

TSRA TRAINING AND CONSULTANCY PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1. PURPOSE OF PREPARATION OF THE INTRODUCTION AND POLICY

This Personal Data Retention and Destruction Policy ("Policy"), the Law on the Protection of Personal Data No. 6698 ("KVKK" or "Law") and the Regulation on the Deletion, Destruction or Anonymization of Personal Data ("Regulation"), which was published in the Official Gazette dated October 28, 2017, which constitutes the secondary regulation of the Law, and the process of determining the maximum storage period required for the purpose for which personal data are processed It has been prepared by TSRA Eğitim ve DANIŞMANLIK ("TSRA") in its capacity as data controller in order to be used as a basis for deletion, destruction and anonymization processes and to inform the relevant persons about these transactions.

2. SCOPE

This policy covers all employees, consultants and affiliates, suppliers, customers and other real and legal persons with whom the institution has other legal relations, personal data defined by law and sensitive personal data that are fully or partially automated or processed non-automatically, provided that they are part of any data recording system. Unless otherwise stated in the policy, personal data and sensitive personal data will be referred to as "Personal Data" together.

3. DEFINITIONS

Explicit Consent: Consent on a specific subject, based on information and expressed with free will.

Relevant User: Persons who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and backup of the data.

Destruction: Deletion, destruction or anonymization of personal data.

Law/KVKK: Law No. 6698 on the Protection of Personal Data.

Recording Media: Any medium containing personal data that is fully or partially automated or processed by non-automatic means, provided that it is a part of any data recording system.

Personal Data: Any information relating to an identified or identifiable natural person.

Processing of Personal Data: Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means, provided that it is a part of any data recording system.

Anonymization of Personal Data: Making personal data unable to be associated with an identified or identifiable natural person in any way, even by matching it with other data.

Deletion of Personal Data: Deletion of personal data; making personal data inaccessible and unusable for the Relevant Users in any way.

Destruction of Personal Data: The process of making personal data inaccessible, unrecoverable and unusable by anyone in any way.

Board: Personal Data Protection Board.

Sensitive Personal Data: Data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Periodic Destruction: In the event that all of the conditions for processing personal data in the Law disappear, the process of deleting, destroying or anonymizing personal data to be carried out ex officio at repeated intervals specified in the personal data storage and destruction policy.

Data Owner/Relevant Person: The real person whose personal data is processed.

Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Regulation: Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette on October 28, 2017.

4. RULES

TSRA acts within the framework of the following principles in the storage and destruction of personal data:

4.1. In the deletion, destruction and anonymization of personal data, the principles listed in Article 4 of the Law and the technical and administrative measures to be taken within the scope of Article 12 and specified in Article 6.2 of this Policy, the provisions of the relevant legislation, the decisions of the Board and this Policy are fully complied with.

4.2. All transactions regarding the deletion, destruction and anonymization of personal data are recorded by TSRA and these records are kept for at least 1 year, excluding other legal obligations.

4.3. Unless otherwise decided by the Board, we choose the appropriate method of deleting, destroying or anonymizing personal data ex officio. However, upon the request of the Relevant Person, the appropriate method will be selected by explaining the reason.

4.4. In the event that all of the conditions for processing personal data in Articles 5 and 6 of the Law are eliminated, personal data is deleted, destroyed or anonymized by TSRA ex officio or upon the request of the person concerned. In case of application to TSRA by the Relevant Person in this regard;

4.4.1. The submitted requests are finalized within 30 (thirty) days at the latest and the relevant person is informed,

4.4.2. In the event that the data subject to the request has been transferred to third parties, this situation is notified to the third party to whom the data has been transferred and it is ensured that the necessary actions are taken before the third parties.

5. EXPLANATIONS REGARDING THE REASONS REQUIRING STORAGE AND DESTRUCTION

Personal data belonging to data subjects, in particular by TSRA

- To be able to maintain service activities,
- Fulfillment of legal obligations,
- Planning and performance of employee rights and benefits
- Managing customer relationships
- In order to carry out the sales activities of goods/services, it is stored securely in the above-mentioned physical or electronic environments within the limits specified in the KVKK and other relevant legislation.

5.1. The reasons for storage are as follows:

- Storing personal data as it is directly related to the establishment and performance of contracts,
- Storing personal data for the purpose of establishing, exercising or protecting a right,
- It is obligatory to store personal data for the legitimate interests of TSRA, provided that it does not harm the fundamental rights and freedoms of individuals,
- Storing personal data for the purpose of fulfilling any legal obligation of TSRA,
- The legislation clearly stipulates the storage of personal data,

- Obtaining the explicit consent of the data owners in terms of storage activities that require the explicit consent of the data owners.

5.2. Pursuant to the Regulation, personal data belonging to data owners are deleted, destroyed or anonymized by TSRA ex officio or upon request in the following cases:

5.2.1. Amendment or abolition of the provisions of the relevant legislation that form the basis for the processing or storage of personal data,

5.2.2. The disappearance of the purpose requiring the processing or storage of personal data,

5.2.3. Elimination of the conditions requiring the processing of personal data in Articles 5 and 6 of the Law.

5.2.4. In cases where the processing of personal data takes place only on the basis of explicit consent, the person concerned withdraws his consent,

5.2.5. The person concerned is entitled to comply with Article 11 of the Law. Acceptance by the data controller of the application for the deletion, destruction or anonymization of personal data within the framework of the rights in subparagraphs (e) and (f) of the article,

5.2.6. In cases where the data controller rejects the application made to him by the person concerned with the request for the deletion, destruction or anonymization of his personal data, his answer is found insufficient or he does not respond within the period stipulated in the Law; A complaint is made to the Board and this request is approved by the Board,

5.2.7. Despite the fact that the maximum period requiring the storage of personal data has passed, there are no conditions that would justify storing personal data for a longer period of time.

6. STORAGE AND DISPOSAL PERIODS

In determining the retention and destruction periods of your personal data obtained by TSRA in accordance with the provisions of the KVKK and other relevant legislation, the following criteria are used, respectively:

6.1. If a period of time is stipulated in the legislation regarding the storage of the personal data in question, this period is complied with. After the expiry of the said period, action is taken on the data within the scope of subparagraph 2.

6.2. In the event that the period stipulated in the legislation regarding the storage of the personal data in question expires or no period is stipulated in the relevant legislation regarding the storage of the data in question, respectively;

6.2.1. Personal data is classified as personal data and sensitive personal data, based on the definition in Article 6 of the KVKK. All personal data that is found to be of a private nature is destroyed. The method to be applied in the destruction of the data in question is determined according to the nature of the data and the importance of its storage before TSRA.

6.2.2. Compliance of the storage of data with the principles specified in Article 4 of the KVKK, for example; It is questioned whether the TSRA has a legitimate purpose in storing the data. Data whose storage is found to be contrary to the principles in Article 4 of the KVKK is deleted, destroyed or anonymized.

6.2.3. It is determined which and which of the exceptions stipulated in Articles 5 and 6 of the KVKK can be considered within the scope of the storage of data.

6.2.4. Within the framework of the exceptions identified, reasonable periods for which the data should be stored are determined. If these periods expire, the data is deleted, destroyed or anonymized.

The storage, destruction and periodic destruction periods determined by TSRA are defined as 1 time in 6 months.

Personal data whose storage period has expired are destroyed in 6-month periods in accordance with the procedures set out in the Policy.

All transactions related to the deletion, destruction and anonymization of personal data are recorded and these records are kept for at least three years, excluding other legal obligations.

7. PROCEDURES FOR STORAGE AND DESTRUCTION OF PERSONAL DATA BY TSRA

7.1. RECORDING MEDIA

Personal data belonging to data owners are securely stored by TSRA in the environments listed in the table below, in accordance with the relevant legislation, especially the provisions of the KVKK, and within the framework of international data security principles:

7.1.1. Electronic media:

- Servers (Domain, backup, email, database, web, file sharing, etc.)
- Software (office software, portal, EBYS, VERBIS.)
- Information security devices (firewall, intrusion detection and blocking, log file, antivirus, etc.)
- Personal computers (Desktop, laptop)
- Mobile devices (phone, tablet, etc.)
- Removable memories (USB, Memory Card, etc.)

7.1.2. Physical environments:

- Paper
- Written, printed, visual media

7.2. TECHNICAL AND ADMINISTRATIVE MEASURES

All administrative and technical measures taken by TSRA within the framework of the principles in Article 12 of the KVKK in order to securely store your personal data, to prevent unlawful processing, access and destruction of data in accordance with the law are listed below:

7.2.1. Administrative Measures:

Within the scope of TSRA administrative measures;

- It restricts internal access to stored personal data to the personnel who are required to access it by job description. In limiting access, whether the data is of special nature and its importance is also taken into account.
- In the event that the processed personal data is obtained by others illegally, it notifies the person concerned and the Board as soon as possible.
- Regarding the sharing of personal data, it signs a framework agreement on the protection of personal data and data security with the persons with whom the personal data is shared, or ensures data security with the provisions added to the existing contract.
- It employs personnel who are knowledgeable and experienced about the processing of personal data and provides necessary training to its personnel within the scope of personal data protection legislation and data security.
- It carries out and has the necessary audits carried out in order to ensure the implementation of the provisions of the Law before its own legal entity. It eliminates the privacy and security vulnerabilities that arise as a result of the audits.

7.2.2. Technical Measures:

Within the scope of TSRA technical measures;

- Performs the necessary internal controls within the scope of the established systems.
- Within the scope of the established systems, it carries out the processes of information technology risk assessment and business impact analysis.
- It ensures that the technical infrastructure that will prevent or observe the leakage of data outside the institution is provided and the relevant matrices are created.
- It provides control of system vulnerabilities by receiving penetration testing services regularly and when needed. e. It ensures that the access rights of employees in information technology units to personal data are kept under control.
- The destruction of personal data is ensured in such a way that it cannot be recycled and does not leave any trace of audit.
- Pursuant to Article 12 of the Law, all kinds of digital media in which personal data are stored are protected by encrypted or cryptographic methods to meet information security requirements.

7.3. STAFF

The personnel involved in the personal data storage and destruction process are determined annually by the KVK Committee and announced within the institution.

7.4. METHODS OF DESTRUCTION OF PERSONAL DATA

Personal data obtained by TSRA in accordance with the KVKK and other relevant legislation will be destroyed by TSRA ex officio or upon the application of the Relevant Person, in accordance with the provisions of the Law and relevant legislation, with the following techniques, in the event that the personal data processing purposes listed in the Law and Regulation disappear. The procedures and principles regarding the techniques for deletion and destruction of personal data by TSRA are listed below:

7.4.1. Deletion of Personal Data:

- **Software-Enabled Deletion:** While deleting data processed by fully or partially automated means and stored in digital media; Methods are used to delete the data from the relevant software in a way that makes it inaccessible and unusable in any way for the Relevant Users.

Deletion of the relevant data in the cloud system by giving the delete command; removal of the user's access rights on the file or directory where the file is located on the central server; Deleting the relevant lines in databases with database commands or deleting the data on portable media, that is, flash media, using appropriate software can be counted within this scope.

However, if the deletion of personal data will result in the inability to access and use other data in the system, personal data will be deemed to be deleted if the personal data is archived by making it unable to be associated with the person concerned, provided that the following conditions are met.

It is closed to the access of any other institution, organization or person,

Taking all necessary technical and administrative measures to ensure that personal data is accessed only by authorized persons.

- **Secure Deletion by Expert:** In some cases, it may agree with an expert to delete personal data on its behalf. In this case, the personal data is securely deleted by the expert in this field in such a way that it is inaccessible and unusable for the Relevant Users in any way.
- **Blackening of Personal Data in Paper Environment:** In order to prevent the misuse of personal data or to delete the data requested to be deleted, it is the method of physically cutting the relevant personal

data out of the document or making it invisible by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.

7.4.2. Destruction of Personal Data:

- **De-magnetization:** It is a method of unreadable distortion of the data on the magnetic media by passing it through special devices where it will be exposed to high magnetic fields. It should be noted that if the destruction is not successful with this method, the destruction process can only be completed by physically destroying the media.
- **Physical Destruction:** Personal data can also be processed non-automatically, provided that it is a part of any data recording system. While destroying such data, the system of physical destruction of personal data is applied in a way that cannot be used later. The destruction of data in paper and microfiche media should also be carried out in this way, since it is not possible to destroy them in any other way.
- **Overwriting:** The overwrite method is a data destruction method that makes it impossible to read and recover old data by writing random data consisting of 0s and 1s at least seven times over magnetic media and rewritable optical media through special software.

During the occurrence of the above-mentioned situations, TSRA; It fully complies with the provisions of KVKK, Regulation and other relevant legislation in order to ensure data security and takes all necessary administrative and technical measures.

7.4.3. Techniques for Anonymizing Personal Data:

The procedures and principles regarding the anonymization techniques of personal data by TSRA are listed below: Anonymization Methods That Do Not Provide Value Irregularity

Anonymization methods that do not provide value irregularity, without any change or addition/removal of the stored personal data; These are the anonymization methods applied by generalization, displacement of any personal data group, or removal of a certain data or sub-data group from the group.

- **Variable Extraction:** After combining the collected data by extracting descriptive data, the "high-order descriptive" variables in the created data set are removed and the existing data set is anonymized.
- **Extracting Records:** In the de-recording method, the data row containing a singularity between the data is removed from the records and the stored data is anonymized. For example, if there is only one employee with a doctorate degree in a company, the remaining data can be anonymized by removing the data of this person from the records where the educational status, department and age data of other employees are kept.
- **Regional Hiding:** In the regional hiding method, if a single data is decisive due to the fact that it creates a rarely visible combination, hiding the relevant data provides anonymization. For example, if only one person among the employees in the company's social activity group has more than 50 years of experience, writing 'Unspecified' instead of 'Seniority:50+' or leaving this field blank in a dataset where seniority, department and position information are stored together will provide anonymization.
- **Lower and Upper Limit Coding:** With the lower and upper limit coding method, the values in a data group with predefined categories are anonymized by combining them by determining a certain criterion.
- **Generalization:** With the data aggregation method, many data are aggregated and personal data is made unassociable with any person. For example; Showing that there are A number of personnel with a bachelor's degree and B number of personnel with a master's degree, without specifying the education levels of the personnel individually.
- **Global Coding:** With the data derivation method, a more general content is created from the content of personal data and it is ensured that personal data cannot be associated with any person.

7.4.4. Anonymization Methods That Provide Value Irregularity

Contrary to those that do not provide value irregularity in anonymization methods that provide value irregularity, it creates deterioration by changing some data in personal data groups. While using these methods, deviations will need to be applied carefully in line with the expected/desired benefit. By ensuring that the total statistics are not distorted, the expected benefit from the data can continue to be achieved.

- **Adding Noise:** The method of adding noise to the data, especially in a data set where numerical data is predominant, is anonymized by adding some deviations in the plus or minus direction to the existing data at the determined rate. The deviation is applied equally to each value.
- **Micro Merge:** In the micro merge method, all data will first be divided into groups by arranging them in a meaningful order (such as from largest to smallest), and anonymization will be achieved by taking the average of the groups and writing the value obtained instead of the relevant data in the current group.
- **Data Exchange:** In the data exchange method, the values of a variable are exchanged between the pairs selected from the stored data. The purpose of this method, which is used for data that can be categorized in general, is to transform the database by replacing the data of the data owners with each other.

Pursuant to Article 28 of the KVKK, if personal data is processed for purposes such as research, planning and statistics by anonymizing it with official statistics, this will be outside the scope of the Law and explicit consent will not be required.

8. MISCELLANEOUS

In case of inconsistency between the provisions of the KVKK and other relevant legislation and this Policy, the provisions of the KVKK and other relevant legislation will be applied first.

This Policy prepared by TSRA entered into force on 04.07.2025. In case of changes in the Policy, the effective date of the Policy and the relevant articles will be updated accordingly.