**POLICY ON STORAGE, DESTRUCTION AND**

**ANONYMIZATION OF PERSONAL DATA**

**0 AIM**

The Policy on the storage, destruction and anonymization of personal data (“Policy”) has been prepared in order to determine the procedures and principles regarding the procedures and principles regarding the storage and destruction activities of personal and sensitive personal data in data recording systems in electronic and physical environments carried out by ONPO Madencilik İnş. San. Tic. A.Ş. (“Company”).

#  SCOPE

Our basic principle as a company is the processing of personal data belonging to company customers, employees, employee candidates, interns, suppliers, service providers, visitors and other third parties in accordance with the Turkish Constitution, international conventions and the Law on the Protection of Personal Data No. 6698 ("**Law**") and other relevant legislation. In this context, it has been determined as a priority that the persons concerned do not lose their rights and use their rights effectively.

This Policy has been prepared in accordance with the provisions of the Law, the Regulation on the Deletion, Destruction or Anonymization of Personal Data ("**Regulation**") and other legislation entered into force in the official gazette dated 28.10.2017 and numbered 30224.

#  DEFINITIONS AND ABBREVIATIONS

|  |  |  |
| --- | --- | --- |
| Explicit Consent | : | A consent about a specific subject based on information and expressed in free will. |
| Recipient Group | : | The real or legal person to whom the personal data is transferred by the data controller legal person category. |
| Anonymization | : | Under no circumstances, even by matching personal data with other data with an identified or identifiable natural person to make it unattributable. |
| A.Ş. | : | Joint Stock Company |
| CD | : | Dense Disc |
| Employed | : | **ONPO Madencilik İnş. San. Tic. A.Ş.** personnel. |
| Doc.  | : | Document  |
| DVD | : | Multipurpose Digital Disk |
| E-mail | : | Electronic Mail |
| Electronic Environment | : | Environments where personal data can be created, read, changed and written with electronic devices |
| Non-Electronic Environment | : | All written, printed, visual, etc. media other than electronic media. |
| Envision | : | Document Management System |
| Service Provider | : | A natural or legal person who provides services under a specific contract with the Personal Data Protection Authority. |
| IMS | : | Integrated Management Systems |
| ISO | : | ISO: (International Standards Organization: |
| Relevant Person  | : | The natural person whose personal data is processed. |
| Relevant User | : | Except for the person or unit responsible for the technical storage, protection and backup of the data, within the organization of the data controller or in line with the authorization and instruction received from the data controller data processors. |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Disposal | : | Deletion, destruction or anonymization of personal data to be brought in. |
| Law | : | Law on Protection of Personal Data No. 6698 |
| Recording Environment | : | Any medium containing personal data that is fully or partially automated or processed by non-automated means, provided that it is part of any data recording system. |
| Personal Data  | : | Any information that makes the person specific or identifiable. |
| Personal Data Processing Inventory | : | Inventory in which data controllers detail the personal data processing activities they carry out depending on their business processes by associating them with the purposes and legal grounds for processing personal data, the data category, the group of recipients transferred and the group of data subjects, and by explaining the maximum retention period required for the purposes for which personal data are processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security. |
| Personal Data Processing | : | All kinds of processes performed on personal data including obtaining, recording, storing, keeping, changing, re-arranging, disclosure, transmission, acquisition, making available, classification or prevention of use in whole or in part, automatically or in non-automatic ways,any action taken on the data, such as classification or prevention of its use. |
| Board | : | Personal Data Protection Board.  |
| No. | : | Number |
| Sensitive personal Data | : | Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data. |
| Periodic Destruction | : | Deletion, destruction or anonymization to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy in the event that all of the conditions for processing personal data specified in the law disappear process. |
| Rev. | : | Revision |
| Deletion | : | Making personal data inaccessible, irretrievable and non-reusable in any way for the Relevant Users. |
| SSI | : | Social Security Institution |
| TR | : | Republic of Türkiye |
| TS | : | Turkish Standards |
| Etc. | : | and so on.  |
| VERBİS | : | Data Controllers Registry Information System, The information system created and managed by the Presidency, accessible via the internet, which data controllers will use in applying to the registry and in other transactions related to the registry. |

|  |  |  |
| --- | --- | --- |
| Data Processor | : | Based on the authorization given by the data controller, the data controller a natural or legal person who processes personal data on behalf of the data subject. |
| Data Registration System | : | Personal data is processed by structuring according to certain criteria registration system. |
| Data Controller | : | The real person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system or legal person. |
| Destruction | : | Making personal data inaccessible, irretrievable and non-reusable by anyone in any way. |
| Regulation | : | On Deletion, Destruction or Anonymization of Personal Data published in the official gazette dated October 28, 2017 Regulation. |

1. DUTIES, AUTHORIZATONS AND RESPONSIBILITIES

Pursuant to subparagraph f of Article 6 of the Regulation, it has been regulated that the titles, duties and units of the persons involved in the storage and destruction of personal data should be specified. In this context, the titles, duties and units of the persons within the Company are specified in order to prevent unlawful processing and access to personal data, to ensure that personal data is stored in accordance with the law, to manage data security, storage and destruction processes, and to take technical and administrative measures.

|  |  |
| --- | --- |
| Title | Task Description |
| **Personal Data Management Committee** | It is obliged to direct all kinds of planning, analysis, research, risk determination studies in the projects carried out in the process of compliance with the law; to manage the processes to be carried out in accordance with the Law, Policy and other policies and Policies regulated, and to make correspondence and decide on the determination of the location of personal data to the relevant units in order to make an evaluation about the requests received by the relevant persons. |
| **Legal Unit and IT Unit** | It is responsible for reporting the requests of the relevant persons to the Personal Data Management Committee for examination and evaluation, and for fulfilling the transactions related to the requests of the relevant persons evaluated and decided by the relevant committee in accordance with the decision of the Committee; auditing the storage and destruction processes and reporting these audits to the Committee; executing the storage and destruction processes. |
| **Human Resources****Unit and Quality Unit** | He/she is responsible for the execution of policies and audits on the protection, storage and destruction of personal data in accordance with his/her job descriptions. |

# IMPLEMENTATION

**4.1 RECORDING MEDIA**

The table below shows the environments in which personal data and sensitive personal data stored by **ONPO Madencilik İnş. San. Tic. A.Ş.** and all its affiliates are recorded. Personal data stored by our company are stored in the most appropriate recording medium according to their nature and legal status.

|  |  |
| --- | --- |
| Data storage medium  | Description |
| Electronic Mediums: | * Servers (backup, email, web, etc.)
* Information Security Device (firewall, intrusion detection and blocking, antivirus, etc.)
* Company Computers (Desktop, etc.)
* Company Owned Mobile Devices (Telephone, etc.)
 |
| Non-Electronic Media: | * Paper
* Written, printed and visual media.
 |

**4.2 EXPLANATIONS ON STORAGE AND DISPOSAL**

Within the Company, personal data of the persons served and the personnel of our Company are processed in accordance with the matters specified by the Law and stored in the recording media specified in this Policy and destroyed in the specified ways.

Personal Data are stored in accordance with Articles 5 and 6 of the Law and based on the personal data processing conditions specified in the clarification texts, and in this context, personal data are stored during the validity of the conditions specified for the processing of personal data, and when the said processing conditions expire or upon the application of the relevant person to our Company, the personal data stored upon request (after checking other legal obligations that our Company must comply with) are deleted, destroyed or anonymized.

## Legal Reasons Requiring Storage

Personal data processed within the framework of the commercial activities shall be stored for the period stipulated in the relevant legislation.

* Turkish Commercial Code No. 6102
* Turkish Code of Obligations No. 6098,
* ç) Law: Law No. 6502 on the Protection of Consumers,
* Law on Protection of Personal Data No. 6698,
* Law No. 5651 on Regulating Internet Broadcasting and Combating Crimes Committed Through Internet Broadcasting,
* Law on Public Procurement no. 4734
* Tax Procedure Law No. 213
* Law on Capital Market no. 6362
* - Law No. 5510 on Social Insurance and General Health Insurance,Occupational Health and Safety Law no. 6331
* Regulation on Health and Safety Measures to be Taken in Workplace Building and Extensions

## Processing Purposes Requiring Storage

The Company keeps the personal data it processes within the framework of its activities for certain purposes. In this context, these purposes are listed below:

* Conducting emergency management processes
* Execution of Information Security Processes
* Execution of Employee Candidate / Intern / Student Selection and Placement Processes
* and is executed with the purpose of
* Employee Contract and Fulfillment of Obligations Arising From Legislation
* Execution of Employee Benefits and Side Benefits Processes
* Conducting Audit / Ethics Activities
* Conducting Training Activities
* Executing Access Authorities,
* Conducting business activities in compliance with legislation
* Conducting financial and accounting works
* Ensuring Physical Space Security
* To conduct assignment processes,
* To follow up and conduct legal affairs,
* Conduct of Internal Audit/Investigation / Intelligence Activities
* Execution of Communication Activities,
* Planning of Human Resources Processes
* Execution / Audit of Business Activities,
* Execution of Occupational Health / Safety Activities
* Providing Business Continuity Activities,
* Execution of Logistics Activities,
* Execution of Goods / Services Purchasing Processes,
* After Sales Support Services for Goods/Services
* Executing Goods/Service Procurement Processes
* Execution of Goods/Service Production and Operation Processes
* Customer Relations management processes,
* Customer satisfaction activities,
* Organization and Event Management
* Marketing analysis activities,
* Advertising/ Campaign/ Promotion Processes,
* Executing Risk Management Processes
* Storage & archiving activities,
* Execution of Social Responsibility and Civil Society Activities
* Execution of Contract Processes
* To conduct sponsorship activities,
* To conduct strategic planning activities,
* Following up requests/complaints,
* Execution of Supply Chain Management Processes
* Execution of Wage Policy
* Marketing Processes for Products/Services,
* Ensuring Security of Data Controller Operations
* Informing authorized persons, organizations and institutions
* Execution of Management Activities

## Reasons for Destruction/Disposal

Personal data

* Amendment or abolition of the relevant legislation provisions that constitute the basis for processing,
* The purpose requiring processing or storage disappears,
* In cases where the processing of personal data is carried out only on the basis of explicit consent, the data subject may withdraw his/her explicit consent,
* Pursuant to Article 11 of the Law, the Company's acceptance of the application made by the data subject regarding the deletion and destruction of his/her personal data within the framework of his/her rights,
* In cases where the Company rejects the application made by the person concerned with the request for the deletion, destruction or anonymization of his personal data, finds the answer insufficient or does not respond within the period stipulated in the Law; In case of a complaint to the Personal Data Protection Authority and this request is approved by the Authority,
* The maximum period for which the personal data is required to be retained has expired and there are no circumstances that would justify retaining the personal data for a longer period of time,
* In cases where the retention periods specified in the relevant legislation expire, it is deleted, destroyed or ex officio by the Company upon the request of the relevant person deleted, destroyed or anonymized.

# TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR SECURE STORAGE, PRESERVING ILLEGAL PROCESSING AND PROHIBITION OF ACCESS TO PERSONAL DATA

**ONPO Madencilik İnş. San. Tic. A.Ş.** and all affiliated companies take all necessary technical and administrative measures in accordance with the nature of the relevant personal data and the environment in which it is kept in order to store personal data securely and to prevent unlawful processing and access. In addition, our Company takes technical and administrative measures within the framework of adequate measures determined and announced by the Personal Data Protection Authority for special categories of personal data in accordance with Article 12 of the Law and the fourth paragraph of Article 6 of the Law. and administrative measures.

## Administrative Measures

Technical and Administrative Measures

**ONPO Madencilik İnş. San. Tic. A.Ş.** and all its affiliated companies take the following technical measures for all environments where personal data is stored, in accordance with the nature of the relevant data and the environment in which the data is stored:

|  |
| --- |
| Network security and application security are ensured. |
| Closed system network is used for personal data transfers through the network. |
| Security measures are taken within the scope of procurement, development and maintenance of information technology systems. |
| There are disciplinary regulations for employees that include data security provisions. |
| Training and awareness raising activities on data security are carried out for employees at regular intervals. |
| Authorization matrix has been created for employees. |

|  |
| --- |
| Access logs are maintained regularly. |
| Confidentiality commitments are made. |
| Employees who are reassigned or leave their jobs are de-authorized in this area. |
| Up-to-date anti-virus systems are used. |
| Firewalls are used. |
| The signed contracts contain data security provisions. |
| Personal data security is monitored. |
| Necessary security measures are taken regarding entry and exit to physical environments containing personal data. |
| Physical environments containing personal data are protected against external risks (fire, flood etc.).  |
| The security of environments containing personal data is ensured. |
| Personal data is reduced as much as possible.  |
| Personal data is backed up and the security of the backed-up personal data is also ensured.  |
| User account management and authority control system are implemented and these are also followed-up.  |
| Log records are maintained in such a way that there is no user intervention.  |
| Intrusion detection and prevention systems are used.  |
| Cyber security measures have been taken and their implementation is constantly monitored. |
| Enciphering is performed. |
| Awareness of data processing service providers on data security is ensured. |

# PERSONAL DATA DESTRUCTION TECHNIQUES

**ONPO Madencilik İnş. San. Tic. A.Ş.** deletes, destroys or anonymizes the personal data that it stores in accordance with the Law and other legislation and the Policy, upon the request of the data subject or ex officio within the periods specified in the Policy, if the reasons requiring the processing of the data disappear.

The deletion, destruction and anonymization techniques used by **ONPO Madencilik İnş. San. Tic. A.Ş.** are listed below:

4.4.1 **Deletion Methods**

Personal data is deleted by the methods given in the table below.

|  |
| --- |
| Deletion Methods for Personal Data Retained in Physical Environment |
| Darken | Personal data in paper media are deleted using the blackout method. The blackout process is done by cutting the personal data on the relevant documents whenever possible, and making them invisible to the relevant users by using fixed ink, which is irreversible and cannot be read with technological solutions. |
| Deletion Methods for Personal Data Stored in the Cloud and Local Digital Media/ Software |
| Securely Deleting Personal Data From Software  | Personal data stored in the cloud or local digital environments are deleted with a digital command and made unusable in a way that other relevant employees, except for the database manager, cannot access in any way. |

|  |
| --- |
| Personal Data on Servers |
| Deleting by Removing Access Authorization | For the personal data on the servers, the access authorization of the relevant users is removed by the system administrator for those whose retention period has expired and deletion is performed. |

**4.4.2 Destruction Methods**

Personal data is destroyed by the methods given in the table below.

|  |
| --- |
| Destruction Methods for Personal Data in Physical/Printed Media |
| Physical Destruction | Documents kept in printed form are destroyed by document shredders in such a way that they cannot be reassembled. |
| Destruction Methods for Personal Data Held in Local Digital Media and Servers |
| Physical Destruction | It is the process of physical destruction of optical and magnetic media containing personal data, in ways and means such as melting, burning or pulverizing. Data is made inaccessible by processes such as melting, burning, pulverizing or passing optical or magnetic media through a metal grinder. |
| Demagnetization (Degauss) | It is the process of degradation of the data on magnetic media in an unreadable manner by exposing it to a high magnetic field. |
| Overwriting | Reading and recovering old data is prevented by writing random data consisting of 0's and 1's at least seven times on magnetic media and rewritable optical media. |
| Disposal by Removing Access Authorization | For those whose period of time requiring storage from the personal data on the servers has expired, the access authority of the relevant users is removed by the system administrator and the destruction process is performed in a way that it cannot be accessed again. |
| Destruction Methods for Personal Data Stored in the Cloud |
| From softwareSecurely Deleting Personal Data From Software  | Personal data held in the cloud environment is deleted by digital command in a way that cannot be recovered again, and when the cloud computing service relationship ends, all copies of the encryption keys necessary to make personal data available are destroyed. The data deleted in this way cannot be accessed again. |

## Anonymization Methods

**ONPO Madencilik İnş. Industry Tra. A.Ş.** and all its affiliated companies; makes personal data that cannot be associated with an identified or identifiable natural person, even through the use of appropriate techniques.

Personal data is anonymized with the methods given in the table below.

|  |
| --- |
| Anonymization Methods for Personal Data in Physical/Printed Media |
| Removing Variables | It is the removal of one or more of the direct identifiers included in the personal data of the person concerned and used to identify the person concerned in any way.This method can be used to anonymize personal data, or it can be used to delete this information if there is information in the personal data that is not suitable for the purpose of data processing |
| Regional Hide | It is the process of deleting information that may be distinctive regarding the data in the data table where the personal data is collectively anonymized. |
| Generalization.  | It is the process of gathering personal data belonging to many people and making them statistical data by removing their distinctive information. |
| Lower and Upper Limit Coding/ Global Coding | For a particular variable, the intervals of that variable are defined and categorized. If the variable does not contain a numerical value, then close data within the variable is categorized. The values within the same category are combined. |
| Micro.Consolidation | With this method, all records in the dataset are first arranged in a meaningful/ tangible order and then the whole set is divided into a certain number of sub-sets. Then, the value of the determined variable of each sub-set is averaged and the value of that variable of this subset is changed with the average value. In this way, since the indirect identifiers in the data will be corrupted, it is difficult to associate the data with the relevant person. |
| Data Mixing and Disruption | The direct or indirect identifiers in the personal data are confused or distorted with other values, their relationship with the relevant person is broken and they are ensured to lose their descriptive qualities. |
| Methods of Anonymizing the Digital Media/Servers/Cloud Media for Retained Personal Data |
| Masking(Encryption, Using Icons, Blurring, Mixing,invalidation | Data masking is making personal data incomprehensible in order to prevent access by unauthorized persons. This method is used to prevent confidential and sensitive information in the institution from leaking inside and outside the institution and from being seized by malicious people. In data masking, the data format is not changed, only the values are changed, but this change is made in a way that cannot be detected and reversed in any way. In addition, by determining who can access which data, it is ensured that only authorized people see the information they need to see and other information is masked. |

# PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

Processed by **ONPO Madencilik İnş. San. Tic. A.Ş.** within the scope of its activities in relation to personal data;

* Retention periods on a personal data basis for all personal data within the scope of activities carried out depending on the processes, in **ONPO Madencilik İnş. San. Tic. A.Ş**’s personal data processing inventory,
* Retention periods based on data categories are recorded in VERBIS;
* Retention periods on a process basis are included in the Policy.

These retention periods will be updated by **PO Madencilik İnş. San. Tic. A.Ş**, if necessary.

## Storage and Disposal Periods

|  |  |  |
| --- | --- | --- |
| Process | Storage Period | Disposal Period |
| Data kept under the Labor Law (e.g. performance records etc.) | 10 years following the end of the business relationship  | Within 180 days after the expiry of the retention period |
| Health Reports | 15 years following the termination of the business relationship  | Within 180 days after the expiry of the retention period |
| Data kept within the scope of SSI legislation | 10 years following the end of the business relationship  | Within 180 days after the expiry of the retention period |
| Work accident/occupational disease documents that can be used in a request/lawsuit | 10 years following the end of the business relationship  | Within 180 days after the expiry of the retention period |
| Data collected in accordance with other applicable legislation  | For the period stipulated in the applicable legislation | Within 180 days after the expiry of the retention period |
| If the relevant personal data is subject to a crime within the scope of the Turkish Penal Code or other criminal legislation | During the statute of limitations | Within 180 days after the expiry of the retention period |
| Data of persons receiving products/services  | 10 years after registration  | Within 180 days after the expiry of the retention period |

* + 1. Data Destruction Periods

ONPO Madencilik İnş. San. Tic. A.Ş. deletes, destroys or anonymizes personal data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymize the personal data for which it is responsible in accordance with the Law, relevant legislation and Policy arises.

When the data subject requests the deletion or destruction of his/her personal data by applying to ONPO Madencilik İnş. San. Tic. A.Ş. pursuant to Article 13 of the Law;

* + If all the conditions for processing personal data have disappeared; ONPO Madencilik İnş. San. Tic. A.Ş. deletes, destroys or anonymizes the personal data subject to the request within 30 (thirty) days from the day it receives the request, explaining the reason for it, with the appropriate destruction method. In order for ONPO Madencilik İnş. San. Tic. A.Ş. and all its affiliated companies to be deemed to have received the request, the person concerned must have made the request in accordance with the principles specified in the Law and secondary legislation.
	+ ONPO Madencilik İnş. San. Tic. A.Ş. and all its affiliated companies shall inform the person concerned about the transaction made in any case.
	+ If all the conditions for processing personal data have not been eliminated, this request may be rejected by ONPO Madencilik İnş. San. Tic. A.Ş. by explaining the reason in accordance with paragraph 3 of Article 13 of the Law and the rejection response shall be sent to the data subject within 30 (thirty) days at the latest. notified in writing or electronically.

**4.5.3 PERIODIC DESTRUCTION PERIOD**

In the event that all of the conditions for processing personal data specified in the Law disappear; **ONPO Madencilik İnş. San. Tic. A.Ş**.and all its affiliated companies delete, destroy or anonymize the personal data whose processing conditions have disappeared by a process to be carried out ex officio at intervals specified in the Policy and repeated every 6 (six) months brings.

**5 PUBLICATION AND STORAGE AND UPDATING OF THE POLICY**

The **policy** is available in two different media, wet signed (printed paper) and electronic media

is published. **Printed paper copy ONPO Madencilik İnş. San. Tic. A.Ş board of directors**

**and kept on file by Personal Data Management.** All personnel within **ONPO Madencilik İnş. San. Tic. A.Ş** and relevant persons whose personal data are processed have the right to access the Policy on the company's website <https://www.onpo.com.tr/> ......

The Policy is reviewed as needed and the necessary sections are updated. The department that first prepared the Policy is responsible for publishing or revising this Policy.

# 6. COMPLIANCE AND AMENDMENTS

**ONPO Madencilik İnş. Industry Trade A.Ş.** has the right to make changes in the storage and destruction policy of personal data in accordance with the provisions of the Legislation or in accordance with the company policy.

This protocol was published on ../../.... and no changes have been made.