

bürotime

**POLICY ON THE STORAGE AND
DESTRUCTION OF PERSONAL
DATA**

CONTENTS

I.	INTRODUCTION.....	1
A.	Purpose and Scope	1
B.	Definitions.....	2
II.	RECORDING ENVIRONMENTS.....	4
A.	Electronic Environments.....	4
B.	Non-Electronic Environments.....	4
III.	EXPLANATIONS ON STORAGE AND DESTRUCTION.....	5
A.	Explanations on Data Storage	5
1.	Legal Grounds Requiring Storage	5
2.	Processing Purposes Requiring Storage	6
B.	Grounds Requiring Destruction	8
IV.	TECHNICAL AND ADMINISTRATIVE MEASURES.....	9
A.	Technical Measures.....	9
B.	Administrative Measures	10
V.	PERSONAL DATA DESTRUCTION TECHNIQUES.....	12
A.	Destruction of Personal Data	12
B.	Removal of Personal Data.....	13
C.	Anonymization of Personal Data	14
VI.	STORAGE AND DESTRUCTION PERIODS.....	14
A.	Storage Period.....	14
B.	Periodic Destruction Time	15
VII.	PUBLICATION AND STORAGE OF THE POLICY.....	15
VIII.	POLICY BREACH AND SANCTIONS	15
IX.	ENFORCEMENT OF THE POLICY.....	15

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

Document Date:

Date of Issue:

Revision Number:

I. INTRODUCTION

A. Purpose and Scope

This Policy has been prepared by the Data Controller **Bürotime** in order to determine the procedures and principles to be followed in accordance with Article 7 of the LPPD.

Bürotime undertakes to comply with the tools, program and processes to be applied on and under this Policy during the deletion, destruction or anonymization of the completely or partially automated personal data held by its side, processed by non-automated means provided that such data is a part of any recording system.

This Policy covers any Employee, Product or Service Recipient, suppliers, supplier authorities, supplier employee, Employee Candidate, potential product or service recipient, trainees, parent / guardian / representatives, business partners, shareholders/partners, people who are the subject of the news, visitors, public officials, employees and authorities of the institutions and organizations with whom they have business relations who are involved in any process where **Bürotime** processes personal data and the personal data of other third parties involved in any process where their personal data is processed.

This Policy covers all destruction activities of **Bürotime** on personal data and will be implemented as the result of any destruction requirements.

This Policy shall not apply to non-personal data.

In the case new relevant legislation is published or the relevant legislation is updated, this Policy shall be updated to comply with the relevant legislation and the legislation requirements.

Bürotime hereby acknowledges that this Policy covers the personal data in the following environments and in all environments that may arise in addition to those environments.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Network devices,
- Shared/non-shared disk drives used for storing data on the network,
- Cloud systems,
- Computers / servers used on behalf of **Bürotime**,
- Flash memories,
- Paper,
- Magnetic tapes,
- Microchip,
- Mobile phones and all storage areas contained inside,
- Optical discs,
- Peripherals such as printers, fingerprint readers.

B. Definitions

Definition	Description
Express Consent	The consent about a specific subject based on information and expressed in free will,
Anonymization	Making personal data unlikely to be associated with any identified or identifiable real person in any way even when personal data is paired with other data.
Bürotime	Tosunoğulları Mobilya San. ve Tic. A.Ş
Employee	Bürotime employees
Employee Candidate	Persons who have filed job applications to Bürotime
Data Subject	Real person whose personal data is processed
Related User	Shall refer to any person who processes personal data in accordance with the authority and order received within the data controller institution or from the data controller, except the person or unit responsible for the technical storage, protection and backup of the data.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

Destruction	Deletion, destruction or anonymization of personal data
Recording Environment	Any media in which the personal data that is entirely or partially automatic or acquired by non-automatic means provided that it shall be a part of any data recording system.
Personal Data	Any information related to the identity of a specific or identifiable real person.
Anonymization of Personal Data	Anonymization of personal data means making personal data unlikely to be associated with any identifiable real person in any way even when personal data is paired with other data
Destruction of Personal Data	Deletion, anonymization or destruction of Personal Data
Deletion of personal data	Refers to the process of making personal data inaccessible to and not reusable by the Related User.
Removal of Personal Data	The irreversible process of destructing personal data and making it inaccessible to and not reusable by anybody.
Committee	Bürotime Personal Data Protection Committee
LPPD	Law on Protection of Personal Data numbered 6698, published in the Official Gazette dated April 7, 2016 and numbered 29677.
PDP Board	Personal Data Protection Board
Sensitive Personal Data	Data about the race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership to an association, foundation or trade union, medical condition, sexual life, criminal conviction and security measures as well as biometric and genetic data of persons
Periodic Destruction	Shall refer to the process of erasing, destroying or anonymizing the personal data stored in the personal data storage and destruction policy in the event that all of the processing conditions of the personal data under the LPPD are removed.
Policy	Bürotime Policy on the Storage and Destruction of Personal Data

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

Instruction	Bürotime Disciplinary Instruction on the Protection of Personal Data
Product or Service Recipient	Real persons or legal entities acting as Dealers, Franchisees, Sub-Franchisees that have a contractual relationship with Bürotime
Data Recording System	The recording system where personal data is processed by means of structuring according to certain criteria,
Data Controller	Refers to real person or legal entity responsible for establishing and managing the data recording system that specifies the objectives and means of processing personal data,
Regulation	Regulation on the deletion, destruction or anonymization of personal data

II. RECORDING ENVIRONMENTS

A. Electronic Environments

- Information security devices (firewall, attack detection and blocking, log file, antivirus etc.)
- Removable memories (USB, memory card, etc.)
- Personal computers (desktop, laptop)
- Mobile devices (phone, tablet, etc.)
- Optical discs (CD, DVD, etc.)
- Servers (Domain, backup, e-mail, database, web, file sharing, etc.)
- Video and audio recording
- Printer, scanner, copier
- Software (Office software, Bsmart, Netsis, IFS, B2Active, CMS Panel, EBA, Mobilas, Pergo, Winper)

B. Non-Electronic Environments

- Paper

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Manual data recording systems (survey forms, visitor entry registry book)
- Written, printed, visual media

III. EXPLANATIONS ON STORAGE AND DESTRUCTION

The personal data of any Employee, Product or Service Recipient, suppliers, supplier authorities, supplier employee, Employee Candidate, potential product or service recipient, trainees, parent / guardian / representatives, business partners, shareholders/partners, people who are the subject of the news, visitors, public officials, employees and authorities of the institutions and organizations with whom they have business relations who processed by **Bürotime** and the personal data of other third parties involved in any process where their personal data is processed shall be retained in compliance with the law and destroyed.

In this context, detailed explanations on the storage and destruction are as follows.

A. Explanations on Data Storage

The concept of processing personal data has been defined under article 3 of the LPPD and in article 4 of the LPPD it has been stated that the processed data should be linked, limited with and proportionate to the purpose of such processing as per the relevant legislation whereas in article 5, the conditions to process personal data have been listed. Accordingly, within the framework of **Bürotime** activities, personal data shall be kept for a period of time specified in the relevant legislation or in accordance with our processing purposes.

1. Legal Grounds Requiring Storage

- Tax Procedural Law No. 213
- Execution and Bankruptcy Code no. 2004
- Customs Law no. 4458
- Labor Law No. 4857
- Regulation Broadcasting in the Internet and fighting against crimes committed through Internet Broadcasting Law no. 5651
- Turkish Code of Obligations no. 6098

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Turkish Commercial Code no. 6102
- Law No. 6502 on the Protection of Consumers,
- Law on the Protection of Personal Data No. 6698
- Law on Industrial Property no. 6769.
- Regulation on the Internet Mass Use Providers
- Regulation on Occupational Health and Safety Services
- Turkish Standards Institute (TSI) Certification Directive
- Communiqué on the Branding of Turkish Products Abroad, Positioning the Image of Turkish Products and Supporting Turquality®
- Regulation on the Payment of Wages, Premiums and any Dues in this Attribute Through Banks

Personal data will be stored for the prescribed period of storage in accordance with these laws and other secondary regulations in force.

2. Processing Purposes Requiring Storage

Bürotime stores the personal data it processes within the scope of its activities for the following purposes:

- Conducting disaster management processes,
- Carrying out information security processes,
- Carrying out the process of selection and recruitment for Employee Candidates/Trainees/Students,
- Carrying out the application process of the Candidate Employee,
- Conducting employee satisfaction and engagement processes,
- Fulfillment of the obligations for the employees of the Company arising from the employment contract and/or the legislation,
- Conducting training activities,
- Conducting activities in accordance with the legislation,

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Conducting financial and accounting works,
- Ensuring the security of physical space,
- To follow up and conduct legal affairs,
- Conducting Internal Audit / Investigation / Intelligence activities,
- Planning of Human Resources processes,
- Conducting / auditing business activities,
- Carrying out occupational health and safety activities,
- Receiving and assessment of suggestions for the improvement of business processes,
- Conducting the activities to ensure business continuity,
- Carrying out logistics activities,
- Carrying out the procurement processes of goods / services,
- Carrying out after-sales support services,
- Carrying out the sales processes of goods and services,
- Carrying out the manufacturing and operation processes of goods / services,
- Carrying out customer relationship management processes,
- Conducting customer satisfaction activities,
- Management of organization and activities,
- Carrying out performance evaluation processes,
- Carrying out advertising / campaign / promotion processes,
- Conducting risk management processes,
- Conducting storage and archiving activities,
- Performance of warranty and maintenance-repair activities for the purchased products,

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Conducting the contract processes,
- Conducting sponsorship activities,
- Tracking the Requests/Complaints,
- Execution of marketing processes of products / services,
- Conducting the registration process of the Industrial Design Department related to the products,
- Conducting the process of obtaining the certificates of conformity related to TSI standards of the products,
- Carrying out the registration process of the products before the Turkish Patent and Trademark Authority,
- Conducting the process of obtaining the International Quality Certificate within the scope of UL Greenguard,
- Carrying out talent/career development activities,
- Registration of documents and instruments received from Authorized Public Institutions and Data Subjects,
- Providing information to authorized persons, institutions and organizations,
- Conducting management activities,
- Conducting embezzlement activities,

B. Grounds Requiring Destruction

In the case **Bürotime** rejects the application filed by the Data Subject upon the request of deletion, destruction or anonymization of the personal data, finds the response made to its side inadequate or does not respond within the time period specified in the LPPD;

- Amendment or abolition of the provisions of the relevant legislation constituting the basis for the processing of personal data,
- The purpose that requires processing or storage not being valid anymore,
- The Data Subject revoking its express consent in cases where the processing of personal data occurs only in accordance with the express consent requirement,

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- The maximum period during which personal data should be stored has passed and there are no conditions to justify the storage of personal data for a longer period of time,
- Placing a complaint to the PPD Board and the request being approved by the PPD Board,
- Bürotime to accept the application for deletion and destruction of personal data within the framework of the rights of the Data Subject in accordance with Article 11 of the LPPD.

In the cases listed above, personal data will be deleted, destructed or ex officio deleted, destructed or anonymized by **Bürotime** upon the request of the Data Subject.

IV. TECHNICAL AND ADMINISTRATIVE MEASURES

For the secure storage of, prevention of processing and access to personal data contrary to the law as well in order to ensure that the personal data is destructed in accordance with the law, technical and administrative measures will be taken by **Bürotime** pursuant to the sufficient measures defined and announced by the PDP Board for sensitive personal data as per paragraph four of article 6 of the LPPD and article 12 of the LPPD.

A. Technical Measures

- Network security and application security are ensured. Closed system network is used for the personal data transfers through the network.
- Key management is applied.
- Information systems are kept up to date and strong passwords are used in electronic environments where personal data is processed.
- Security measures are taken within the scope of the procurement, development and maintenance of information technology systems.
- An authorization matrix has been created for the employee.
- Other **Bürotime** regulations are established and implemented for access authorization and role distributions.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- The authorities of the employees whose positions have changed or who have left their job shall be removed.
- Up-to-date anti-virus systems are used.
- Security vulnerabilities are monitored and appropriate security patches are installed and firewalls are used.
- The security of the environments containing personal data is ensured.
- Personal data is backed up and the security of the backed up personal data is also ensured.
- Backup programs are used to ensure the secure storage of personal data and access to personal data stored in electronic or non-electronic environments is restricted according to the principles of access.
- User account management and authorization control system are applied and these are monitored respectively.
- Necessary measures are taken for the physical security of the information systems equipment, software and data of the institution.
- Attack detection and prevention systems are used.
- Penetration Test is applied.
- Cyber security measures have been taken and the implementation of such measures is continuously monitored.
- Encryption is done.
- Sensitive personal transferred to flash memory, CD, DVD media should be encrypted before the transfer process.
- Data loss prevention software is used.

B. Administrative Measures

- Disciplinary regulations are in place for the employee with data security provisions applied.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Training and awareness procedures are conducted at regular intervals on data security for the employee.
- The employee will have to sign non-disclosure agreements.
- The qualifications and technical knowledge / skills of the employee are being improved.
- Other Bürotime regulations on access, information security, usage, storage and destruction have been prepared and started to be implemented.
- Undertaking Confidentiality Letters are executed. The contracts signed contain data security provisions.
- Disciplinary procedures are applied to the Employee who does not comply with other **Bürotime** regulations. The obligation to make disclosure to the Data Subjects is fulfilled, in-house periodic and random audits are conducted and information security trainings are provided for the Employee.
- Trainings are provided on communication techniques and the relevant legislation.
- Personal data security have been determined by other **Bürotime** regulations.
- Necessary security measures are taken for entering and exiting physical environments containing personal data.
- Physical environments containing personal data are protected against external risks (fire, flood, etc.).
- The obligation to disclose to the Data Subjects before the processing of personal data is fulfilled.
- Personal Data is reduced to the extent possible.
- Illicit access to personal data is prevented.
- Illicit processing of personal data is prevented.
- The retention of personal data is provided.
- In-house periodic and random audits are conducted and information security trainings are provided for the Employee.
- Existing risks and threats have been identified.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

- Sensitive personal data security has been determined by other **Bürotime** regulations and is being applied.
- Destruction processes in accordance with this Policy are defined and implemented.

V. PERSONAL DATA DESTRUCTION TECHNIQUES

Personal data shall be destroyed by **Bürotime** either ex officio or upon the application of the Data Subject at the end of the storage period set forth in the relevant legislation or required for the purpose for which it is processed, again in accordance with the provisions of the relevant legislation.

A. Destruction of Personal Data

Personal data shall be destroyed by **Bürotime** or, if deemed necessary, by a third party designated by **Bürotime** by the following methods.

Personal Data In Electronic Environment	Among the personal data in the electronic environment, those whose required period of retention has expired shall be made inaccessible to and not reusable by the other Employee (Data Subject) except for the data base manager.
Personal Data In Physical Environment	Among the personal data in the physical environment, those whose required period of retention has expired shall be made inaccessible to and not reusable by the other Employee (Data Subject) except for the responsible department manager. Furthermore, blackout by scratching / painting / wiping is performed to make the data unreadable.
Blackout of Personal Data On Paper	It is a method of physically cutting or removing the relevant personal data from the document or making it invisible by using fixed ink, which cannot be recovered and read by means of using technological solutions in order to prevent the unintended use of personal data or to delete the data that has been requested to be deleted.
Personal Data On Servers	Among the personal data on the servers and the retention period of which has expired, such data shall be deleted by the system

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

	administrator by removing the access authority of the Data Subject.
Personal Data On Removable Memory Tools	Expired personal data stored in flash-based storage media will be stored in secure environments with encryption keys, which are encrypted by the system administrator and given only to the system administrator.
Secure Deletion By the Specialist	In some cases, it may agree with a specialist to have the personal data deleted on its behalf. In this case, the personal data shall be securely wiped by the relevant specialist to make the data inaccessible and not reusable.
Secure Deletion from the Software	When deleting the data processed by fully or partially automated means and stored in digital media, methods are used to delete the data from the respective software in such a way that it is inaccessible and not reusable by the Related Users. The deletion of related data in the cloud system by giving the command to delete, deletion of the related user's right of access on the file or the directory where the file is located on the central server, deletion of the relevant rows in the databases with database commands or deletion of the data in the flash media using the appropriate software can be considered to be included within this scope.

B. Removal of Personal Data

Personal data shall be destroyed by **Bürotime** by the following methods.

Personal Data In Physical Environment	Among the personal data in the paper environment, those whose required period of retention has expired shall be irreversibly destroyed in paper shredders.
Physical Destruction	Personal data can be processed with non-automated means provided that it is a part of any data registry system. While destroying such data, a system of physical destruction of personal data shall be implemented in a manner as cannot be used later. Destruction of data on paper environment

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

	should also be done in this manner since it is not possible to destroy it in any other way.
In Optical/Magnetic Media Personal Data	For the data included in the optical media and magnetic media and for which the period required for retention has expired, the procedure to melt, burn or powderize to destroy the physical form will be applied. Furthermore, the magnetic media will be passed through a special device and exposed to a high magnetic field, making the data on it unreadable.
Overwriting	Overwriting is a destruction method making it impossible to read and recover the old data by writing at least seven times a random data comprising at figures 0 and 1 over magnetic media and rewritable optical media through special software.

Bürotime complies with the provisions of the LPPD, the Regulation and other relevant legislation in order to ensure data security and takes all necessary administrative and technical measures during the realization of the above-mentioned situations.

C. Anonymization of Personal Data

Anonymization of personal data means making personal data unlikely to be associated with any identifiable real person in any way even when personal data is paired with other data.

For the personal data to be anonymized, personal data must not be associated with any identifiable real person in any way in terms of any recording environment even when personal data is paired with other data and/or recovered by the data controller or third parties as well as by means of using the appropriate techniques in terms of the relevant field of activity.

VI. STORAGE AND DESTRUCTION PERIODS

A. Storage Period

While determining the storage periods of personal data, a determination shall be made by **Bürotime** taking into consideration the legislation in force and the purpose of processing the data subject to the process.

POLICY ON THE STORAGE AND DESTRUCTION OF PERSONAL DATA

Storage periods are, in any case, determined in the light of statutory obligations and the respective statute of limitations.

Updates to such storage periods can be made by **Bürotime** if deemed necessary. In the case the purpose for the processing data has been removed, the data will be deleted, destroyed or anonymized, unless there is any other legal ground or basis for the retention of data.

B. Periodic Destruction Time

Bürotime has determined the periodic destruction time as 6 months pursuant to Article 11 of the Regulation. Accordingly, periodic destruction is carried out every year in months January and June.

VII. PUBLICATION AND STORAGE OF THE POLICY

The policy will be published in two different media, i.e on printed paper with original signature and in electronic media and will be announced on the official website. The copy of the printed paper will also be stored in **Bürotime**.

VIII. POLICY BREACH AND SANCTIONS

In the case of this Policy is violated, the disciplinary process applicable at that time may be executed in accordance with the Instruction and warning, reprimand, collection of fine and one or more of the contract termination sanctions may be applied and furthermore legal action may be initiated.

IX. ENFORCEMENT OF THE POLICY

This Policy, set out by **Bürotime**, has entered into force on date 28.04.2020 and in the case the entire Policy or certain articles are renewed, necessary updates will be made.

This Policy will be implemented, updated and announced by the Committee.