webfleet



Die Datenschutz-Grundverordnung

BRIDGESTONE
Solutions for your journey

„Große Mengen an Flottendaten gehen unvermeidlich mit Risiken in Sachen Datensicherheit und Datenschutz einher.“



HAFTUNGSAUSSCHLUSS: Die in der Webfleet-Dokumentation und im Internet enthaltenen Informationen dienen nur zu Informationszwecken und geben lediglich unsere Position zu dem jeweiligen Thema wieder. Diese Angaben dürfen nicht als Rechtsberatung zu diesem Thema betrachtet werden. Darüber hinaus entsprechen die in diesen Dokumenten und im Internet enthaltenen Informationen möglicherweise nicht den neuesten rechtlichen Entwicklungen. Daher sollten Sie diese Informationen ohne einschlägige Rechtsberatung nicht als Grundlage für Entscheidungen wählen.

Die Nutzung und der Austausch von Flotteninformationen durch Unternehmen wird für einen sicheren und effizienten Geschäftsbetrieb immer wichtiger.

Große Mengen an Flottendaten, die zu einem großen Teil mit Telematik-Anwendungen generiert und verwaltet werden, gehen unvermeidlich mit Risiken in Sachen Datensicherheit und Datenschutz einher. Durch die Einführung der EU-Datenschutz-Grundverordnung (DSGVO) stehen diese Risiken nunmehr im Fokus.

Die meisten Anforderungen der DSGVO sind bereits gesetzlich verankert, so dass die DSGVO für Unternehmen, die bereits nach bewährten Verfahren vorgehen, unserer Meinung nach weitgehend als „business as usual“ betrachtet werden kann.

Flottenbetreiber und ihre Lieferketten müssen dafür Sorge tragen, dass sie über die Infrastruktur, die Verfahren und das richtige Bewusstsein verfügen, um Verstöße gegen die DSGVO zu vermeiden. Die Folgen von Verstößen gegen die DSGVO können schwerwiegend sein. Webfleet berücksichtigt die Datenschutz-Grundverordnung (DSGVO) sehr genau, denn Datensicherheit und Datenschutz bilden einen wesentlichen Teil der Beratungs- und Unterstützungsleistungen, die wir unseren Kunden anbieten.

Im Folgenden erläutern wir, was die DSGVO für Ihr Unternehmen und Ihren Fuhrpark bedeuten könnte, und bieten praktische Hinweise dazu, wie Sie sich rechtskonform verhalten.

Jan-Maarten,

President Fleet Management Solutions

Bridgestone Mobility Solutions

Die DSGVO im Überblick

Unsere digitale Welt ist eine ganz andere als die, in der wir lebten, als die EU-Datenschutzrichtlinie im Jahr 1995 eingeführt wurde.

Zwar sind die Grundprinzipien dieser Richtlinie nach wie vor gültig, doch wurde die Richtlinie durch Einführung der DSGVO umfassend aktualisiert. Durch die am 25. Mai 2018 in Kraft getretene DSGVO werden die Datenschutzvorschriften in ganz Europa harmonisiert, damit alle EU-Bürger ausreichend geschützt sind.

Im Wesentlichen geht es um den Schutz von personenbezogenen Daten. Dabei handelt es sich um solche, welche sich auf eine "identifizierte oder identifizierbare natürliche Person beziehen".

Somit ist die Datenschutz-Grundverordnung für Flottenbetreiber von besonderer Bedeutung, denn Flottenbetreiber müssen häufig auf Fahrerdaten zugreifen oder diese verwalten.

Die neuen Vorschriften sind jedoch nicht als vollständige Überarbeitung der bislang geltenden Datenschutzvorschriften zu betrachten, sondern vielmehr als Erweiterung der bestehenden Vorschriften und Verfahren, die die Unternehmen derzeit anwenden.

> Durch die DSGVO werden die Datenschutzvorschriften in ganz Europa harmonisiert, damit alle EU-Bürger ausreichend geschützt sind.



WELCHE ÄNDERUNGEN ERGEBEN SICH AUS DER DSGVO FÜR DEN DATENSCHUTZ IM ZUSAMMENHANG MIT DER TELEMATIK?

Es gibt mehrere wichtige Änderungen im Rahmen der DSGVO eingeführten Datenschutzvorschriften, die ggf. besondere Auswirkungen auf das Flottenmanagement und den Einsatz von Telematik haben.

1 **DER MENSCH STEHT IM MITTELPUNKT.** Ein zentrales Element der DSGVO besteht darin, den betroffenen Personen die Kontrolle zu geben. Es gilt, die Menschen, deren Daten erhoben werden, umfassend darüber zu informieren, welche Daten verwendet werden, warum sie verwendet werden, wie lange sie verwendet werden und von wem sie verwendet werden. Die betroffenen Personen können ihre Zustimmung erteilen oder verweigern und (mit einigen Einschränkungen) verlangen, dass die Verwendung ihrer Daten eingestellt wird.

2 **RISIKOBEWERTUNG UND PRÜFPFAD.** Bei der Verwendung von personenbezogenen Daten müssen die Unternehmen das Risiko des Datenmissbrauchs bewerten und mindern. Außerdem müssen sie dokumentieren, wie die Daten verwendet werden und welche Maßnahmen zur Einhaltung der Vorschriften getroffen werden.

3 **BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN.** Die DSGVO verpflichtet Unternehmen zur Benennung eines Datenschutzbeauftragten, wenn das Unternehmen bestimmte Arten von Verarbeitungstätigkeiten durchführt. Ein solcher Fall liegt beispielsweise vor, wenn die Kerngeschäftstätigkeit des Unternehmens eine groß angelegte, regelmäßige und systematische Überwachung von Personen erfordert. Weitere Kriterien sind in dem vorliegenden Dokument aufgeführt.

4 **REGULIERUNG DURCH AUFSICHTSBEHÖRDE.** Unternehmen, die in verschiedenen europäischen Ländern tätig sind, insbesondere solche, deren Fahrzeuge zwischen mehreren Ländern verkehren, unterliegen jetzt einem einzigen Regelwerk und müssen sich nur noch mit einer einzigen Regulierungsbehörde auseinandersetzen, nämlich der des Landes, in dem sie ihren Sitz haben.

5 **STRENGERE SICHERHEITSANFORDERUNGEN.** Personenbezogene Daten sind nun gegen unbefugte Nutzung jeder Art geschützt, wobei eine Bewertung der Sensibilität der Daten zugrunde gelegt wird. Die von einem Telematiksystem gelieferten GPS-Standortdaten können sehr sensibel sein, da sie ggf. viel über die betroffene Person verraten.

6 **HÖHERE GELDSTRAFEN BEI VERSTÖSSEN.** Laut Datenschutz-Grundverordnung beträgt die Höchststrafe für Verstöße 20 Mio. Euro bzw. vier Prozent des Umsatzes, je nachdem, welcher Betrag höher ist.



WELCHE FUNKTIONEN KENNT DIE DSGVO?

Die DSGVO kennt die (für die Datenverarbeitung) „Verantwortlichen“ und die „Auftragsverarbeiter“. In den meisten Fällen ist ein Unternehmen der Verantwortliche, während seine Lieferanten als Auftragsverarbeiter gelten. Die vollständigen Definitionen beider Begriffe lauten wie folgt:

- Ein **Auftragsverarbeiter** ist eine Organisation, die personenbezogene Daten im Auftrag eines (für die Datenverarbeitung) Verantwortlichen verarbeitet. Webfleet gilt als Auftragsverarbeiter für alle personenbezogenen Daten, die von Kunden und Partnern über unsere Systeme und Plattformen bereitgestellt werden.

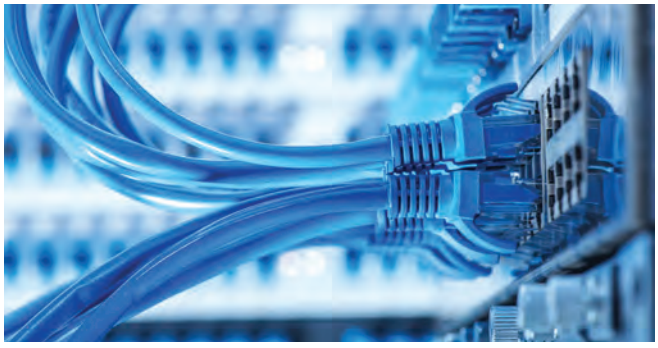
- Ein **Verantwortlicher** ist eine Organisation, die die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten festlegt. Wenn es beispielsweise um die Flottendaten geht, die von unserer Software-as-a-Service (SaaS)-Flottenmanagementlösung Webfleet bereitgestellt werden, gilt das Unternehmen als Verantwortlicher, da das Unternehmen entscheidet, wie diese Daten verwendet werden – zum Beispiel, um die Sicherheit seiner Mitarbeiter im Straßenverkehr zu gewährleisten.

Eine der wichtigsten Änderungen an den durch die DSGVO eingeführten Vorschriften, besteht darin, dass nun auch die Verarbeiter die Vorschriften einhalten müssen, während die Verantwortung bisher allein bei den Verantwortlichen lag.

WAS SIND IHRE PFLICHTEN?

Die Hauptaufgaben von Unternehmen sind in den Datenschutzgrundsätzen der DSGVO festgelegt. Personenbezogene Daten müssen:

- Rechtmäßig, in fairer Art und Weise und transparent verarbeitet werden;
- Für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- Angemessen, sachdienlich und auf das beschränkt sein, was zur Erreichung der Zwecke, für die sie verarbeitet werden, erforderlich ist;
- Zutreffend und ggf. auf dem neuesten Stand sein. Es sind alle zumutbaren Maßnahmen zu treffen, um sicherzustellen, dass unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden;
- In einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, und zwar nur so lange, wie dies für die Erfüllung des Zwecks der Datenverarbeitung erforderlich ist;
- Angemessen und sicher verarbeitet werden.





WELCHE ARTEN VON PERSONENBEZOGENEN DATEN FALLEN UNTER DIE DSGVO?

Eine „betroffene Person“ im Sinne der DSGVO kann mittelbar oder unmittelbar identifiziert werden. Personenbezogene Daten können alles sein, vom Namen einer Person bis hin zu Daten, die mit eindeutigen Identifikatoren verbunden sind, wie z. B. ein Kfz-Kennzeichen oder eine Fahrzeugidentifikationsnummer (VIN). Wenn die betroffene Person anhand der Daten identifiziert werden kann, gelten diese Daten als personenbezogene Daten, und zwar auch dann, wenn eine solche Identifizierung nicht erfolgt.

Die Arten von personenbezogenen Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen, können sowohl Meinungen als auch Tatsachen umfassen und können Informationen aller Art umfassen, von Daten über die Arbeitsleistung über die Einstellungsunterlagen bis hin zu Gesprächsnotizen.

Anonymisierte Daten fallen nicht in den Anwendungsbereich der Datenschutz-Grundverordnung, wenn es aufgrund der getroffenen Vorkehrungen unmöglich oder nicht praktikabel ist, personenbezogene Daten einer identifizierbaren Person zuzuordnen.

Für die Weitergabe von sensiblen personenbezogenen Daten, d. h. von „personenbezogenen 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“ ist die ausdrückliche Zustimmung der betroffenen Person erforderlich.



RECHTSGRUNDLAGE FÜR DIE DATENVERARBEITUNG

Zur Verarbeitung von personenbezogenen Daten muss ein gültiger rechtmäßiger Grund vorliegen, und der Verwendungszweck muss im Voraus festgelegt werden.

Die vielleicht offensichtlichste Rechtsgrundlage ist die ausdrückliche Zustimmung der Person, deren Daten verarbeitet werden. Dies kann jedoch problematisch sein, wenn die betroffene Person bei dem Unternehmen beschäftigt ist, da es in diesem Fall schwierig ist nachzuweisen, dass die Zustimmung freiwillig erteilt wurde.

Daher kommen auch andere Rechtsgrundlagen für die Verarbeitung von Daten in Frage; ganz gleich, welche Rechtsgrundlage Sie wählen, der entsprechende Grund muss stets eindeutig dokumentiert werden.



- **ZUSTIMMUNG**
  In diesem Fall muss eine Person aus freien Stücken ihre Zustimmung zur Verarbeitung ihrer Daten für einen bestimmten Zweck geben. Die Zustimmungserklärung muss eindeutig sein, sie darf nicht abgeleitet werden und kann jederzeit widerrufen werden.
- **BERECHTIGTE INTERESSEN**
  In diesem Fall müssen Sie oder ein Dritter ein berechtigtes Interesse an der Datenverarbeitung haben, das nicht mit den Grundrechten der betroffenen Person kollidiert.
- **VERTRAGSERFÜLLUNG**
  Diese Rechtsgrundlage ist gegeben, wenn die Daten im Rahmen eines mit der betreffenden Person geschlossenen oder zu schließenden Vertrages erhoben und verarbeitet werden müssen.
- **GESETZLICHE VERPFLICHTUNG**
  Die Daten können verarbeitet werden, wenn dies notwendig ist, damit Sie Ihren gesetzlichen Verpflichtungen nachkommen.
- **LEBENSWICHTIGE INTERESSEN**
  Eine Bearbeitung von Daten kann auch dann erfolgen, wenn dies zum Schutz des Lebens einer Person erforderlich ist.
- **ÖFFENTLICHE AUFGABEN**
  In diesem Fall muss die Datenverarbeitung zur Wahrnehmung einer gesetzlichen Aufgabe im öffentlichen Interesse erforderlich sein.



Flottenbetreiber haben im Allgemeinen ein berechtigtes Interesse oder eine Vertragsgrundlage für die Verarbeitung von personenbezogenen Daten.

Bei Flottenbetreibern kann sich das berechtigte Interesse auf so unterschiedliche Bereiche wie die Verarbeitung von Kilometerständen im Zusammenhang mit Leasingverträgen, die Erhebung von Kraftstoffverbrauchsdaten zur Verhinderung von Betrug oder die Erfassung von Daten über das Fahrerverhalten zum Schutz der Gesundheit und Sicherheit der Fahrer beziehen.

Zu den vertraglichen Gründen für die Verarbeitung von Daten gehören beispielsweise die Verwendung von Telematikdaten zur Erfassung der Arbeits- und Lenkzeiten der Fahrer. Diese Rechtsgrundlage ist ggf. im Arbeitsvertrag geregelt.

Dabei ist zu beachten, dass die betroffene Person ein „Recht auf Vergessenwerden“ hat und dementsprechend die Löschung ihrer Daten verlangen kann. Dies kann der Fall sein, wenn die betroffene Person ihre Zustimmung zur Datenverarbeitung widerruft, wenn die Daten für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind, oder wenn die betroffene Person Widerspruch gegen die Datenverarbeitung einlegt und kein berechtigtes Interesse die Fortsetzung der Datenverarbeitung rechtfertigt.



ZWECKE DER DATENVERARBEITUNG

Gemäß der Datenschutz-Grundverordnung muss der Zweck der Datenverarbeitung im Voraus klar dargelegt werden. Der genannte Zweck muss konkret und klar definiert sein, damit die betroffene Person ihn leicht nachvollziehen kann.

TELEMATIKDATEN KÖNNEN UNTER ANDEREM ZU FOLGENDEN ZWECKEN VERARBEITET WERDEN:

- Verfolgung von Fahrzeugen zur Gewährleistung der Sicherheit und zur Flottenoptimierung.
- Überwachung des Fahrverhaltens zur Verbesserung der Fahrsicherheit und zur Senkung der Kraftstoffkosten.
- Kommunikation mit den Fahrern zur Verbesserung von Arbeitssicherheit und Arbeitseffizienz.
- Verwendung von Fahrtenschreiberdaten und Lenkzeiten zur Einhaltung der Arbeitszeit.
- Managementberichte für die Prozessoptimierung (Verbesserung von Kundendienst oder Flotteneffizienz).
- Integration mit der Hardware- oder Softwarelösung eines Drittanbieters.

WER TRÄGT VERANTWORTUNG?

Jeder Mitarbeiter eines Unternehmens trägt für Datenschutz Verantwortung, denn Datenschutzverstöße können an verschiedenen Stellen innerhalb der Lieferkette und in unterschiedlicher Form auftreten.

Dennoch ist es angebracht, eine bestimmte Person oder ein Team einzusetzen, dass für Datenschutz zuständig ist. So lässt sich sicherstellen, dass die Prozesse zur Einhaltung der Datenschutzvorschriften im Unternehmen korrekt umgesetzt werden.



Es ist unwahrscheinlich, dass der Bereich „Flottenmanagement“ eines Unternehmens die Hauptverantwortung für die Einhaltung der Datenschutzvorschriften trägt. Es ist aber durchaus möglich, dass ein Flottenmanager in anderer Weise einen entscheidenden Beitrag zum Datenschutz leistet, bspw. dadurch, dass er:

- Lieferantenbeziehungen steuert und dafür sorgt, dass entsprechende Verträge bestehen;
- Sich vergewissert, dass es eine Rechtsgrundlage für die Verwendung von Daten über Fahrer oder Mitarbeiter des Flottenmanagements gibt;
- Bei Bedarf die Zustimmung der Teammitglieder einholt;
- Mit dem Personal und den wichtigsten Akteuren des Flottenmanagements kommuniziert und dafür sorgt, dass sie wissen, was ihre Aufgaben sind;
- Die für einen Compliance-Prüfpfad erforderlichen Informationen bereitstellt, z. B. Verträge und Zustimmungserklärungen.

Auf organisatorischer Ebene kann die Hauptverantwortung einem eigens dafür eingesetzten Datenschutzbeauftragten zugewiesen werden, aber auch die Abteilungen Personal, operative Prozesse und IT spielen in vielen Fällen eine wichtige Rolle in diesem Prozess.



Entwicklung eines Maßnahmenplans

Bei Flottenbetreibern kommen zahlreiche unterschiedliche Daten zusammen, woraus ein besonders hohes Risiko im Rahmen der DSGVO resultiert.

Vor diesem Hintergrund kann es für ein Unternehmen sinnvoll sein, in einem ersten Schritt eine umfassende Risikobewertung durchzuführen, die dazu beiträgt, sich ein detailliertes Bild von den verschiedenen Teilen der Lieferkette zu machen, über die Daten ausgetauscht werden, und mögliche Schwachstellen zu ermitteln, an denen die Wahrscheinlichkeit eines Verstoßes besonders hoch ist.

Danach können geeignete Maßnahmen zur Beseitigung bzw. Minderung der ermittelten Risiken getroffen werden.

In bestimmten Fällen schreibt die Datenschutz-Grundverordnung eine solche Risikobewertung vor. Sie wird als Datenschutz-Folgenabschätzung bezeichnet.

Eine Datenschutz-Folgenabschätzung ist besonders dann wichtig, wenn ein Unternehmen einen neuen Datenprozess, ein neues System oder eine neue Technologie einführt. Eine Datenschutz-Folgenabschätzung kann aber auch dazu verwendet werden, die Verantwortlichkeit im Rahmen der DSGVO nachzuweisen und einem Unternehmen dabei zu helfen, die Vorschriften einzuhalten und nachzuweisen, dass geeignete Vorkehrungen getroffen wurden, um die Einhaltung der Datenschutzvorschriften dauerhaft zu gewährleisten.

Bei Flottenbetreibern kommen zahlreiche unterschiedliche Daten zusammen, woraus ein besonders hohes Risiko im Rahmen der DSGVO resultiert.



Nach der Datenschutz-Grundverordnung ist eine Datenschutz-Folgenabschätzung erforderlich, wenn die Datenverarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat“. Dies gilt insbesondere für folgende Fälle:

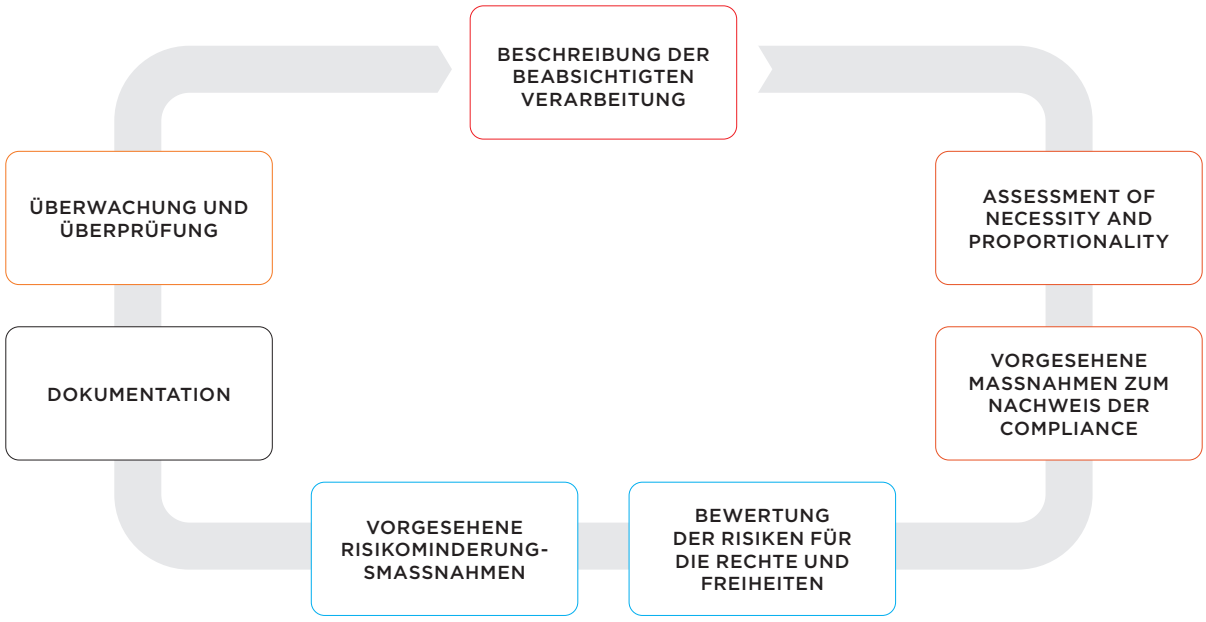
- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die auf automatisierter Verarbeitung einschließlich Profiling gründet;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten;
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Diese drei Bedingungen treffen auf einen großen Teil der Flottendaten zu, z. B. auf den Einsatz von Telematik-Technologien zur Überwachung von Fahrern, was als systematische Überwachung der Arbeitnehmer an ihrem Arbeitsplatz angesehen werden kann.

Die gemeinsamen europäischen Datenschutzbehörden haben Leitlinien für die Anforderungen an eine erfolgreiche Datenschutzfolgenabschätzung erstellt, doch die Grundsätze können auch durch einen Best-Practice-Ansatz zum Schutz von personenbezogenen Daten erfüllt werden.

Mit den folgenden Maßnahmen lassen sich die Datenschutzvorschriften einfacher einhalten:

- Erfassung aller Datenströme
- Analyse der Lieferketten
- Abschluss geeigneter Verträge
- Einrichtung eines Verfahrens zur Bearbeitung von Datenanfragen
- Notfallplan zum Umgang mit Datenschutzverstößen
- Aufklärung der Mitarbeiter über ihre Aufgabe





ERFASSUNG ALLER DATENSTRÖME

Ein nützlicher Ausgangspunkt für die Durchführung einer ausreichenden Risikobewertung ist die Erfassung aller Datenströme in der Lieferkette.

Dazu sind die verschiedenen ein- und ausgehenden Datenströme sowie die sonstigen an diesen Transaktionen beteiligten Personen oder Unternehmen zu dokumentieren.

Eine visuelle Darstellung der Datenströme kann hilfreich sein, um die verschiedenen Teile der Lieferkette zügig zu analysieren.

In jedem Fall sollte ermittelt werden, wer der Verantwortliche und wer der Auftragsverarbeiter ist. Anschließend ist zu prüfen, ob die entsprechenden Vereinbarungen geschlossen wurden.

Im Ergebnis erhält das Unternehmen einen guten Überblick darüber, wie gut es auf die Einführung der DSGVO vorbereitet ist und wo ggf. noch Handlungsbedarf besteht.

TYPISCHE DATENSTRÖME BEI FLOTTENBETREIBERN

Flottenbetreiber müssen eine große Anzahl von Datenströmen verarbeiten, sowohl innerhalb als auch außerhalb des Unternehmens. Beispiele für unternehmensfremde Akteure, mit denen sensible personenbezogene Daten ausgetauscht werden können, sind:

- Telematik- und andere Softwareanbieter
- Leasinggesellschaften
- Autohändler
- Versicherer
- Anbieter von Risikomanagementleistungen
- Anbieter von Unfallmanagementleistungen
- Kfz-Zulassungsstellen
- Werkstätten
- Tankkartenanbieter





ANALYSE DER LIEFERKETTEN

Unternehmen können für Verstöße in ihrer gesamten Lieferkette zur Rechenschaft gezogen werden. Daher ist es wichtiger denn je, dafür zu sorgen, dass alle Lieferanten, die sensible Daten verarbeiten, dazu nachweislich sichere Verfahren anwenden.

Jeder Auftragsverarbeiter, der bei der Erfassung der Datenströme ermittelt wird, sollte in der Lage sein, ausreichende Garantien dafür zu bieten, dass die Anforderungen der DSGVO erfüllt und die Rechte der betroffenen Personen gewahrt werden.

Das Gleiche gilt für alle potenziellen neuen Lieferanten. Dabei ist es wichtig, einen klaren Prüfpfad für alle Fälle zu erstellen, in denen personenbezogene Daten verarbeitet werden. Ferner ist zu beachten, dass diese Lieferanten eventuell mit eigenen Lieferanten zusammenarbeiten, die die betreffenden Daten eventuell ebenfalls verwenden.

> Unternehmen können für Verstöße in der gesamten Lieferkette zur Rechenschaft gezogen werden

ABSCHLUSS GEEIGNETER VERTRÄGE

Für jeden Datenstrom ist zu ermitteln, ob eine neue Einwilligung erforderlich ist, um zu gewährleisten, dass die Transaktion die Anforderungen der DSGVO erfüllt.

Wurde beispielsweise der Zweck der Nutzung von Telematikdaten in der Vergangenheit klar definiert, bspw. Senkung der Treibstoffkosten, Verbesserung der Sicherheit oder ein anderer Zweck? Ist dies nicht der Fall, sollte dies korrigiert werden, um dem Mitarbeiter klar zu machen, warum die Verarbeitung von personenbezogenen Daten erforderlich ist.

Wenn ein Verantwortlicher einen Auftragsverarbeiter einsetzt, muss ein schriftlicher Vertrag geschlossen werden, in dem die Nutzungsbedingungen festgelegt sind. Ein solcher Vertrag sorgt außerdem dafür, dass beide Parteien ihre Aufgaben und Pflichten kennen. In der DSGVO wird dargelegt, welche Punkte in einem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter geregelt sein sollten.





EINRICHTUNG EINES VERFAHRENS ZUR BEARBEITUNG VON DATENANFRAGEN

Gemäß der DSGVO hat eine betroffene Person ein Recht auf Zugang zu ihren personenbezogenen Daten, die von einem Unternehmen gespeichert werden. Bei Telematikdaten kann es sich dabei um Standort- und Fahrtinformationen, Kilometerstände oder Statistiken zum Fahrverhalten und viele andere Datenkategorien handeln.

Macht eine Person von ihrem Auskunftsrecht Gebrauch, so muss ihr mitgeteilt werden, welche Daten gespeichert sind und ob sie verarbeitet werden. Diese Angaben müssen spätestens innerhalb eines Monats nach Eingang des Verlangens bereitgestellt werden, wobei diese Frist bei komplexen oder bei zahlreichen Anfragen um zwei weitere Monate verlängert werden kann.

Zur Einhaltung der Datenschutzvorschriften sind die Unternehmen gut beraten, ein klares Verfahren für die Bearbeitung derartiger Anfragen festzulegen. Dies kann die Zuweisung von Zuständigkeiten unter den Mitarbeitern und die Überprüfung der Identität der antragstellenden Person umfassen.

Außerdem sollten die Daten leicht zugänglich sein. Im Zusammenhang mit Telematikdiensten kann dies bedeuten, dass Ihr Unternehmen mit einem Anbieter zusammenarbeitet, der leicht zugängliche, aber dennoch umfassende Berichte liefert, aus denen hervorgeht, welche Daten über jeden Mitarbeiter gespeichert sind.

Ihr Unternehmen kann beispielsweise auch eine spezielle E-Mail-Adresse einrichten, an die Anfragen gerichtet werden können. Zu den best practices zählen auch Selbstbedienungssysteme, bei denen die antragstellende Person direkten Remote-Zugriff auf ihre Daten hat.



> Macht eine Person von ihrem Auskunftsrecht Gebrauch, so muss ihr mitgeteilt werden, welche Daten gespeichert sind und ob sie verarbeitet werden.



NOTFALLPLAN ZUM UMGANG MIT DATENSCHUTZVERSTÖSSEN

Auch wenn ein Unternehmen zahlreiche Risikominderungsmaßnahmen getroffen hat, muss es über ein Verfahren zum Umgang mit Datenschutzverstößen verfügen.

Ein Datenschutzverstoß kann in folgender Form gegeben sein:

- Zugriff auf personenbezogene Daten durch Unbefugte
- Vorsätzlicher oder versehentlicher Datenschutzverstoß durch einen Verantwortlichen oder einen Auftragsverarbeiter
- Übermittlung von personenbezogenen Daten an einen falschen Empfänger
- Verlust oder Diebstahl von Datenverarbeitungsgeräten, auf denen personenbezogene Daten vorliegen
- Änderung von entsprechenden personenbezogenen Daten ohne Genehmigung
- Verlust der Verfügbarkeit von personenbezogenen Daten

Es empfiehlt sich, solide Verfahren zur Aufdeckung, Untersuchung und internen Meldung von Datenschutzverstößen einzuführen. Derartige Verfahren tragen dazu bei, dass eine fundierte Entscheidung darüber getroffen werden kann, ob ein Verstoß so schwerwiegend ist, dass er der zuständigen Aufsichtsbehörde gemeldet werden muss, was nach Möglichkeit innerhalb von 72 Stunden geschehen muss. Besteht ein hohes Risiko, dass durch den Datenschutzverstoß die Rechte und Freiheiten von Personen beeinträchtigt werden, so ist auch die betroffene Person zu benachrichtigen.

Zur Unterstützung dieses Prozesses können die Mitarbeiter darin geschult werden, woran ein Datenschutzverstoß zu erkennen ist und bei welcher Stelle im Unternehmen sie Datenschutzverstöße melden können.

CHECKLISTE ZUM UMGANG MIT DATENSCHUTZVERSTÖSSEN

Folgende Anforderungen sind zu erfüllen, um auf Datenschutzverstöße sachgerecht reagieren zu können:

- Einrichtung eines Verfahren zur Bewertung der Risiken, die aufgrund von potenziellen Datenschutzverstößen zu Lasten von betroffenen Personen bestehen
- Dokumentation, welche Aufsichtsbehörde für die Datenverarbeitung durch Ihr Unternehmen zuständig ist
- Einrichtung eines Verfahrens, mit dem die zuständige Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden eines Datenschutzverstoßes benachrichtigt wird, auch wenn noch nicht alle Einzelheiten bekannt sind.
- Information der Mitarbeiter darüber, welche Angaben zu dem Datenschutzverstoß, gegenüber der zuständigen Aufsichtsbehörde, zu machen sind
- Einrichtung eines Verfahrens, mit dem die betroffenen Personen über einen Datenschutzverstoß informiert werden, wenn sich aus dem Datenschutzverstoß ein hohes Risiko für ihre Rechte und Freiheiten ergibt
- Betroffenen Personen unverzüglich in Kenntnis setzen
- Information der Mitarbeiter darüber, welche Angaben gegenüber einer betroffenen Person über einen Datenschutzverstoß zu machen sind und welche Hinweise man ihnen dazu geben kann, wie sie sich vor den Folgen des Datenschutzverstoßes schützen können
- Dokumentation aller Datenschutzverstöße, selbst wenn sie nicht meldepflichtig sind.[1]

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



AUFKLÄRUNG DER MITARBEITER ÜBER IHRE AUFGABEN

Manchmal herrscht der Glaube vor, dass der Datenschutz allein in der Verantwortung des im Unternehmen dafür eingesetzten Verantwortlichen liegt. Doch tatsächlich können alle Mitarbeiter einen Beitrag dazu leisten, dass das Unternehmen die Datenschutzvorschriften einhält. Selbst alltägliche Vorgänge wie das Versenden einer E-Mail können zu einem Datenschutzverstoß führen, wenn personenbezogene Daten versehentlich an jemanden gesendet werden, der nicht die Erlaubnis hat, sie einzusehen.

Daher ist es wichtig, eine positive Unternehmenskultur zu fördern und alle Mitarbeiter für den Schutz von personenbezogenen Daten zu sensibilisieren.

Dabei kann Kommunikation einen wichtigen Beitrag leisten, bspw. durch einfache Maßnahmen wie E-Mail-Bulletins an die Mitarbeiter oder gezielte Schulungen und Workshops. Ein Unternehmen sollte auch dafür sorgen, dass seine Mitarbeiter sich ihrer Verantwortung für den Datenschutz bewusst sind, alle mit Datenschutzrisiken behafteten Vorgänge kennen, und wissen, wie sie sich verhalten sollten, wenn sie den Eindruck haben, dass sie zu einem Datenschutzverstoß beigetragen haben.

Im Flottenmanagement stellt die Kommunikation mitunter eine besondere Herausforderung dar, da die Mitarbeiter viel Zeit auf der Straße verbringen. Daher ist es sinnvoll, sich Gedanken darüber zu machen, wie die Kommunikation am besten erfolgt. So können über die Fahrerterminals in den Fahrzeugen Nachrichten an die Mitarbeiter gesendet oder ein kurzes Handbuch, das in jedem Fahrzeug mitgeführt wird, erstellt werden. Dies alles kann Teil eines strukturierten, methodischen Ansatzes für den Datenschutz sein. Dabei können Unternehmen durch die Umsetzung von best practices gute Voraussetzungen für die Einhaltung der Datenschutzvorschriften schaffen.

Zwar kann dies ein umfangreiches Unterfangen sein, doch sollten unbedingt Zeit und Ressourcen aufgewendet werden, damit die entsprechenden Systeme eingerichtet und kontinuierlich auf ihre Eignung hin überprüft werden.

Ebenso wichtig ist die Zusammenarbeit mit Lieferanten, die dieselben hohen Datenschutzstandards erfüllen. Bei bereits bestehenden Lieferantenbeziehungen sollte überprüft werden, ob ausdrücklich vereinbart wurde, wofür die Daten verwendet werden dürfen. Zu den best practices zählt auch der Abschluss von schriftlichen Vereinbarungen, in denen die spezifischen Nutzungsbedingungen festgelegt werden.

> Sie sollten als Unternehmen eine positive Unternehmenskultur fördern und alle Mitarbeiter für den Schutz von personenbezogenen Daten sensibilisieren.



Wie Webfleet Ihnen helfen kann, Ihre Pflichten aus der DSGVO zu erfüllen

Für Flottenbetreiber ist die Erfüllung der DSGVO eine komplexe Herausforderung.

Zwar stellen die neuen Vorschriften lediglich eine Erweiterung und Verstärkung bestehender Vorschriften zu Datensicherheit und Datenschutz dar, doch insgesamt hat sich die Verantwortung, die Unternehmen tragen, sicherlich erhöht.

Die DSGVO zu ignorieren ist keine Option. Die neue Verordnung hat nicht nur die Beziehung zwischen Flottenbetreibern und Fahrern in den Mittelpunkt gerückt, sondern auch die Beziehung zwischen Verantwortlichen und Auftragsverarbeitern, darunter nicht zuletzt Telematikanbieter.

Die Unternehmen müssen sich darauf verlassen können, dass ihr Telematiksystem nicht gegen die neuen Vorschriften verstößt, so dass sie bei Verstößen gegen den Datenschutz und die Datensicherheit mit Strafen belegt werden.

Seit die ersten Entwürfe für die DSGVO 2012 veröffentlicht wurden, arbeitet Webfleet daran, die Anforderungen der Datenschutz-Grundverordnung zu erfüllen. Daher wurde bei der Entwicklung der Lösungen, die wir unseren Kunden anbieten, die Regulierung besonders berücksichtigt. Sie können also sicher sein, dass wir alle notwendigen Maßnahmen getroffen haben, um zu gewährleisten, dass Sie in Sachen Datenschutz auf der sicheren Seite sind.

> Webfleet erfüllt die Anforderungen der DSGVO bereits seit 2012



INFORMATIONSSICHERHEIT GEHT UNS ALLE AN

Der Grundsatz, dass Datenschutz durch technische Maßnahmen und geeignete Voreinstellungen erreicht wird, unterstreicht die Bedeutung von Datenschutz und Datensicherheit und ist integraler Bestandteil der Datenschutz-Grundverordnung.

So ist Ihr Unternehmen von Anfang an dazu verpflichtet, technische und organisatorische Vorkehrungen zu treffen, um nachzuweisen, dass der Datenschutz Teil Ihrer Datenverarbeitungsprozesse ist.



Die DSGVO verpflichtet die Entwickler von Technologien, den Schutz der Privatsphäre bereits in ihrem Produktdesign zu berücksichtigen. Da Webfleet Auftragsverarbeiter für die personenbezogenen Daten seiner Kunden ist, hat Webfleet seit der Veröffentlichung der ersten Entwürfe der DSGVO im Jahr 2012 intensiv daran gearbeitet, allen damit verbundenen Pflichten nachzukommen. Wie wir dies erreichen, möchten wir im Folgenden beschreiben.

AKKREDITIERTE DATENSICHERHEIT

Wir haben sehr strenge Regeln für Datenschutz und Datensicherheit und setzen auf *best practices*, um sicherzustellen, dass wir die höchsten Standards einhalten. Belegt wird dies durch die Zertifizierung nach ISO/IEC 27001, die Webfleet erreicht hat und deren Anforderungen von allen Mitarbeitern erfüllt werden müssen.

Unser Managementsystem für die Informationssicherheit (ISMS) umfasst alle unsere kritischen Geschäftsprozesse, die zur Sicherung der Informationswerte im Zusammenhang mit der WEBFLEET Service Platform erforderlich sind. Dazu zählen gemäß der Norm ISO/IEC 27001 die Bereiche Architektur, Technik, Qualitätssicherung und IT-Dienste sowie unsere sicheren Rechenzentren in der Europäischen Union. **Die sichere, verschlüsselte Anmeldung und Datenübertragung zu unserer Serviceplattform entspricht den höchsten Standards der EV SSL-Verschlüsselung (Extended Validation SSL Certificate).**



Dabei gewährleisten unsere sicheren Kodierungsprinzipien und -prozesse einen agilen Produktlebenszyklus. Dieser umfasst Peer Reviews für Design und Kodierung, Stilrichtlinien, Funktions- und Lasttests im Rahmen der Qualitätssicherung, ein systematisches Release- und Änderungsmanagement sowie statische Codeprüfungen.

Darüber hinaus setzen wir auf Sicherheitsschulungen für unsere Mitarbeiter, Sicherheitstests und -überprüfungen auf Implementierungsebene, Maßnahmen zur Systemhärtung, die Behebung von Schwachstellen und die Einführung von Patches sowie Sicherheitstests für Webanwendungen.

Unser ISMS-Team führt regelmäßige Überprüfungen von rechtlichen oder sicherheitsrelevanten Anforderungen durch, die sich auf unsere Telematikplattform oder Informationswerte auswirken könnten.

Unser ISMS umfasst folgende Elemente:

- Detaillierte Sicherheitsrichtlinien, die die Richtung vorgeben und das ISMS sowie alle betrieblichen Maßnahmen unterstützen;
- Sicherheitsprotokolle für das Personalwesen mit Hinweisen zur Auswahl der richtigen Mitarbeiter sowie zu kontinuierlichen, individuellen Schulungen;
- Kontrollmechanismen für das Asset Management. Dazu zählen die Inventarisierung, Überwachung und Wartung der Vermögenswerte während des gesamten Lebenszyklus, um eine ordnungsgemäße Kategorisierung, Kennzeichnung und Zuweisung zu Risikoverantwortlichen zu gewährleisten. Dazu gehört auch der sichere Umgang mit dem geistigen Eigentum des Unternehmens sowie mit Kundendaten.
- Eine Zugangssteuerung nach dem Prinzip der minimalen Rechtevergabe und dem Grundsatz, dass jeder Mitarbeiter nur Zugang zu den Vermögenswerten hat, die er für die Erfüllung seiner Aufgaben unbedingt benötigt. Zusätzliche Kontrollmechanismen tragen dazu bei, dass unbefugte Zugriffe verhindert werden.
- Kryptotechnologien, die die Vertraulichkeit und Integrität der Daten unserer Kunden und unserer operativen Systeme schützen.
- Physische und Umgebungssicherheit mit Tier3+-Rechenzentren, einer aktiven Konfiguration mit Notfallwiederherstellung sowie regelmäßig getestete Hochverfügbarkeitsfunktionen.
- Operative Sicherheit auf der Grundlage von Sicherheitsgrundsätzen und präzise gesteuerten, wiederholbaren Prozessen.
- Kommunikationssicherheit durch Maßnahmen wie Netzwerktrennung, VLAN-Trennung, DMZ mit mehrstufigen Firewalls, Network Access Controls (NAC) und Verschlüsselung nach den neuesten Branchenstandards.



FAHRERDATEN – SIE ENTSCHEIDEN

Da sich die Telematikdaten auf Ihre Fahrer beziehen, entscheiden Sie, wie und zu welchem Zweck sie verwendet werden.

Wir haben mit Datenschutzinitiativen, Betriebsräten und Gewerkschaften zusammengearbeitet und damit unter Beweis gestellt, dass wir den Schutz der Privatsphäre Ihrer Fahrer sehr ernst nehmen. Damit alle Beteiligten mit der Verwendung ihrer Daten vertraut sind, stellen wir umfangreiches Erklärungsmaterial zur Verfügung, darunter Online-Handbücher und Schulungsunterlagen. Diese können über die Explore Webfleet Support-Informationen und Nutzerhandbücher auf unserem Webfleet-Kundenportal abgerufen werden.

Darüber hinaus ist die Webfleet-Lösung granular konfigurierbar, so dass Sie entscheiden können, welche Daten wann und wie lange gesammelt werden.



DATENSPEICHERUNG UND -AUFBEWAHRUNG

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

Die WEBFLEET Service Platform bietet Standardoptionen für die Datenspeicherung, die auf typischen Kundenanforderungen beruhen, aber angepasst werden können.

Textnachrichten, Aufträge, Fahrzeugstatusmeldungen, Positionsdaten sowie Daten zu Fahrten und Geschwindigkeitsüberschreitungen werden automatisch 90 Tage lang gespeichert. Die Reisedaten werden nicht nur für das laufende Jahr, sondern für zwei volle Kalenderjahre gespeichert. Die archivierten Berichte werden bis zu 36 Monate lang gespeichert.

Alle von Webfleet verarbeiteten Kundendaten werden redundant in Rechenzentren gespeichert, die sich in sauerstoffarmen Bunkern befinden.



DATENSCHUTZ UND DATENZUGANG

Webfleet unterliegt Kontrollen und Audits, mit denen gewährleistet wird, dass Webfleet die Anforderungen der DSGVO erfüllt.
Der Zugang zu Webfleet ist nur mit einem registrierten Konto, dem Nutzernamen und dem zugehörigen Passwort möglich. Der Zugang zu allen Webfleet-Daten für alle Nutzer wird nur selten notwendig oder verhältnismäßig sein, so wie es in der DSGVO vorgesehen ist.

Art und Umfang der den registrierten Nutzern zur Verfügung stehenden Daten können somit auf der Grundlage ihres konkreten Informationsbedarfs eingeschränkt werden. Ein Personalmanager, der Leiter des Rechnungswesens, ein Vertriebsmitarbeiter und ein Prozessverantwortlicher benötigen beispielsweise alle Zugang zu unterschiedlichen Informationen, um ihre jeweiligen Aufgaben erledigen zu können.

Die Fahrer von Fahrzeugen, die mit unserer Flottenmanagementlösung ausgestattet sind, können zwischen den Modi für Betriebs-, Pendler- und Privatfahrten wechseln, um die Ortung ihres Fahrzeugs zu aktivieren oder zu deaktivieren.

Webfleet unterstützt seine Kunden auch bei der Wahrung der Auskunfts- und Löschrechte von betroffenen Personen.

Bei einer Datenlöschung werden die Daten als dereferenziert markiert und überschrieben, um zu verhindern, dass sie von Unbefugten wiederhergestellt werden können.



Webfleet unterliegt Kontrollen und Audits, mit denen gewährleistet wird, dass Webfleet die Datenschutzvorschriften erfüllt.

ZEHN FRAGEN, DIE SIE IHREM TELEMATIKANBIETER STELLEN SOLLTEN

Wir haben dargelegt, wie Webfleet Sie bei der Erfüllung Ihrer Datenschutzpflichten unterstützt – vergewissern Sie sich, dass Ihr bevorzugter Anbieter Ihnen hilft, sich rechtskonform zu verhalten.

1. **Sind Sie Auftragsverarbeiter oder Verantwortlicher im Sinne der DSGVO?**
2. **Ist Ihr System DSGVO-konform und entspricht es den internationalen Datensicherheits- und Datenschutzstandards?**
3. **Welche Arten von Daten werden bei Ihnen gespeichert?**
4. **Wo und wie lange werden die personenbezogenen Daten der Fahrer gespeichert?**
5. **Können die Kunden steuern, wie lange die Daten gespeichert werden?**
6. **Bietet Ihr System eine Nutzerverwaltung, die den Datenzugriff so einschränkt, dass nur diejenigen Zugriff haben, die die Daten auch wirklich benötigen?**
7. **Ist mit Ihrem System die Löschung von personenbezogenen Daten möglich?**
8. **Werden Kundendaten an Dritte weitergegeben?**
9. **Können die Fahrer ihre Privatsphäre bei privaten Fahrten schützen?**
10. **Stellen Sie Ihren Kunden Kommunikationsmaterial zur Verfügung, das sie an die Fahrer weitergeben können, um ihnen zu erklären, wie ihre personenbezogenen Daten verwendet werden?**



webfleet



HAFTUNGSAUSSCHLUSS: Die in der Webfleet-Dokumentation und im Internet enthaltenen Informationen dienen nur zu Informationszwecken und geben lediglich unsere Position zu dem jeweiligen Thema wieder. Diese Angaben dürfen nicht als Rechtsberatung zu diesem Thema betrachtet werden. Darüber hinaus entsprechen die in diesen Dokumenten und im Internet enthaltenen Informationen möglicherweise nicht den neuesten rechtlichen Entwicklungen. Daher sollten Sie diese Informationen ohne einschlägige Rechtsberatung nicht als Grundlage für Entscheidungen wählen.

BRIDGESTONE
Solutions for your journey