Wie werden Ihre Daten verarbeitet?

Hält sich das Unternehmen an die DSGVO und hat es Maßnahmen zur Gewährleistung der Informationssicherheit getroffen?

- Ja, das Unternehmen verfügt über eine Datenschutzrichtlinie.
- Ja, das Unternehmen verfügt über eine Richtlinie zur Gewährleistung der Informationssicherheit.
- Ja, das Unternehmen hat einen Datenschutzbeauftragten benannt.
- Ja, das Unternehmen wendet bewährte Verfahren und angemessene Sicherheitsvorkehrungen an.
- Ja, das Unternehmen führt regelmäßig Schulungen für seine MitarbeiterInnen durch.

Wo werden Ihre Daten gespeichert?

- Das Unternehmen speichert alle Daten auf geografisch getrennten Servern. Die betreffenden Systemserver befinden sich innerhalb der EU.

Wie lange werden Ihre Daten gespeichert?

Datentyp	Speicherdauer
Koordinaten	24 Monate
Startvorgänge	24 Monate
Fahrten	24 Monate online, weitere 60 Monate auf Anfrage im Archiv zugänglich
Berichte	6 Monate
Ereignisse	24 Monate
Ereignisbenachrichtigungen	1 Monat
Mitteilungen	24 Monate
Aufgaben	24 Monate
Tacho-Downloads	24 Monate
Verstöße	24 Monate
Fahreraktivitäten	24 Monate
Eco-Fahrdaten	24 Monate

Wie werden die Daten geschützt?

- **Passwort/Authentifizierung:**
Das System prüft die Komplexität und Gültigkeit der Passwörter. Die Systemauthentifizierung erfolgt mit Oauth 2.0.
- **Backups:**
Die Backups werden verschlüsselt und das Unternehmen führt regelmäßig Wiederherstellungstests durch, um sicherzustellen, dass die Integrität der Daten auch im Notfall gewährleistet ist.
- **Projekt- und Change-Management:**
Alle Systemänderungen werden in Jira dokumentiert. Alle Änderungen werden mit personalisierten Daten in einer eigenen Testumgebung getestet.
- **Umgang mit Vorfällen:**
Vorfälle werden in Zendesk dokumentiert. Die Zuständigkeiten für die Bearbeitung von Vorfällen wurden durch das Unternehmen fest definiert.
- **Protokollierung:**
Systemprotokolle werden gesammelt und gespeichert. KundInnen haben das Recht, personenbezogene Daten zu löschen, die nicht mehr relevant sind.
- **Zugriffskontrolle:**
Kunden erhalten Administrator-Berechtigungen, können jedoch als Datenverantwortliche ausschließlich auf ihre eigenen Daten zugreifen. KundInnen können den Zugriff über Objekte bzw. Module einschränken. MitarbeiterInnen mit Administrator-Berechtigungen können alle Daten sehen, die sie für die Erfüllung ihrer direkten Aufgaben benötigen.
Die Registrierung, Änderung und Entfernung von NutzerInnen erfolgt durch das Support-Team des Unternehmens.
- **Dienstanbieter:**
Das Unternehmen nimmt die Zusammenarbeit mit Dienstanbietern erst und schließt daher mit ihnen Datenverarbeitungsverträge und Vertraulichkeitsvereinbarungen ab.
- **Scans von Schwachstellen:**
Das Unternehmen setzt ein geeignetes Tool für Schwachstellen-Prüfungen ein und führt diese regelmäßig durch.
- **Vertraulichkeit:**
Alle MitarbeiterInnen des Unternehmens haben Vertraulichkeitsvereinbarungen gelesen und unterzeichnet.

Was geschieht, wenn Daten durch einen Vorfall verloren gehen oder beschädigt werden?

- Der Vorfall wird sofort untersucht, und Datenschutzbehörden und KundInnen werden darüber informiert.
- Falls Daten durch einen Vorfall verändert werden oder verloren gehen, werden die Daten mithilfe von Backups wieder hergestellt.

Pflichten des Datenverarbeiters

- Als Ihre Datenverarbeiter unterstützen wir Sie:
    - bei der Berichtigung, Löschung und dem Export von Daten
    - bei der Umsetzung der Betroffenenrechte
    - bei der Bewertung von Datenschutzvorfällen
    - bei der Umsetzung sonstiger Compliance-Anforderungen
    - indem wir Ihre Fragen beantworten

Der Schutz der uns anvertrauten personenbezogenen Daten hat für uns höchste Priorität und wir ergreifen alle erforderlichen Maßnahmen, um diesen zu gewährleisten.
Falls Sie weitere Fragen haben, erreichen Sie uns:per E-Mail an dpo@linqo.io oder postalisch unter Perkūnkiemio-Str. 6, Vilnius, Litauen.