# PERSONAL DATA RETENTION AND DESTRUCTION POLICY

## Personal Data Retention and Destruction Policy

This Personal Data Retention and Destruction Policy (the “Policy”) has been prepared by Aselsan Malatya Elektronik Sanayi ve Ticaret Anonim Şirketi (“Aselsan Malatya”), acting as data controller, to fulfill its obligations under the Personal Data Protection Law No. 6698 (“Law”) and the Regulation on the Erasure, Destruction or Anonymization of Personal Data (“Regulation”), and to inform data subjects of the criteria for determining the maximum retention period necessary for processing and the procedures for erasure, destruction and anonymization.

## Definitions

- Explicit consent: Freely given consent relating to a specific matter and based on information.
- Data subject: A natural person whose personal data is processed.
- Relevant user: A person processing personal data within the data controller’s organization or according to the data controller’s authority and instructions, excluding units responsible solely for technical storage, protection and backup.
- Destruction: Erasure, destruction or anonymization of personal data.
- Recording medium: Any medium containing personal data processed automatically, partially automatically, or non-automatically as part of a data filing system.
- Personal data: Any information relating to an identified or identifiable natural person.
- Processing of personal data: Any operation performed on data, including collection, recording, storage, retention, alteration, rearrangement, disclosure, transfer, acquisition, retrieval, classification or restriction of use.
- Anonymization: Rendering data impossible to associate with an identified or identifiable natural person, even by matching it with other data.
- Erasure: Rendering personal data inaccessible and unusable by relevant users.
- Destruction: Rendering personal data inaccessible, irretrievable and unusable by anyone.
- Board: The Personal Data Protection Board established under the Law.
- Periodic destruction: Erasure, destruction or anonymization carried out ex officio at recurring intervals specified in the retention and destruction policy once all legal conditions for processing have ceased to exist.

## Principles

Aselsan Malatya observes the following principles when retaining, erasing, destroying or anonymizing personal data:

- Full compliance with the Law, relevant legislation, Board decisions and this Policy.
- All erasure, destruction and anonymization operations are recorded, and records are kept for at least three years unless a longer period is required under applicable law.
- Unless the Board decides otherwise, data is destroyed when the specified retention period expires.
- Data is destroyed if all processing conditions under Articles 5 and 6 of the Law cease to apply.

If a data subject requests erasure, destruction or anonymization, Aselsan Malatya responds within thirty days. If the data has been transferred to third parties pursuant to the Personal Data Protection and Processing Policy, the third parties are notified and necessary measures are secured.

## Reasons for Retention and Destruction

Personal data is retained within the limits established by the Law and relevant legislation, particularly for continuing commercial activities, fulfilling legal obligations and administering employee rights and benefits.

- Retention directly related to the establishment or performance of contracts.
- Retention necessary for establishing, exercising or protecting a right.
- Retention necessary for the legitimate interests of Aselsan Malatya, provided fundamental rights and freedoms are not harmed.
- Retention necessary to satisfy Aselsan Malatya’s legal obligations.
- Retention expressly provided for by legislation.
- Existence of the data subject’s explicit consent where consent is required.

Under the Regulation, personal data is destroyed in the following circumstances:

- The legal provisions underlying processing or retention have changed or been repealed.
- The purpose requiring processing or retention no longer exists.
- The conditions for processing under Articles 5 or 6 of the Law no longer apply.
- The data subject withdraws consent where processing is based solely on explicit consent.
- The data controller accepts a request for erasure, destruction or anonymization made under Article 11.
- The Board upholds a complaint following a rejected, insufficiently answered or unanswered request.
- The maximum retention period has elapsed and no justification remains for longer retention.

## Retention and Destruction Periods

Where legislation specifies a retention period, that period is observed. Once it expires, or where legislation does not specify a period, data is assessed in light of the relevant activity, Aselsan Malatya’s practices and generally accepted commercial practices. The following review is performed:

- Personal data is classified as ordinary or special-category personal data pursuant to Article 6; the nature and importance of the data determine the destruction method.
- Compliance with Article 4 and whether there is a legitimate purpose for continued retention are assessed; data retained contrary to these principles is destroyed.
- The applicable conditions and exceptions under Articles 5 and 6 are identified, reasonable retention periods are set, and the data is destroyed after those periods end.

Personal data whose retention period has expired is destroyed at six-month intervals pursuant to this Policy. All destruction operations are recorded and those records are kept for at least three years, except where other legal obligations require otherwise.

## Retention and Destruction Procedures; Technical and Administrative Measures

Personal data is processed and stored where necessary for performance of contractual duties, establishment of rights, customer services, commercial, financial and legal obligations, security and other legitimate objectives. Digitally retained copies are stored on Aselsan Malatya servers. Administrative and technical measures are applied under Article 12 of the Law to ensure security, prevent unlawful processing and unauthorized access, and ensure lawful destruction.

### Administrative measures

- Internal access to retained data is limited to staff requiring access for their duties, with account taken of sensitivity.

- Any unlawful acquisition of personal data is reported to the data subject and the Board as soon as possible.
- Data-sharing partners sign confidentiality and data-protection agreements or equivalent contractual provisions.
- Qualified staff are employed and receive training on data protection and information security.
- Internal audits are conducted and confidentiality or security deficiencies are remedied.
- Physical safeguards are provided against electrical faults, fire, flooding, theft and unauthorized entry.

**Technical measures**

- Comply with applicable information security policies and rules.
- Apply periodic information security checks in accordance with ISO 27001.
- Provide information-security awareness training at least once annually.
- Manage information-security risks and opportunities and adopt risk-mitigation measures.
- Apply centralized authentication, network access control, antivirus protection, port control and other security controls.
- Encrypt portable computers and storage devices containing sensitive information.
- Adjust access permissions when job roles change and immediately revoke or block departing employees' access.
- Provide network and application security and use closed network systems when transferring personal data.
- Implement encryption and key management.
- Apply security measures to the procurement, development and maintenance of information technology systems.
- Keep access logs regularly and implement corporate access, security, use, retention and destruction policies.
- Apply data masking where required and execute confidentiality agreements with vendors working on critical systems.
- Use centrally managed malware-prevention software and firewalls when connecting networks of different security levels.
- Back up personal data and protect backups.
- Apply user account management, permission controls, tamper-resistant logs, intrusion detection/prevention and penetration testing.
- Continuously monitor cybersecurity controls.
- Use data-loss-prevention software and require periodic password changes.

## Duties and Powers of the Personal Data Committee

The Personal Data Committee, consisting of senior managers of relevant Aselsan Malatya units, is responsible for communicating the Policy to the relevant units, monitoring compliance and carrying out necessary actions. The Committee can be contacted at kvk@aselsanmalatya.com.tr.

## Entry into Force, Violations and Sanctions

The Policy enters into force upon notification to all Aselsan Malatya employees and binds Aselsan Malatya and everyone processing personal data on its behalf. Employees who violate the Policy may face disciplinary action under internal regulations.

To exercise your rights under Article 11 of Law No. 6698, complete the application form available at www.aselsanmalatya.com.tr and submit a signed copy by e-mail to kvk@aselsanmalatya.com.tr, in person with identity-verification documents or through a notary to Aselsan Malatya Elektronik Sanayi ve Ticaret Anonim

Şirketi, 2. OSB Mah. 2. Cad. No:18/2 Yeşilyurt/Malatya, Türkiye, or by other legally permitted methods. The form may also be sent with a secure electronic signature to the registered electronic mail (KEP) address aselsanmalatya@hs01.kep.tr.

## Annex 1 — List of Staff Titles, Units and Duties

The list of employees authorized to process personal data, including their titles, units and duties, is maintained confidentially by Aselsan Malatya.