set are first sorted according to a meaningful sequence and the whole set is later separated into a certain number of sub sets. Later, by calculating the average of the values belonging to the sub set's determined variable, the value belonging to that variable of the sub set is changed with the average value. This way, the average value of that variable valid for the whole data set will not have changed.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	19/23

**b. Data Exchange**

The data exchange method is the entry changes obtained by the exchange of values belonging to the lower set variable between a selected pair from the entries. This method is basically used for variables which can be categorized and the main idea is to transform the database by changing the values of variables in entries belonging to individuals.

**c. Noise Addition**

With this method, additions or eliminations are done to create distortions within a certain measure in a selected variable. This method is mostly applied to data sets consisting of numeric values. Distortion is applied to each value at an equal rate.

**9.3.3. Statistical Methods Strengthening Anonymization**

As a result of some values in the entries found in anonymized data sets coming together with individual scenarios, the possibility of persons in the entries becoming identifiable or the possibility of estimations derived in relation to the Personal Data may arise. For this reason, anonymization is strengthened by means of reducing the singularity of the entries in the data set to a minimum by implementing various statistical methods in the anonymized data sets

The main purpose of these methods is to keep the benefit to be gained from the data set at a certain level by reducing the risk of the anonymization being ruined to a minimum.


**a K-Anonymity**

K-anonymity has been developed to prevent private information displaying singularities in certain combinations from being exposed by means of ensuring more than one person to be identified in certain areas of a data set. In the event of more than one entry belonging to combinations created by the integration of some variables in the data set being found, the identifiability of people who fit this combination reduces.

**b L-Diversity**

Created as a result of the studies carried out on the insufficiencies of K-anonymity, the L-diversity method takes into account the variety created by sensitive variables fitting the same variable combinations.

**c T-Closeness**

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	20/23

T-Closeness is the process of anonymization which involves calculating the degree of closeness of values amongst themselves and separating the data set into sub classes according to these degrees of closeness.

## X. STORAGE AND DESTRUCTION DURATION

### 10.1. Periodic Destruction and Legal Storage Duration

Physical and digital data which have reached the end of their legal storage and destruction duration are periodically destroyed. In the first periodical destruction process following the date on which the obligation to delete, destroy or anonymize Personal Data is due, ÜNITEKS shall delete, destroy or anonymize Personal Data. Periodic Destruction is carried out every 6 months for all Personal Data. Legal storage and destruction durations to take into account during Periodic Destruction are indicated in the ÜNITEKS Personal Data Processing Inventory and this Policy. ÜNITEKS guarantees adherence to new duration periods in the event which the Board shortens these periods in the framework of the Regulation clause 11(4).

Transactions related to the data which has been deleted, destroyed and anonymized are kept for at least 3 years, free of other legal obligations. ÜNITEKS reserves the right to store Personal Data resulting from other legal obligations.

### 10.2. Erasure and Destruction Periods in the Event of Data Owners Request

In case that data owners submit a request to ÜNITEKS for their Personal Data to be erased or destroyed, ÜNITEKS shall evaluate the current situation of Personal Data processing conditions and take the relevant actions accordingly.

If all conditions of Personal Data processing have been removed, Personal Data in question is erased, destroyed or anonymized. ÜNITEKS resolves the request of the related person in thirty days the latest, and informs the related person.

If the Personal Data processing conditions have been completely removed and the Personal Data in question has been transferred to third parties, the Data Controller informs the third party of

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	21/23


the situation; it is ensured that necessary procedures are carried out within the framework of the Regulation before the third party.

If the Personal Data processing conditions have not completely been removed, ÜNITEKS may reject the request by justifying it to the related data owner and informs the related person of their response of rejection in thirty days the latest, either in written form or via an electronic platform.

## **XI. INFORMATION OF PEOPLE TO TAKE PART IN THE STORAGE AND DESTRUCTION PROCESSES**

ÜNITEKS has formed the “ÜNITEKS LPDP Committee” within itself in adherence to the deliberation of the ÜNITEKS Board of Directors in order to manage this Policy along with other policies related with this Policy. The responsibilities of this committee are indicated below.

- a.** Preparing the basic policies related to the Protection and Processing of Personal Data and submitting them to the Executive Board for implementation.
- b.** Deciding how the implementation and supervision of the Protection and Processing of Personal Data will be carried out and assigning duties within the company in this framework, and submitting matters of ensuring coordination to the Executive Board.
- c.** Identifying provisions which need to be ensured for adherence to the law and relevant regulations and submitting necessary actions to the Executive Board, monitoring the implementation and ensuring coordination.
- d.** Increasing awareness of organizations within ÜNITEKS and those in collaboration with ÜNITEKS in terms of the Protection and Processing of Personal Data.
- e.** Ensuring necessary measures are taken upon determining the possible risks in the company’s Personal Data processing operations; submitting suggestions of improvement to the Executive Board.
- f.** Designing and ensuring the carrying out of training in Personal Data Protection and practicing policies.
- g.** Resolving the applications of Personal Data owners at the utmost level.
- h.** Coordinating the implementation of briefing and training operations to ensure Personal Data owners are informed about Personal Data processing operations and legal rights.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	22/23

- i. Preparing the changes in the basic policies related to the Protection and Processing of Personal Data and submitting them to the Executive Board for implementation.
- j. Keeping track of the developments and regulations concerning the Protection of Personal Data; presenting the Executive Board with suggestions regarding what is required to be done within the Company in accordance with these developments and regulations.
- k. Coordinating the relations with the Board and Authority.
- l. Carrying out other duties assigned by the Executive Board regarding the protection of Personal Data.

Member No.	Title	Unit
1.	Chief Financial Officer / Data Controller Representative	Financial Affairs Department
2.	R&D Manager / Contact Person	Research & Development Center
3.	Internal Audit and Project Consultant	Internal Audit and Project Department
4.	Human Resources and Organizational Transformation Coordinator	Human Resources Department
5.	Information Technologies Manager	Information Technologies Department
6.	Foreign Trade Manager	Foreign Trade Department
7.	Human Resources Manager	Human Resources Department
8.	Purchasing Manager	Purchasing Department
9.	Supplier Relations Manager	Supplier Development Department
10.	Production Manager	Production Department
11.	Plant Manger	Motor Division

## XII. CHANGES TO BE IMPLEMENTED IN THE POLICY

**12.1.** Following all kinds of official changes to be made in the PDP Regulations, modifications can be made by ÜNITEKS with the approval of the Executive Board to ensure conformity to these changes. In case of discrepancy between the PDP Regulations in force and the Policy, the provisions of the PDP Regulations shall prevail.

	<b>POLICY ON STORAGE, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA</b>	İlk Yayın Tarihi	21.01.2020
		Doküman No	KVK.UNI-EN-002
		Revizyon No	00
		Revizyon Tarihi	21.01.2020
		Sayfa No	23/23

**12.2.** ÜNİTEKS will share the changes made to this Policy as well as the updated Policy in a trackable manner with its employees via e-mail or via their corporate intranet for the access of their employees.

### **XIII. EFFECTIVE DATE OF POLICY**

This version of the Policy on Storage, Destruction and Anonymization of Personal Data has entered into force on **21/01/2020** upon approval of the Executive Board of the ÜNİTEKS.