1) PRIVACY POLICY (DATA PROTECTION NOTICE)
Effective: from 2 January 2026
Version: 1.0

1. **Data Controller**
   The data controller: ECGO Group Limited Liability Company (ECGO Group Kft.)
   Registered office: 1144 Budapest, Kerepesi út 140–142., 9th floor, Door 119
   Company registration number: 01 09 451423
   Tax number: 32957420-2-42
   E-mail: ecgogroup@ecgogroup.hu
   Web: www.e-cargoo.com
   Data protection contact e-mail address:
   Contact: ecgogroup@ecgogroup.hu
2. **Purpose and scope of this notice**
   This notice describes how ECGO Group Kft. processes personal data in connection with the use of the e-cargoo.com freight exchange / freight management platform (hereinafter: Platform) and the related websites/applications.

   Who does it affect?

   • registered users (carriers, clients, freight forwarders, logistics service providers),
   • contacts and representatives (B2B),
   • visitors (website),
   • customer service inquiries.

3. **Definitions (brief)**

   • Personal data: any information relating to an identified or identifiable natural person.
   • Data controller: the entity that determines the purposes and means of processing (ECGO Group Kft.).
   • Data processor: a party processing data on behalf of the controller (e.g. hosting, e-mail service provider).
   • GDPR: Regulation (EU) 2016/679.

4. **Categories of processed data**
   Depending on the operation of the Platform, we may process the following data:

4.1. Account and identification data

• name, contact person’s name
• e-mail address, phone number
• username, password (only in hashed form)
• account status, permission level, role (client/carrier/freight forwarder/admin)
• language, country, time zone

4.2. Company and business data (B2B)

• company name, registered office, site, country
• tax number / EU VAT / company registration number
• billing details, subscription type, pricing plan
• position of contact persons, employer details
• documents related to the company (e.g. licenses, references)

4.3. Freight and listing content

• freight offer / cargo data (loading and unloading region, time window, vehicle type, weight/volume, ADR marking, notes)
• requests for quotation, responses, prices
• internal messages, chat, attachments
• ratings, feedback, complaints
• contact person’s name, phone number

4.4. Payment and billing data

• pricing plan, transaction identifiers, invoice number
• payment status, payment method

4.5. Customer service data

• content of inquiries, ticket IDs
• call center recordings
• bug tickets, screenshots, log excerpts

4.6. Technical and log data

• IP address, device identifiers, browser and operating system data
• access logs (login, time, failed attempts)

• cookie identifiers, session ID
• security events, fraud prevention alerts

4.7. Marketing and preferences (upon subscription)

• newsletter subscription fact, time, IP (in case of double opt-in)
• marketing preferences, unsubscription time
• campaign measurement (UTM, conversions – with cookie consent)

4.8. Special categories of data

In the normal use of the Platform, we do not request or process special categories of data (e.g. health data, biometrics). Please do not share such data with us!

5. **Purposes and legal bases of processing**
   The purposes and legal bases of processing are defined by purpose.

5.1. Registration, account creation, login

• Purpose: account creation, identification, providing access
• Legal basis: GDPR Article 6(1)(b) performance of a contract / steps prior to entering into a contract

5.2. Service provision (freight offers, search, matching, messaging)

• Purpose: core functions of the Platform, supporting business connections
• Legal basis: GDPR Article 6(1)(b) contract

5.3. Subscription, billing, financial administration

• Purpose: handling payments, issuing invoices, accounting
• Legal basis: GDPR Article 6(1)(c) legal obligation (accounting/tax) and 6(1)(b) contract

5.4. Customer service, complaint handling, communication

• Purpose: answering questions, fixing errors, handling complaints
• Legal basis: Article 6(1)(b) contract and/or 6(1)(f) legitimate interest

5.5. Security, abuse prevention, fraud and risk management

• Purpose: preventing unauthorized access, fraud/scams, account abuse, spam filtering
• Legal basis: Article 6(1)(f) legitimate interest (security of the Platform and users)

5.6. Quality assurance, statistics, development

• Purpose: service development, error detection, performance measurement
• Legal basis: Article 6(1)(f) legitimate interest (service improvement)
• Note: where possible, we use aggregated/pseudonymised data.

5.7. Enforcement and defense of legal claims

• Purpose: debt collection, legal disputes, evidence
• Legal basis: Article 6(1)(f) legitimate interest or Article 6(1)(c) legal obligation

5.8. Marketing (newsletters, direct offers)

• Purpose: sending newsletters, promotions, product updates
• Legal basis:
  o Article 6(1)(a) consent (classic newsletters), and/or
  o Article 6(1)(f) legitimate interest
• Unsubscribe: one click in every message.

5.9. Cookies and online identifiers

• Necessary cookies: Article 6(1)(f) legitimate interest / ePrivacy exemption
• Statistics/marketing cookies: Article 6(1)(a) consent (separate cookie banner)

6. Source of data

• directly from the user (registration, use, messages),
• from the user's organization (data provided by corporate admin),
• from technical sources (logs, cookies),
• from third parties (e.g. payment provider transaction status, authentication service provider, fraud prevention alerts).

7. Data transfers, recipients, processors

We only transfer personal data if necessary for the service, required by law, or requested by the user.

7.1. Sharing with other users
When using the Platform, certain data become visible to other users for the performance of the contract, for example:

- company name, country, profile data,
- contact name/phone number/e-mail (if provided and set by the user),
- freight offer content,
- messages to recipient(s),
- ratings

Settings: where possible, we provide data visibility settings (e.g. hiding phone number; sharing only in messages).
Users contacting each other on the Platform act as independent data controllers towards each other in the business relationship established between them.

7.2. Typical categories of data processors

- hosting provider / cloud infrastructure
- e-mail sending service (transactional e-mails)
- SMS service provider (2FA/notifications)
- customer support ticketing system
- analytics service provider (with consent, if required)
- payment service provider
- accountant, invoicing system
- IT operations, development partner
- security monitoring / log analysis

Data processing agreement: we conclude GDPR Article 28-compliant agreements with all processors.

7.3. Authorities and legal recipients

- upon request of courts, police, supervisory authorities,
- auditors, legal representatives (legitimate interest / legal claims).

8. **International data transfers**
   In the operation of the Platform, some of our processors and service providers may process personal data outside the European Economic Area (EEA) – in particular in the United States of America.
   Personal data are transferred outside the EEA only if one of the following conditions is met:

a) based on an adequacy decision, if the European Commission has determined that the third country ensures an adequate level of protection; or
b) by applying the Standard Contractual Clauses (SCC) adopted by the European Commission; or
c) on the basis of other appropriate safeguards set out in Articles 46–49 of the GDPR.
In connection with data transfers – in line with relevant case law – we apply supplementary technical and organizational measures where necessary, in particular:

- encryption and pseudonymisation,
- access restrictions,
- Transfer Impact Assessments,
- contractual commitments of recipients.

Typical cases where data transfers outside the EEA may occur:

- cloud infrastructure and hosting services,
- e-mail and notification systems,
- customer support and ticketing solutions,
- analytics and security monitoring tools,
- payment service providers.

Upon request, we provide information about the specific legal basis of a given transfer and the related safeguards at ecgogroup@ecgogroup.hu.

9. **Data retention periods (retention)**
We store personal data only for as long as necessary. Typical periods:

- Account data: for the duration of the account + 12 months (security/log purposes)
- Contractual and billing data: for the period required by applicable laws (typically 8 years for accounting records)
- Logs (security): 6 months, longer in case of incidents
- Messages / chat: for the duration of the account or until deletion at the request of the parties, but up to 120 days in backups
- Marketing consent: until withdrawal, thereafter on a suppression list (only the fact of unsubscription) – 1 year for evidentiary purposes
- Cookies: according to the cookie table (see Cookie section)

10. **Data security**

We apply appropriate technical and organizational measures, such as:

• TLS encryption, password hashing (modern algorithms), access control
• logging and monitoring
• backups and recovery
• incident management procedure
• privilege management (least privilege)

Large platforms also describe security measures and incident management in detail.

11. **Automated decision-making and profiling**

As a rule, we do not make decisions based solely on automated processing that would produce legal effects concerning the user.
However, the following may occur:

• automatic restrictions due to suspected spam/fraud (e.g. too many failed logins, mass messaging),
• risk scoring (fraud scoring) to protect the Platform.

In such cases, we ensure the possibility of human review, and the data subject may object.

12. **Data subject rights**

The user (data subject) has the right to:

• access (request a copy),
• rectification,
• erasure (“right to be forgotten”), if there is no other legal basis,
• restriction of processing,
• data portability (subject to contractual/legal conditions),
• object (to processing based on legitimate interest),
• withdraw consent (at any time; processing before withdrawal remains lawful).
Submission of requests: ecgogroup@ecgogroup.hu
Deadline: 30 days.

Recommended final text – HUNGARIAN (13. Right to lodge a complaint, supervisory authority)

13. Right to lodge a complaint, supervisory authority and judicial remedy

13.1. Lodging a complaint in Hungary (NAIH)

If you believe that the processing of your personal data violates applicable data protection laws, you may lodge a complaint with the Hungarian supervisory authority:

• National Authority for Data Protection and Freedom of Information (NAIH)
https://www.naih.hu/
Registered office: 1055 Budapest, Falk Miksa utca 9–11.
Postal address: 1363 Budapest, Pf. 9.

13.2. Lodging a complaint in the EU/EEA (foreign users, contacts of EU companies)

• As the data controller is established in Hungary, data subjects may primarily lodge a complaint with the Hungarian supervisory authority:
National Authority for Data Protection and Freedom of Information (NAIH)
Registered office: 1055 Budapest, Falk Miksa utca 9–11.
Postal address: 1363 Budapest, Pf. 9.
Website: https://www.naih.hu/

• A data subject residing in the EU/EEA is entitled to lodge a complaint with the supervisory authority of his/her habitual residence, place of work, or the place of the alleged infringement.
List of national data protection authorities (EDPB – "supervisory authorities" list):
https://www.edpb.europa.eu/about-edpb/contact-us_en

13.3. Data subjects from third countries

a) with the Hungarian supervisory authority (NAIH), as the data controller is established in Hungary and the processing is linked to the Hungarian organization. If the data subject lives outside the EU/EEA, they may still lodge a complaint with:
National Authority for Data Protection and Freedom of Information (NAIH)
Registered office: 1055 Budapest, Falk Miksa utca 9–11.
Postal address: 1363 Budapest, Pf. 9.
Website: https://www.naih.hu/
b) with the data protection authority available in their own country (if such an authority exists and has jurisdiction).

13.4. Judicial remedy

The data subject is also entitled to seek judicial remedy, in particular if they believe that their rights have been infringed. The possibility of judicial remedy exists independently of lodging a complaint with a supervisory authority.

14. Cookies and similar technologies

The Platform and related websites use cookies and similar technologies to ensure the operation of the service, improve user experience, perform statistical measurements and – with consent – for marketing purposes.
Detailed rules on the use of cookies, the types of cookies, their purposes, expiry

periods and the method of managing consent are set out in the separate Cookie Policy.
The Cookie Policy is available here:
Cookie Policy

15. **Communication, notifications**

• Transactional messages (account, security, system messages): part of the service and cannot be fully disabled.
• Marketing messages: only with consent, can be unsubscribed at any time.

16. **Minors**

The Platform is for business purposes; it is not intended for persons under 16 years of age. If we become aware of such registration, we will delete it.

17. **Changes**

We may update this notice from time to time. We will notify you of material changes on the Platform or by e-mail.