Personal Data Storage and Destruction Policy

Purpose

This Personal Data Storage and Destruction Policy ("Policy") has been issued by data controller, BITES Defence and Aerospace Tech. Inc. ("Company"), to enable Data Controller perform its obligations pursuant to the Law Nr. 6698 on the Protection of Personal Data ("Law") and the Regulation on Erasure, Destruction of Anonymization of Personal Data constituting secondary regulation of the Law ("Regulation") and relevant legislation and to inform relevant parties about the guidelines on maximum storage periods required for processing purposes of personal data and about erasure, destruction and anonymization thereof.

Scope

This Policy covers individuals whose personal data is processed by BITES through automated or non-automated means subject to being a part of any data recording system.

Abbreviations

Abbreviation	Description
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

Definitions

Definition	Description
Explicit Consent	Consent concerning a specific matter, based upon being informed and described with free will.
Data Subject	Refers to natural person whose personal data is processed.
Destruction	Erasure, destruction or anonymization of personal data
Law	Refers to the Law Nr. 6698 on the Protection of Personal Data published on Official Gazette dd. 07.04.2016 and nr. 29677.
Recording Media	Refers to any kind of media containing personal data processed through means that are fully or partially automated or that are non-automated, subject to being part of any data recording system.

Definition	Description
Personal Data	Any information relating to an identified or identifiable natural person.
Anonymization of Personal Data	Rendering personal data impossible to associate with a specific or identifiable natural person, even if is paired with other data.
Processing of Personal Data	Any action performed on data including but not limited to obtaining, recording, storing, keeping, altering, reorganizing, describing, transferring, taking over, making available, classifying or preventing the use of personal data through completely or partially automated or non-automated means subject to being a part of data recording system
Personal Data Owner	Natural person whose personal data is processed
Deletion of Personal Data	Process of making personal data inaccessible and unavailable for the users concerned
Destruction of Personal Data	Process of making personal data inaccessible, non-retrievable, and re-usable by any person in any way.
Board	Board for the Protection of Personal Data
Periodic Destruction	the process of erasing, destroying or anonymizing, specified in BITES personal data storage and destruction policy, which will be carried out ex officio at certain intervals in the event that the conditions for processing personal data, as defined in the Law, completely disappear.
Data Processor	Natural person or legal entity who process personal data on behalf of and based upon the authorities vested by data controller
Data Recording System	Recording system in which personal data is configured and processed by certain criteria.
Data Controller	Recording system in which personal data is configured and processed by certain criteria.
Regulation	Regulation on Erasure, Destruction or Anonymization of Personal Data published on Official Gazette dd. 28.10.2017 and nr. 30224

References And Sources

Reference/Source Nr.	Name of Reference/Source
6698	Law on the Protection of Personal Data
-	Regulation on the Erasure, Destruction or Anonymization of Personal Data

Reference/Source Nr.	Name of Reference/Source
-	Communique on Principles and Procedures in Fulfilling the Obligation of Clarifications
-	Communique on Principles and Procedures for Application to Data Controller
ISO/IEC 27001:2013	Information Security Management System

Recording Media of Personal Data

Your personal data is processed and kept in accordance with our legal obligations and according to the characteristics of relevant data.

Recording media that is used for storing personal data are in general hard copies and digital media including servers, hard drives or portable disks available at the Company.

Company takes all necessary technical and administrative measures in compliance with the qualities of recording media of relevant personal data in order to safely store or prevent illegal processing of and access to personal data.

Such measures include but are not limited to the following administrative and technical measures to the extent being applicable to the nature of relevant data and its recording media within the scope of ISO/IEC 27001:2013 Information Security Management System.

All processes performed with regard to erasure, destruction and anonymization of personal data are recorded by the Company and such records are kept for at least 2 (two) years unless other laws/legislations require longer storage periods.

Unless otherwise decided by the Board, personal data will be destroyed by the Company upon the expiry of storage periods specified if and when processing conditions for personal data specified in Articles 5 and 6 completely disappear.

Erasure, destruction and anonymization of personal data are in complete and full conformity with the Law and relevant legislations, Board decision and this Policy.

In case where Data Subject requests from the Company for the erasure, destruction or anonymization of personal data, such requests are responded within at latest 30 (thirty) days. In case where such requested data has been transferred to third parties in accordance with the Policy on the Protection and Processing Personal Data, such case shall be notified to that third party to whom such data has been transferred to ensure any necessary actions are taken by such third parties.

Technical Measures

Company takes the following technical measures in accordance with the characteristics of all media where personal data is kept, of all data and of all media where data is kept:

- Network security and application security are ensured.
- Closed-system network is used for data transfer through network.
- Key management is implemented.
- Security measures within the scope of supply, development and maintenance of information technologies systems are taken.
- Personal data stored on cloud is secured.
- Access logs are kept regularly.
- Data masking is applied whenever necessary.
- Authorities of employees, who are reassigned or have resigned, are cancelled.
- Current anti-virus systems are used.
- Firewalls are used.
- Personal data is backed up and such backed up personal data is also secured.
- User account management and authority control systems are applied and monitored accordingly.
- Log records are kept in a way to prevent user intervention.
- Secure encryption/cryptographic keys are used and managed by different units for sensitive personal data.
- Intrusion detection and prevention systems are used.
- Cyber security measures have been taken and are continually monitored for application.
- Encryption is performed.
- Data loss prevention software are used.

Administrative Measures

Company takes the following administrative measures in accordance with characteristics of all media where personal data is kept, of all data and of all media where data is kept:

- Disciplinary regulations containing data security provisions are in place for employees.
- Trainings and awareness exercises about data security are provided to employees at certain intervals.
- Authority matrix is created for employees.
- Corporate policies have been issued and are being implemented with regard to access, information security, use, storage and destruction.
- Non-disclosure agreements are made.
- Agreements signed contain data security provisions.
- Additional security measures are taken for hard-copied personal data and such documents are sent in classified format.
- Policies and procedures for personal data security have been defined.
- Issues about personal data security are reported immediately.
- Security of personal data is being monitored.
- All security measures necessary to enter into and exit from physical media that contain personal data are taken.
- Physical media that contain personal data are secured against external risks (fire, flood etc.)
- Media that contain personal data is secured.
- Personal data is reduced wherever possible.
- Current risks and measures have been defined.

- Protocols and procedures for the security of sensitive personal data have been defined and are currently in use.
- If sensitive personal data is to be sent through electronic mail, they are necessarily sent encrypted and via KEP (Registered Electronic Mail) or corporate mail address.
- Sensitive personal data transferred to flash memories, CD, DVD are subject to encryption.
- Internal periodic and/or random inspections are conducted and ordered.
- Data processing service providers are subject to inspections at certain intervals for data security.
- Awareness of data processing service providers about data security is increased.

Remarks about Storage and Destruction of Personal Data

Personal data of employees, employee candidates, visitors and any other related individuals, and employees of related institutions and organizations are stored and destroyed in accordance with Law. In this context, detailed descriptions of storage and destruction are provided below, respectively.

Descriptions about Storage

Personal data within the scope of our Company's activities shall be kept for a period stipulated in the relevant legislation and for a period suitable for our purposes of processing.

Legal Grounds Requiring Storage

Our company keeps personal data that are processed within the scope of its activities for a period stipulated in the relevant legislation.

Storage and Destruction Periods

Your personal data is retained and processed in accordance with the personal data processing terms stipulated in Articles 5 and 6 of the Law and will be erasure, destroyed or anonymized ex officio upon request by data subject in the event that the conditions for processing personal data completely disappear.

Destruction Techniques of Personal Data

All destruction processes are processed by our company and any relevant records are kept for at least 2 (two) years notwithstanding other legal obligations.

Unless otherwise decided by the Board, our Company selects the most suitable method for ex officio deletion, destruction or anonymization of personal data depending on technological possibilities and application costs, and also justifies such suitable method upon request by personal data subject.

Deletion Methods of Personal Data

Deletion of personal data refers to the process of making personal data inaccessible and non-reusable for concerned users in any way. Our company takes all technical and administrative measures depending on technological possibilities and application costs to render such deleted personal data inaccessible and non-reusable for concerned users.

In this context, our Company applies the following methods to delete personal data:

Data Recording Media	Description
Personal Data on Servers	For those personal data on servers that expire after necessary storage period, IT Team Leader cancels clearance of concerned users for deletion purposes.
Personal Data on Electronic Media	For those personal data on electronic media that expire after necessary storage period, they are made inaccessible and non-reusable for employees (concerned users) other than database administrator.
Personal Data on Physical Media	Personal data on hard-copy shall be deleted by using blanking method. Blanking process shall be done by cutting off the personal data on relevant document if possible and if not possible, rendering the personal data invisible to users by using fixed ink in such a way that they cannot be retrieved and read through technological solutions.

Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, non-retrievable, and re-usable by any person in any way. Our company takes all necessary technical and administrative measures depending on technological possibilities and application method concerning the destruction of personal data.

In this context, our Company applies the following methods for destruction of personal data:

Data Recording Media	Description
Personal Data on Physical Media	Those personal data on hard-copies that expire after necessary storage period are destroyed irreversibly at paper shredders.
Personal Data on Magnetic Media	Those personal data on magnetic media that expire after necessary storage period are physically destroyed by melting, incinerating or pulverizing.

Anonymization of Personal Data

Anonymization of personal data means rendering personal data impossible to associate with a specific or identifiable natural person, even if it is paired with other data. For anonymization of personal data, personal data must be rendered impossible to associate with a specific or identifiable natural person even through the use of techniques suitable to the recording media and relevant scope of activity such as pairing with other data and retrieval by receiver or receiver groups by our Company. Our Company takes all necessary technical and administrative measures according to technological possibilities and application costs with regard to anonymization of personal data.

Storage and Destruction Periods of Personal Data

Data Category	Storagen Period	Destruction Period
Identity	10 years	In the first periodic destruction period upon expiry of storage period
Contact	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Personal Information	15 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period

Legal Action	2 years after termination of legal relation or rejection of application	In the first periodic destruction period upon expiry of storage period
Customer Transaction	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Physical environment safety	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Transaction security	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Risk management	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Finance	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Professional experience	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Marketing	10 years after termination of legal relation	In the first periodic destruction period upon expiry of storage period

Audio and video records	6 months after termination of legal relation or rejection of application	In the first periodic destruction period upon expiry of storage period
Medical Information	10 years	In the first periodic destruction period upon expiry of storage period
Convictions and security precautions	1 year after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Biometric data	1 month after termination of legal relation	In the first periodic destruction period upon expiry of storage period
Race and ethnicity	2 years after termination of legal relation or rejection of application	In the first periodic destruction period upon expiry of storage period
Philosophical belief, religion, sect and other ethos	2 years after termination of legal relation or rejection of application	In the first periodic destruction period upon expiry of storage period

Duties and Authorities of Personal Data Board

Board for the Protection of Personal Data that consists of top executives and staff members of the relevant departments of BITES is responsible from announcing this Policy to all concerned departments and from monitoring if actions necessary are taken accordingly and from all acts and actions necessary during such process. To contact the Board for the Protection of Personal Data, please e-mail to: kvkk@bites.com.tr .

Updating & Harmonization

Company reserves the right to modify this Personal Data Processing and Destruction Policy due to the changes in Law in accordance with the Board decision or in line with industrial progresses.