Datenschutz-Folgenabschätzung
Telematik – Portal Cargofleet

Inhalt

1. Gutachten des DSB

Nach momentaner Sachlage ist der Einsatz vertretbar und die mit der Verarbeitung verbundenen Risiken auf ein akzeptables Maß reduziert. Den Betroffenen stehen wirksame Schutzmechanismen zur Verfügung.

1.1. Einholung der Meinung der Betroffenen

Die Meinung betroffener Personen wurde nicht eingeholt.

1.2. Grund, warum die Meinung der Betroffenen nicht erfragt wurde

Betroffene sind derzeit nicht bekannt. Diese Pflicht trifft den jeweiligen Kunden.

2. Allgemeine Angaben

2.1 Welche Verarbeitung ist geplant?

Die von IDEM angebotenen Leistungen dienen der Unterstützung von Kunden bei deren Flottenmanagement.
Durch den Einbau der von idem zur Verfügung gestellten Telematik-Geräte in den Fahrzeugen können Fahrzeug- und Fahrerdaten erfasst werden. Die Datenerfassung erfolgt nach Wahl des Kunden in Intervallen zwischen einer Minute bis 15 Minuten. Im Rahmen der vom Kunden gebuchten Dienste werden die erfassten Daten über das Mobilfunknetz an einen von IDEM betriebenen Server übertragen. Die Daten werden dann in einem geschützten Portal des Kunden ausgewertet angezeigt.

2.2 Welche Zuständigkeiten bestehen für die Verarbeitung?

Verantwortlich für den Einsatz ist der jeweilige Auftraggeber/Kunde von Kögel. Kögel ist als Lieferant der Fahrzeuge mit Telematik-Funktion als Auftragsverarbeiter für die Einrichtung der Kundenzugänge und den Support zuständig. Betreiber der Telematik-Infrastruktur (Server, Netzwerk, Sendegeräte) ist die Firma IDEM, die als weiterer Auftragsverarbeiter auftritt.

2.3 Gibt es Normen oder Standards für die Verarbeitung?

Nein, Vorgabenormen sind nicht ersichtlich und allgemeingültige Standards nicht definiert.

<u>Bewertung</u> : akzeptabel

3. Daten, Prozesse und Unterstützung

3.1 Welche Daten werden verarbeitetet?

- Fahrerstammdaten
- Userstammdaten (cargofleet Portal und TCC Administration)
- Positionsdaten von Fahrzeugen (Truck/Trailer-Dienste)
- Fahrzeugdaten wie Geschwindigkeit, Beladungsgewicht, Reifendruck-Messwerte, Bremssystem-Status, Laderaum-Türöffnungs-Status (Truck/Trailer-Dienste)
- Zuordnung Fahrer / Fahrzeug (Truck-Dienste)
- Lenkzeiten von Fahrern (Truck Dienste)

3.2 Wie verläuft der Lebenszyklus von Daten und Prozessen?

Die Daten werden jeweils auf einem mobilen Endgerät im Fahrzeug erzeugt und dort zwischengespeichert. Sobald eine Mobilfunkverbindung aufgebaut werden kann, werden die Daten an die Telematik-Zentrale übermittelt und dort in einer Datenbank gespeichert. In der Datenbank werden sie regelmäßig 18 Monate gespeichert, sofern der Auftraggeber keine anderweitige Weisung erteilt.

3.3 Mit Hilfe welcher Betriebsmittel erfolgt die Datenverarbeitung?

- mobiles Endgerät erzeugt Daten und speichert zwischen
- Übermittlung über Mobilfunknetz, sobald Verbindung erfolgreich hergestellt
- Empfang und Speicherung in Rechenzentrum (Standort Deutschland)
- Speicherung in RAID-System

Bewertung : akzeptabel

4. Grundlegende Prinzipien

4.1. Verhältnismäßigkeit und Notwendigkeit

4.1.1. Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?

Das Tracking der Fahrzeuge dient dem Flottenmanagement und der Unterstützung der Fahrer bei Arbeitszeiterfassung, Einhaltung der Lenk- und Ruhezeiten sowie der Spesenabrechnung. Der Verantwortliche erfolgt damit berechtigte Organisationsinteressen und automatisiert die Abstimmung.

Bewertung : akzeptabel

4.1.2. Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?

Berechtigte Interessen des Verantwortlichen, Art 6 Abs. 1 S. 1 f) DSGVO; Zwecke des Beschäftigungsverhältnisses, § 26 BDSG

Bewertung : akzeptabel

4.1.3. Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?

Die Standortdaten sind erforderlich, um die Routen der Fahrzeuge zu verfolgen und die Fahrer bei der Planung zu unterstützen. Sollten Fahrer nicht erreichbar oder Fahrzeuge als gestohlen gemeldet sein, kann der Standort des Fahrzeuges ermittelt und der Vorfall aufgeklärt werden. Solange die Zweckbindung eingehalten wird, sind die verarbeiteten Daten sinnvoll, nützlich und auf das notwendige Maß beschränkt.

Bewertung : akzeptabel

4.1.4. Sind die Daten korrekt und auf dem neuesten Stand?

Die Daten werden ständig aktualisiert, sobald eine Mobilfunkverbindung besteht. Die Richtigkeit der Daten könnte nur durch defekte Messeinheiten/Sensoren der mobilen Endgeräte oder gezielte Manipulation beeinträchtigt werden.

Bewertung : akzeptabel

4.1.5. Welche Speicherdauer haben die Daten?

Regelmäßig 18 Monate, entsprechend der Vorgabe von IDEM. Anpassungen sind auf Weisung des Verantwortlichen möglich.

Bewertung : akzeptabel

4.2. Maßnahmen zum Schutz der Persönlichkeitsrechte der betroffenen Personen

4.2.1. Wie werden die betroffenen Personen über die Verarbeitung informiert?

Der Verantwortliche hat die Information der betroffenen Personen sicherzustellen.

Bewertung : akzeptabel

4.2.2. Wenn anwendbar, wie wird die Einwilligung der betroffenen Personen eingeholt?

Zuständigkeit des Verantwortlichen.

Bewertung : akzeptabel

4.2.3. Wie können Betroffene ihre Rechte auf Auskunft und Datenübertragbarkeit ausüben?

Anfrage beim Verantwortlichen. Die Auftragsverarbeiter unterstützen den Verantwortlichen bei der Wahrung der Betroffenenrechte.

Bewertung : akzeptabel

4.2.4. Wie können betroffene Personen ihr Recht auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?

Anfrage beim Verantwortlichen. Die Auftragsverarbeiter unterstützen den Verantwortlichen bei der Wahrung der Betroffenenrechte.

Bewertung : akzeptabel

4.2.5. Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?

Anfrage beim Verantwortlichen. Die Auftragsverarbeiter unterstützen den Verantwortlichen bei der Wahrung der Betroffenenrechte.

Bewertung : akzeptabel

4.2.6. Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?

Grundsätzlich ja. Vertragsschluss liegt in der Verantwortung des Auftraggebers. Die Auftragnehmer stellen entsprechende Vereinbarungen zur Verfügung.

Bewertung : akzeptabel

4.2.7. Soweit Datenübermittlungen in Länder außerhalb der Europäischen Union stattfinden, werden die Daten angemessen geschützt?

Es erfolgen keine Drittstaatentransfers.

Bewertung : akzeptabel

5. Risiken

5.1. Geplante oder bestehende Maßnahmen

5.1.1. Datentrennung

Die Datenbestände sind jeweils kundenbezogen logisch getrennt.

Bewertung : akzeptabel

5.1.2. Archivierung

Während des Speicherzeitraums werden die Daten regelmäßig in Backups archiviert, um Wiederherstellbarkeit und rasche Verfügbarkeit zu gewährleisten.

Bewertung : akzeptabel

5.1.3. Datenminimierung

Die Daten werden nur im erforderlichen Maße erfasst. Die Telematik-Daten werden nicht live sondern im Abstand von 15 Minuten abgefragt. Die Daten werden auf den mobilen Endgeräten nur bis zur erfolgreichen Übertragung zwischengespeichert. Aus der Datenbank werden die Daten nach einem definierten Zeitraum entfernt.

Bewertung : akzeptabel

5.1.4. Bekämpfung von Malware

Sowohl IDEM als auch Kögel haben wirksamen Maßnahmen zur Erkennung und Bekämpfung von Malware auf ihren Datenverarbeitungssystemen installiert und halten diese stetig aktuell.

Bewertung : akzeptabel

5.1.5. Auftragsverarbeitungsvertrag

Sowohl Kögel als auch die IDEM bieten Auftragsverarbeitungsverträge an. Kögel hat mit IDEM einen wirksamen AV-Vertrag entsprechend der Vorgaben aus Art. 28 DSGVO geschlossen.

Bewertung : akzeptabel

5.1.6. Zugangskontrolle

Die Zugänge zu dem Rechenzentrum der IDEM sind beschränkt und werden kontrolliert.

Bewertung : akzeptabel

5.2. Unrechtmäßiger Zugriff auf Daten

5.2.1. Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

arbeitsrechtliche Sanktionen / Maßregelungen, Überwachungsdruck für Fahrer, übermäßige Verdichtung der Arbeitsaufträge, Verletzung der Privatsphäre der Fahrer

5.2.2. Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Verletzung der Zweckbindung, Verwendung der Daten zur Verhaltens-/Leistungskontrolle

5.2.3. Was sind die Risikoquellen?

Überwachungsexzess des Verantwortlichen, Verletzung interner Vorgaben durch Mitarbeitende der Verwaltung, Fehlerhafte Messdaten, Fehlerhafte Übertragungen, Manipulation der Datenbankbestände

5.2.4. Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Datentrennung, Datenminimierung, Bekämpfung von Malware, Auftragsverarbeitungsvertrag, Zugangskontrolle, Archivierung

5.2.5. Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Substantiell, da durchaus empfindliche Folgen vorstellbar sind, diese jedoch in den meisten Fällen nach den Vorgaben des Arbeitsrechts prüfbar wären.

5.2.6. Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Überschaubar, da Manipulationen und unzulässige Überwachungen durch Belehrung/Sensibilisierung der Zugriffsberechtigten weitgehend ausgeschlossen sein dürften. Anzeichen für erhebliche Fehleranfälligkeiten sind nicht bekannt.

Bewertung : akzeptabel

5.3. Unerwünschte Veränderung von Daten

5.3.1. Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

arbeitsrechtliche Sanktionen / Maßregelungen

5.3.2. Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Verletzung der Zweckbindung

5.3.3. Was sind die Risikoquellen?

Verletzung interner Vorgaben durch Mitarbeitende der Verwaltung, Manipulation der Datenbankbestände

5.3.4. Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Zugangskontrolle, Archivierung

5.3.5. Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Substantiell, da durch die Manipulation sowohl die Einhaltung arbeitsrechtliche Vorgaben als auch von Abrechnungen und Lenk-/Ruhezeiten (also auch gesetzlicher Vorgaben) nicht mehr nachgewiesen werden könnte.

5.3.6. Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Überschaubar, da die befähigten Verwaltungsmitarbeiter auf die ordnungsgemäße Aufgabenwahrnehmung verpflichtet sind.

Bewertung : akzeptabel

5.4. Datenverlust

5.4.1. Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?

arbeitsrechtliche Sanktionen / Maßregelungen

5.4.2. Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?

Malware, menschliche Fehler, un-/beabsichtigte Löschung

5.4.3. Was sind die Risikoquellen?

Fehlerhafte Übertragungen, Manipulation der Datenbankbestände, Verletzung interner Vorgaben durch Mitarbeitende der Verwaltung

5.4.4. Welche der identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?

Archivierung, Datentrennung, Bekämpfung von Malware

5.4.5. Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?

Groß, Durch den Datenverlust wären wesentliche Daten zum Flottenmanagement nicht mehr verfügbar. Somit könnten sowohl abrechnungsrelevante als auch Daten für gesetzliche Nachweispflichten nicht mehr genutzt werden.

5.4.6. Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplante Maßnahmen?

Geringfügig, denn durch redundante Systeme und regelmäßige Backups sind vollständige Datenverluste mit hoher Wahrscheinlichkeit ausgeschlossen. Über die Wiederherstellbarkeit dürften allenfalls vorübergehende Ausfälle zu befürchten sein.

Bewertung : akzeptabel

Risikomatrix