

PRIVACY POLICY

CtrlChain B.V., having its registered office at Schimmelt 22, 5611 ZX Eindhoven, The Netherlands, and registered with the Dutch Chamber of Commerce under number 72617217 (“CtrlChain”, “we”, “us”, “our”), is committed to protecting the privacy and personal data of individuals in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation – “GDPR”), as well as other applicable data protection and privacy laws, including the Dutch Telecommunications Act (“Telecommunicatiewet”).

This Privacy Policy describes how CtrlChain processes personal data of natural persons (“Data Subjects”, “you”) when you interact with the CtrlChain System, our website (www.ctrlchain.com), our Mobile Application (the CtrlChain System, the website and the Mobile Application hereinafter collectively referred to as the “CtrlChain Environment”), and when we provide you with our services (“Services”).

Data Controller & Data Subjects

CtrlChain acts as the data controller within the meaning of Article 4(7) GDPR for the processing of your personal data. For inquiries, you may contact us at: dpo@ctrlchain.com or via the postal address: Schimmelt 22, 5611ZX, Eindhoven, Netherlands.

CtrlChain implements strict measures to protect data related to individual users (natural persons) of the CtrlChain Environment. If your personal data is processed, you are considered a data subject within the meaning of the GDPR.

Legal Basis and Purposes of Processing

CtrlChain processes personal data lawfully based on one or multiple of the following legal grounds:

- Performance of a contract/ agreement with you or to take measures before the conclusion of an agreement (Art. 6(1)(b) GDPR)
- Our compliance with legal obligations (Art. 6(1)(c) GDPR)
- Legitimate interests pursued by CtrlChain (Art. 6(1)(f) GDPR), ensuring these interests are not overridden by your fundamental rights and freedoms
- Your consent (Art. 6(1)(a) GDPR), where applicable

We process your personal data for one or more of the following purposes (depending on our relationship with you):

- Executing an agreement: We process your personal data as necessary within the context of the Services provided by us, including the exchange of personal data for quotations, the execution and completion (including invoicing) of an order, service request or assignment.
- Compliance with legal obligations: We process your personal data as necessary to comply with legal obligations. For example, the collection and storage of data and the provision of information to the tax authorities and supervisory authorities.
- Marketing purposes: We use your personal data to send out newsletters, invitations to our events and other marketing communications that may be relevant to you, as well as in the context of (registration for) one of our marketing events. When you have attended one of our events, we may also contact you for feedback.
- Job applications and recruitment: The data you share with us if you apply for a job with us (via email/mail, the job application form on our website or via social media) or that we receive via recruiters, is processed by us to contact you for the purposes of our job application procedures and

to deal with your job application. We may also process your personal data in the context of (a registration for) an internship at one of our branches.

- Access control and security: For safety purposes (evacuation in case of calamities) we keep a list of visitors to our business premise(s). These lists are destroyed at the end of the day in question.
- Use and improvement of our website: We process statistical data about your visit and use of our website. We do this to analyze and improve the content, layout, and use of our website.
- Other processing: We may also process your data to carry out customer satisfaction surveys, or to handle any questions or complaints.

Source of Data

We collect personal data directly from you when you use our System, and Mobile Application.

Necessity of Data Provision

Provision of certain personal data is necessary to enter into or perform a contract with CtrlChain. Failure to provide such data may result in the inability to provide the requested Services.

Categories of Personal Data Processed

Identity & Contact Data: First and last name, title, gender, company name (employer), registered address / postal address, email address, phone number, Chamber of Commerce number (if applicable), VAT number (if applicable).

Financial Data: Name of account holder, IBAN / Bank account number, BIC number, invoices and purchase records, payment transactions (both outgoing and incoming).

Operational & Technical Data: Location data of affiliated carriers, IP address, statistical data regarding usage of our websites (such as browsing behavior, interaction patterns).

Communication & Correspondence Data: Messages and correspondence via live chat, contact forms submitted through our website, email communication records.

Job Application Data: Application letters, Curriculum Vitae (CV), date of birth, education and career information, any other personal data provided during the job application process.

Other Personal Data: Any additional personal data provided by you or obtained from you in the context of our Services or interactions, which are used strictly for the purposes mentioned above.

We do not always process all the above data, this depends on the type of relationship, the service in question and (if applicable) the consent you have given us.

Automated Decision-Making

CtrlChain utilizes automated decision-making processes for selecting carriers based on location and operational parameters. In accordance with Article 22 GDPR, you have the right to request human intervention if such decisions significantly affect you.

Data Retention

Personal data is retained for no longer than is necessary for the purposes for which it is processed, or as required by applicable laws (e.g., financial records retained for seven (7) years in accordance with tax regulations). Data is securely deleted when no longer necessary.

CtrlChain may retain certain personal data in a blacklist or internal register where necessary for the prevention, investigation, or prosecution of fraud, non-payment, abuse of our Services, or other wrongful acts. Such processing is carried out on the basis of CtrlChain's legitimate interests in safeguarding its business operations, as permitted under Article 6(1)(f) GDPR. Data subjects shall have the right to object to such processing, in accordance with Article 21 GDPR.

The storage of personal data in such registers shall be limited to what is strictly necessary, and data shall not be retained longer than required for the purposes for which it is processed.

Sharing of Personal Data

CtrlChain engages trusted third-party processors for the processing of personal data strictly in accordance with the GDPR. These processors are contractually bound by Data Processing Agreements (DPAs), which ensure they:

- Process personal data solely on CtrlChain's documented instructions;
- Implement appropriate technical and organizational measures to ensure data security;
- Refrain from processing personal data for their own purposes;
- Comply with GDPR and all other applicable data protection laws.

CtrlChain's cooperation with such third-party service providers is essential for the performance, operation, and continuous improvement of the CtrlChain Environment, and its Services. All processing activities performed by these third parties are governed by enforceable contractual obligations, ensuring compliance with the GDPR and related legal requirements.

CtrlChain collaborates with the following third-party processors:

Qubiz, Enjins, Pionative, CO3, PTV, DeliveryMatch, U-turn, Hubspot, Snowflake, Google, Microsoft Azure, Exact online, Zenvoices, Netsuite, Fivetran, DBT, Airbyte, GitHub, DltHub, PowerBI, Deeploy.

The categories of third-party processors we engage include, but are not limited to:

- Logistics Planning Providers assisting with transport planning, live track & trace, and carrier matching.
- Business Software Providers supporting financial administration, invoicing, and enterprise resource planning (ERP).
- Customer Relationship Management (CRM) Platforms managing client interactions and communication workflows.
- Cloud Infrastructure and Hosting Providers ensuring secure storage and hosting of our data and digital infrastructure.
- Analytics and Performance Monitoring Tools enabling optimization of the CtrlChain Environment, and Services.

Personal data will also be shared if required by law or pursuant to a legal obligation.

Health & Activity Data

The CtrlChain mobile application may access physical activity data (such as movement detection and activity recognition) on your device. This data is used solely for detecting driver activity status during active transport assignments. It is not shared with third parties for marketing or advertising purposes, and is not used for any purpose beyond those described in this policy. You may revoke this permission at any time via your device settings.

Data Protection Impact Assessments (DPIAs)

CtrlChain conducts Data Protection Impact Assessments (DPIAs) where processing operations are likely to result in a high risk to the rights and freedoms of individuals, in accordance with Article 35 GDPR.

International Data Transfers

All information you provide to us via our websites will be stored on servers in the European Economic Area (EEA). If necessary, we may share information with our affiliated companies in and outside the EEA.

If we share and or store personal information outside the EEA, appropriate safeguards will be put in place. We shall never transfer your personal data to other countries or to other parties than those mentioned above.

Data Security

CtrlChain has implemented appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or alteration, including:

- Encryption of digital files
- Secure network connections using SSL/TLS protocols
- Role-based access controls
- Multi-factor authentication for access to systems containing personal data

Personal Data Breaches

In the event of a personal data breach, CtrlChain shall assess the nature and scope of the incident in accordance with Article 33 and 34 of the GDPR. Where required, we will:

- Notify the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals;
- Notify affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms;
- Maintain an internal breach register to document the facts relating to the breach, its effects, and remedial action taken.

Notification to data subjects will include at least:

- A description of the nature of the breach;
- The name and contact details of our Data Protection Officer;
- Likely consequences of the breach;
- Measures taken or proposed to address and mitigate its adverse effects.

Children

We do not knowingly collect personally identifiable information from children. If you become aware that a child has provided us with personal data, please contact us.

Links

CtrlChain's Environment may contain hyperlinks or references to external websites operated by third parties. Such websites are not controlled by CtrlChain, and we accept no responsibility or liability for the content, data processing activities, or privacy practices of these third parties. We strongly advise data subjects to carefully review the privacy policies and terms of use applicable to such external websites prior to disclosing any personal data.

Cookies

CtrlChain uses cookies and similar technologies on its website to enhance user experience, secure the System, and analyze website performance. You can manage or disable cookies via your browser settings. For more information, refer to our Cookie Statement at: www.ctrlchain.com/cookiestatement.

Amendments

CtrlChain reserves the right to amend this Privacy Policy. Changes will be published on our website and System. It is therefore advisable to consult our website regularly to keep up to date with any changes.

Data Subject Rights

As a Data Subject, you have the right to request us to access, rectify, erase, restrict, and/or transfer your personal data. You also have the right to object to the processing of your personal data.

As far as the processing of your personal data is based on consent, you have the right to revoke this consent at any time. Any withdrawal of your consent does not affect the lawfulness of processing based on consent before its withdrawal.

These rights are subject to certain legal limitations, such as statutory retention requirements, the rights of third parties, or the legitimate interests of CtrlChain, and may not always be granted.

A request may be denied in part or in full following these restrictions, such as legal obligations, the rights of third parties and the legitimate interests of CtrlChain. If we are unable to grant a particular request, we will inform you of this, with a statement of reasons.

You may exercise these rights by submitting a request to dpo@ctrlchain.com. We will respond within one month in accordance with GDPR Article 12(3). For a full explanation of your rights and the procedures for exercising them, please refer to Annex I - Data Subject Rights Procedures at the end of this Privacy Policy.

Complaints

If you believe that CtrlChain processes your personal data in violation of applicable data protection laws, you have the right to lodge a complaint with a supervisory data protection authority. A list of all EU supervisory authorities is available on the European Data Protection Board website: https://edpb.europa.eu/about-edpb/board/members_en. In the Netherlands this is the Autoriteit Persoonsgegevens (the Dutch Data Protection Authority) via www.autoriteitpersoonsgegevens.nl.

Contact

For questions, comments, or to exercise your data protection rights, you may contact:

CtrlChain

Schimmelt 22, 5611 ZX Eindhoven

T: +31 (0) 85 00 13 700

E: dpo@ctrlchain.com

Annex I – Data Subject Rights Procedures

Introduction

CtrlChain is committed to protecting and respecting the privacy and personal data of our users. This Annex outlines the rights of data subjects and the procedures we have in place to support these rights, in accordance with the Regulation (EU) 2016/679 of the European Parliament (GDPR).

Your Rights- FAQ

Q1. How can I access my personal data?

You may request a copy of the personal data we hold about you, as well as information on how we use and share it. Requests can be submitted to dpo@ctrlchain.com, including your full name, contact information, and details of the data you wish to access. We will respond within one month (extendable by up to two additional months for complex requests).

Q2. What if my personal data is incorrect or incomplete?

You can request correction or completion of inaccurate or incomplete data. We will confirm the update or explain if we cannot comply.

Q3. Can I ask you to delete my data?

Yes. You may request erasure of your data when it is no longer necessary for the purposes for which it was collected, when consent is withdrawn, or when processing is unlawful. Legal retention obligations may prevent immediate deletion.

Q4. Can I restrict how you use my data?

Yes. You may request that we limit the processing of your data under certain circumstances, such as when accuracy is contested or you object to processing.

Q5. Can I take my data to another company?

Yes. You have the right to receive your data in a structured, commonly used, and machine-readable format and to transmit it to another controller, where technically feasible. This right applies when the processing is based on consent or a contract and is carried out by automated means.

Q6. Can I object to how you process my data?

Yes. You may object to the processing of your personal data on grounds relating to your particular situation, including profiling and direct marketing. We will stop processing unless we demonstrate compelling legitimate grounds.

Q7. What if I gave consent but changed my mind?

You may withdraw consent for the collection and processing of your personal data at any time. This does not affect the lawfulness of processing carried out before withdrawal.

Q8. What if I'm unhappy with how you handle my data?

You also have the right to lodge a complaint with a data protection supervisory authority regarding the processing of your personal data. You can contact the Dutch Data Protection Authority via the following link: <https://www.autoriteitpersoonsgegevens.nl/en> or the Spanish Agencia Española de Protección de Datos (AEPD) <https://www.aepd.es/la-agencia/en-que-podemos-ayudarte>

Q9. Does it cost anything to exercise my rights?

No. Exercising your rights is free of charge. If requests are manifestly unfounded or excessive, we may charge a reasonable fee or refuse to act, in accordance with Article 12(5) GDPR.

Q10. How will you verify my identity?

We may ask for proof of identity to protect your data. We will only request the minimum information necessary and will securely delete it after verification.

Procedures for Exercising Your Rights

- **Submit a request:** Contact our Data Protection Officer (DPO) at dpo@ctrlchain.com with your request (include your full name and contact details).
- **Verification:** We may request proof of identity. Only minimal information will be requested, and it will be deleted after verification.
- **Processing:** We will handle requests within one month. Complex requests may be extended by up to two additional months, upon notice.
- **Communication:** If we cannot comply, we will explain the reasons and inform you of your right to complain to a supervisory authority.