BMS GERİ DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ

PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. PURPOSE AND SCOPE

The Personal Data Retention and Destruction Policy ("Policy") has been prepared in order to determine the procedures and principles regarding the works and transactions related to the storage and destruction activities carried out within BMS GERI DÖNÜŞÜM SANAYİ VE TİCARET ANONİM ŞİRKETİ (hereinafter referred to as the "Data Controller").

As a Data Controller, our basic principle is; Shareholder/Partner, Employee, Product or Service Buyer, Supplier Official, Supplier Employee, Visitor, Potential Product or Service Buyer, Other - Switchboard - Telephone Call Call Party, Other - Public Official, Parent / Guardian / Representative, Other - Lawsuit, Enforcement File Party, Intern, Other - Doctor, Employee Candidate, Other - Occupational Health and Safety Specialist and other third parties personal data belonging to the relevant persons T.C. Constitution, It is processed in accordance with 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 Personal Data Retention and Destruction Policy has been prepared in accordance with the provisions of the Law on the Protection of Personal Data No. 6698, 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.

2. DEFINITIONS

Recipient Group	Recipient Group: The category of natural or legal person to whom personal data is transferred by the data controller.
Explicit Consent	Explicit Consent Consent on a specific subject, based on information and expressed with free will.
Anonymization	Making personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data.
Employee	Employee Data Controller personnel.
Electronic Media	Electronic Media Environments where personal data can be created, read, modified and written by electronic devices.
Non-Electronic Media	All other media other than electronic media such as written, printed, visual, etc.
Service Provider	A natural or legal person who provides services within the framework of a specific contract with the Data Controller.
Contact Person	Relevant Person The natural person whose personal data is processed.
Related 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.

Annihilation	Destruction: Deletion, destruction or anonymization of personal data.
Law	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 part of any data recording system.
Personal data	Any information that makes a person specific or identifiable.
Personal Data Processing Inventory	Personal data processing activities carried out by data controllers depending on their business processes; The inventory that they create by associating the purposes and legal reason for processing personal data with the data category, the transferred recipient group and the data subject group, and the maximum retention period required for the purposes for which personal data is processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.
Processing of Personal Data	Obtaining, recording, storing, storing, 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.
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 deletion, destruction or anonymization process to be carried out ex officio at repeated intervals specified in the personal data storage and destruction policy.
Policy	Personal Data Retention and Destruction Policy.
Data Processor	A natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the data controller.
Data Recording System	A recording system in which personal data is structured and processed according to certain criteria.
Data Controller	The natural or legal person responsible for the establishment and management of the data recording system, determining the purposes and means of processing personal data.
Data Controllers Registry Information System	The information system to be used by data controllers in applying to the Registry and other related transactions related to the Registry, accessible over the internet, created and managed by the Presidency.
VERBIS	Data Controllers Registry Information System.
Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated October 28, 2017.

3. RECORDING MEDIA

The table below shows the environments in which the personal data stored by the Data Controller are recorded. Personal data stored by the Data Controller are stored in the most appropriate recording environment according to their nature and legal status.

Storage Media
Computer
Locked Archive Cabinet
Archive Cabinet
Archive Room
Double Locker in Controlled Zone
Locker
Hard Disk
Paper
Unit Archive
Business Server
Overseas Email Server
Domestic Email Server
Excel Program
Server
Flash Memory
Access Restricted File

4. DISTRIBUTION OF RESPONSIBILITIES AND DUTIES

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

Appellation	Job Description
Personal Data Administrator	Personal Data Manager Directing all kinds of planning, analysis, research and risk determination studies in the projects carried out in the process of compliance with the Law; It is obliged to manage the

	processes to be carried out in accordance with the Law, the Personal Data Processing and Protection Policy and the Personal Data Retention and Destruction Policy and other policies and procedures regulated and to decide on the requests received by the relevant persons.
Data Controller Personal Data Protection Specialist (Technical and Administrative)	Data Controller Personal Data Protection Specialist (Technical and Administrative) Examining the requests of the relevant persons and reporting them to the Personal Data Manager for evaluation; Fulfillment of the procedures regarding the requests of the relevant person evaluated and decided by the Personal Data Manager in accordance with the decision of the Personal Data Manager; auditing the storage and destruction processes and reporting these audits to the Personal Data Manager; It is responsible for the execution of storage and disposal processes.

5. EXPLANATIONS REGARDING STORAGE AND DISPOSAL

Within the Data Controller, personal data are processed in accordance with the matters specified by the Law and are stored in the recording media specified in this Policy, but they are also destroyed as specified in this policy.

Personal Data, based on one or more of the personal data processing conditions specified in Articles 5 and 6 of the Law, and within this scope, personal data is stored for the validity of the conditions specified for the processing of personal data, when the said processing conditions expire or upon the application of the data subject to the Data Controller, upon the request of the person concerned, if deemed appropriate (after checking the other legal obligations that the Data Controller must comply with) Stored personal data is deleted, destroyed or anonymized.

5.1. Legal Reasons Requiring Retention

Personal data processed within the framework of the activities of the Data Controller are kept for the period stipulated in the relevant legislation. In this context, personal data;

- Labor Law No. 4857,
- Turkish Commercial Code No. 6102,
- Turkish Code of Obligations No. 6098,
- Law No. 6502 on Consumer Protection,
- Vocational Education Law No. 3308,
- Occupational Health and Safety Law No. 6331,
- Law No. 6698 on the Protection of Personal Data,
- Tax Procedure Law No. 213,
- Social Insurance and General Health Insurance Law No. 5510,
- Law No. 6563 on the Regulation of Electronic Commerce,

- Regulation on Occupational Health and Safety Services,
- Regulation on Commercial Communication and Commercial Electronic Messages,
- Identification Law No. 1774
- Turkish Employment Agency Law No. 4904

It is stored for the retention periods stipulated within the framework of other secondary regulations in force in accordance with these laws.

5.2. Processing Purposes Requiring Storage

The Data Controller stores the personal data it processes within the framework of its activities for certain purposes. In this context, the objectives are listed below:

Processing Purposes
Execution / Supervision of Business Activities
Execution of Finance and Accounting Affairs
Execution of Management Activities
Follow-up and Execution of Legal Affairs
Execution of Audit / Ethics Activities
Conducting Internal Audit / Investigation / Intelligence Activities
Execution of Goods / Services After-Sales Support Services
Execution of goods / services production and operation processes
Execution of Goods / Services Procurement Processes
Execution of Supply Chain Management Processes
Ensuring the security of movable property and resources
Fulfillment of Obligations Arising from Employment Contract and Legislation for Employees
Creation and follow-up of visitor records
Ensuring Physical Space Security
Execution of Logistics Activities
Execution of Communication Activities
Execution of Goods / Services Sales Processes
Execution of Business Continuity Activities
Providing information to authorized persons, institutions and organizations
Execution of Contract Processes

Execution of Occupational Health / Safety Activities
Execution of Activities in Accordance with the Legislation
Execution of Risk Management Processes
Ensuring the Security of Data Controller Operations
Execution of Customer Relationship Management Processes
Follow-up of Requests / Complaints
Planning Human Resources Processes
Receiving and Evaluating Suggestions for the Improvement of Business Processes
Execution of Benefits and Benefits Processes for Employees
Execution of Wage Policy
Execution of Employee Candidate / Intern / Student Selection and Placement Processes
Execution of Application Processes of Employee Candidates
Execution of Assignment Processes
Execution of Educational Activities
Other - Execution of Termination Proceedings
Other - Execution of Human Resources Processes
Execution of Emergency Management Processes
Execution of Information Security Processes
Execution of Access Authorizations
Execution of Company / Product / Services Loyalty Processes
Execution of Marketing Analysis Studies

5.3. Reasons Requiring Destruction

Personal data;

- The disappearance of the purpose that requires its processing or storage,
- In cases where the processing of personal data takes place only on the basis of explicit consent, the person concerned withdraws his explicit consent,
- Pursuant to Article 11 of the Law, the application made by the data subject regarding the deletion and destruction of personal data within the framework of their rights is accepted by the Data Controller,
- In cases where the Data Controller rejects the application made by the data subject with the request for deletion, destruction or anonymization of his personal data, finds his answer insufficient or does not respond within the period stipulated in the Law; To

make a complaint to the Personal Data Protection Authority and this request is approved by the Authority,

- The maximum period requiring the storage of personal data has expired and there are no conditions that justify storing personal data for a longer period of time,

- Expiry of the retention periods in the relevant legislation,

6. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN TO PREVENT THE SECURE STORAGE, UNLAWFUL PROCESSING AND ACCESS OF PERSONAL DATA

The Data Controller takes all necessary technical and administrative measures in accordance with the characteristics 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, in accordance with Article 12 of the Law and the fourth paragraph of Article 6 of the Law, the Data Controller also takes technical and administrative measures within the framework of adequate measures determined and announced by the Personal Data Protection Authority for sensitive personal data.

These measures include, but are not limited to, the following administrative and technical measures to the extent appropriate to the nature of the relevant personal data and the environment in which it is kept.

6.1. Technical Measures

The Data Controller takes the following technical measures in accordance with the characteristics of all environments where personal data is stored, the relevant data and the environment in which the data is kept:

Technical Measures
Network security and application security are ensured
Closed system network is used for personal data transfers via network
Key management is implemented
Security measures are taken within the scope of procurement, development and maintenance of information technology systems
Access logs are kept regularly
Data masking measures are applied when necessary
Up-to-date anti-virus systems are used
Firewalls are used
Personal data is backed up and the security of the backed up personal data is also ensured
User account management and authorization control system are implemented and these are also monitored
Log records are kept in such a way that there is no user intervention

Cyber security measures have been taken and their implementation is constantly monitored
Encryption is done

6.2 Administrative Measures

The Data Controller takes the following administrative measures in accordance with the characteristics of all environments where personal data is stored, the relevant data and the environment in which the data is kept:

Administrative Measures
Disciplinary regulations with data security provisions are in place for employees
Training and awareness activities are carried out at regular intervals on data security for employees
An authorization matrix has been created for employees
Confidentiality commitments are made
Employees who have a job change or leave their job are removed from their authority in this area
The signed contracts contain data security provisions
Personal data security policies and procedures have been determined
Personal data security issues are reported quickly
Personal data security is monitored
Necessary security measures are taken regarding entry and exit to physical environments containing personal data
The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured
The security of environments containing personal data is ensured
Personal data is reduced as much as possible
Periodic and/or random audits are carried out and carried out in-house
Existing risks and threats have been identified
Protocols and procedures for the security of sensitive personal data have been determined and implemented
Data processing service providers are periodically audited on data security

7. PERSONAL DATA DESTRUCTION TECHNIQUES

Data Controller, personal data stored in accordance with the Law and other legislation and the Personal Data Processing and Protection Policy,

Causes of Destruction
Personal Data Protection Board's Decision on the Destruction of Personal Data
Expiry of Retention Period
Contact Request

deletes, destroys or anonymizes ex officio within the periods specified in this Personal Data Retention and Destruction Policy.

The deletion, destruction and anonymization techniques used by the Data Controller are listed below:

7.1 Deletion Methods

Deletion of personal data is the process of making personal data **inaccessible and unusable for** the relevant users in any way.

Personal data is deleted using one or more of the methods given in the table below.

Deletion Methods for Personal Data Held in Physical Media	
Blackout	Personal data in the physical environment is deleted using the blackout method. The blackout process is done by cutting the personal data on the relevant document where possible, and in cases where it is not possible, making it invisible by using fixed ink in a way that cannot be reversed and cannot be read with technological solutions.
Deletion Methods for Personal Data Held in Cloud and Local Digital Media / Software	
Soft safe deletion	Personal data kept in the cloud or local digital environments are deleted by digital command and made unusable again in a way that other relevant employees, except for the database administrator, cannot access in any way, upon the expiry of the period requiring storage.
Personal Data Contained on the Servers	
Delete access by deauthorizing it	Deletion by removing access authorization: For those whose personal data on the servers have expired, the access authorization of the relevant users is removed by the system administrator and the deletion process is performed.

7.2 Disposal Methods

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way.

Personal data is destroyed using one or more of the methods given in the table below.

Destruction Methods for Personal Data Held in Physical/Printed Media	
Physical destruction	Physical destruction: Documents kept in printed media are destroyed in such a way that they cannot be reassembled with document shredders.
Destruction Methods for Personal Data Held in Local Digital Environment and Servers	
Physical destruction	It is the process of physical destruction of optical and magnetic media containing personal data, such as melting, burning or pulverizing. Processes such as melting, burning, pulverizing, or passing optical or magnetic media through a metal grinder make data inaccessible.
De-magnetization (degauss)	De-magnetization (degauss) is the process of unreadable distortion of the data on the magnetic media by exposing it to a high magnetic field.
Overwrite	Random data consisting of 0's and 1's is written at least seven times on magnetic media and rewritable optical media, preventing reading and recovering old data.
Destroy access by deauthorizing it	Destruction by removing access authorization: For those who have expired to be stored from the personal data on the servers, the access authorization of the relevant users is removed by the system administrator and the destruction process is carried out so that they cannot be accessed again.
Destruction Methods for Personal Data Kept in the Cloud	
Soft safe deletion	Personal data kept in the cloud environment is deleted with a digital command so that it cannot be recovered, and when the cloud computing service relationship ends, all copies of the encryption keys required to make personal data usable are destroyed. Data deleted in this way cannot be accessed again.

7.3 Anonymization Methods

Anonymization of personal data is the rendering of personal data that cannot be associated with an identified or identifiable natural person in any way, even if it is matched with other data.

Personal data is anonymized using one or more of the methods given in the table below.

Anonymization Methods for Personal Data Held in Physical/Printed Media	
Extracting variables	It is the removal of one or more of the direct identifiers in the personal data of the person concerned that will be 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 personal data if there is information that does not comply with

	the purpose of data processing.
Regional obfuscation	It is the process of deleting information that may be distinctive regarding the data that is exceptional in the data table where personal data is collectively anonymized.
Globalization	Generalization is the process of bringing together the personal data of many people, removing their distinctive information and turning them into statistical data.
Lower and upper limit coding / Global coding	Lower and upper limit coding / Global coding For a certain variable, the ranges of that variable are defined and categorized. If the variable does not contain a numeric value, then the data within the variable that is close to each other is categorized. Values that fall within the same category are combined.
Micro-incorporation	With this method, all the records in the dataset are first arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Then, by taking the average of the value of each subset of the specified variable, the value of that variable of the subset is replaced 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 hashing and corruption	Data hashing and distortion: Direct or indirect identifiers in personal data are confused or distorted with other values, breaking their relationship with the person concerned and ensuring that they lose their descriptive qualities.
Anonymization Methods for Personal Data Held in Digital Environment/Servers/Cloud Environment	
Masking (Encryption, iconization, blurring, scrambling, overriding)	Masking (Encryption, using symbols, blurring, scraming, invalidating) Data masking is the rendering of personal data incomprehensible in order to prevent it from being accessed by unauthorized persons. This method is used to prevent the leakage of confidential and sensitive information in the institution into and outside the institution and to prevent it 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 such a way that it will not be detected and reversed in any way. In addition, it is determined who can access which data, so that only authorized people can see the information they need to see and other information is masked.

8. PERSONAL DATA STORAGE AND DESTRUCTION PERIODS

Regarding the personal data processed by the Data Controller within the scope of the activities;

- Retention periods on the basis of personal data related to all personal data within the scope of the activities carried out depending on the processes are in the Data Controller Personal Data Processing Inventory,

- Retention periods on the basis of data categories are recorded with VERBIS,

- Process-based retention periods are in the Personal Data Retention and Destruction Policy

- Retention periods on the basis of personal data related to all personal data within the scope of the activities carried out depending on the processes are in the Data Controller Personal Data Processing Inventory,

- Retention periods on the basis of data categories are recorded with VERBIS,

- Process-based retention periods are in the Personal Data Retention and Destruction Policy

8.1 Storage and Disposal Periods

Data Category	Retention Period
Identity	Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship Other - 10 years from the termination of the purpose of data processing Other - 10 Years from the end of the activity Other - 10 Years from the termination of the purpose of processing Other - 15 years from the termination of the employment contract Other - 10 Years from the termination of the legal relationship Other - 15 Years from the termination of the employment relationship Other - 15 years from the termination of the employment contract Other - 5 years from the termination of the purpose of processing 1 Year
Audiovisual Recordings	Other - 15 years from the termination of the employment contract
Aslam	Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship
Legal Action	Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship
Communication	Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship Other - 10 years from the termination of the purpose of data processing

	Other - 10 Years from the end of the activity Other - 10 Years from the termination of the purpose of processing Other - 10 Years from the termination of the legal relationship Other - 15 Years from the termination of the employment relationship Other - 5 years from the termination of the purpose of processing 1 Year
Physical Space Security	Other - 15 years from the termination of the employment contract 1 Month
Criminal Conviction and Security Measures	Other - 10 years from the termination of the legal relationship Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the purpose of data processing
Finance	Other - 10 years from the termination of the purpose of data processing Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship Other - 10 Years from the end of the activity Other - 10 Years from the termination of the legal relationship
Location	Other - 10 years from the termination of the legal relationship Other - 15 years from the termination of the employment contract Other - 15 years from the termination of the employment contract Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the purpose of data processing
Customer Transaction	Other - 10 years from the termination of the legal relationship Other - 15 years from the termination of the employment contract Other - 10 Years from the end of the activity
Risk Management	Other - 15 years from the termination of the employment contract Other - 10 Years from the end of the activity Other - 10 years from the termination of the legal relationship
Other - Vehicle Info	Other - 15 years from the termination of the employment contract Other - 10 years from the termination of the legal relationship Other - 15 years from the termination of the

	employment contract
Health Information	Other - 10 Years from the end of the activity Other - 15 years from the termination of the employment contract Other - 15 Years from the termination of the employment relationship
Professional Experience	Other - 10 Years from the end of the activity Other - 15 years from the termination of the employment contract
Other - Employee Family Member and Relative Information	Other - 15 years from the termination of the employment contract
Transaction Security	Other - 10 years from the termination of the purpose of data processing Other - 5 years from the termination of the purpose of processing
Marketing	Other - 10 years from the termination of the purpose of data processing

8.2 Data Destruction Times

The Data Controller 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, Personal Data Processing and Protection Policy and this Personal Data Storage and Destruction Policy arises.

When the person concerned applies to the Data Controller pursuant to Article 13 of the Law and requests the deletion or destruction of his/her personal data;

- If all the conditions for processing personal data have disappeared; The Data Controller deletes, destroys or anonymizes the personal data subject to the request within 30 (thirty) days from the day of receipt of the request, explaining the reason for it, with the appropriate destruction method. In order for the Data Controller to be deemed to have received the request, the person concerned must have made the request in accordance with the Personal Data Processing and Protection Policy. In any case, the Data Controller informs the relevant person about the transaction made.

- If all of the conditions for processing personal data have not been eliminated, this request may be rejected by the Data Controller in accordance with the third paragraph of Article 13 of the Law, and the rejection response is notified to the relevant person in writing or electronically within thirty days at the latest.

9. PERIODIC DISPOSAL TIME

In the event that all of the conditions for processing personal data in the law disappear; The Data Controller deletes, destroys or anonymizes the personal data whose processing conditions have disappeared by a process specified in this Personal Data Retention and Destruction Policy and to be carried out ex officio at repeated intervals.

Periodic disposal processes for the first time ..... and repeats every 6 (six) months.

Personal data whose records are kept with the Data Controller are subject to destruction as part of the periodic destruction processes due to the expiry of the retention period and/or legal retention periods in accordance with the Policy, and the process is documented with the Personal Data Destruction Report.

10. PUBLICATION AND STORAGE AND UPDATING OF THE POLICY

The policy is published in three different ways: wet signed (printed paper), printed or electronic QR Code and directly electronically, and is disclosed to the public on the https://www.bmsgeridonusum.com.tr/ website of the Data Controller. The printed paper copy is also kept in the KVKK file by the Data Controller Board of Directors or the Personal Data Manager.

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

11. ADAPTATION AND CHANGES

The Data Controller has the right to make changes in the personal data storage and destruction policy in accordance with the provisions of the Legislation or in accordance with the Data Controller's policy.