GDPR PRIVACY & COOKIE POLICY

Eyso Global İç ve Dış Ticaret Sanayi Limited Şirketi

Effective date: 23 November 2023 | Website: www.eysoglobal.com

This policy explains how Eyso Global collects and uses personal data relating to visitors, business contacts, distributor candidates and other individuals in the European Economic Area (EEA). It is intended to provide the information required by Articles 12-14 of Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR").

1. Who we are

Eyso Global İç ve Dış Ticaret Sanayi Limited Şirketi ("Eyso Global", "we", "us" or "our") is the controller of the personal data described in this policy, unless we expressly state otherwise.

Company information	Details
Registered name	Eyso Global İç ve Dış Ticaret Sanayi Limited Şirketi
Address	Adalet Mahallesi, Manas Bulvarı, Folkart Towers No: 47B, Office 2601, Bayraklı, İzmir, Türkiye
MERSIS number	0383095226400001
Trade Registry number	251247
Email	export@eysoglobal.com
Registered electronic mail (KEP)	eysoglobal@hs01.kep.tr
Website	www.eysoglobal.com

EU representative: Not applicable, based on the nature and scope of our current processing activities.

2. Scope and application of the GDPR

This policy applies to personal data processed through our website and through related business communications. The GDPR applies to our processing to the extent that we offer goods or services to individuals in the EEA or monitor their behaviour in the EEA. Other applicable privacy laws, including Türkiye's Law No. 6698 on the Protection of Personal Data (KVKK), may apply in parallel.

Our website does not currently provide user accounts, online ordering or payment processing. If those functions are introduced, this policy and the related notices will be updated before the new processing begins.

3. Personal data, purposes, legal bases and retention

We collect only the data reasonably necessary for the purposes below. Where legitimate interests are relied upon, we balance our interests against the individual's rights and reasonable expectations.

Data / source	Purpose and GDPR legal basis	Retention approach
Business identity and contact data: name, title, employer, email, phone and correspondence; collected from you or your organisation.	Answer enquiries; evaluate distributor, quotation and cooperation requests; negotiate or perform a contract. Article 6(1)(b) (pre-contract/contract) and Article 6(1)(f) (legitimate interests in B2B communications and relationship management).	For the active relationship, then normally up to 3 years after the last substantive contact; longer where needed for legal claims or mandatory records.
Enquiry, complaint and rights-request data: message content, attachments, request history, identity-verification data and our response.	Handle requests and complaints; comply with privacy obligations; establish, exercise or defend legal claims. Article 6(1)(c) and 6(1)(f).	Rights requests: normally 3 years after closure. Other correspondence: according to the purpose and applicable limitation periods.
Technical and security data: IP address, device/browser data, timestamps, URLs, server logs and security events; collected automatically.	Operate, secure and troubleshoot the website; prevent misuse; maintain evidence of security events. Article 6(1)(f); Article 6(1)(c) where a legal duty applies.	Security/server logs are normally retained for up to 12 months, unless an incident, claim or legal requirement justifies longer retention.
Cookie and analytics data: cookie identifiers, consent status, approximate location, pages viewed, interactions, referral source and session data; collected via the website.	Store or access strictly necessary information; measure performance and improve the website; deliver targeted content only if enabled. Article 6(1)(f) for strictly necessary processing and Article 6(1)(a) consent for non-essential analytics, functionality and marketing technologies.	For the duration shown in the live cookie settings or cookie list; consent records may be retained for up to 5 years to demonstrate compliance.
Legal and compliance records: transaction or corporate records where communications lead to business activity.	Comply with accounting, tax, commercial and regulatory duties and protect legal rights. Article 6(1)(c) and 6(1)(f).	For the period required by applicable law, commonly 5-10 years depending on the record and jurisdiction.

If we need personal data to enter into or perform a contract or to comply with law, we will identify the required fields. If required data is not provided, we may be unable to respond fully, enter into the arrangement or provide the relevant service.

4. Special-category data

The website is not designed to collect special categories of personal data under Article 9 GDPR (for example health, biometric, political, religious or trade-union information) or criminal-conviction data. Please do not send such information unless it is necessary. If you provide it, we will process it only where a valid Article 9 condition and any applicable national-law condition are satisfied, or delete it where it is not needed.

5. How we collect personal data

- Directly from you when you email us, submit a contact or quotation form, or communicate with our personnel.
- From your employer, colleague, business partner or a publicly available professional source when relevant to a genuine B2B relationship.
- Automatically from your device through server logs, cookies and similar technologies when you use the website.
- From service providers that support website hosting, security, email delivery, analytics or consent management.

If we obtain your data from another source, we will provide any additional Article 14 GDPR information within the applicable period unless an exemption lawfully applies.

6. Who receives personal data

We may disclose personal data on a need-to-know basis to:

- website hosting, IT, cybersecurity, email, cloud storage, analytics and consent-management providers acting as processors or independent controllers, as applicable;
- professional advisers, including lawyers, accountants, auditors and insurers;
- logistics providers, manufacturers, distributors and other commercial partners where needed to answer or perform your request;
- public authorities, courts, regulators or law-enforcement bodies where disclosure is required or permitted by law; and
- a buyer, investor or successor in connection with a proposed or completed corporate transaction, subject to appropriate confidentiality and data-protection measures.

We do not sell personal data. We require processors to act only on documented instructions, protect the data and assist us with GDPR compliance.

7. International transfers

Eyso Global is based in Türkiye, so personal data sent to us from the EEA is processed outside the EEA. Our service providers may also process data in Türkiye, the United States or other countries. Where a recipient is outside the EEA and the European Commission has not adopted an adequacy decision for the destination, we use an appropriate safeguard where required, such as the European Commission's Standard Contractual Clauses under Article 46 GDPR, together with supplementary measures where appropriate. A copy or summary of relevant safeguards may be requested using the contact details in section 1, subject to lawful redactions.

8. Cookies and similar technologies

Cookies are small text files stored on a device. Similar technologies may include pixels, local storage and tags. Strictly necessary technologies may operate without consent where permitted by applicable law. All non-essential technologies are disabled until the visitor gives freely given, specific, informed and unambiguous consent through the cookie banner. Rejecting non-essential cookies must be as easy as accepting them, and consent can be withdrawn at any time without affecting prior lawful processing.

Category	Typical purpose	Default status
Strictly necessary	Security, network management, consent preference storage and functions expressly requested by the visitor.	Always active where legally permitted.
Functional	Remember optional preferences such as language or enhanced features.	Off until consent.
Analytics / performance	Measure visits, interactions and website performance, including tools such as Google Analytics if actually enabled.	Off until consent.
Advertising / targeting	Measure campaigns or personalise advertising across services, if such tools are enabled.	Off until consent.

The authoritative, current cookie list—including each cookie or technology's name, provider, purpose, category and lifespan—is available through the "Cookie Preferences" link or panel on the website. That list forms part of this policy and must reflect the technologies actually deployed. You may change or withdraw consent there at any time. Browser settings can also block or delete cookies, but blocking strictly necessary cookies may affect site operation.

9. Your GDPR rights

Subject to the conditions and exceptions in the GDPR, you may:

- request access to your personal data and a copy of it;
- request correction of inaccurate or incomplete data;
- request erasure of personal data;
- request restriction of processing;
- receive data you provided in a structured, commonly used, machine-readable format and transmit it to another controller where Article 20 applies;
- object at any time to direct marketing and object, on grounds relating to your situation, to processing based on legitimate interests;
- withdraw consent at any time, without affecting processing already carried out lawfully; and
- lodge a complaint with the data-protection authority in the EEA country where you live or work, or where you believe an infringement occurred.

We do not currently make decisions based solely on automated processing that produce legal or similarly significant effects. If that changes, we will provide the information and safeguards required by Article 22 GDPR.

10. How to exercise your rights

Send a clear description of your request to export@eysoglobal.com or to our postal address in section 1. We may ask for information reasonably necessary to verify identity and protect personal data. We will respond without undue delay and normally within one month. Where permitted by Article 12 GDPR, that period may be extended by two further months for a complex or numerous request; we will explain any extension within the first month. Requests are normally free of charge, although a reasonable fee or refusal may apply to manifestly unfounded or excessive requests.

11. Security and personal data breaches

We use proportionate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures may include access controls, encryption in transit, system hardening, backups, vendor controls, confidentiality obligations and incident response. No internet transmission or storage method is completely secure. If a personal data breach occurs, we will assess it and notify the competent supervisory authority and affected individuals where Articles 33 and 34 GDPR require this.

12. Children

Our website and B2B services are not directed to children, and we do not knowingly collect children's data through the website. If we learn that a child's personal data has been submitted without a valid legal basis or required parental authorisation, we will delete it or take other appropriate action.

13. Third-party websites

The website may contain links to third-party websites or social-media services. Those parties determine their own processing, and their privacy notices apply after you leave our website. We encourage you to review them.

14. Changes to this policy

We may update this policy to reflect changes in law, technology or our processing. The current version will be posted on the website with a revised effective date. If a change materially affects processing based on consent, we will request new consent where required.

15. Contact and complaints

Questions, objections or requests may be sent to export@eysoglobal.com. You also have the right to contact the competent EEA supervisory authority. A list of EEA supervisory authorities is available from the European Data Protection Board website.