EagleBurgmann®

a member of EKK and FREUDENBERG

RELY ON EXCELLENCE

PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. The purpose of this policy is to set out the procedures and principles for the deletion, destruction or anonymization of personal data that are processed in a fully or partially automatic or non-automated way, provided that they are part of any data recording system.

2. This policy; It has been prepared in accordance with the Regulation on the Deletion, Elimination, or Anonymization of Personal Data prepared on the basis of subparagraph (e) of the first paragraph of Article 22 and the third paragraph of Article 7 of Law No. 6698.

3. Company; It has prepared this personal data retention and destruction policy in accordance with personal data processing inventory.

4. Definitions

4.1. Recipient group: It is the category of natural or legal person to whom personal data is transferred by the data controller.

4.2. Relevant user: Persons who process personal data within the data controller organization or in accordance 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.

4.3. Destruction: It is the process of deleting, destroying or anonymizing personal data.

4.4. Recording medium: It refers to any medium in which personal data are processed, which are fully or partially automated or processed in non-automated ways, provided that they are part of any data recording system.

4.5. Personal data processing inventory: Personal data processing activities carried out depending on the business processes of the data responsible; is the inventory that they detailed by describing the purpose of processing personal data, the data category, the group of recipients transmitted, and the maximum time required for the purposes for which the personal data is processed, the personal data foreseen to be transferred to foreign countries, and the measures taken for data security.

4.6. Personal data retention and destruction policy: It is the policy that data supervisors make the basis for determining the maximum time required for the purpose for which the personal data is processed, and for deleting, destroying and anonymizing.

4.7. Periodic destruction: Refers to the process of deleting, destroying or anonymizing personal data, which will be carried out ex officio at regular intervals specified in the policy of destruction and in the event that all of the personal data contained in the law disappear.

4.8 Registration: It refers to the records of data officers kept by the Presidency of Personal Data Protection Authority.

4.9. Data recording system: It refers to the recording system where personal data is processed according to certain criteria.

4.10. Data controller: It refers to the real 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.

4.11. Deleting personal data Deleting personal data is the process of making personal data inaccessible and unusable for the users concerned.

4.12. Destruction of personal data The destruction of personal data is the process of making personal data inaccessible, irreversible and reusable by anyone.

4.13. Anonymizing personal data It is in any way that personal data can not be associated with an identified or identifiable natural person even if it is matched with other data. In order for personal data to be anonymized; personal data must be rendered unrelated to an identifiable or identifiable natural person, even by using appropriate techniques for the recording environment and related field of activity, such as bouncing, recipient or groups of recipients, and matching data with other data.

5. Recording media organized by personal data retention and destruction policy:

5.1. Paper media

5.1.1. Paper

5.1.2. Manual data recording systems (forms visitor entry book)

5.1.3. Written, printed, visual media

5.2. Electronic environments

5.2.1. Servers (Domain, backup, email, database, web, file sharing, etc.)

5.2.2. software

5.2.3. Information security devices (firewall, intrusion detection and blocking, log file, antivirus etc.)

5.2.4. Personal computers (Desktop, laptop)

5.2.5. Mobile devices (phone, tablet etc.)

5.2.6. Optical discs (CD, DVD etc.)

5.2.7. Removable memory (USB, Memory Card etc.)

5.2.8. Printer, scanner, copier

6. Legal Reasons Requiring Storage

6.1. Law No. 6698 on Protection of Personal Data,

6.2. Turkish Code of Obligations No. 6098, 6.3. Public Procurement Law No. 4734,

6.4. Civil Servants Law No. 657,

6.5. Social Insurance and General Health Insurance Law No. 5510,

6.6. Editing the Publications on the Internet No. 5651 and These Publications

6.7. Law on Combating Crimes Committed Through

6.8. Public Financial Management Law No. 5018,

6.9. Occupational Health and Safety Law No. 6331,

6:10. Law of Information Retrieval, No. 4982,

6:11. Law on Exercise of the Right to Petition No. 3071

6:12. Labor Law No. 4857,

6:13. Higher Education Law No. 2547,

6.14. Retirement Health Law No. 5434,

6.15. Social Services Law No. 2828

6.16. Implementing Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Add-ons,

6.17. Regulation on Archive Services

6.18. Other secondary regulations in force under these laws within the framework of the prescribed storage periods.

7. Processing Purposes Requiring Storage

7.1. Execution of Emergency Management Processes

7.2. Execution of Information Security Processes

7.3. Conducting Employee Candidate / Trainee / Student Selection and Placement Processes

7.4. Execution of the Application Process of Candidate Candidates

7.5. Execution of Employee Satisfaction and Loyalty Processes

7.6. Fulfillment of Liabilities Arising from Employment Contracts and Legislation for Employees

7.7. Execution of Benefits and Benefits Processes for Employees

7.8. Execution of Audit / Ethics Activities

7.9. Execution of Training Activities

7.10. Enforcement of Access Rights

7.11. Execution of Activities in Compliance with Legislation

7:12. Execution of Financial and Accounting Affairs

7.13. Execution of Loyalty Processes for Firms / Products / Services

7.14. Provision of Physical Space Security

7.15. Execution of Appointment Processes

7.16. Legal Affairs Tracking And Execution

7.17. Conducting Internal Audit / Investigation / Intelligence Activities

7.18. Conducting Communication Activities

7.19. Planning Human Resources Processes

7.20. Execution / Control of Business Activities

7.21. Conducting Occupational Health / Safety Activities

7.22. Receiving and Evaluating Suggestions for Improving Business Processes

7.23. Conducting Business Continuity Activities

7.24. Execution of Logistics Activities

7.25. Execution of Goods / Services Purchasing Processes

7.26. Execution of Goods / Services After Sales Support Services

7.27. Execution of Goods / Services Sales Processes

7.28. Execution of Goods / Services Production and Operation Processes

7.29. Execution of Customer Relationship Management Processes

7.30. Execution of Activities for Customer Satisfaction

7.31. Organization and Event Management

7.32. Conducting Marketing Analysis Studies

7.33. Execution of Performance Evaluation Processes

7.34. Execution of Advertising / Campaign / Promotion Processes

7.35. Execution of Risk Management Processes

7.36. Execution of Custody and Archive Activities

7.37. Conducting Social Responsibility And Civil Society Activities

7:38. Execution of Contract Processes

7:39. Conducting Sponsorship Activities

7:40. Execution of Strategic Planning Activities

7:41. Requests / Complaints Tracking

7:42. Ensuring the Security of Movable Goods and Resources

7:43. Execution of Supply Chain Management Processes

7:44. Execution of Wage Policy

7:45. Execution of Marketing Processes of Products / Services

7:46. Ensuring the Security of Data Responsible Operations

7:47. Foreign Personnel Work and Residence Permit Procedures

7:48. Execution of Investment Processes

7:49. Execution of Talent / Career Development Activities

7:50. Giving Information to Authorized Persons, Institutions and Organizations

7:51. Execution of Management Activities

7:52. Creating and Tracking Visitor Records

8. Reasons Requiring Destruction

8.1. In the event that all the processing conditions of the personal data disappear, the personal data must be deleted, destroyed or anonymized by the data controller ex officio or upon the request of the person concerned.

8.2. Although it has been processed in accordance with the provisions of the relevant law, as stipulated in Article 138 of the Turkish Penal Code and Article 7 of the Law on KVK, in the event that the reasons requiring its processing disappear, the personal data will be deleted, destroyed or destroyed upon the decision of the Company or upon the request of the personal data owner. is made anonymous.

8.3. When the relevant person applies to the Company and requests the deletion or destruction of his personal data, he is evaluated immediately to fulfill this request.

8.4. If all the conditions for processing personal data have disappeared; The company deletes, destroys or anonymizes the personal data subject to the request. The company finalizes the request of the person within thirty days at the latest and informs the person concerned.

8.5. If all the conditions for processing personal data have been eliminated and the personal data subject to the request have been transferred to third parties, the Company notifies this to the third party; ensures that the necessary actions are taken within the scope of this policy before the third party.

8.5. If all the conditions for processing personal data have been eliminated and the personal data subject to the request have been transferred to third parties, the Company notifies this to the third party; ensures that the necessary actions are taken within the scope of this policy before the third party.

8.6. If all the conditions for processing personal data have not disappeared, this request may be rejected by the Company, explaining its justification, and the rejection response will be notified to the concerned person in writing or electronically within thirty days at the latest.

9. Technical and administrative measures taken to safely store personal data and prevent it from being processed and accessed illegally

9.1. Technical Measures

9.1.1. Network security and application security are provided.

9.1.2. In data streams via network, closed system network is used.

9.1.3. Key management is implemented.

9.1.4. Security measures are taken within the scope of information technology systems procurement, development and maintenance.

9.1.5. An authority matrix has been created for employees.

9.1.6. Access logs are kept regularly.

9.1.7. Corporate policies on access, information security, usage, retention and disposal have been prepared and implemented.

9.1.8. When necessary, data masking method is applied.

9.1.9. Personal data security issues are reported quickly.

9.1.10. Personal data security is monitored.

9.1.11. Necessary security precautions are taken for entering and exiting physical environments containing personal data.

9.1.12. Physical environments containing personal data are protected against external risks (fire, flood etc.).

9.1.13. Security of environments containing personal data is ensured.

9.1.14. Personal data is backed up and the security of the backed-up personal data is also ensured.

9.1.15. User account management and authority control system are implemented and these are also tracked.

9.1.16. Periodic and / or random audits are carried out within the organization and made.

9.1.17. Log records are kept in such a way that there is no user intervention.

9.1.18. Existing risks and threats have been identified.

9.1.19. If special quality personal data will be sent by e-mail, it is sent in encrypted form and using KEP or corporate mail account.

9.1.20. Secure encryption / cryptographic keys are used for special personal data and are managed by different units.

9.1.21. Intrusion detection and prevention systems are used.

9.1.22. Penetration test is applied.

9.1.23. Cyber ��security measures have been taken and their implementation is constantly monitored.

9.1.24. Encryption is done.

9.1.25. Data processing service providers are audited periodically on data security.

9.1.26. Data processing service providers are aware of data security.

9.1.27. Data loss prevention software is used.

9.2. Administrative Measures

9.2.1. Disciplinary regulations are available for employees, including data security provisions.

9.2.2. Training and awareness studies are carried out at certain intervals on data security for employees.

9.2.3. Corporate policies on access, information security, usage, retention and disposal have been prepared and implemented.

9.2.4. Confidentiality commitments are made.

9.2.5. The signed contracts contain data security provisions.

9.2.6. Extra security measures are taken for personal data transmitted via paper and the relevant documents are sent in the form of a confidential document.

9.2.7. Personal data security policies and procedures have been determined.

9.2.8. Security of environments containing personal data is ensured.

9.2.9. Personal data is reduced as much as possible.

9.2.10. Periodic and / or random audits are carried out within the organization and made.

9.2.11. There are protocols and procedures for special data security.

10. Technical and administrative measures taken to dispose of personal data lawfully

10.1. All transactions related to deletion, destruction and anonymization of personal data are carried out and recorded by authorized persons in accordance with policies and procedures.

10.2. These records are kept for at least three years, excluding other legal obligations.

11. Personalization, Elimination, and Anonymization Techniques of Personal Data

11.1. Physical Destruction Personal data can also be processed in non-automated ways, provided that it is part of any data recording system. While erasing / destroying such data, the system of physical destruction of personal data, which cannot be used later, is implemented. Example: Disposing of the relevant file, document, and disposing of the document.

11.2. Secure Deletion from the Software When deleting / destroying data processed in completely or partially automated ways and stored in digital media; methods are used to delete the data from the related software, so that it is very unlikely to be recovered again.

11.3. Securely Deletion by the Expert In some cases, the company may agree with a specialist to delete personal data on his behalf. In this case, the personal data is securely deleted / destroyed by the person skilled in the art, so that it cannot be recovered again.

11.4. Techniques to Anonymize Personal Data

11.4.1. Anonymizing personal data implies that personal data can not be associated with a specific or identifiable natural person even by matching it with other data. The company can anonymize personal data when the reasons that require the processing of personal data processed in accordance with the law are eliminated.

11.4.2. In accordance with Article 28 of the KVK Law; Anonymized personal data can be processed for purposes such as research, planning and statistics. Such transactions are outside the scope of the KVK Law. Since the personal data processed by being anonymized will be outside the scope of the KVK Law, the rights regulated in section 10 of the policy will not be valid for these data.

11.4.3. Masking Data masking is the method of making anonymity of personal data by removing the basic determinant information of personal data from the data set. Example: Name, TR Identity No, name, surname etc. that enables identification of the personal data owner. converting the personal data owner into a dataset in which it becomes impossible to identify it by extracting the information.

11.4.4. Aggregation With the data aggregation method, many data are aggregated and personal data can not be associated with any person. Example: To reveal that there are 100 customers born in 1975 without showing the birth years of the customers one by one.

11.4.5. Data Derivation With the data derivation method, a more general content is created than the content of the personal data and it is ensured that the personal data cannot be associated with any person. Example: Indicating ages instead of birth dates; Indication of the town or city of residence instead of the full address.

11.4.6. Data Hash (Data Shuffling, Permutation) With the data hash method, the values in the personal data set are mixed and the connection between the values and individuals is broken. Example: By changing the quality of the sound recordings, making the sound and the data owner unrelated or unrecognizable.

12. Titles, units and job descriptions of those involved in the process of storing and destroying personal data:

12.1. IT Manager; Manages all IT processes of the company.

12.2. Human Resources Manager (Personnel related issues) manages all the personnel processes of the Company.

12.3. Sales and Marketing Manager (on customer information related issues); Manages all sales marketing processes of the company.

13. Table showing the storage and disposal times

NO	DATA CATEGORY	DATA STORAGE TIME
1	ID	10 YEARS
2	Contact	10 YEARS
3	Location	2 YEARS
4	briefness	10 YEARS
5	Legal action	10 YEARS
6	Customer Transaction	10 YEARS
7	Physical Space Security	2 YEARS
8	Transaction Security	10 YEARS
9	Risk management	10 YEARS
10	finance	10 YEARS
11	Professional experience	10 YEARS
12	Marketing	10 YEARS
13	Visual and Audio Recordings	10 YEARS
14	Disguise and Dress	10 YEARS
15	Health Information	10 YEARS
16	Criminal Conviction And Security Measures	10 YEARS
17	Association Membership	10 YEARS
18	Biometric Data	5 YEARS

15. Periodic destruction times,

15.1. The company will destroy the personal data whose expiration period expires within 180 days from the expiration date of the retention period.

15.2. Company; Deletes, destroys or anonymizes personal data in the first periodic destruction following the date on which the obligation to delete, destroy, or anonymize personal data.

15.3. The time interval for the periodic destruction will be determined by the data controller in accordance with the personal data retention and destruction policy, procedures and the workflow of the company. This period cannot exceed six months in any case.

16. Publishing and Retention of the Policy

The policy is published in two different media: wet signature (printed paper) and electronic media, and publicly disclosed on the website.

17. Update Period

The policy is revised as needed and the necessary sections are updated.

18. Entry into Force

The policy is considered to have come into force after it has been published on the Company's website.