



Data policy Connected Load Carrier (CLC)

Version 1.0, dated February 2024

As Connected Load Carrier (CLC), we are committed to ensuring the security of your and our data. This data policy outlines our practices regarding the collection, use, and protection of data when you use our services. We understand the importance of asset visibility and its impact on logistics operations, and we strive to provide tailored solutions that address the diverse needs of various industries and asset types. Please read the following carefully to understand our views and practices regarding the data CLC collects and how we will treat it.

Within this data policy we describe the following:

1. Introduction.....	2
2. Definitions used in this policy.....	2
3. Data Collection and Sources.....	3
4. Data Usage	3
5. Data Security	3
6. Data Retention and Deletion	4
7. Data Transfer and Storage	4
8. Compliance with Regulations	4
9. Data Subject Rights.....	4
10. Data Breach Response.....	4
11. Training and Awareness.....	4
12. Data Ownership and Control	5
13. Insurance	5
14. Changes to this Policy.....	5
15. Contact Information	5



1. Introduction

Connected Load Carrier (CLC) places a strong emphasis on the importance of asset visibility and its impact on logistics operations. Our solutions are tailored to address the needs of a diverse range of industries and asset types. This data policy outlines (together with any terms and conditions applicable to any goods and/or services we supply) how we collect, use, protect, and manage data, particularly data related to the tracking of non-powered assets within logistics ecosystems. At CLC we have several key principles for which CLC needs to collect, analyse and use data. The four key principles are:

- **Asset Visibility and Tracking:** CLC offers solutions designed to track various non-powered assets, e.g. carts, plates, barrels, pallets, and roll cages. Our wide coverage ensures that businesses can monitor and manage a diverse array of assets within their logistics ecosystem.
- **Tracking and Management:** Our core feature is tracking, enabling businesses to have visibility into the location and movement of their assets. This capability empowers companies to respond swiftly to changes in asset status or movement.
- **Operational Excellence:** CLC's solutions are developed with the goal of optimising internal processes. By providing Data, businesses can optimize asset utilization, streamline processes, and make informed decisions for more effective logistics operations.
- **Sustainability and Circularity:** We are committed to sustainability and environmental responsibility. Our solutions help lower Co2 footprints and contribute to more sustainable supply chain practices by optimizing asset use and reducing unnecessary transportation. We align with the growing emphasis on sustainability and promoting circularity in logistics.

2. Definitions used in this policy

In this policy the following words have the following meanings:

Customer(s), you: Means any of our customers who have a contract with us for the supply of our products and services.

CLC, we, us: Means the limited liability company Non-Powered Asset Control B.V., operating under the tradename 'Connected Load Carrier' or CLC, registered in the Dutch trade register under number 82337314.

Data: All types of data as mentioned in chapter 3.

GDPR (General Data Protection Regulation): GDPR is a comprehensive data protection regulation that applies across the EU and the European Economic Area (EEA). It sets out rules for the processing of personal data, including how personal data should be collected, stored, used, and protected. GDPR also grants various rights to individuals regarding their personal data.

ISO (International Organization for Standardization) Standards: Standards related to data and information security that are relevant to organizations operating within the European Union. ISO 27001 is one of the most well-known standards for information security management systems (ISMS). It provides a framework for organizations to establish, implement, maintain, and continually improve their information security management processes. ISO 27701 is an extension of ISO 27001 specifically focused on privacy management within an ISMS, which is essential for complying with EU data protection regulations like GDPR.



3. Data Collection and Sources

When using the service of CLC, we collect Data primarily, but not limited, through our tracking solutions. We, depending on the setup of hardware and configuration, collect the following types of Data:

1. Telemetry data: e.g. location data, movement data, temperature data, battery-voltage data;
2. Asset data: e.g. asset identification, asset photo, asset sizes;
3. Calculated data: e.g. dwell-time, balance sheet;
4. Location data: e.g. customer (depot, warehouse) locations data, location types data;
5. User data: e.g. name, email, phone number;
6. Company data: e.g. company name, logo's, employees with role in the project.

4. Data Usage

Data is used for the following:

- Provision of our services: e.g. asset management dashboard, key-statistic on asset pool;
- Improvement of CLC services, e.g. by looking at which (parts of) our products and services are or are not popular and which functionalities can still be improved;
- For statistics about the use of our products & services;
- To further secure our products and services against misuse;
- To comply with all legal obligations that apply to us;
- To settle any disputes;
- To respond to customer inquiries and support requests;
- To use Telemetry, Asset and Calculated data for commercial purposes.

CLC utilizes User data and Company data information in order to send quotes and invoices and provide access to our tracking platform. The processing of certain personal data (User data) is necessary for the performance of our contract with you.

We do never give/sell User data or Company data to third parties. However, we may share data with:

- Business partners and/or suppliers who help us deliver our services;
- Legal authorities if required by law.

5. Data Security

We are committed to ensuring the security of the Data. We employ encryption methods for data transmission and data is stored complying with security certifications such as ISO 27001. Comprehensive access controls and monitoring are in place to prevent unauthorized use, access and respond to security incidents. CLC has implemented stringent measures to safeguard the Data:

- Data Encryption: We use state-of-the-art encryption methods to protect data during transmission and storage, ensuring that information regarding your assets remains confidential and secure.
- Security Certifications: CLC maintains security certifications, including ISO 27001, and undergoes regular security audits to maintain the highest standards of data security.
- Access Control: We employ robust access control mechanisms to prevent unauthorized access to data, both internally and externally. Role-based access controls limits data access based on user roles and responsibilities.
- Security Incident Response: CLC has a comprehensive procedure for monitoring, detecting, and responding to potential security incidents or breaches. We maintain a record of past incidents and can provide examples of how they were handled.

Please note, however that despite all measures that have been taken by CLC, there are inherent risks in transmission of information over the Internet.



6. Data Retention and Deletion

What period of time do we keep Data accessible or when will it be deleted:

- **User Authentication:** We authenticate and authorize users who access Data to ensure that only authorized personnel can view, manage, and manipulate data.
- **Data Deletion:** CLC has a clear process for handling data deletion requests from customers regarding Company and/or User data and/or Location data. We ensure that all copies, including backups, are properly deleted upon request.
- **User data** will be processed during the term of your contract and will be deleted 3 months after termination of the contract.

7. Data Transfer and Storage

Data is stored conform stringent data protection standards:

- **Data Storage:** We store data only within the European Union (EU)/European Economic Area (EEA) or in countries with adequate data protection levels ensured. Our data centres are strategically located so we can guarantee best up-time in case of a geo-local incident.
- **International Data Transfers:** We do not share any type of data we collect nationally and internationally other than described under 4 Data usage.

8. Compliance with Regulations

CLC is committed to complying with all relevant data protection regulations, including GDPR. We have documented compliance measures and processes for international data transfers. CLC adheres to GDPR and data protection laws.

9. Data Subject Rights

CLC respects data subject rights, including access, rectification, and data portability requests. We have established procedures to address such requests promptly. You have certain rights regarding User and Company Data, including:

- The right to access and review;
- The right to correct inaccuracies;
- The right to request data deletion;
- The right to object to data processing;
- The right to submit a complaint to the Dutch Data Protection Authority.

To exercise these rights or if you have any questions or concerns about User and Company data, please contact us.

10. Data Breach Response

We have a robust procedure for detecting, reporting, and responding to data breaches. Affected parties and authorities are notified promptly, and we assess the impact of breaches on individuals and organizations. Our procedure for detecting, reporting, and responding to data breaches is comprehensive:

- **Notification:** We notify affected parties and authorities promptly in the event of a data breach;
- **Impact Assessment:** We assess the impact of a data breach on affected individuals and your organization.

11. Training and Awareness

CLC employees receive regular training on data protection and privacy practices. We maintain relevant certifications and credentials. Our team is well-prepared:

- **Employee Training:** We provide training to our employees regarding data protection and privacy practices;
- **Awareness Programs:** We conduct regular awareness programs on data protection.



12. Data Ownership and Control

Our terms of service include provisions related to Data ownership and intellectual property rights. We clarify Data ownership:

- Ownership: We (CLC) retain ownership of the Telemetry data, Asset data, Calculated data.
- Location, User and Company data remains the property of the Customer.
- Customers can use Telemetry and Calculated data for internal operational use only; it is not permitted to use or sell Telemetry and/or Calculated data in any shape or form with or to any third party.
- Data Retrieval: Customers can retrieve a copy of their Calculated data via API.
- When a Customer wants to acquire Data that falls out of scope of this contract, CLC can make this Data available with additional commercial terms, but will never be obliged to do so.

13. Insurance

CLC maintains insurance coverage for potential data breaches and data-related incidents.

- Insurance: We have insurance that covers potential data breaches or mishandling of data.
- Coverage: Our insurance covers data breaches and data-related incidents.

14. Changes to this Policy

We may update this data policy to reflect changes in our data handling practices. Any changes will be posted on our website, and we encourage you to review this policy periodically. We may change this policy from time to time to take account of:

- changes to Data Protection Laws and other laws which may affect this policy;
- guidance issued by the ICO and others;
- issues raised by our customers, partners and end users.

15. Contact Information

If you have any questions, concerns, or requests regarding our data policy or your data, please contact us at:

- Mail: info@connected-load-carrier.com
- Telephone number: +31 (0) 85 107 0997