How do we process your data?

Do the company follows GDPR and information security?

- Yes, the company have approved Data protection policy.
- Yes, the company have approved Information security policy.
- Yes, the company has appointed Data protection officer.
- Yes, the company applies best practices and compliant security measures.
- Yes, the company organises regular training for employees.

Where do we store the data?

- The company stores all data on geographically separated servers. The identified system servers are stored in the EU.

What are the data retention periods?

Type of information	Retention period
Coordinates	24 months
Ignition detections	24 months
Trips	24 months accessible online; another 60 months accessible from archive upon request
Reports	6 months
Events	24 months
Events notifications	1 month
Communication	24 months
Tasks	24 months
Tacho downloads	24 months
Violations	24 months
Driver activity	24 months
Eco driving data	24 months
Geozone detection	24 months
Inspections report	12 months
Malfunctions	12 months

How do we protect the data?

- **Password/authentication:**

The system ensures password complexity and validity and uses the Oauth 2.0 implementation of the system's authentication.

- **Backups:**

Backups are encrypted and the company ensures periodical backups recovery testing to be sure that in case of emergency Organization won't lost data integrity.
Project and change management:
All changes to the system are recorded in Jira. All changes are tested in a separate, test environment with personalized data.

- **Incident management:**

Incidents are registered in Zendesk. The company has assigned responsibilities for resolving incidents.

- **Technical journals:**

System logs are collected and stored. The client has the right to delete personal data that is no longer relevant.

- **Access control:**

The company grants the client the right to be administrators, but access is granted exclusively to the client's own data as data controller. Clients can restrict accessibility via object/module. Employees with admin rights can see everything as they need it to perform their direct functions.
The company support team carries out the process of registering, modifying and de-registering a user.

- **Supplier management:**

The company takes the use of suppliers seriously and therefore signs personal data processing contracts and confidentiality agreements with suppliers.

- **Vulnerability scanning:**

For vulnerability scanning, the company has an appropriate tool that performs regular checks.

- **Confidentiality:**

All employees of the company have read and signed confidentiality agreements.

What happens in case of incident when data somehow lost, damaged?

- The incident is immediately investigated, and the supervisory authorities and customers are informed.
- In cases where data is altered or lost during an incident, data recovery is ensured from backups.

Data processors obligations

- As your data processors, we will help you:
  - correct, delete or export data
  - enforce the rights of data subjects
  - carry out data protection impact assessments
  - implementing other compliance requirements
  - answer questions that arise

We care about the security of the personal data entrusted to us, so we make every effort to ensure it.
If you have any further questions, please do not hesitate to contact us: dpo@linqo.io or Perkūnkiemio str. 6, Vilnius, Lithuania.