webfleet solutions
a Bridgestone company

DIE DATENSCHUTZ-GRUNDVER-ORDNUNG

„Mit dem verstärkten Aufkommen von Big Data für Fuhrparks entstehen zwangsläufig Bedenken bezüglich Sicherheit und Privatsphäre.“

Verwendung und Austausch von Daten zum Fuhrpark in Unternehmen sind zunehmend wichtige Faktoren für einen sicheren und effizienten Geschäftsbetrieb.

Mit dem verstärkten Aufkommen von Big Data für Fuhrparks, in hohem Maße unterstützt durch die Telematik, entstehen zwangsläufig Bedenken bezüglich Sicherheit und Privatsphäre. Durch die Einführung der neuen EU-Datenschutz-Grundverordnung (DSGVO) müssen diese Bedenken jetzt genauer unter die Lupe genommen werden.

Die meisten Anforderungen der DSGVO sind bereits gesetzlich verankert. Für Unternehmen, die die Gesetzgebung beachten und Best Practices einsetzen, ergeben sich durch die DSGVO unserer Ansicht nach keine größeren Veränderungen.

Fuhrparkbetreiber und deren Lieferkette müssen dafür sorgen, dass eine angemessene Infrastruktur, richtige Verfahren und eine entsprechende Unternehmenskultur vorhanden sind, um Verstöße gegen die DSGVO zu vermeiden. Bei einer Zuwiderhandlung müssen Unternehmen mit schwerwiegenden Auswirkungen rechnen. Bei den Lösungen von Webfleet Solutions wird die DSGVO in hohem Maße berücksichtigt und dies ist die Grundlage für die Beratung und Unterstützung, die wir unseren Kunden bieten.

In diesem Dokument wird erläutert, was die Verordnung für Ihr Unternehmen und Ihren Fuhrpark bedeutet. Sie erhalten praktische Ratschläge, damit Sie immer gesetzeskonform handeln.

Thomas Schmidt,
Managing Director, Webfleet Solutions

DIE DSGVO: **ÜBERBLICK**

Die digitale Welt hat sich sehr verändert, seitdem 1995 die EU-Datenschutzrichtlinie verabschiedet wurde.

Die Grundprinzipien gelten zwar nach wie vor, doch mit der Einführung der Datenschutz-Grundverordnung (DSGVO) wurde die Gesetzgebung auf den neuesten Stand gebracht. Die DSGVO tritt am 25. Mai 2018 in Kraft und bedeutet eine Harmonisierung der Datenschutzgesetze in ganz Europa, um allen EU-Bürgern angemessenen Schutz zu bieten.

Im Grunde geht es dabei um den Schutz personenbezogener Daten, definiert als „Daten, die als Informationen über eine identifizierte oder identifizierbare natürliche Person betrachtet werden". Daher ist die DSGVO besonders für Fuhrparkbetreiber wichtig, die häufig auf Fahrerdaten zugreifen bzw. diese verwalten.

Die neuen Regeln sind keine völlige Überarbeitung der Datenschutzgesetzgebung, sondern eher eine Erweiterung der vorhandenen Bestimmungen und der aktuell von Unternehmen umgesetzten Best-Practices-Verfahren.

> Die DSGVO harmonisiert die Datenschutzgesetze in ganz Europa, um sicherzustellen, dass alle EU-Bürger angemessen geschützt sind.

INWIEWEIT ÄNDERT SICH DER DATENSCHUTZ MIT DER DSGVO IM HINBLICK AUF DIE TELEMATIK?

Mit der DSGVO werden mehrere wichtige Änderungen an den Datenschutzgesetzen eingeführt, die sich insbesondere auf das Fuhrparkmanagement und den Einsatz von Telematik auswirken.

1 DIE EINZELPERSON STEHT IM MITTELPUNKT. Zweck der DSGVO ist es, Einzelpersonen so zu befähigen, dass sie im Voraus umfassend informiert werden, welche Daten warum und von wem erhoben werden und wie lange sie verarbeitet werden. Sie können dann ihr Einverständnis erteilen oder verweigern und, mit gewissen Einschränkungen, beantragen, dass die Verarbeitung ihrer Daten eingestellt wird.

2 RISIKOBEURTEILUNGEN UND PRÜFNACHWEISE SIND ERFORDERLICH. Unternehmen müssen bei der Verarbeitung personenbezogener Daten die Risiken eines Datenmissbrauchs identifizieren und eingrenzen sowie dokumentieren, wie die Daten verwendet werden und welche Maßnahmen getroffen werden sollten, um die Bestimmungen zu erfüllen.

3 BESTIMMTE ORGANISATIONEN MÜSSEN AUCH EINEN DATENSCHUTZBEAUFTRAGTEN BENENNEN. Laut der DSGVO sind Sie zur Benennung eines Datenschutzbeauftragten verpflichtet, wenn Sie bestimmte Arten der Datenverarbeitung durchführen. Beispielsweise, wenn Ihre Hauptaktivitäten eine umfangreiches, regelmäßiges und systematisches Monitoring von betroffenen Personen erfordern. Weitere Kriterien finden Sie nachfolgend in diesem Dokument.

4 UNTERNEHMEN UNTERSTEHEN EINER EINZIGEN REGULIERUNGSBEHÖRDE. Unternehmen in verschiedenen europäischen Ländern, insbesondere wenn ihre Fahrzeuge über Landesgrenzen hinweg betrieben werden, unterliegen jetzt einer einzigen Gesetzgebung und unterstehen einer einzigen Regulierungsbehörde, und zwar im Land des Firmenhauptsitzes.

5 VERSCHÄRFTE SICHERHEITSANFORDERUNGEN. Personenbezogene Daten sind jetzt vor jeglicher unbefugten Verwendung geschützt. Maßgeblich ist dabei die Sensitivitätseinstufung der Daten. Die durch Telematiksysteme bereitgestellten GPS-Standortdaten können als sensibel eingestuft werden, da sie viel über eine Einzelperson preisgeben.

6 HÖHERE GELDSTRAFEN BEI VERSTÖSSEN. Gemäß der DSGVO liegt die maximale Geldstrafe für Verstöße bei 20 Millionen Euro oder vier Prozent des Jahresumsatzes, je nachdem, welcher Wert höher ist.

WIE SIEHT DIE ROLLENVERTEILUNG GEMÄSS DER DSGVO AUS?

Datenverantwortliche und Auftragsverarbeiter fallen beide unter die Bestimmungen der DSGVO. In den meisten Fällen fungiert ein Unternehmen als Datenverantwortlicher und die jeweiligen Zulieferer werden als Auftragsverarbeiter eingestuft. Die vollständigen Definitionen sind wie folgt:

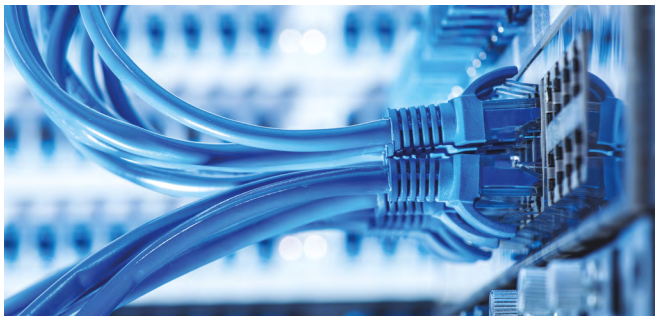
- Ein **Auftragsverarbeiter** ist ein Unternehmen, das personenbezogene Daten für einen Verantwortlichen verarbeitet. Webfleet Solutions fungiert als Auftragsverarbeiter für alle personenbezogenen Daten, die durch Kunden und Partner über unsere Systeme und Plattformen bereitgestellt werden.
- Ein **Datenverantwortlicher** ist ein Unternehmen, das den Zweck und die Mittel für die Verarbeitung personenbezogener Daten festlegt. Wenn es beispielsweise um die Daten für Fuhrparks geht, die über unsere Software-as-a-Service (SaaS) Fuhrparkmanagement-Lösung WEBFLEET bereitgestellt werden, fungiert dieses Unternehmen als Datenverantwortlicher, da es entscheidet, wie diese Daten verwendet werden, z. B. zur Gewährleistung der Sicherheit der Mitarbeiter auf der Straße.

Eine der wichtigsten mit der DSGVO eingeführten Änderungen an den Datenschutzvorschriften besteht darin, dass die Auftragsverarbeiter sich jetzt ebenfalls an die Bestimmungen halten müssen. Bisher waren ausschließlich die Datenverantwortlichen hierfür zuständig.

WIE SEHEN DIE ZUSTÄNDIGKEITEN AUS?

Die Zuständigkeiten von Unternehmen sind in den Datenschutzprinzipien der DSGVO dargelegt. Danach müssen personenbezogene Daten:

- auf rechtmäßige Weise, nach Treu und Glauben und transparent verarbeitet werden.
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
- dem Zweck angemessen und relevant sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden.
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- in einer Weise verarbeitet werden, die angemessen und sicher ist.



WELCHE ARTEN VON PERSONENBEZOGENEN DATEN FALLEN UNTER DIE VERORDNUNG?

Die Definitionen von personenbezogenen Daten wurden unter der DSGVO erweitert.

Eine Einzelperson – oder laut Bezeichnung in der Verordnung: „betroffene Person" – kann direkt oder indirekt identifiziert werden. Kennungen für personenbezogene Daten umfassen alles vom Namen einer Einzelperson bis hin zu Daten mit eindeutigen Kennungen, zum Beispiel Fahrzeugkennzeichen oder Fahrgestellnummern. Wenn die betroffene Person mithilfe der Daten identifiziert werden kann – selbst wenn keine Identifizierung stattfindet –, handelt es sich um personenbezogene Daten.

Die Arten personenbezogener Daten im Hinblick auf eine identifizierte oder identifizierbare Person kann Meinungen und Fakten umfassen sowie alle möglichen Daten, angefangen von Informationen zur Leistung am Arbeitsplatz bis hin zu Unterlagen zur Mitarbeiteranwerbung und Notizen aus Bewerbungsgesprächen.

Anonymisierte Daten fallen nicht unter die Bestimmungen der DSGVO, wenn die getroffenen Maßnahmen es unmöglich machen, die personenbezogenen Daten mit einer identifizierbaren Person zu verbinden.

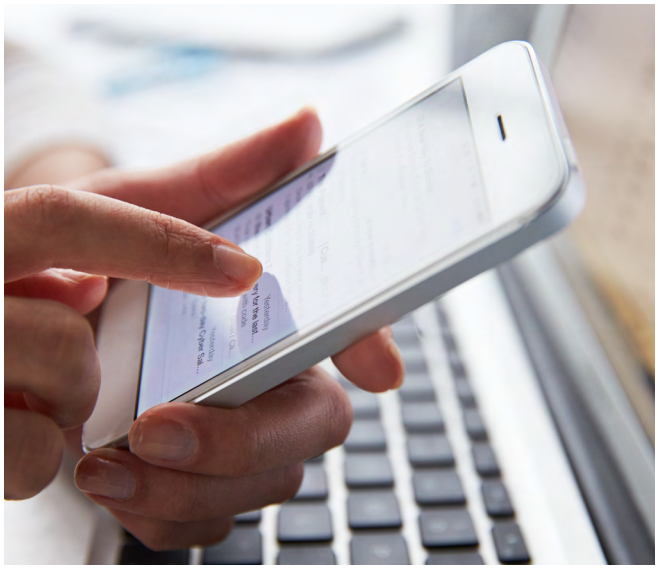
Eine explizite Einwilligung ist für die Freigabe personenbezogener Daten erforderlich – „personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person".

DIE GESETZLICHE GRUNDLAGE FÜR DIE DATENVERARBEITUNG

Zur Verarbeitung personenbezogener Daten muss ein gültiger rechtmäßiger Grund vorliegen und der Zweck der Datenverwendung muss im Voraus bestimmt sein.

Die nächstliegende Rechtfertigung liegt wahrscheinlich darin, die explizite Einwilligung der Person zu haben, deren Daten verarbeitet werden. In einem Berufsverhältnis kann dies jedoch problematisch sein, da nur schwer argumentiert werden kann, dass eine solche Einwilligung freiwillig erteilt wurde.

Daher stehen andere rechtmäßige Gründe für eine Datenverarbeitung zur Auswahl, wobei die gewählte Option klar dokumentiert werden muss.



- **EINWILLIGUNG**
  Eine klare Einwilligung muss frei von einer Einzelperson erteilt werden, damit ihre Daten zu einem bestimmten Zweck verarbeitet werden können. Es sollte beachtet werden, dass diese Einwilligung unmissverständlich sein muss. Sie darf nicht stillschweigend sein und kann jederzeit widerrufen werden.
- **BERECHTIGTES INTERESSE**
  In diesem Fall müssen Sie oder ein Dritter ein berechtigtes Interesse haben, das nicht mit den Grundrechten einer Person in Konflikt steht.
- **ERFÜLLUNG EINES VERTRAGS**
  Dieser Grund ermöglicht die Datenverarbeitung, wenn dies für einen Vertrag erforderlich ist, den Sie mit der Person eingegangen sind oder eingehen wollen.
- **RECHTLICHE VERPFLICHTUNG**
  Die Verarbeitung kann erfolgen, wenn dies zur Erfüllung Ihrer rechtlichen Verpflichtungen notwendig ist.
- **LEBENSWICHTIGE INTERESSEN**
  Eine Verarbeitung darf auch erfolgen, wenn dies zum Schutz des Lebens einer Person erforderlich ist.
- **AUFGABE IM ÖFFENTLICHEN INTERESSE**
  In diesem Fall muss die Verarbeitung notwendig sein, um eine rechtliche Aufgabe im öffentlichen Interesse durchzuführen.

Es ist zu beachten, dass Fuhrparkbetreiber generell häufig ein **berechtigtes Interesse** oder eine **vertragliche Rechtfertigung** für die Verarbeitung personenbezogener Daten haben.

Für Fuhrparkbetreiber umfasst **ein berechtigtes Interesse** Bereiche wie die Verarbeitung von Kilometerdaten zur Verwaltung von Verträgen für Leasing-Fahrzeuge, von Kraftstoffdaten zur Betrugsverhinderung oder von Daten zum Fahrverhalten, um die Gesundheit und Sicherheit des Fahrers zu gewährleisten.

Vertragliche Gründe für die Verarbeitung von Daten umfassen beispielsweise den Einsatz von Telematikdaten, um Arbeitszeitbeginn und -ende der Fahrer aufzuzeichnen. Dies ist möglicherweise in den Arbeitsverträgen der Fahrer aufgeführt.

Wichtig ist außerdem, dass eine betroffene Person das „Recht auf Vergessenwerden“ hat und eine Datenlöschung anfordern kann. Dies tritt möglicherweise auf, wenn die Einwilligung widerrufen wird, wenn die Daten im Hinblick auf den Zweck ihrer Erfassung nicht mehr erforderlich sind oder wenn die betroffene Person der Verarbeitung widerspricht und kein berechtigtes Interesse mehr vorliegt, um eine weitere Verarbeitung zu rechtfertigen.

ZWECKE DER DATENVERARBEITUNG

Unter der DSGVO müssen der bzw. die Zwecke für die Datenverarbeitung klar im Voraus dargelegt werden. Der genannte Zweck muss spezifisch und klar definiert sein, sodass er von der betroffenen Person leicht verstanden werden kann.

TELEMATIKDATEN KÖNNEN U. A. ZU FOLGENDEN ZWECKEN VERWENDET WERDEN:

- Ortung von Fahrzeugen zur Fahrzeugsicherheit und Fuhrparkoptimierung.
- Monitoring des Fahrverhaltens zur Verbesserung von Fahrersicherheit und Senkung der Kraftstoffkosten.
- Kommunikation mit Fahrern, um Mitarbeitersicherheit und Arbeitseffizienz zu erhöhen.
- Verwendung von Tachograph- und Arbeitszeitdaten der Fahrer, um die Einhaltung von Arbeitszeitregelungen zu gewährleisten.
- Managementberichte zur Geschäftsoptimierung, einschließlich Verbesserungen am Kundendienst oder der Fuhrparkeffizienz.
- Integration mit einer Hardware- oder Softwarelösung eines Drittanbieters.

WER MUSS VERANTWORTUNG ÜBERNEHMEN?

Es muss betont werden, dass jeder Unternehmensmitarbeiter Verantwortung für den Datenschutz übernehmen sollte, da Datenschutzverletzungen an einer Vielzahl verschiedener Punkte innerhalb der Lieferkette und auf sehr unterschiedliche Weise auftreten können.

Trotzdem ist es angebracht, die Hauptverantwortung an eine speziell bestimmte Person oder ein Team zu übertragen, um sicherzustellen, dass die Unternehmensprozesse zur Einhaltung der Bestimmungen korrekt umgesetzt werden.

Es ist unwahrscheinlich, dass die Abteilung für das Fuhrparkmanagement letztendlich die Verantwortung für die Einhaltung der Bestimmungen trägt. Ein Fuhrparkmanager kann aber auf andere Weise eine wichtige Rolle spielen, beispielsweise in den folgenden Bereichen:

- Managen der Lieferantenbeziehungen und gewährleisten, dass Verträge bestehen.
- Überprüfen, ob eine gesetzliche Grundlage für die Verwendung von Daten zu Fahrern oder Mitgliedern der Abteilung für das Fuhrparkmanagement vorliegt.
- Einholen der Einwilligung von Teammitgliedern, falls erforderlich.
- Kommunikation mit Mitarbeitern und wichtigen Beteiligten in der Abteilung für das Fuhrparkmanagement, um sicherzustellen, dass sich alle ihrer Verantwortung bewusst sind.
- Bereitstellen der notwendigen Informationen für einen Prüfnachweis der Einhaltung, wie Verträge und Einwilligungsdokumente.

Auf betrieblicher Ebene kann die Hauptverantwortung an einen speziellen Datenschutzbeauftragten übertragen werden. Oft spielen aber auch die Personalabteilung, die Betriebsabteilung (Operations) oder die IT-Abteilung eine führende Rolle in diesem Prozess.

ENTWICKLUNG **EINES AKTIONSPLANS**

Aufgrund der hohen Anzahl von Datenübertragungen innerhalb der Fuhrpark-Lieferkette besteht für Fuhrparkbetreiber unter der DSGVO ein besonders hohes Risiko.

Beispielsweise bezieht ein Unternehmen Führerscheindaten sowohl von der entsprechenden Zulassungsbehörde wie auch dem Fahrer selbst, um dessen Fahrtauglichkeit zu festzustellen. Diese Daten werden dann aber möglicherweise auch an Serviceanbieter in den Bereichen Fahrzeugleasing, Risikomanagement oder Versicherung weitergegeben.

Angesichts des hohen Risikos könnte der erste Schritt in einem Unternehmen darin bestehen, eine umfassende Risikoeinschätzung durchzuführen. Dies ergibt ein detailliertes Bild über die verschiedenen Schnittstellen in der Lieferkette, an denen Daten ausgetauscht werden und die potenzielle Quellen für Sicherheitsverletzungen darstellen könnten.

Anschließend können Maßnahmen bezüglich jeder einzelnen Schnittstelle ergriffen und Schritte eingeleitet werden, um das Risiko für betroffene Personen wo immer möglich zu mindern oder ganz zu beseitigen.

Eine solche Risikoeinschätzung ist gemäß der DSGVO in bestimmten Situationen sogar vorgeschrieben und wird als **Datenschutz-Folgenabschätzung** bezeichnet.

Eine Datenschutz-Folgenabschätzung ist besonders bei der Einführung neuer Datenprozesse, Systeme oder Technologien in einem Unternehmen relevant. Sie kann auch zum Nachweis der Rechenschaftspflicht gemäß der DSGVO verwendet werden, um Unternehmen bei den Schritten zur Einhaltung zu unterstützen und aufzuzeigen, dass angemessene Maßnahmen für eine fortlaufende Einhaltung getroffen wurden.

Unter der DSGVO ist eine Datenschutz-Folgenabschätzung erforderlich, wenn die Datenverarbeitung „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat“. Dies gilt insbesondere in Situationen, bei denen Daten folgendermaßen verwendet werden:

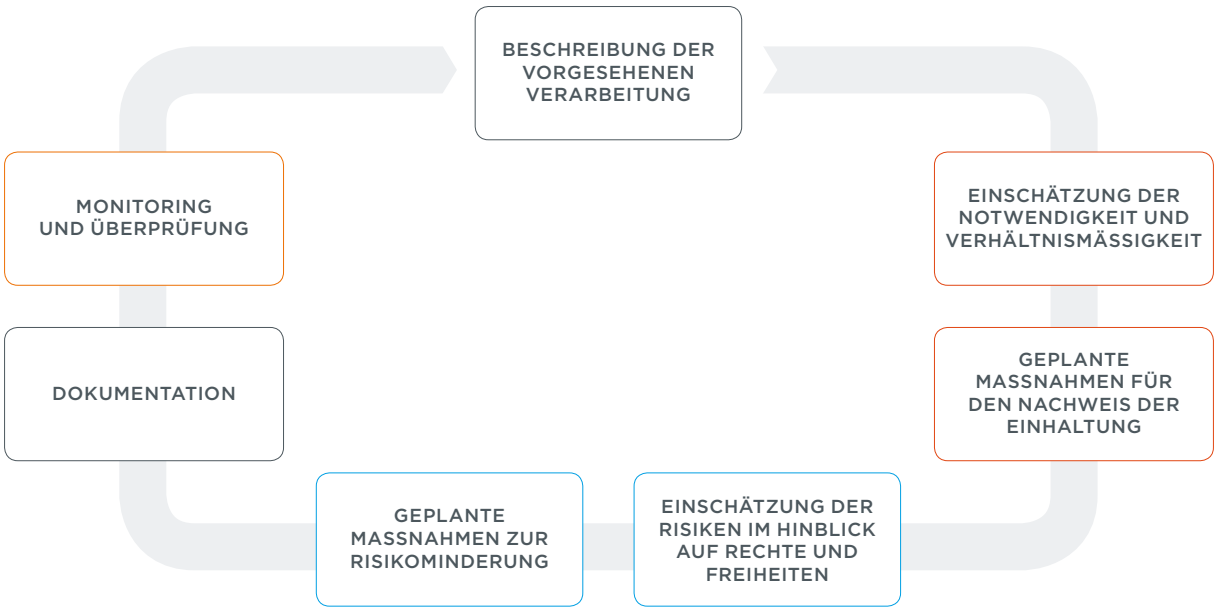
- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, einschließlich Profiling.
- Umfangreiche Verarbeitung vertraulicher Daten.
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Ein großer Teil der Fuhrparkdaten wird durch diese drei Bedingungen abgedeckt, beispielsweise der Einsatz von Telematiktechnologie zum Monitoring der Fahrerleistung, was als systematische Überwachung von Mitarbeitern am Arbeitsplatz angesehen werden kann.

Die europäischen Datenschutzbehörden haben Anleitungen zur erfolgreichen Durchführung einer Datenschutz-Folgenabschätzung herausgegeben, aber die Grundprinzipien werden auch durch einen Best-Practice-Ansatz beim Schutz personenbezogener Daten umgesetzt.

Mit den folgenden Schritten lässt sich die Einhaltung der Bestimmungen erleichtern:

- Alle Datenübertragungen aufzeichnen
- Die Lieferkette überprüfen
- Sicherstellen, dass angemessene Verträge vorhanden sind
- Einen Prozess für Datenabfragen definieren
- Einen Plan für den Fall von Datenschutzverletzungen aufstellen
- Dafür sorgen, dass Mitarbeiter ihre Rollen verstehen



ALLE DATENÜBERTRAGUNGEN KARTIEREN

Das Kartieren aller Datenübertragungen in der Lieferkette für den Fuhrpark ist ein guter Ausgangspunkt für eine angemessene Risikoeinschätzung.

Dazu müssen alle unterschiedlichen ein- und ausgehenden Datenübertragungen sowie weitere Einzelpersonen oder Unternehmen vermerkt werden, die an diesen Transaktionen beteiligt sind.

Für eine schnelle Analyse der verschiedenen Schnittstellen in der Kette ist möglicherweise eine Darstellung als visuelles Diagramm hilfreich.

In jedem Fall muss identifiziert werden, wer Datenverantwortlicher und wer Verarbeiter ist. Außerdem muss überprüft werden, ob geeignete Verträge vorhanden sind.

Dadurch kann ein Unternehmen feststellen, ob es auf die DSGVO vorbereitet ist und wo potenzielle Probleme bestehen.

TYPISCHE DATENSTRÖME BEIM FUHRPARKMANAGEMENT

Unternehmen, die einen Fuhrpark betreiben, müssen eine Vielzahl von ein- und ausgehenden Datenströmen bewältigen. Beispiele für Drittunternehmen, mit denen u. U. vertrauliche personenbezogene Daten ausgetauscht werden, sind:

- Telematik- und andere Software-Anbieter
- Leasing-Unternehmen
- Fahrzeughändler
- Versicherungen
- Anbieter im Bereich Risikomanagement
- Anbieter im Bereich Schadenmanagement
- Fahrzeug-Zulassungsbehörden
- Service-, Wartungs- und Reparaturunternehmen
- Tankkartenanbieter

DIE LIEFERKETTE ÜBERPRÜFEN

Unternehmen können für Datenschutzverletzungen über die gesamte Lieferkette hinweg zur Rechenschaft gezogen werden. Daher ist es wichtiger als je zuvor, dafür zu sorgen, dass jeder Fuhrpark-Anbieter, der vertrauliche Daten verarbeitet, dies auf nachweislich sichere Art und Weise tut.

Jeder bei der Aufzeichnung des Datendiagramms identifizierte Auftragsverarbeiter muss ausreichende Garantien bereitstellen können, dass die Anforderungen der DSGVO eingehalten und die Rechte der betroffenen Personen geschützt werden.

Das Gleiche gilt für potenzielle neue Lieferanten und es müssen unbedingt klare Prüfnachweise für alle Situationen aufgestellt werden, in denen personenbezogene Daten verarbeitet werden. Auch darf nicht außer Acht gelassen werden, dass diese Anbieter möglicherweise mit weiteren Anbietern zusammenarbeiten, die ebenfalls die jeweiligen Daten nutzen.

Unternehmen können für Datenschutzverletzungen über die gesamte Lieferkette hinweg zur Rechenschaft gezogen werden.

SICHERSTELLEN, DASS ANGEMESSENE VERTRÄGE VORHANDEN SIND

Bei jeder Datenübertragung muss festgestellt werden, ob eine neue Einwilligung erforderlich ist, damit die Transaktion die Anforderungen der DSGVO erfüllt.

Beispiel: Wurde der Zweck für die Verwendung von Telematikdaten in der Vergangenheit klar dargelegt, also zur Senkung der Kraftstoffkosten, zur Verbesserung der Sicherheit oder für einen anderen Zweck? Wenn dies nicht der Fall war, muss dies korrigiert werden, damit sich der Mitarbeiter darüber im Klaren ist, warum seine personenbezogenen Daten verarbeitet werden.

Wann immer ein Datenverantwortlicher einen Verarbeiter nutzt, muss ein schriftlicher Vertrag über die Nutzungsbedingungen vorliegen. Anhand dieser Verträge lässt sich außerdem sicherstellen, dass beide Parteien ihre Verantwortlichkeiten und Verpflichtungen verstehen. In der DSGVO ist angegeben, was ein Vertrag zwischen einem Verantwortlichen und einem Verarbeiter enthalten sollte.

EINEN PROZESS FÜR DATENANFORDERUNGEN AUFSTELLEN

Gemäß der DSGVO hat eine betroffene Person das Recht auf Zugang zu den über sie in einem Unternehmen gespeicherten personenbezogenen Daten. Im Fall von Telematikdaten umfasst dies unter vielen anderen Datenkategorien Dinge wie Orts- und Fahrtverlaufsdaten, Kilometerzahlen oder Statistiken zum Fahrverhalten.

Wenn eine betroffene Person Zugang beantragt, muss ihr mitgeteilt werden, welche Daten über sie gespeichert sind und ob diese Daten verarbeitet werden. Die Informationen müssen spätestens innerhalb von einem Monat nach Empfang des Antrags bereitgestellt werden. Bei komplexen oder einer großen Zahl von Anträgen kann dieser Zeitraum um weitere zwei Monate verlängert werden.

Unternehmen wären gut beraten, einen klaren Prozess für die Verarbeitung solcher Anfragen aufzustellen, um vorschriftsmäßig zu handeln. Dazu gehört u. a. die Zuweisung der Verantwortung an einen geeigneten Mitarbeiter und Schritte zur Identitätsprüfung der anfragenden Person.

Außerdem muss dafür gesorgt werden, dass die Daten einfach zugänglich sind. Im Fall von Telematikdaten bedeutet dies möglicherweise die Zusammenarbeit mit einem Lieferanten, der leicht zugängliche und trotzdem umfassende Reports bereitstellt, aus denen klar hervorgeht, welche Daten über welchen Mitarbeiter gespeichert sind.

Weiterhin könnten Unternehmen eine spezielle E-Mail-Adresse für Anfragen einrichten. Ein Best-Practice-Ansatz besteht darin, betroffenen Personen über ein sicheres Selbstbedienungssystem Remotezugang zu ihren Daten zu ermöglichen.

> Wenn eine betroffene Person Zugang beantragt, muss ihr mitgeteilt werden, welche Daten über sie gespeichert sind und ob diese Daten verarbeitet werden.

EINEN PLAN FÜR DEN FALL VON DATENSCHUTZVERLETZUNGEN AUFSTELLEN

Es gibt eine ganze Reihe von Maßnahmen zur Risikominimierung, es muss aber unbedingt ein Prozess für die Handhabung von Datenschutzverletzungen aufgestellt werden.

Mögliche Fälle von Datenschutzverletzungen:

- Zugang zu personenbezogenen Daten durch einen nicht befugten Dritten.
- Eine absichtliche oder versehentliche Verletzung durch einen Datenverantwortlichen oder einen Auftragsverarbeiter.
- Das Senden personenbezogener Daten an einen falschen Empfänger.
- Verlust oder Diebstahl eines Computers, auf dem personenbezogene Daten gespeichert sind.
- Unbefugtes Ändern personenbezogener Daten.
- Verlust der Verfügbarkeit personenbezogener Daten.

Zur Erkennung, Untersuchung und internen Berichterstattung von Datenschutzverletzungen müssen robuste Prozesse aufgestellt werden. Dadurch kann eine fundierte Entscheidung darüber gewährleistet werden, ob eine Verletzung so schwerwiegend ist, dass sie der relevanten Aufsichtsbehörde gemeldet werden muss. Dies muss, wann immer möglich, innerhalb von 72 Stunden geschehen. Wenn ein hohes Risiko besteht, dass die Rechte und Freiheiten einer betroffenen Person durch die Datenschutzverletzung beeinträchtigt werden, muss die betroffene Person ebenfalls informiert werden.

Zur Erleichterung dieses Prozesses könnten die Mitarbeiter darin geschult werden, eine Datenschutzverletzung zu erkennen, und angewiesen werden, wem eine solche Verletzung innerhalb des Unternehmens zu melden ist.

CHECKLISTE FÜR DATENSCHUTZVERLETZUNGEN

Unternehmen müssen in der Lage sein, alle folgenden Anforderungen zu erfüllen, um angemessen auf eine Datenschutzverletzung zu reagieren:

- Es muss ein Prozess vorhanden sein, um das wahrscheinliche Risiko einer erfolgten Datenschutzverletzung für die betroffenen Personen einzuschätzen.
- Das Unternehmen muss wissen, welche Aufsichtsbehörde für seine Verarbeitungsaktivitäten zuständig ist.
- Es muss ein Prozess vorhanden sein, um der relevanten Aufsichtsbehörde die Datenschutzverletzung innerhalb von 72 Stunden nach Bekanntwerden zu melden, selbst wenn noch nicht alle Einzelheiten vorliegen.
- Das Unternehmen muss wissen, welche Informationen über eine Datenschutzverletzung an die relevante Aufsichtsbehörde gemeldet werden müssen.
- Es muss ein Prozess vorhanden sein, um betroffene Personen über eine Verletzung zu informieren, wenn diese wahrscheinlich ein hohes Risiko für deren Rechte und Freiheiten bedeutet.
- Betroffene Personen müssen unverzüglich informiert werden.
- Das Unternehmen muss wissen, welche Informationen über die Verletzung den betroffenen Personen bereitgestellt werden müssen und wie es sich selbst vor den Auswirkungen schützen kann.
- Alle Datenschutzverletzungen müssen dokumentiert werden, selbst wenn keine Meldung erforderlich ist[1].

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

DAFÜR SORGEN, DASS MITARBEITER IHRE ROLLEN VERSTEHEN

Bisweilen wird angenommen, dass ausschließlich der benannte Datenschutzverantwortliche in einem Unternehmen für den Schutz von Daten zuständig ist. In Wirklichkeit spielen aber alle Mitarbeiter eine Rolle dabei, für die Einhaltung der Richtlinien im Unternehmen zu sorgen. Selbst alltägliche Aufgaben wie das Senden einer E-Mail können zu einer Datenschutzverletzung führen, wenn beispielsweise personenbezogene Daten versehentlich an einen Empfänger geschickt werden, für den keine Einwilligung zum Einsehen der Daten vorliegt.

Daher müssen Unternehmen unbedingt eine positive Unternehmenskultur fördern und alle Mitarbeiter dabei unterstützen, am Schutz von personenbezogenen Daten mitzuwirken.

Zu diesem Zweck ist gute Kommunikation sehr wichtig, angefangen bei einfachen Maßnahmen wie E-Mail-Bulletins bis hin zu gezielten Schulungen und Workshops. Außerdem sollten Unternehmen unbedingt sicherstellen, dass sich die Mitarbeiter ihrer Verantwortung für den Datenschutz bewusst sind und wissen, welche Aktivitäten Risiken für eine Datenschutzverletzung bergen und wie sie reagieren sollten, wenn sie ihrer Meinung nach zu einer solchen Verletzung beigetragen haben.

Die Kommunikation beim Fuhrparkmanagement kann besonders problematisch sein, da die Mitarbeiter häufig unterwegs sind. Daher sollten Unternehmen erwägen, welche Art der Kommunikation am besten ist. Nachrichten könnten zum Beispiel über die Driver Terminals im Fahrzeug an den Mitarbeiter gesendet werden. Alternativ könnte ein Leitfaden erstellt werden, der in allen Fahrzeugen mitgeführt wird. All dies kann im Rahmen eines strukturierten, methodischen Ansatzes für den Datenschutz unter Beachtung von Best Practices erfolgen, wodurch Unternehmen in einer starken Position sind, um die Vorschriften einzuhalten.

Auch wenn der Aufwand erheblich sein mag, sollten Zeit und Ressourcen dafür bereitgestellt werden, angemessene Systeme einzurichten und fortlaufend deren dauerhaftes Funktionieren sicherzustellen.

Weiterhin ist es überaus wichtig, mit Lieferanten zusammenzuarbeiten, die die gleichen hohen Standards in Sachen Datenschutz umsetzen. Daher müssen möglicherweise vorhandene Beziehungen zu Lieferanten, mit denen Daten geteilt werden, überprüft werden. Ziel ist es zu gewährleisten, dass der Verwendungszweck der Daten explizit vereinbart wurde. Zu einem Best-Practice-Ansatz gehört auch, die einzelnen Verwendungsbedingungen in diesen Vereinbarungen schriftlich darzulegen.

SO KANN WEBFLEET SOLUTIONS **SIE BEI IHREN DSGVO-VERPFLICHTUNGEN UNTERSTÜTZEN**

Als Fuhrparkbetreiber haben Sie vielleicht das Gefühl, bei den komplexen Bestimmungen der DSGVO den Überblick zu verlieren.

Die neuen Regeln sollten zwar als Erweiterung und Bekräftigung der vorhandenen Gesetze zu Datenschutz und Datensicherheit betrachtet werden, aber die Verantwortungslast hat sich sicherlich erhöht.

Die Vorschriften nicht zu erfüllen, ist keine Alternative. Dabei müssen nicht nur die Beziehungen zwischen Fuhrparkbetreibern und ihren Fahren genauer unter die Lupe genommen werden, sondern auch die Beziehungen zwischen Betreibern (Datenverantwortlichen) und Auftragsverarbeitern – insbesondere Telematikanbietern.

Unternehmen müssen sich sicher sein können, dass ihr Telematiksystem die neuen Regelungen erfüllt und sie nicht Gefahr laufen, aufgrund von Verletzungen in den Bereichen Datenschutz und Datensicherheit Strafen zahlen zu müssen.

Webfleet Solutions richtet sich bereits seit der Veröffentlichung des ersten Entwurfs im Jahr 2012 nach den Anforderungen der DSGVO. Daher wurden die neuen Regeln bei der Entwicklung von Lösungen für unsere Kunden eingehend berücksichtigt. Sie können also beruhigt sein, dass wir alle möglichen Schritte unternommen haben, damit Sie in den besten Händen sind.

INFORMATIONSSICHERHEIT IST UNERLÄSSLICH

Die Implementierung des Datenschutzes sowohl bereits in der Designphase als auch innerhalb der Voreinstellungen verstärkt die Datensicherheit und ist ein wesentlicher Bestandteil der DSGVO.

Sie sind von vornherein verpflichtet, technische und betriebliche Maßnahmen zu implementieren, um aufzuzeigen, dass der Datenschutz in Ihre Aktivitäten zur Datenverarbeitung integriert ist.

Somit werden Technologieentwickler in die Pflicht genommen, den Datenschutz direkt beim Produktdesign zu berücksichtigen. Webfleet Solutions fungiert als Auftragsverarbeiter für die personenbezogenen Daten unserer Kunden und richtet sich bereits seit der Veröffentlichung der ersten Entwürfe der DSGVO im Jahr 2012 nach diesen Bestimmungen. Unten wird erläutert, wie wir dies mit unseren Lösungen erreichen, die durch unseren Datenschutzbeauftragten kontrolliert und geprüft werden.

ZERTIFIZIERTE DATENSICHERHEIT

Wir haben äußerst strenge Vorschriften in Bezug auf Datenschutz und Datensicherheit und befolgen Best Practices, um höchste Standards zu gewährleisten. Der Nachweis hierfür ist die Zertifizierung nach ISO/IEC 27001:2013, die Webfleet Solutions verliehen wurde und die alle Mitarbeiter befolgen müssen.

Unser Information Security Management System (ISMS) umfasst sämtliche kritische Unternehmensprozesse, um die Informationsbestände bezüglich der Webfleet Solutions-Serviceplattform zu sichern. Gemäß dem Standard ISO/IEC 27001:2013 umfasst dies die Bereiche Architektur, Engineering, Qualitätssicherung und IT-Services sowie die Standorte unserer sicheren Rechenzentren innerhalb der Europäischen Union. **Die sichere, verschlüsselte Anmeldung und Datenübertragung an unsere Serviceplattform erfüllen die höchsten Standards der EV SSL-Verschlüsselung (Extended Validation SSL Certificate).**

Unsere sicheren Codierungsprinzipien und -prozesse sorgen für einen flexiblen Produktlebenszyklus. Diese gelten für Entwurf und Codierung nach dem Vier-Augen-Prinzip, Stilrichtlinien, Funktions-/Lasttests bei der Qualitätssicherung, Veröffentlichungs- und Änderungsmanagement sowie statische Codeüberprüfungen.

Daneben haben wir die folgenden Programme eingeführt: Sicherheitsschulung für unsere Mitarbeiter, Sicherheitstests- und -prüfungen auf Implementierungsebene, Systemabhärtung, Schwachstellen-/Patchmanagement, Sicherheitstests für Webanwendungen.

Unser ISMS-Team (Information Security Management System) überprüft regelmäßig die rechtlichen und Sicherheitsanforderungen, die sich auf unsere Telematik-Plattform oder unsere IT-Ressourcen auswirken könnten.

Unser Managementsystem zur Informationssicherheit umfasst:

- **Detaillierte Sicherheitsrichtlinien**, die das Informationsmanagement-System und alle betrieblichen Aktivitäten mit konkreten Vorgaben unterstützen.
- **HR-Sicherheitsprotokolle**, beispielsweise zur Auswahl der richtigen Mitarbeiter und für die Bereitstellung kontinuierlicher und individueller Schulungen.
- **Assetmanagement-Kontrollen**, die Inventarisierung, Verantwortlichkeitszuweisung und Pflege während des gesamten Assetlebenszyklus umfassen, um eine ordnungsgemäße Kategorisierung, Kennzeichnung und Zuordnung von Risikoeignern sicherzustellen. Dies beinhaltet den sicheren Umgang mit betriebseigenem geistigen Eigentum und Kundendaten.
- **Zugriffskontrollen**, bei denen der Zugriff nach dem „Need-to-have“- und dem „Need-to-know“-Prinzip erfolgt. Der nicht autorisierte Zugriff wird zudem durch weitere Kontrollmechanismen verhindert.
- **Verschlüsselungstechnologien**, um die Vertraulichkeit und Integrität der Daten unserer Kunden und unserer operativen Systeme zu schützen.
- **Physische und Umgebungssicherheit**, welche Rechenzentren des Typs Tier3+ umfasst, eine aktive Konfiguration, die regelmäßig getestete Funktionen zur Notfallwiederherstellung und Hochverfügbarkeit bietet.
- **Betriebliche Sicherheit**, gestützt durch Sicherheitsrichtlinien und untermauert durch gemanagte, strikte und wiederholbare Prozesse.
- **Kommunikationssicherheit** durch Maßnahmen wie Netzwerkisolierung, VLAN-Trennung, DMZ mit mehrstufigen Firewalls, Netzwerkzugriffskontrollen (Network Access Controls, NAC) und standardmäßige Verschlüsselung nach den neuesten Industriestandards.

IHRE FAHRERDATEN – IHRE ENTSCHEIDUNG

Da sich die Telematikdaten auf Ihre Fahrer beziehen, treffen Sie die Entscheidung, wie und zu welchem Zweck diese Daten verwendet werden dürfen.

Wir haben eng mit Datenschutzgruppen und Betriebsräten zusammengearbeitet, um unser Engagement für die Privatsphäre der Fahrer in die Tat umzusetzen. Um dafür zu sorgen, dass alle mit der Verwendung ihrer Daten einverstanden sind, stellen wir umfangreiches Erläuterungsmaterial wie Online-Handbücher und Schulungsmaterialien zur Verfügung. Der Zugriff darauf erfolgt über die Supportinformationen und Benutzerhandbücher unter Explore WEBFLEET im Kundenportal von Webfleet Solutions.

Darüber hinaus ist die Webfleet Solutions-Lösung hochgradig konfigurierbar, sodass Sie entscheiden können, welche Daten wann erfasst und wie lange sie aufbewahrt werden.

DATENSPEICHERUNG UND DATENAUFBEWAHRUNG

Gemäß der DSGVO müssen Sie dokumentieren, welche personenbezogenen Daten Sie speichern, woher diese Daten stammen und an wen Sie diese weitergeben.

Die Webfleet Solutions Service-Plattform bietet Standardoptionen für die Datenspeicherung, die auf typischen Kundenanforderungen beruhen, aber angepasst werden können.

Textnachrichten, Auftrags- und Fahrzeugstatusmeldungen, Positions-Datenspuren sowie Daten zu Fahrmanövern und Tempoverstößen werden automatisch 90 Tage lang gespeichert. Tourdaten werden zusätzlich zum aktuellen Jahr für zwei volle Kalenderjahre gespeichert. Archivierte Reports werden 36 Monate lang gespeichert.

Alle durch Webfleet Solutions verarbeiteten Daten werden in sauerstoffreduzierten Rechenzentren mit doppelter Redundanz gespeichert.

DATENSCHUTZ UND DATENZUGRIFF

In Übereinstimmung mit der DSGVO wird Webfleet Solutions auf die Einhaltung der Datenschutzrichtlinien kontrolliert und geprüft.

Der Zugriff auf WEBFLEET ist nur mit einem registrierten Zugangsnamen, Benutzernamen und Passwort möglich. Gemäß den Anforderungen der DSGVO ist der Zugriff auf alle WEBFLEET-Daten für Benutzer fast nie erforderlich oder angemessen.

Die für registrierte Benutzer verfügbaren Daten können folglich je nach deren spezifischen Informationsanforderungen eingeschränkt werden. Personalverantwortliche, Finance-Direktoren und Vertriebs- oder Verkaufsexperten benötigen für ihre jeweiligen Geschäftsfunktionen beispielsweise alle Zugriff auf unterschiedliche Daten.

Fahrer von Fahrzeugen, die mit unserer Fuhrparkmanagement-Lösung ausgestattet sind, können zwischen den Modi für geschäftliche Fahrten, Arbeitswege oder Privatfahrten umschalten, um die Fahrzeugortung zu aktivieren bzw. zu deaktivieren.

Webfleet Solutions unterstützt seine Kunden auch dabei, den Rechten von betroffenen Personen in Bezug auf den Datenzugang und die Datenlöschung nachzukommen.

Bei einer Datenlöschung werden die Daten als dereferenziert markiert und überschrieben, um die Datenwiederherstellung durch andere Parteien zu verhindern.

Webfleet Solutions wurde auf die Einhaltung von Datenschutzrichtlinien überprüft.

ZEHN FRAGEN, DIE SIE IHREM TELEMATIKANBIETER STELLEN SOLLTEN

Wir haben erläutert, wie Webfleet Solutions Sie beim Einhalten der Bestimmungen unterstützen kann. Stellen Sie sicher, dass Ihr bevorzugter Anbieter Sie dabei unterstützt, gesetzeskonform zu handeln.

1. **Fungieren Sie als Auftragsverarbeiter oder Datenverantwortlicher gemäß der DSGVO?**
2. **Erfüllt Ihr System die Anforderungen der DSGVO sowie internationale Standards für Datensicherheit und Datenschutz?**
3. **Welche Art von Daten speichern Sie?**
4. **Wo und für wie lange werden die personenbezogenen Daten von Fahrern gespeichert?**
5. **Haben Kunden Kontrolle darüber, wie lange Daten gespeichert werden?**
6. **Bietet Ihr System eine Benutzerverwaltung, bei der der Datenzugriff auf Personen beschränkt wird, die ihn wirklich benötigen?**
7. **Können personenbezogene Daten in Ihrem System gelöscht werden?**
8. **Werden Kundendaten an Drittanbieter weitergeleitet?**
9. **Sind die Fahrer in der Lage, ihre Privatsphäre bei privaten Fahrten zu schützen?**
10. **Stellen Sie Ihren Kunden Kommunikationsmaterialien bereit, die diese mit ihren Fahrern teilen können und die darlegen, wie deren personenbezogene Daten verwendet werden?**

webfleet solutions