

MİKROELEKTRONİK ARAŞTIRMA GELİŞTİRME TASARIM VE TİCARET LİMİTED ŞİRKETİ

PERSONAL DATA STORAGE AND DISPOSAL POLICY

TABLE OF CONTENTS

1. Introduction	2
1.1. Purpose	2
1.2. Abbreviations and Definitions.....	2
2. Principles.....	3
3. Explanations Regarding the Reasons Requiring Storage and Disposal.....	3
3.1. Storage and Disposal Periods	4
4. Administrative and Technical Measures	5
4.1. Administrative Measures.....	5
4.2. Technical Measures.....	5
5. Duties and Powers of the Personal Data Committee.....	6
6. Entry into Force of the Policy, Breach Situations, and Sanctions	6

1. Introduction

1.1. Purpose

This Personal Data Storage and Disposal Policy (“Policy”) has been prepared by Mikroelektronik Araştırma Geliştirme Tasarım ve Ticaret Limited Şirketi (“MKR-IC”), acting as the data controller, in order to fulfill its obligations pursuant to the Personal Data Protection Law No. 6698 (“Law”) and the Regulation on the Erasure, Destruction, or Anonymization of Personal Data (“Regulation”), which constitutes secondary legislation under the Law, and to inform data subjects about the principles for determining the maximum storage period necessary for the purpose for which their personal data are processed, as well as the processes for erasure, destruction, and anonymization.

1.2. Abbreviations and Definitions

The abbreviations and definitions used in this Policy are set out below. Where the same abbreviation is also defined in MKR-IC’s other policies or guidelines, the definition in this Policy shall prevail.

Explicit Consent: Consent relating to a specific matter, based on information and expressed freely.

Data Subject: The natural person whose personal data are processed.

Relevant User: Persons who process personal data within the data controller’s organization, or in accordance with the authority and instructions received from the data controller, excluding the person or unit responsible for the technical storage, protection, and backup of the data.

Disposal: The erasure, destruction, or anonymization of personal data.

Recording Medium: Any environment in which personal data processed wholly or partly by automated means or by non-automated means, provided that such processing forms part of a data recording system, are stored.

Personal Data: Any information relating to an identified or identifiable natural person.

Processing of Personal Data: Any operation performed on personal data, including obtaining, recording, storing, retaining, altering, reorganizing, disclosing, transferring, taking over, making available, classifying, or blocking the use of personal data, whether wholly or partly by automated means or by non-automated means provided that such processing forms part of a data recording system.

Anonymization of Personal Data: Rendering personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching with other data.

Erasure of Personal Data: Rendering personal data inaccessible and unusable in any way for data subjects.

Destruction of Personal Data: The process of rendering personal data inaccessible, irretrievable, and unusable by anyone in any way.

Board: The Personal Data Protection Board defined under the Law.

Periodic Disposal: The recurring ex officio erasure, destruction, or anonymization process to be carried out at the intervals specified in the Personal Data Storage and Disposal Policy when all conditions for processing personal data set out in the Law cease to exist.

Employee: MKR-IC personnel.

Service Provider: A natural or legal person providing services to MKR-IC within the framework of a specific contract.

Data Processor: A natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller.

Data Recording System: A recording system in which personal data are structured and processed according to specific criteria.

Data Controller: A natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system.

2. Principles

MKR-IC acts in accordance with the following principles in the storage, erasure, destruction, and anonymization of personal data:

- MKR-IC acts in full compliance with the Law, applicable legislation, Board decisions, and this Policy in the erasure, destruction, and anonymization of personal data.
- All actions taken by MKR-IC in relation to the erasure, destruction, and anonymization of personal data are recorded, and such records are retained for at least three (3) years unless they are required to be retained for longer periods under other laws or legislation.
- Unless the Board decides otherwise, personal data shall be disposed of by MKR-IC at the end of the determined storage periods.
- Where all conditions for processing personal data set out in Articles 5 and 6 of the Law cease to exist, personal data shall be disposed of by MKR-IC.

Where a data subject requests MKR-IC to erase, destroy, or anonymize personal data, the submitted requests shall be responded to within thirty (30) days at the latest. Where the data subject's personal data have been transferred to third parties in accordance with the MKR-IC Personal Data Protection and Processing Policy, this situation shall be notified to the relevant third party to which the data were transferred, and the necessary actions shall be ensured at such third parties.

3. Explanations Regarding the Reasons Requiring Storage and Disposal

Personal data belonging to data subjects are stored by MKR-IC, particularly for

(i) the continuation of commercial activities, (ii) the fulfillment of legal obligations, and (iii) the planning and performance of employee rights and fringe benefits, within the limits set out in the Law and other applicable legislation. The reasons for storing personal data are set out below:

- Storage of personal data because it is directly related to the establishment and performance of contracts;
- Storage of personal data for the establishment, exercise, or protection of a right;
- Storage of personal data where it is necessary for MKR-IC's legitimate interests, provided that it does not prejudice the fundamental rights and freedoms of individuals;
- Storage of personal data for the purpose of fulfilling any legal obligation of MKR-IC;
- Where storage of personal data is expressly prescribed by legislation;
- Where the data subjects have explicit consent in respect of storage activities that require their explicit consent.

Pursuant to the Regulation, personal data belonging to data subjects shall be disposed of by MKR-IC in the following cases:

- Where it is necessary due to amendment or repeal of the relevant legislative provisions forming the basis for the processing or storage of personal data;
- Where the purpose requiring the processing or storage of personal data ceases to exist;
- Where the conditions requiring the processing of personal data under Articles 5 and 6 of the Law cease to exist;
- Where processing of personal data is based solely on explicit consent and the data subject withdraws such consent;
- Where the data controller accepts the application made by the data subject, within the scope of the rights under Article 11 of the Law, for the erasure, destruction, or anonymization of their personal data;
- Where the data controller rejects the application submitted by the data subject requesting the erasure, destruction, or anonymization of their personal data, where the response is found insufficient, or where no response is given within the period prescribed by the Law, and a complaint is lodged with the Board and such request is found appropriate by the Board;
- Where the maximum period requiring storage of personal data has expired and no condition exists that would justify storing personal data for a longer period.

3.1. Storage and Disposal Periods

Where a storage period is prescribed in legislation for determining the storage and disposal periods of your personal data obtained by MKR-IC in accordance with the Law and other applicable legislation, that period shall be observed. Following the expiry of such period, or where no period is prescribed by legislation, the actions specified below shall be taken in respect of the data at the end of the period required for processing, in accordance with MKR-IC's practices and commercial customs, depending on the activity carried out while processing the relevant data.

- Personal data are classified as personal data and special categories of personal data on the basis of the definition in Article 6 of the Law. All personal data determined to be special categories of personal data shall be disposed of. The method to be applied for the disposal of such data shall be determined according to the nature of the data and the degree of importance of storing it at MKR-IC.
- Matters such as whether storage of the data complies with the principles set out in Article 4 of the Law and whether MKR-IC has a legitimate purpose in storing the data are assessed. Personal data

whose storage is determined to be contrary to the principles set out in Article 4 of the Law shall be disposed of.

- It is determined under which exception or exceptions set out in Articles 5 and 6 of the Law the storage of the data may be assessed. Reasonable periods for which the data must be stored are determined within the framework of the identified exceptions. The data shall be disposed of upon expiry of such periods.

Personal data whose storage periods determined by MKR-IC have expired are disposed of at six-month intervals in accordance with the procedures set out in this Policy. All actions taken in relation to the disposal of personal data are recorded, and such records are retained for at least three (3) years, excluding other legal obligations.

4. Administrative and Technical Measures

Where it is necessary to process your personal data for MKR-IC to fulfill its obligations arising from an education or employment contract, where data processing is necessary for the establishment of a right, where you may benefit from other opportunities or where MKR-IC is required to fulfill commercial, financial, or legal responsibilities and obligations related to them, to ensure MKR-IC's security, or for MKR-IC's legitimate purposes, the personal data to be collected are entered into the data storage system. In addition, all data stored in digital-copy form are recorded on MKR-IC servers.

The technical and administrative measures taken by MKR-IC, within the framework of the principles set out in Article 12 of the Law, to ensure that your personal data are stored securely, are not processed unlawfully, unauthorized access is prevented, and data are disposed of in accordance with the law are listed below.

4.1. Administrative Measures

- Internal access to stored personal data at MKR-IC is limited to personnel who require access due to their job description. Whether the data are special categories of personal data and their level of importance are also considered when restricting access.
- Where processed personal data are unlawfully obtained by others, MKR-IC notifies the data subject and the Board of this situation as soon as possible.
- MKR-IC employs personnel who are knowledgeable and experienced in the processing of personal data and provides its personnel with the necessary training on personal data protection legislation and data security.
- MKR-IC carries out and has carried out the necessary audits to ensure the implementation of the provisions of the Law within its legal entity. It remedies confidentiality and security vulnerabilities identified as a result of such audits.
- MKR-IC ensures that adequate security measures are taken according to the environment in which personal data are located, including against electrical leakage, fire, flooding, theft, and similar risks, and prevents unauthorized entry into and exit from such environments.

4.2. Technical Measures

- Network security and application security are ensured.
- A closed system network is used for the transfer of personal data over a network.

- Key management is implemented.
- Security measures are taken within the scope of procurement, development, and maintenance of information technology systems.
- Access logs are retained regularly.
- Corporate policies regarding access, information security, use, storage, and disposal have been prepared and implemented.
- Data masking measures are applied where necessary.
- Up-to-date antivirus systems are used.
- Firewalls are used.
- The security of physical environments containing personal data is ensured against external risks, including fire and flooding.
- Personal data are backed up, and the security of backed-up personal data is also ensured.
- A user-account management and authorization-control system is implemented and monitored.
- Log records are retained in a manner that prevents user intervention.
- Intrusion-detection and intrusion-prevention systems are used.
- Penetration testing is conducted.
- Cybersecurity measures have been taken, and their implementation is continuously monitored.
- Encryption is used.
- Special categories of personal data transferred through portable memory devices, CDs, or DVDs are transferred in encrypted form.
- Awareness of data security is ensured among service providers that act as data processors.
- Data loss prevention software is used.

5. Duties and Powers of the Personal Data Committee

The Personal Data Committee, consisting of senior managers of MKR-IC's relevant units, is responsible for announcing the Policy to the relevant business units, monitoring fulfillment of its requirements, and carrying out all work and transactions required in this process. The Personal Data Committee can be contacted at kvk@mkr-ic.com.

6. Entry into Force of the Policy, Breach Situations, and Sanctions

The Policy shall enter into force upon being announced to all MKR-IC employees and shall be binding on MKR-IC and all authorized persons who process personal data on behalf of MKR-IC as of its entry into force. Disciplinary action shall be taken by MKR-IC in accordance with its internal regulations against employees who act in violation of the Policy.

To exercise the rights stated above, you may complete the form available at www.mkr-ic.com/KVK and submit your request, containing the information necessary to identify you clearly and your explanations regarding the right under Article 11 of the Personal Data Protection Law No. 6698 that you wish to exercise, by sending a signed copy of the form to kvk@mkr-ic.com, delivering it in person together with documents verifying your identity to Reşitpaşa Mah. Katar Cad. 4 ARI 3 Teknokent B203, 34467 Sarıyer/İstanbul, sending it through a notary public or by other methods specified in the

Personal Data Protection Law No. 6698, or sending the relevant form with a secure electronic signature to MKR-IC's Registered Electronic Mail (KEP) address: mikroelektronik@hs03.kep.tr.

The list containing the titles, units, and duties of employees authorized to process personal data at MKR-IC is kept confidential by MKR-IC.