

Privacy Policy

1. Purpose of the Data Processing Notice

This Data Processing Notice (hereinafter: the “Notice”) aims to transparently and thoroughly present the data protection and processing principles applied by IRON-TECH Kereskedelmi, Szolgáltató és Gyártó Korlátolt Felelősségű Társaság (registered office: 7900 Szigetvár, Dencsházai utca 12., tax number: 28803366-2-02, company registration number: 02-09-086481, represented jointly by managing directors Norbert Konczos and Miklós Péter Staub) (hereinafter: the “Data Controller”), and to provide information on data subjects’ rights and how to exercise them.

2. Legal Compliance

This Notice is to be applied in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and the Council (hereinafter: “Regulation” or “GDPR”), the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: “Infotv.”), its complementary provisions, and relevant sector-specific legal requirements.

3. Data Controller Information

3.1. Name and Contact Information

- Name: IRON-TECH Kereskedelmi, Szolgáltató és Gyártó Korlátolt Felelősségű Társaság
- Registered office: 7900 Szigetvár, Dencsházai utca 12.
- Company registration number: Cg.02-09-086481
- Tax number: 28803366-2-02
- Representatives: Norbert Konczos and Miklós Péter Staub
- Email: info@iron-tech.hu
- Phone: +36 73 510 132

3.2. Availability of this Notice

This Notice is available electronically on the website www.iron-tech.hu and in printed form upon request at our customer service office.

4. Definitions

4.1. Key GDPR Definitions

- *Personal Data*: Any information relating to an identified or identifiable natural person (“data subject”).
- *Data Controller*: A natural or legal person that determines the purposes and means of the processing of personal data.
- *Data Processor*: A natural or legal person that processes personal data on behalf of the Data Controller.
- *Consent*: A freely given, specific, informed, and unambiguous indication of the data subject’s wishes.

- *Data Subject*: Any identified or identifiable natural person to whom personal data relates.

4.2. Definition of a Data Breach

A data breach is any event that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

5. Principles of Data Processing

5.1. Legal Bases and Principles

- *Lawfulness, Fairness, and Transparency*: Data is processed for specific and lawful purposes only.
- *Purpose Limitation*: Data is collected for specified purposes and not further processed incompatibly.
- *Data Minimization*: Only the necessary personal data is collected and processed.
- *Accuracy*: Data must be accurate and kept up to date.
- *Storage Limitation*: Data is retained only for as long as necessary.
- *Integrity and Confidentiality*: Appropriate security measures protect personal data.

5.2. Data Accuracy and Security

- Both the Data Controller and the data subject are responsible for keeping data up to date.
- The Data Controller ensures data accuracy and applies security measures to prevent unauthorized access.

6. Purpose, Legal Basis, and Duration of Processing

Purpose	Data Processed	Legal Basis	Retention Period
Request for quote, business inquiry	Name, company name, contact info, message	Legitimate interest (GDPR Article 6(1)(f))	1 year after closure of contact
Contract execution, production, delivery	Name, company name, contact person, billing info	Contract performance (GDPR Article 6(1)(b))	5 years after contract termination
Invoicing, accounting	Name, company name, address, tax number	Legal obligation (GDPR Article 6(1)(c))	8 years (Accounting Act requirement)
Employee data processing	Personal data, social security number, bank info	Legal obligation / employment contract (Art. 6(1)(c))	5–8 years after employment ends
Surveillance (if any)	Facial image, footage	Legitimate interest (property protection) (Art. 6(1)(f))	Max. 3 days, except in case of legal dispute

Purpose of Data Processing

The Data Controller processes data to comply with applicable national and international laws and to support its business activities.

The Data Controller processes data under GDPR Article 6(1)(a), (b), (c), and (f), adhering to the principles set out in Article 5(1), such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and confidentiality.

6.1. Source of Data

Data is obtained:

- Directly from the data subject (e.g. quote requests, orders, CVs)
- From business partners (during assignments)
- From public databases (e.g. company information)

Only necessary personal data is processed with proper notification to the data subject. Adequate information security measures are applied to ensure confidentiality, integrity, and availability of the data.

Questions can be directed to info@iron-tech.hu. The Data Controller will respond within 15 days.

7. Data Transfers and Data Processors

7.1. Data Access and Transfers

Only authorized staff have access to personal data. Data may be shared with:

- Accounting / payroll service providers – for administrative purposes
- Hosting / IT providers – for email and data storage
- Delivery partners – for logistics
- Authorities – where required by law

Written contracts are in place with all data processors in compliance with GDPR. These contracts specify that partners act only on the Data Controller's instructions, for defined purposes and duration.

Hosting Provider Details:

- Name: KETSH Korlátolt Felelősségű Társaság
- Address: 7622 Pécs, Nagy Lajos király útja 14. fszt. 3.
- Role: Operating the web server, technical maintenance; data is processed only per instructions.

7.2. Data Security Measures

Electronic Protection:

- Multi-level access control
- Regular backups
- Antivirus and firewall use

Technical/Organizational Measures:

- Secured office network and Wi-Fi
- Paper documents stored in locked cabinets

- Regular data protection training for employees and processors

8. Data Subject Rights

8.1. Rights of the Data Subject

The data subject has the right to:

- Access personal data
- Request rectification, deletion, or restriction
- Object to processing (e.g. in case of video surveillance)
- Request data portability (for contract- or consent-based processing)
- File a complaint with the Hungarian Data Protection Authority (NAIH)

Supervisory Authority:

- Name: Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
- Address: 1055 Budapest, Falk Miksa utca 9-11.
- Mailing address: 1363 Budapest, Pf. 9.
- Phone: +36-1-391-1400
- Fax: +36-1-391-1410
- Email: ugyfelszolgalat@naih.hu
- Website: <http://www.naih.hu>

8.2. Legal Remedies

Data subjects may contact the Data Controller via any contact method listed on the website. The Controller must respond to rights requests without undue delay and no later than one month from receipt.

If objections are raised, the Controller must assess them within 15 days and inform the subject in writing. If justified, data processing must stop, data locked, and all prior data recipients informed.

If the data subject disagrees with the decision, they may go to court within 30 days. Legal proceedings are handled urgently, and the burden of proof lies with the Controller.

9. Cookie Management

Our website uses cookies for improved user experience, traffic analysis, and marketing. Visitors can modify cookie settings and withdraw consent at any time.

9.1. Legal Basis for Cookies:

- *Consent* (GDPR Article 6(1)(a)) – for non-essential cookies
- *Legitimate Interest or Contract Performance* (Article 6(1)(f) or (b)) – for essential technical cookies

9.2. Purpose and Types of Cookies

- **Session cookies:** Essential for the proper functioning of the website. These are deleted when the browser is closed.
- **Functional cookies:** Enhance user convenience by remembering login credentials or selected language preferences.
- **Analytical cookies (e.g., Google Analytics):** Used for statistical purposes to help understand user behavior and improve website performance.
- **Marketing cookies:** Enable the display of relevant advertisements and support the measurement of advertising effectiveness.

9.3. Managing User Preferences

- Users can manage cookies through their browser settings, including disabling or deleting them.
- Changing cookie settings may affect the functionality of certain features on the website.
- Upon the user's first visit to the website, a pop-up window allows them to accept or reject non-essential cookies (e.g., marketing cookies).

10. Data Protection Officer

The Data Controller is **not required** to appoint a Data Protection Officer pursuant to Article 37 of the GDPR.

11. Final Provisions

The Data Controller reserves the right to unilaterally amend this Privacy Notice, particularly in response to changes in legislation, the introduction of new data processing activities, or recommendations issued by supervisory authorities.

Any amendments will be published on the website. By continuing to use the services after the changes take effect, users are deemed to have accepted the updated terms.