Foto: Jürgen Fälchle/AdobeStock

Stichtag 25. Mai 2018 | Bis dahin muss es eine Dokumentation der Datenverarbeitung im Fuhrpark und Pflichtinformationen für Fahrzeugnutzer geben

Keine Zeit verlieren

Neues europäisches Datenschutzrecht | Im Mai 2018 wird die europäische Datenschutz-Grundverordnung wirksam und ersetzt das Bundesdatenschutzgesetz. Für Fuhrparkverantwortliche hat das weitreichende Folgen.

Die neue Datenschutzverordnung ist in der EU verbindlich von allen Unternehmen und – mit wenigen Ausnahmen – auch von Behörden zu beachten. Ziel der europäischen Datenschutz-Grundverordnung (DS-GVO oder DSGVO) ist ein einheitliches Datenschutzrecht für ganz Europa, in dem es nur wenige nationale Besonderheiten gibt.

In Deutschland tritt deshalb zum 25. Mai 2018 das Bundesdatenschutzgesetz (BDSG) außer Kraft und wird durch ein neues BDSG mit gänzlich anderen Inhalten ersetzt. Für Fuhrparkverantwortliche hat das weitreichende Folgen. Und schon jetzt besteht Handlungsbedarf: Wer noch nicht mit der Umsetzung begonnen hat, sollte keine weitere Zeit verlieren.

Grundsatz: Verbot mit Erlaubnisvorbehalt bleibt | Im Datenschutz gilt ein „Verbot mit Erlaubnisvorbehalt": Personenbezogene Daten dürfen nur verarbeitet werden, wenn es dafür eine ausdrückliche Erlaubnis gibt. Diese Erlaubnis kann sich aus einer Einwilligung der Betroffenen, einem Gesetz (heute z.B. das BDSG, zukünftig die DSGVO) oder einer Betriebs- oder Dienstvereinbarung ergeben. Daran ändert sich durch die DSGVO nichts.

Nach dem Gesetz ist eine Datenverarbeitung wie heute schon insbesondere zulässig, wenn diese zur Erfüllung eines Vertrags mit dem Betroffenen erforderlich ist (zum Beispiel Erfassung von Fahrstrecken für Kostenabrechnungen) oder das Unternehmen hieran ein berechtigtes, meist wirtschaftliches oder organisatorisches Interesse hat und die Persönlichkeitsrechte der Betroffenen nicht über Gebühr beeinträchtigt werden (Erfassung von Standortdaten via GPS zur Routenplanung in der Logistikbranche oder aus Sicherheitsgründen bei Werttransporten). Zudem stellen DSGVO und das neue BDSG ausdrücklich klar, dass Beschäftigte gegenüber ihrem Arbeitgeber wirksam in Datenverarbeitungen einwilligen können, wenn dies freiwillig und informiert geschieht (beispielsweise Verwendung von Fotos für Firmen-Website). Dies war bislang sehr strittig.

Beim Führerschein-Scan müssen nicht erforderliche Merkmale automatisch geschwärzt werden.

Achtung: Für die Beachtung des Datenschutzes ist nicht der Datenschutzbeauftragte verantwortlich, sondern das Unternehmen oder die Behörde selbst. Noch deutlicher als unter dem BDSG macht die DSGVO den Datenschutzbeauftragten zu einem Überwacher, der – vergleichbar mit der Revision – die Maßnahmen des Verantwortlichen zum Datenschutz prüft und bewertet, im Übrigen aber nur beratend tätig werden soll.

Datenverarbeiter sind damit gezwungen, in der Organisation auch die Verantwortlichkeit für den Datenschutz festzulegen. Das kann gegebenenfalls durch Delegation bei einem dezentralen Ansatz auch Aufgabe des Fuhrparkverantwortlichen sein, der aber die nötige Fachkunde besitzen muss.

Auch pseudonyme Daten sind personenbezogene Daten | Auch unter einer Kennziffer oder anderem Pseudonym verarbeitete Daten sind personenbeziehbar, wenn die Rückführung auf den Betroffenen möglich ist. Das war schon unter dem BDSG so und ändert sich mit der DSGVO nicht. Kennziffern liegen nicht nur bei Verarbeitung von Kfz-Kennzeichen oder Fahrzeug-Identifizierungsnummer (FIN) vor, sondern auch bei der Nutzung von Personalnummern, Bankverbindungen und anderen Kennungen. Auf solche pseudonymen Daten ist das Datenschutzrecht immer anzuwenden.

Nur bei anonymen Daten greift der Datenschutz nicht. Anonym sind Daten aber nur dann, wenn auch beim Hinzuspeichern weiterer Daten der Personenbezug nicht mehr hergestellt werden kann. Darunter fallen beispielsweise aggregierte Daten für sta-

tistische Zwecke. Beispiele: „Wann passieren bei uns im Fuhrpark die meisten Unfälle?", ist eine zulässige Auswertung ohne Personenbezug, während die Erstellung der „Top 10 der Unfallverursacher im Fuhrpark mit Schadenssumme nach Kennzeichen" für die Veröffentlichung im Intranet trotz Pseudonymisierung datenschutzrechtlich unzulässig ist.

Strengere Anforderungen an Dokumentation und Transparenz | Die Pflicht zum Verfahrensverzeichnis über alle Datenverarbeitungen gibt es heute schon. Das gilt auch für die Pflicht, angemessene technische und organisatorische Maßnahmen zu treffen, um Datenpannen zu vermeiden. Diese Pflichten werden durch die DSGVO deutlich erweitert: Zu den Schutzmaßnahmen gehört jetzt auch eine bislang nur aus der IT-Sicherheit bekannte Geschäftsfortführungsplanung für potenzielle Ausfälle von Systemen zur Datenverarbeitung sowie eine Bedarfsplanung zur fortlaufenden Prüfung der Wirksamkeit der getroffenen Maßnahmen.

Ergänzt werden diese nach innen gerichteten Pflichten zukünftig durch Informationspflichten gegenüber den Betroffenen: Jedes Unternehmen muss jederzeit die wesentlichen Details der Datenverarbeitungen den Betroffenen unentgeltlich und leicht verständlich zugänglich machen, zum Beispiel welche Daten warum über das Fahrverhalten aufgezeichnet werden. Dies kann durch Flyer in den Fuhrpark-Kfz geschehen, ebenso aber auch auf der Website oder im Intranet des Fuhrparkverantwortlichen.

Ebenso wichtig: Anders als bislang müssen die Aufsichtsbehörden im Datenschutz nicht nur über schwere Datenpannen informiert werden, sondern über jede Datenschutzverletzung, wenn diese – auch noch so unbedeutende – Auswirkungen auf Betroffene haben kann.

Neues Vergehen | Achtung: Die leicht feststellbaren Zuwiderhandlungen gegen die Dokumentations- und Informationspflichten sind unter der DSGVO Ordnungswidrigkeiten – das war unter dem BDSG nicht so. Die Bußgelder steigen von bis zu 300.000 Euro im Einzelfall auf bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten, gegebenenfalls konzernweiten Vorjahresumsatzes. Die Aufsichtsbehörden haben bereits angekündigt, intensiver zu prüfen und den Bußgeldkatalog auszureizen. Heute noch als Kavaliersdelikte geltende Formverstöße im Datenschutz können dann existenzbedrohend sein. Organisationsfehler sind schwere Compliance-Verstöße von Unternehmens- oder Fuhrparkleitung.

Datenschutz durch Technik und Datenschutz-Folgeabschätzung | Mit der DSGVO halten die Grundsätze „Data Protection by Design" und „Data Protection by Default" Einzug. Damit sind IT-Systeme zukünftig so zu konfigurieren, dass nur die zwingend erforderlichen personenbezogenen Daten verarbeitet werden; Zusatzfunktionen müssen optional aktivierbar sein. Außerdem ist bereits bei der Beschaffung von IT-Systemen und der Nutzung von Cloud-Services zu prüfen, ob diese überhaupt datenschutzkonform eingesetzt werden können.

Fuhrparks müssen das zukünftig zum Beispiel bei ihrer für die elektronische Führerscheinkontrolle oder das Fahrzeug- und Fahrermanagement eingesetzten Software beachten. Beispiel: Das Speichern eines kompletten Scans von Vorder- und Rückseite des Führerscheins ist für die Kontrolle nicht erforderlich – alle nicht erforderlichen Merkmale auf dem Führerschein müssten deshalb durch eine entsprechende Software automatisch geschwärzt werden.

Sascha Kremer | Fachanwalt für IT-Recht bei Login Partners, Pulheim, sowie externer Datenschutzbeauftragter, Datenschutzauditor und Lehrbeauftragter

Online-Dienste | Sehr wichtig ist das auch, wenn im Fuhrpark Premium- und Online-Dienste der Fahrzeughersteller genutzt werden (wie Park- und Routenservices oder Standortermittlung von Fahrzeugen).

Außerdem müssen zukünftig für Verfahren mit voraussichtlich hohen Risiken für die Daten der Betroffenen sogenannte Datenschutz-Folgeabschätzungen durch den Verantwortlichen durchgeführt werden, die über die bisherige Vorabkontrolle des Datenschutzbeauftragten deutlich hinausgehen.

Eine solche Folgenabschätzung ist immer zwingend erforderlich, wenn sensible Daten verarbeitet werden (zum Beispiel Gesundheitsdaten von Beschäftigten) oder Daten zum „Profiling" geeignet sind. Unter das Profiling fallen jedenfalls alle Daten, die zur Kontrolle von Leistung oder Verhalten eines Fahrers geeignet sind, etwa die regelmäßige Abfrage von Standortdaten oder die sonstige Auswertung des Fahrverhaltens.

Achtung: Die Datenschutz-Folgeabschätzung ist eine Risikobewertung, deren Ergebnisse zu dokumentieren sind. Weist eine Verarbeitung hohe Risiken auf, sind zusätzliche Maßnahmen zur Reduzierung der Risiken zu treffen, beispielsweise die Anonymisierung oder Pseudonymisierung bestimmter Daten.

Außerdem ist bei solchen Verarbeitungen zwingend die zuständige Datenschutzaufsicht zu konsultieren, damit diese Empfehlungen aussprechen kann. Hierbei sind die Verfahrensdokumentation und das Ergebnis der Folgeabschätzung vorzulegen. Auch so werden Fehler in der Datenschutz-Dokumentation (siehe oben) sichtbar und verfolgbar.

Schließlich verlangt die DSGVO ein Löschkonzept. Daten, die nicht mehr benötigt werden, sind zu löschen. Das ist immer der Fall, wenn es keine Erlaubnis für die weitere Speicherung mehr gibt, weil der Speicherzweck weggefallen ist. Den Betroffenen ist bereits bei Erhebung der Daten mitzuteilen, wann diese voraussichtlich gelöscht werden (zum Beispiel: „Wir löschen die Daten über die Nutzung unseres Fuhrparks durch Sie drei Jahre nach Ende des Kalenderjahres, in dem Sie als Beschäftigter bei uns ausgeschieden sind.").

Wichtig: Das BDSG hebt die Löschpflicht ausnahmsweise auf, wenn die Löschung der Daten technisch nicht möglich oder mit unverhältnismäßigem Aufwand verbunden ist. Diese Ausnahme entfällt mit der DSGVO.

Achtung: Auch Zuwiderhandlungen gegen die Pflichten im technischen Datenschutz und bei der Folgeabschätzung sind Ordnungswidrigkeiten mit Bußgeldern von bis zu zehn Millionen Euro oder bis zu zwei Prozent des weltweiten, gegebenenfalls konzernweiten Vorjahresumsatzes.

Fazit: verschärfte Pflichten | Die DSGVO verschärft die formalen Pflichten im Datenschutz deutlich, erhöht die Bußgelder um ein Vielfaches und führt zugleich neue, leicht feststellbare Bußgeldtatbestände ein.

Das betrifft unmittelbar auch Fuhrparkverantwortliche: Spätestens ab dem 25. Mai 2018 muss es eine den formalen Anforderungen entsprechende Dokumentation der Datenverarbeitungen im Fuhrpark geben. Außerdem müssen die Pflichtinformationen für die Nutzer bereitgestellt sein, damit sie die Datenverarbeitungen nachvollziehen können.

Ein Delegieren auf den Datenschutzbeauftragten ist nicht möglich. Dieser darf zwar beraten, aber muss am Ende prüfen, ob die Anforderungen der DSGVO richtig umgesetzt wurden. | *Sascha Kremer*