USERSDOT TECHNOLOGY AND CONSULTING INC.

USERSDOT DATA RETENTION AND DISPOSAL POLICY

2024

TABLE OF CONTENTS

1. PURPOSE

USERSDOT TECHNOLOGY AND CONSULTANCY INC. has prepared the 'Personal Data Retention and Disposal Policy' in order to determine the procedures and principles regarding the storage and disposal (deletion, destruction, anonymization) activities carried out. In line with the fundamental principles,

USERSDOT TECHNOLOGY AND CONSULTANCY INC. has prioritized the lawful processing of personal data of individuals categorized as employees, shareholders/partners, job candidates, real person customers/employees/authorities, employees/authorities of legal person customers, employees/authorities of potential business partners, employees/authorities of business partners, and third-party visitors in accordance with the Constitution, International Treaties, GDPR, Personal Data Protection Law No. 6698, and other relevant legislation, as well as ensuring effective exercise of the rights of the relevant individuals. The procedures for the storage and disposal of personal data are carried out in accordance with the policy prepared in this direction."

2. SCOPE

The personal data of individuals categorized as employees, shareholders/partners, job candidates, real person customers/employees/authorities, employees/authorities of legal person customers, employees/authorities of potential business partners, employees/authorities of business partners, and third-party visitors, collected, transferred to, and processed by USERSDOT TECHNOLOGY AND CONSULTANCY INC. fall within the scope of this policy. This policy regulates the rules for deletion, destruction, or anonymization of all personal data collected by the Company, transferred to the Company, and processed by the Company. This policy applies to all record environments where the personal data owned by the Company is processed and/or shared within its own structure or by third parties, as well as to activities related to personal data processing.

3. DEFINITIONS AND ABBREVIATIONS

Recipient Group: The category of natural or legal persons to whom personal data is transferred by the data controller.

Explicit Consent: Consent based on information regarding a specific issue and expressed with free will.

Anonymization: Rendering personal data in such a way that the identity of the data subject cannot be identified or linked to any identifiable individual, even when combined with other data.

Employee: An individual who works for the company.

Electronic Environment: Environments where personal data can be created, read, modified, and written using electronic devices.

Non-Electronic Environment: All other environments excluding electronic environments, such as written, printed, visual, etc.

Service Provider: An individual or legal entity providing services to the company under a specific contract.

Data Subject: The natural person whose personal data is processed.

Related User: Individuals processing personal data within the data controller organization, excluding those responsible for the technical storage, protection, and backup of data, or individuals processing personal data within the data controller organization based on authorization and instructions received from the data controller.

Destruction: Deleting, destroying, or anonymizing personal data.

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

Record Environment: Any environment where personal data, either entirely or partially automated or non-automated, is processed as part of any data recording system.

Personal Data: Any kind of information related to an identified or identifiable natural person.

Personal Data Processing Inventory: An inventory created by data controllers, associating their personal data processing activities with the purposes and legal bases for processing personal data, data categories, recipient groups to whom the data are transferred, and the group of data subjects, detailing the maximum retention period necessary for the purposes of processing, any personal data intended for transfer to foreign countries, and the measures taken for data security.

Processing of Personal Data: Any operation performed on personal data, whether wholly or partially automated, or non-automated, including obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, taking over, making it available, classifying, or preventing its use.

Board: Personal Data Protection Board.

Institution: Personal Data Protection Institution.

Special Category Personal Data: According to Article 6 of the Law, these are data that, if disclosed, could lead to discrimination or cause harm to the individuals concerned. According to the Law, these data include information about individuals' race, ethnic origin,

political opinion, philosophical belief, religion, sect, or other beliefs, appearance and clothing, membership of associations, foundations, or unions, health, sexual life, criminal conviction, and data related to security measures, as well as biometric and genetic data.

Periodic Destruction: The process of deletion, destruction, or anonymization stipulated within the personal data retention and destruction policy, to be automatically conducted at recurring intervals in the event that all processing conditions for personal data specified in the law cease to exist.

Policy: Personal Data Retention and Destruction Policy.

Registry: The registry maintained by the Presidency of the Personal Data Protection Authority, containing information about data controllers.

Data Processor: The individual processing personal data on behalf of the data controller, acting under the authorization granted by said data controller.

Data Recording System: The system in which personal data is structured and processed according to specific criteria.

Data Controller: The legal or natural person responsible for determining the purposes and methods of processing personal data, as well as for establishing and managing the data recording system.

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

4. RECORDING MEDIA

Personal data is securely stored in compliance with the law by the Company in the environments listed in Table 1.

Table 1: RECORDİNG MEDİA OF PERSONAL DATA

Electronic Environment	Non-Electronic Environment
➢ Servers (domain, cloud, backup, email, database, web, file sharing, etc.) ➢ Software (office software, portal) ➢ Information security devices (firewall, intrusion detection and prevention, log files, antivirus, etc.) ➢ Personal computers (desktop, laptop) ➢ Mobile devices (phone, tablet, etc.) ➢ Optical disks (CD, DVD, etc.) ➢ Removable storage devices (USB, memory card, etc.)	➢ Paper ➢ Manual data recording systems (visitor logbook) ➢ Written, printed, visual media

5. ROLE AND RESPONSIBILITY

USERSDOT TECHNOLOGY AND CONSULTING INC. provides active support to responsible units within all employees and departments of the company to ensure the proper implementation of technical and administrative measures taken within the scope of the Policy, to increase the training and awareness of unit employees, to monitor and continuously audit, and to prevent the unlawful processing of personal data, prevent unauthorized access to personal data, and ensure the lawful storage of personal data in all environments where personal data is processed.

The Company is responsible for the approval of this Policy. It is the authorized approval mechanism to ensure the creation, publication, updating when necessary, and abolition of this Policy. The implementation of practices related to the Policy, the enhancement and monitoring of activities within the company, are the responsibility of the Company. The Company determines relevant units and takes measures for the execution of authorization and supervision processes.

6. LEGAL OBLIGATION

6.1.Information Obligation

The data controller, within the framework of Article 10 of the Law No. 6698 on the Protection of Personal Data, is obliged to provide the following information to the relevant individual personally or through an authorized person during the acquisition of personal data:

- The identity of the data controller and, if any, its representative,
- The purpose of processing personal data,
- To whom and for what purpose personal data may be transferred,
- The method and legal reason for collecting personal data,
- Other rights listed in Article 11 of the Law.

6.2. Obligation to Ensure Data Security

According to Article 12 of the Law regarding data security, the data controller is obliged to:

- Prevent the unlawful processing of personal data,
- Prevent unauthorized access to personal data,
- Ensure the security of personal data.

7. EXPLANATIONS REGARDING STORAGE AND DISPOSAL

The personal data of individuals categorized as employees, shareholders/partners, job candidates, real person customers/employees/authorized persons, employees/authorized persons of legal entity customers, employees/authorized persons of potential business partners, employees/authorized persons of business partners, and third-party visitors by USERSDOT TECHNOLOGY AND CONSULTANCY INC. are stored and disposed of in accordance with Law No. 6698 on the Protection of Personal Data.

In this context, detailed explanations regarding storage and disposal are provided below in sequence.

7.1.Disclosures Regarding Retention

In accordance with Article 3 of Law No. 6698 on the Protection of Personal Data, the concept of processing personal data is defined, and Article 4 stipulates that processed personal data must be relevant, limited to the purpose for which they are processed, and kept for the period prescribed by the relevant legislation or for the duration necessary for the purpose of processing. Articles 5 and 6 list the conditions for processing personal data. Accordingly, within the scope of our activities as the data controller, personal data is stored for the period prescribed by the relevant legislation or for the duration necessary to achieve our processing purposes.

7.2.Legal Reasons Requiring Retention

Personal data processed within the activities of USERSDOT TECHNOLOGY AND CONSULTING INC. is kept for the duration prescribed by the relevant legislation. In this context, personal data is retained for the periods stipulated under the following laws and regulations:

- Law No. 6698 on the Protection of Personal Data

- Turkish Code of Obligations No. 6098

- Law No. 5651 on Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications

- Turkish Commercial Code No. 6102

- Social Insurance and General Health Insurance Law No. 5510

- Occupational Health and Safety Law No. 6331

- Labor Law No. 4857

- Social Services Law No. 2828

- Tax Procedure Law No. 213

- Law No. 6502 on the Protection of Consumers

- Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Attachments

Personal data is retained until the need for the data ceases or until the first periodic destruction process after the need ceases, in cases where the law does not prescribe a specific duration for retention.

7.3.Reasons Requiring Destruction

Personal datas;

- Changes or annulments in the relevant legislation provisions constituting the basis for processing,
- Cessation of the purpose that requires processing or storage,
- In cases where the processing of personal data occurs solely based on explicit consent, the withdrawal of consent by the data subject,
- Acceptance by USERSDOT TECHNOLOGY AND CONSULTING INC. of the application made by the data subject for the deletion and destruction of personal data within the framework of the rights of the data subject in accordance with Article 11 of the Law on the Protection of Personal Data No. 6698,
- In cases where USERSDOT TECHNOLOGY AND CONSULTING INC. rejects the application made by the data subject for the deletion, destruction, or anonymization of personal data, finds the response inadequate, or fails to respond within the period prescribed by the Law; filing a complaint with the Board and the Board finding the complaint appropriate,
- In cases where the maximum period requiring the storage of personal data has expired and there are no conditions justifying the storage of personal data for a longer period, upon the request of the data subject, the personal data is deleted, destroyed, or anonymized by USERSDOT TECHNOLOGY AND CONSULTING INC. or ex officio deleted, destroyed, or anonymized.

8. TECHNICAL AND ADMINISTRATIVE MEASURES

Personal data controller companies take technical and administrative measures within the framework of the adequate precautions determined and announced by the Board, pursuant to Article 12 and the fourth paragraph of Article 6 of the Law No. 6698 on the Protection of Personal Data, to securely store personal data, prevent their unlawful processing and access, and ensure the lawful destruction of personal data, especially for sensitive personal data.

8.1.Technical Measures

The Company takes the following measures as a minimum in order to ensure the security of the personal data it processes, to prevent unlawful access and to prevent unlawful data processing.

- Network security and application security are ensured.
- Closed system networks are used for transferring personal data over the network
- Key management is implemented.
- Security measures are taken in the procurement, development, and maintenance of

information technology systems.

- Security of personal data stored in the cloud is ensured.
- An authorization matrix is created for employees.
- Access logs are regularly maintained.
- Corporate policies on access, information security, usage, storage, and disposal have been developed and implemented.
- Data masking measures are implemented when necessary.
- Current anti-virus systems are utilized.
- Firewalls are employed.
- Signed contracts include data security provisions.
- Personal data is backed up, and the security of backed-up personal data is ensured.
- Log records are maintained in a manner that prevents user intervention.
- Secure encryption/cryptographic keys are used for sensitive personal data and managed by different units.
- Intrusion detection and prevention systems are used.
- Penetration testing is conducted.
- Cybersecurity measures are implemented and continuously monitored for compliance.
- Encryption is applied.
- Data loss prevention software is used.

8.2.Administrative Measures

- Discipline regulations containing data security provisions are in place for employees.
- Regular training and awareness programs on data security are conducted for employees.
- Privacy commitments are made.
- The permissions of employees undergoing role changes or leaving the company in this field are revoked.
- Policies and procedures for personal data security are established.
- Personal data security issues are promptly reported.
- Monitoring of personal data security is conducted.
- Necessary security measures are taken for access to physical environments containing personal data.
- Security against external risks (fire, flood, etc.) is ensured for physical environments containing personal data.
- Security of environments containing personal data is maintained.
- Personal data is minimized whenever possible.
- Internal periodic and/or random audits are conducted.
- Existing risks and threats are identified.
- Protocols and procedures for the security of special category personal data are established and implemented.
- Data processing service providers undergo regular audits regarding data security.
- Data processing service providers are made aware of data security practices.

9. PERSONAL DATA DESTRUCTION METHODS

At the end of the period prescribed by the relevant legislation or the necessary storage period for the purposes for which they were processed, personal data is destroyed by USERSDOT TECHNOLOGY AND CONSULTING INC, either ex officio or upon the request of the data subject, in accordance with the relevant legislation, using the techniques specified below.

9.1.Deletion of Personal Data

Data erasure is the process of rendering personal data inaccessible and unusable for the relevant users. Even if processed in compliance with the relevant legal provisions, personal data may be erased or destroyed at its own discretion or upon the request of the data subject when the reasons requiring processing cease to exist and situations regulated in the Regulation arise.

During the erasure of data, the following rules and standards prescribed by the legislation must be adhered to:

- Data must be erased from the physical documents in which they are recorded.
- Data must be erased from the physical files in which they are recorded.
- Data must be erased from the digital environments in which they are stored.
- Data must be erased from magnetic media such as camera recordings or tape backups in which they are stored.
- In cases where the destruction of the entire medium is not necessary, data erasure procedures must be performed.
- Data must be erased from backup devices and storage units used for backup purposes (e.g., cloud storage, etc.) that are not actively used.
- Data processed entirely or partially through automated means and stored in digital environments are erased using the data deletion methods of the relevant software.

9.2.Destruction of Personal Data

Data destruction is the process of rendering personal data inaccessible, irretrievable, and unusable by anyone. The destruction process is carried out when data is processed in physical record environments. Through this process, the data is made irrecoverable.

During data destruction, compliance with the procedures/standards prescribed by the legislation and the following rules is essential:

- Data is destroyed in a manner that renders it unusable from the physical documents in which it is recorded.

- Data is destroyed in a manner that renders it unusable from the physical files in which it is recorded.
- Data is destroyed in a manner that renders it unusable from the digital environments in which it is stored.
- Data is destroyed in a manner that renders it unusable from the magnetic media in which it is stored.
- If data is present in digital or magnetic environments but does not require the destruction of the entire medium, deletion procedures are performed, and the data is destroyed.

9.3.Anonymization of Personal Data

Anonymization of personal data refers to rendering personal data such that it cannot be associated with any identified or identifiable natural person, even when combined with other data.

The process of anonymizing personal data can be achieved through the following methods and procedures prescribed by legislation:

a) Data Masking:

Data masking involves encrypting directly identifiable personal data to protect it within the database or storing it in a manner that eliminates uniqueness, preventing the retrospective identification of the individual's data. For example, the T.C. Identification number field within the personal data can be masked using a cryptographic method such as sha512 upon the individual's request. However, the same method is not applied to the individual's name, as applying the same method could potentially lead to identifying a unique person based on individuals sharing the same name. Another example of masking is applying the same graphical information while destroying fingerprint images.

b) Data Derivation:

Data derivation aims to prevent the association of personal data with the individual by restructuring it in a way that makes recycling impossible, using methods such as spreading parasites or scattering random characters. For instance, grouping the city data from openly addressable locations, and randomly populating the remaining fields (street, house number, etc.) with characters.

During the anonymization process, various methods can be applied based on the characteristics of the data fields and the capabilities of the relevant databases and software. Different methods can be used for different data fields, such as using distinct methods for T.C. Identification numbers and addresses. Successfully anonymized data can no longer be considered personal data. Therefore, obtaining the explicit consent of the individual is not required for the anonymization process, and the individual cannot exercise the rights provided by the Personal Data Protection Law (KVKK) and relevant legislation regarding anonymized information.

10. STORAGE AND DISPOSAL PERIODS

The company ensures that the personal data processed within the scope of its activities is stored in compliance with the legal statutory periods, and the process of resensitively deleting, destroying, or anonymizing personal data whose storage periods have expired is carried out by the Data Controller.

In accordance with Article 11 of the Regulation, USERSDOT TECHNOLOGY AND CONSULTING INC. has determined the periodic destruction period as 6 months. Accordingly, periodic destruction is carried out in the company every year in June and December.

11. PUBLICATION AND STORAGE OF THE POLICY

The policy is published in two different formats: wet-signed (printed paper) and electronic, and it is also available on the company's website.

12. UPDATING THE POLICY

The policy is updated and republished as needed.

USERSDOT TECHNOLOGY AND CONSULTING INC.