POLICY ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

IC INTECHRON TEKNOLOJİ TİCARET ANONİM ŞİRKETİ

Publication Date: 13.08.2026

1. Purpose and Scope

The purpose of this Policy is to set out the fundamental principles governing the processing, protection, transfer and retention of personal data processed by IC Intechron in accordance with Law No. 6698 on the Protection of Personal Data (the "Law") and the relevant secondary legislation, as well as the deletion, destruction or anonymization of such data when the conditions for processing cease to exist.

This Policy applies to natural persons whose personal data is processed within the scope of IC Intechron's website, communication and quotation processes, recruitment and candidate assessment activities, newsletter/corporate communication processes, customer-supplier-business partner relationships, and data subject applications under the Law.

2. Data Controller

Data Controller	IC INTECHRON TEKNOLOJİ TİCARET ANONİM ŞİRKETİ
Address	Mutlukent Mahallesi, 2045 Sokak, No:19, Çankaya/Ankara, Türkiye
Registered Electronic Mail (KEP)	icintechron@hs03.kep.tr
General E-mail	info@intechron.com.tr

3. Fundamental Principles

IC Intechron processes personal data in accordance with the principles set out in Article 4 of the Law:

- Processing lawfully and fairly.
- Being accurate and, where necessary, kept up to date.
- Being processed for specified, explicit and legitimate purposes.
- Being relevant, limited and proportionate to the purposes for which they are processed.
- Being retained for the period prescribed by applicable legislation or required for the purposes for which they are processed.

4. Data Subject Groups

Data Subject Group	Scope
Website visitors	Persons who visit the website and use online services.
Communication / request submitters	Persons who submit information, quotation, technical support, request or complaint messages.
Job applicants	Persons who apply for employment or participate in interview or assessment processes.
Reference persons	Persons identified as references by job applicants.
Customer / prospective customer contact persons	Natural persons who communicate with IC Intechron on behalf of customer or prospective customer organizations.
Supplier / business partner contact persons	Natural persons who communicate with IC Intechron on behalf of suppliers, consultants or business partners.
Newsletter subscribers	Persons who indicate a communication preference to receive technical news, product/solution updates or corporate announcements.

Data Subject Group	Scope
Data subject applicants	Persons who submit applications to IC Intechron under Articles 11 and 13 of the Law.

5. Personal Data Categories

Data Category	Illustrative Scope
Identity	Name and surname; other identity information only at stages where it is genuinely necessary for the relevant process.
Contact	E-mail, telephone, address, KEP and communication preference information.
Request / Complaint	Request, message, complaint, technical support and resolution records.
Job Applicant	CV/resume, education, experience, competencies, interview/assessment, offer and application-related information.
Reference	Business contact details of the reference person and information obtained during the reference interview.
Customer / Business Relationship	Corporate contact person information, correspondence and transaction records within the scope of quotations and business relationships.
Transaction Security / Web	IP address and security/log records, form transaction time, session and cookie preference information, only to the extent necessary.
Marketing / Communication Preference	Newsletter subscription, commercial electronic communication consent/refusal record and preference timestamp.
Legal Transaction	Data subject applications, legal requests and records relating to the protection of rights.
Special Categories of Personal Data	As a rule, not requested through website or initial job application forms. Where processing is required, such data is processed in a limited and secure manner in accordance with Article 6 of the Law and applicable legislation.

6. Purposes and Legal Grounds for Processing

Process	Main Purpose	Legal Ground
Communication, quotation and request management	Receiving, assessing and responding to requests, directing them to the relevant unit and conducting pre-contractual discussions.	Establishment/performance of a contract, legal obligation, establishment-exercise-protection of a right, or legitimate interests.
Recruitment	Application, interview, assessment, offer and pre-employment preparation processes.	Necessity for steps to establish a contract, legitimate interests, legal obligation, and establishment-exercise-protection of a right.
Candidate pool	Assessment and communication for suitable future vacancies after the current application.	Separate explicit consent given freely.
Web and information security	Website, form and system security; prevention of unauthorized access and misuse.	Legal obligation and legitimate interests.
Newsletter / commercial electronic communications	Sending technical news, product/solution updates, event information and corporate announcements; managing consent and refusal records.	Commercial electronic communication consent under Law No. 6563 and applicable legislation; for personal data processing, explicit consent and/or other applicable processing conditions depending on the activity.
Legal proceedings and data subject applications	Exercise of rights, management of disputes and response to requests from authorized authorities.	Legal obligation and establishment-exercise-protection of a right.

Personal data processing activities are, to the extent possible, based on processing conditions under the Law other than explicit consent. Explicit consent is obtained only where the relevant processing activity cannot be based on another processing condition under the Law or where legislation expressly requires consent; it is specific, informed and freely given.

7. Collection of Personal Data

Personal data may be collected electronically or physically through the website and forms, e-mail, telephone, career platforms and professional networks, face-to-face meetings, documents submitted by applicants, contracts, correspondence within the scope of business relationships, and technical system/security records.

8. Transfer of Personal Data

Personal data may, to the extent limited and proportionate to the processing purpose, be transferred to relevant IC Intechron employees and managers; information technology, hosting, e-mail, security and similar service providers processing data on behalf of the Company; consultancy, legal and audit service providers; customers, suppliers and business partners depending on the nature of the business relationship; IC Holding and other group companies to the extent necessary; and legally authorized public authorities and institutions and authorized private law persons, in accordance with Article 8 of the Law.

Where a process requires transfer of personal data abroad, such transfer shall be carried out only where the conditions and appropriate safeguards prescribed under Article 9 of the Law and the relevant secondary legislation are satisfied.

9. Special Categories of Personal Data

As a rule, IC Intechron does not request special categories of personal data through its website or initial job application forms. Where processing of special categories of personal data becomes necessary due to the position, nature of the business relationship or applicable legal/security requirements, data minimization is observed, an appropriate legal ground is identified in accordance with Article 6 of the Law and applicable legislation, and the necessary technical and administrative measures are implemented.

10. Retention and Disposal

Personal data is retained for the periods prescribed by applicable legislation and for as long as necessary for the purposes for which it is processed. When all processing conditions cease to exist, personal data is deleted, destroyed or anonymized in accordance with the IC Intechron Personal Data Retention and Disposal Policy and applicable legislation.

11. Data Security

- Access to personal data is restricted on the basis of duties, authorization and need-to-know.
- Appropriate technical and administrative security measures are implemented in environments where personal data is stored and transferred.
- Confidentiality, data security and data processing obligations are contractually regulated in relationships with service providers.
- Unnecessary data collection and duplication of personal data beyond operational need are prevented.
- Access authorizations are reviewed and necessary access rights are revoked upon a change of duty or termination of the business relationship.
- Additional security measures prescribed by applicable legislation are implemented for special categories of personal data.

12. Information and Explicit Consent

When obtaining personal data, IC Intechron informs the data subject about the identity of the data controller, purposes of processing, transfers, method and legal ground of collection, and the rights under Article 11 of the Law. The obligation to provide information is independent of whether the data subject gives explicit consent.

Where processing requires explicit consent, the privacy notice and the explicit consent statement are presented separately. Explicit consent is not made a mandatory condition of a service or application, and the data subject may withdraw consent at any time.

13. Rights of the Data Subject and Application

Under Article 11 of the Law, as a data subject you have the following rights:

- To learn whether your personal data is being processed.
- To request information if your personal data has been processed.
- To learn the purpose of processing your personal data and whether it is used in accordance with that purpose.
- To know the third parties to whom your personal data has been transferred within Türkiye or abroad.
- To request correction of your personal data if it has been processed incompletely or inaccurately.
- To request deletion or destruction of your personal data under the conditions set out in Article 7 of the Law.

- To request notification of correction, deletion or destruction operations to third parties to whom your personal data has been transferred.
- To object to a result arising against you through analysis of processed data exclusively by automated systems.
- To claim compensation if you suffer damage due to unlawful processing of your personal data.

You may submit your requests in writing to Mutlukent Mahallesi, 2045 Sokak, No:19, Çankaya/Ankara, Türkiye; from your KEP account to icintechron@hs03.kep.tr; by using a secure electronic signature or mobile signature to info@intechron.com.tr; or from an e-mail address previously notified to IC Intechron and registered in the Company's systems to info@intechron.com.tr. The Data Subject Application Form is available on the Personal Data Protection page to facilitate complete submission of requests. Applications are concluded as soon as possible and in any event within 30 days depending on the nature of the request; where the transaction requires an additional cost, the fee set by the Turkish Personal Data Protection Board may apply.

14. Updates and Effective Date

This Policy was published on 13.08.2026. It shall be updated where there are changes in legislation, personal data processing activities or technical infrastructure. The current version is published on the IC Intechron website.