

## Data security & data protection – information for users

Protecting the data of our app and telematics users is our top priority. The following guidelines and tips describe the principles and measures we apply to reliably ensure the protection of your data and how you can contribute to this.

### 1. Why are data security and data privacy important?

Our software and apps process various technical vehicle data, configuration data from your telematics unit, and customer-related order data.

This information supports the daily operation, analysis and management of vehicles. At the same time, this is sensitive data that must be protected against unauthorised access – just like your smartphone/tablet itself.

The protection of this data and mobile devices is a shared responsibility:

We provide secure technology – you as a user can provide additional protection with simple measures.

### 2. How does the app protect your data?

When developing our app, we place great importance on data security and privacy:

- Communication between the app, telematics unit and backend system takes place via secure protocols and interfaces
- Access to sensitive functions is only possible for authorised users
- Only data necessary for operation is processed and stored
- Security-related functions are regularly checked and improved
- Regular updates improve stability and security

### 3. What you can do yourself to protect your data

Since the app is installed on an Android device, protection begins with the device itself:

#### Secure your smartphone

- Always activate a screen lock (PIN, password, pattern, fingerprint or facial recognition)
- Do not use PINs that are used multiple times or are easy to guess (e.g. 1234, 0000)
- Activate biometric locks if possible
- Lock your device as soon as you are not using it

#### Access to the app

- Do not leave your smartphone/tablet unattended with other people
- Log out after use if the app supports logout

### Keep your system and app up to date

- Install Android updates
- Always keep the app up to date
- Only install apps from trusted sources (e.g. Google Play Store or idem homepage)

### Be careful with networks

- Avoid using public or insecured Wi-Fi networks
- Preferably use known company networks or, if in doubt, mobile data

### Protect your telematics unit

- Set a configuration PIN when you first start using your telematics unit. (You can also set a configuration PIN at a later date) [cargofleet Service app]
- Protect the data on your telematics unit with a data PIN [cargofleet Connect app]

### General information

- Do not disclose passwords or PINs to third parties
- Protect yourself from prying eyes when entering your PIN

## 4. Shared use of assets

In many companies, Android devices are used by several people (e.g. driver changes, shift work).

In this case, please note the following in particular:

- Protect your mobile device with a suitable screen lock (no biometric locks)
- Only use your own user account, if available
- Log out properly after use
- Do not disclose your login details to unauthorised persons
- Before use, check that you are logged in with the correct user account
- Only make changes to configurations if you are authorised to do so

## 5. Compliance with company policies

In addition to these general security instructions, your company's internal guidelines always apply, e.g.:

- IT and security guidelines
- Password guidelines
- Data security and privacy requirements
- Regulations on the use of company mobile phones
- Requirements for user management and role allocation

Please adhere to these requirements.

If you are unsure, please contact your supervisor, administrator or IT support.

## 6. What to do in case of loss or theft

If your Android device is lost or stolen:

- Lock the device immediately (e.g. via Google's 'Find My Device')
- Inform your company or the responsible administrator immediately
- Change access data or passwords if necessary
- Have someone check whether access or authorisations need to be deactivated
- Contact idem telematics GmbH support to have SIM cards or assets deactivated

## 7. Questions, support and responsibility

Data security depends on vigilance and responsible handling.

If you have any questions about using the app or data protection, please contact the relevant person in your company or our support team.