Data protection impact assessment
Telematics– cargofleet Portal

Contents

1. The DPO's expert opinion

As things stand at present, the use is justifiable and the risks associated with the processing are reduced to an acceptable level. Effective protection mechanisms are available to the data subjects.

1.1. Seeking the data subjects' opinion

The data subjects' opinion was not sought.

1.2. Reason why the data subjects' opinion was not requested

No data subjects are known at this time. This obligation is incumbent on the customer in question.

2. General information

2.1 What processing is planned?

The services offered by IDEM are designed to assist customers with their fleet management operations.
Both vehicle and driver data can be recorded by installing the telematics devices provided by idem in the vehicles. Data is collected at intervals of between 1 minute and 15 minutes, at the customer's discretion. In the context of the services booked by the customer, the data collected is transmitted to a server operated by IDEM over the mobile network. The data is then displayed in evaluated form within a protected portal belonging to the customer.

2.2 What are the responsibilities for processing?

Each of Kögel's clients / customers are responsible for use. As the supplier of the vehicles with a telematics function, it is Kögel's responsibility as the processor to set up customer access and support. The operator of the telematics infrastructure (server, network, transmission devices) is the company IDEM, which acts as another processor.

2.3 Are there norms or standards for processing?

No. Specification standards are not apparent, and generally valid standards are not defined.

Rating: Acceptable

3. Data, processes and support

3.1 What data is processed?

- Driver master data
- User master data (cargofleet Portal and TCC Administration)
- Vehicles' position data (truck / trailer services)
- Vehicle data such as speed, load weight, tyre pressure readings, braking system status, loading area door opening status (truck / trailer services)
- Driver / vehicle assignment (truck services)
- Drivers' driving times (truck services)

3.2 What is the life cycle of data and processes?

The data is generated and temporarily stored on a mobile device in the vehicle. As soon as a mobile connection can be established, the data is transmitted to the telematics centre, where it is stored in a database. The data is regularly stored in the database for 18 months, unless the client instructs otherwise.

3.3 What resources are used for data processing?

- Mobile device generates and temporarily stores data
- Transmission over mobile network as soon as connection successfully established
- Receipt and storage in data centre (located in Germany)
- Storage in RAID system

Rating: Acceptable

4. Basic principles

4.1. Proportionality and necessity

4.1.1. Are the processing purposes clearly defined and lawful?

Vehicle tracking is used for fleet management purposes and to assist the drivers in recording working hours, complying with driving and rest times, and reporting expenses. The controller is thus acting on legitimate organisational interests and automating the coordination.

Rating: Acceptable

4.1.2. What is the legal basis for the processing?

The controller's legitimate interests: Art. 6 (1), sentence (1) (f) of the GDPR; purposes of the employment relationship: Section 26 of the German Federal Data Protection Act.

Rating: Acceptable

4.1.3. Is the data collected required, relevant and limited to what is necessary for data processing?

Location data is required to track vehicle routes and help drivers plan ahead. If drivers cannot be reached or vehicles are reported stolen, the vehicle's location can be determined and the incident resolved.
As long as the purpose limitation is respected, the data processed is meaningful, useful and limited to what is necessary.

Rating: Acceptable

4.1.4. Is the data correct and up to date?

The data is constantly updated as soon as a mobile connection is established. The accuracy of the data could only be affected by defective measuring units / sensors on the mobile devices or deliberate tampering.

Rating: Acceptable

4.1.5. How long is the data stored?

Regularly 18 months, according to IDEM's specifications. Adjustments may be made on the controller's instructions.

Rating: Acceptable

4.2. Measures to protect data subjects' privacy

4.2.1. How are data subjects informed of the processing?

The controller must ensure that the data subjects are informed.

Rating: Acceptable

4.2.2. If applicable, how is consent obtained from data subjects?

This is the controller's responsibility.

Rating: Acceptable

4.2.3. How can data subjects exercise their rights of access and portability?

They can send a request to the controller. Processors assist the controller in safeguarding data subjects' rights.

Rating: Acceptable

4.2.4. How can data subjects exercise their rights to rectification and deletion (right to be forgotten)?

They can send a request to the controller. Processors assist the controller in safeguarding data subjects' rights.

Rating: Acceptable

4.2.5. How can data subjects exercise their right to restriction of processing or right to object?

They can send a request to the controller. Processors assist the controller in safeguarding data subjects' rights.

Rating: Acceptable

4.2.6. Are the processors' obligations clearly defined and contractually regulated?

Basically, yes. Conclusion of the contract is the client's responsibility. Contractors provide appropriate agreements.

Rating: Acceptable

4.2.7. Where data is transferred to countries outside the European Union, is the data adequately protected?

Transfers to third countries do not take place.

Rating: Acceptable

5. Risks

5.1. Planned or existing measures

5.1.1. Data separation

The data records are logically separated for each customer.

Rating: Acceptable

5.1.2. Archiving

During the storage period, data is regularly archived in backups to ensure recoverability and rapid availability.

Rating: Acceptable

5.1.3. Data minimisation

Data is collected only to the extent necessary. The telematics data is not queried live, but at 15-minute intervals. The data is only temporarily stored on the mobile devices until successful transmission. The data is removed from the database after a defined period of time.

Rating: Acceptable

5.1.4. Combating malware

Both IDEM and Kögel have installed effective measures to detect and combat malware on their data processing systems and to keep them constantly updated.

Rating: Acceptable

5.1.5. Processing contract

Both Kögel and IDEM offer processing contracts. Kögel has concluded a valid processing contract with IDEM in accordance with the requirements set out in Art. 28 of the GDPR.

Rating: Acceptable

5.1.6. Access control

Access to IDEM's data centre is restricted and monitored.

Rating: Acceptable

5.2. Unlawful access to data

5.2.1. What could be the main implications for the data subjects if the risk materialises?

Sanctions under labour law / disciplinary measures, monitoring pressure on drivers, excessive compression of work assignments, violation of drivers' privacy.

5.2.2. What are the main threats that could lead to the risk?

Breach of the purpose limitation, use of data to monitor behaviour / performance.

5.2.3. What are the sources of risk?

Excessive monitoring by the controller, violation of internal guidelines by administrative staff, erroneous measurement data, erroneous transmission, tampering with database records.

5.2.4. Which of the identified measures help to manage the risk?

Data separation, data minimisation, combating malware, processing contract, access control, archiving.

5.2.5. How do you rate the severity of the risk, especially in terms of potential impacts and planned measures?

Substantial, since quite sensitive consequences are plausible, but, in most cases, they would be verifiable according to the specifications set out in labour law.

5.2.6. How do you rate the risk's probability of occurrence, especially with regard to threats, sources of risk and planned measures?

Negligible, since tampering and impermissible monitoring should be largely ruled out through instruction / raising the awareness of those with access permissions. There are no known indications of significant susceptibility to error.

Rating: Acceptable

5.3. Undesirable modification of data

5.3.1. What could be the main implications for the data subjects if the risk materialises?

Sanctions under labour law / disciplinary measures.

5.3.2. What are the main threats that could lead to the risk?

Breach of the purpose limitation.

5.3.3. What are the sources of risk?

Violation of internal guidelines by administrative staff, tampering with database records.

5.3.4. Which of the identified measures help to manage the risk?

Access control, archiving.

5.3.5. How do you rate the severity of the risk, especially in terms of potential impacts and planned measures?

Substantial, since the tampering would make it impossible to prove compliance with specifications set out in labour law, as well as with billing and driving / rest times (i.e. legal requirements too).

5.3.6. How do you rate the risk's probability of occurrence, especially with regard to threats, sources of risk and planned measures?

Negligible, since the empowered administrative staff are committed to properly performing their duties.

Rating: Acceptable

5.4. Data loss

5.4.1. What could be the main implications for the data subjects if the risk materialises?

Sanctions under labour law / disciplinary measures.

5.4.2. What are the main threats that could lead to the risk?

Malware, human error, (un)intentional deletion.

5.4.3. What are the sources of risk?

Erroneous transmissions, tampering with database records, violation of internal guidelines by administrative staff.

5.4.4. Which of the identified measures help to manage the risk?

Archiving, data separation, combating malware.

5.4.5. How do you rate the severity of the risk, especially in terms of potential impacts and planned measures?

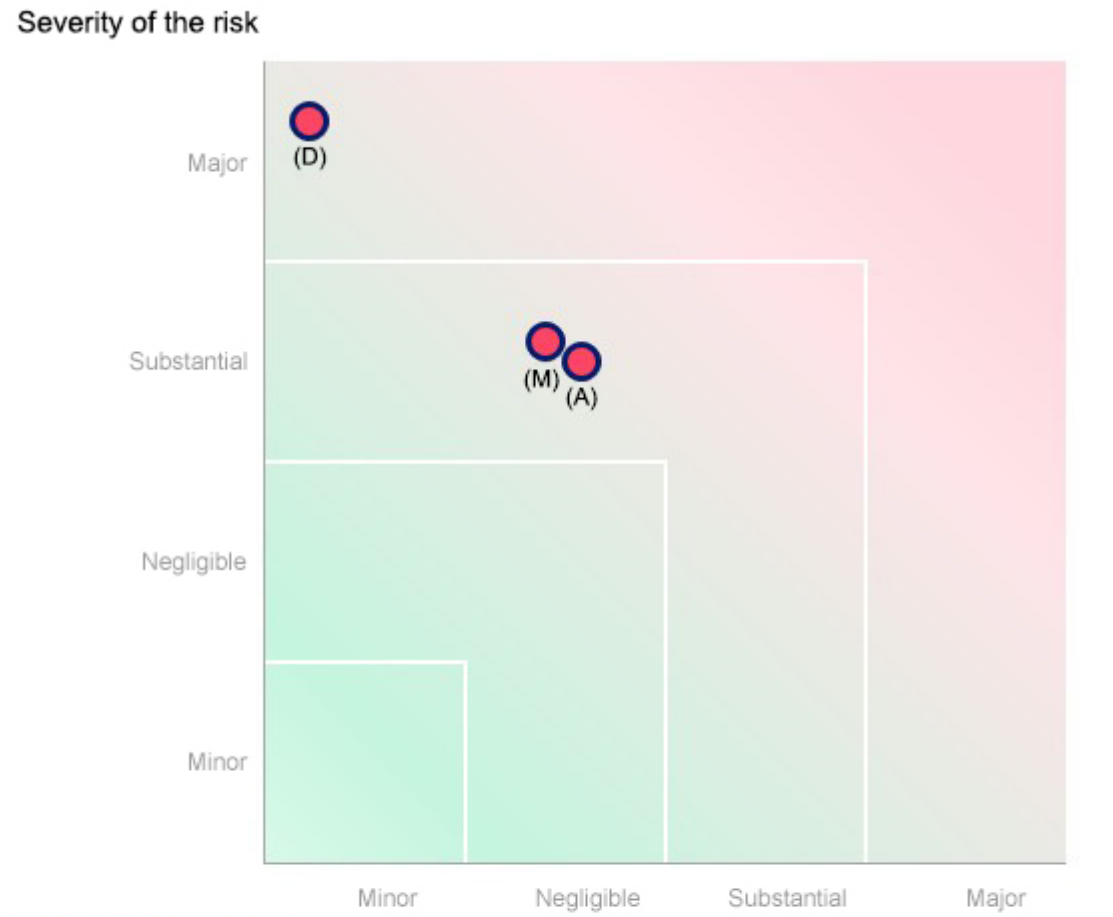
Major. The data loss would make essential fleet management data unavailable. This would mean that both billing-related data and data for statutory verification requirements could no longer be used.

5.4.6. How do you rate the risk's probability of occurrence, especially with regard to threats, sources of risk and planned measures?

Minor, because redundant systems and regular backups mean that complete data loss is highly unlikely. With respect to recoverability, only temporary failures are possible.

Rating: Acceptable

Risk matrix



- Planned or existing measures
- With the corrective measures introduced
- (A) Unlawful access to data
- (M) Undesirable modification of data
- (D) Data loss

11/06/2021