RECHT

Das neue Datenschutzrecht

Ein erster Überblick über die ab dem 25. Mai 2018 geltenden Regelungen

Stand: Oktober 2017

INHALT

A. Einleitung

Die **EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679; kurz: DS-GVO)** ist am 27. April 2016 in Kraft getreten und gilt nach Ablauf einer zweijährigen Übergangsfrist ab dem

25. Mai 2018

unmittelbar in allen europäischen Mitgliedstaaten. Ziel des europäischen Gesetzgebers ist es, mit dem Instrument einer Verordnung eine möglichst weitreichende Vereinheitlichung des Datenschutzrechts in der gesamten EU zu erreichen.

Die DS-GVO enthält an vielen Stellen sogenannte **Öffnungsklauseln**, die es den nationalen Gesetzgebern ermöglichen, die Regelungen der Verordnung zu konkretisieren und zu ergänzen. Auf Bundesebene ist dies durch das sogenannte Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (**Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU**) erfolgt, das zeitgleich mit der DS-GVO am 25. Mai 2018 zur Anwendung kommt. Mit diesem Gesetz wird u.a. das neue Bundesdatenschutzgesetz (**BDSG-neu**) in Kraft gesetzt.

Die neuen Datenschutzregelungen sind ausgesprochen umfangreich und komplex. Da das bisherige Bundesdatenschutzgesetz den Umgang mit personenbezogenen Daten in Deutschland bereits sehr detailliert und auf einem hohen Niveau geregelt hat, dürften die Konzepte und Prinzipien der DS-GVO und des BDSG-neu jedoch keine übermäßig großen Neuerungen darstellen. **Drastisch erhöht wurde indes der Bußgeldrahmen für Datenschutzverstöße**. Kfz-Betriebe sollten die Zeit bis zum 25. Mai 2018 daher nutzen, um ihre bisherige Datenschutzpraxis zu überprüfen und an die neuen gesetzlichen Vorgaben anzupassen.

Für die praktische Umsetzung des neuen Datenschutzrechts soll dieser Leitfaden den Kfz-Betrieben einen **ersten Überblick** geben. Der Leitfaden nimmt nicht für sich in Anspruch, das neue Recht vollumfänglich und im Detail darzustellen. Der Fokus liegt vielmehr auf den Änderungen zum bisherigen Recht, die für das Tagesgeschäft der Kfz-Betriebe relevant sein können. Der Leitfaden enthält zahlreiche Links auf öffentlich zugängliche Merkblätter und Praxisratgebern von Datenschutzbehörden und –organisationen, die eine vertiefende Auseinandersetzung mit dem jeweiligen Thema ermöglichen. **Keinesfalls ersetzt der Leitfaden jedoch die Notwendigkeit einer individuellen Prüfung der Einhaltung der Datenschutzvorschriften im Einzelfall.**

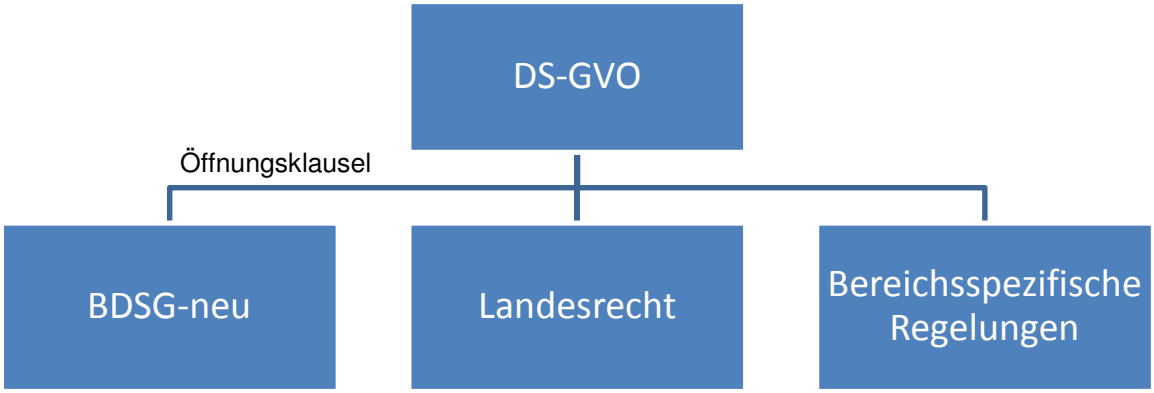
Mangels praktischer Erfahrungswerte und Rechtsprechung zum neuen Recht, ist der Leitfaden als **fortlaufendes, elektronisches Dokument** konzipiert. Dies gilt insbesondere auch für die Bereitstellung von **Mustern**, wie z.B. einer Einwilligungserklärung oder einer Muster-Verpflichtungserklärung für Mitarbeiter, die zum jetzigen Zeitpunkt noch nicht zur Verfügung stehen aber nachgereicht werden sollen.

B. Die Inhalte der DS-GVO und des BDSG-neu

I. Zusammenspiel von europäischer DS-GVO und nationalen Datenschutzvorschriften

Die DS-GVO gilt ab dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten. Einen gesonderten Umsetzungsakt bedarf es hierfür nicht.

Für die Anwendung der Datenschutzregelungen bedeutet dies, dass in einem **ersten Schritt** immer zunächst die Regelungen der DS-GVO zu prüfen sind. Nur für den Fall, dass die DS-GVO sogenannte **Öffnungsklauseln** enthält, ist in einem **zweiten Schritt** auf das BDSG-neu oder die allgemeinen Landesdatenschutzgesetze sowie bereichsspezifischen Regelungen auf Bundes- und Landesebene zurückzugreifen. Es empfiehlt sich daher insbesondere die DS-GVO und das BDSG-neu immer parallel zu lesen. Eine gute Übersicht zu den einzelnen Regelungen der DS-GVO nebst Zuordnung der BDSG-neu Vorschriften kann der GDD-Praxishilfe in den vertiefenden Hinweisen entnommen werden.



Vertiefende Hinweise:

Gesetzestext DS-GVO:
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

BDSG-neu (Datenschutz-Anpassungs- und Umsetzungsgesetz):
https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Neues-Bundesdatenschutzgesetz/BDSG-neu.pdf

GDD-Praxishilfe: Textausgabe DS-GVO mit Zuordnung des BDSG:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf

Maßnahmenplan zur Umsetzung der DS-GVO für Unternehmen:
https://www.lda.bayern.de/media/dsk_kpnr_8_massnahmenplan.pdf

II. Was ändert sich im Vergleich zum bisherigen Datenschutzrecht?

Nachfolgend werden die wesentlichen Änderungen bzw. Grundsätze dargestellt, die für Kfz-Betriebe besonders relevant sind. Auf eine Wiedergabe und Erläuterung sämtlicher neuen Vorgaben der DS-GVO wird verzichtet.

1. Neue Begriffsbestimmungen, Artikel 4 DS-GVO

Der Schutz der DS-GVO umfasst **personenbezogene Daten**. Hierzu zählen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen, Artikel 4 Nr. 1 DS-GVO. Für die Identifizierbarkeit einer betroffenen Person genügt die Möglichkeit zur indirekten, d.h. unter Nutzung von Zusatzwissen erfolgenden Identifizierung. Beispielhaft seien Online-Kennungen wie IP-Adressen, Cookie-Kennungen oder rein technische Daten (z.B. Status des Gurtstraffers) genannt, soweit zusätzliche Daten gespeichert werden, die eine Identifizierbarkeit ermöglichen. Der Begriff der personenbezogenen Daten wird also sehr weit verstanden.

Neu ist, dass der Begriff **„Verarbeitung“** zukünftig alle bisherigen Nutzungsformen (Erhebung, Verarbeitung, Nutzung) von personenbezogenen Daten umfasst. Es wird daher einheitlich nur noch von einer Verarbeitung von personenbezogenen Daten gesprochen.

2. Grundsätze für die Verarbeitung personenbezogener Daten, Artikel 5 DS-GVO

Auch unter dem neuen Datenschutzregime gelten gemäß Artikel 5 abs. 1 DS-GVO die allgemeinen Datenschutz-Grundsätze für eine rechtmäßige Datenverarbeitung fort, u.a.:

- **Transparenz:**

  Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

- **Zweckbindung und Zweckänderung:**

  Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Erhebung zu nicht bestimmten Zwecken, wie z.B. bei einer Vorratsdatenspeicherung, ist damit unzulässig.

  Eine Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden (**Zweckänderung**), ist nur zulässig, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, Artikel 6 Abs. 4 DS-GVO. Die betroffene Person ist vor einer Weiterverarbeitung der personenbezogenen Daten zu anderen Zwecken entsprechend zu informieren, Artikel 13 Absatz 3 DS-GVO iVm. § 32 BDSG-neu. § 24 BDSG-neu sieht zudem zwei Fälle vor, in denen nichtöffentliche

Stellen eine Datenverarbeitung vornehmen dürfen, auch wenn diese mit dem ursprünglichen Zweck nicht vereinbar ist. Hierbei handelt es sich um Zwecke der Gefahrenabwehr und der Verfolgung von Straftaten sowie der Geltendmachung, Ausübung und Verteidigung zivilrechtlicher Ansprüche.

Mit Erreichen des Zwecks besteht eine Löschungspflicht der personenbezogenen Daten.

- **Datenminimierung:**

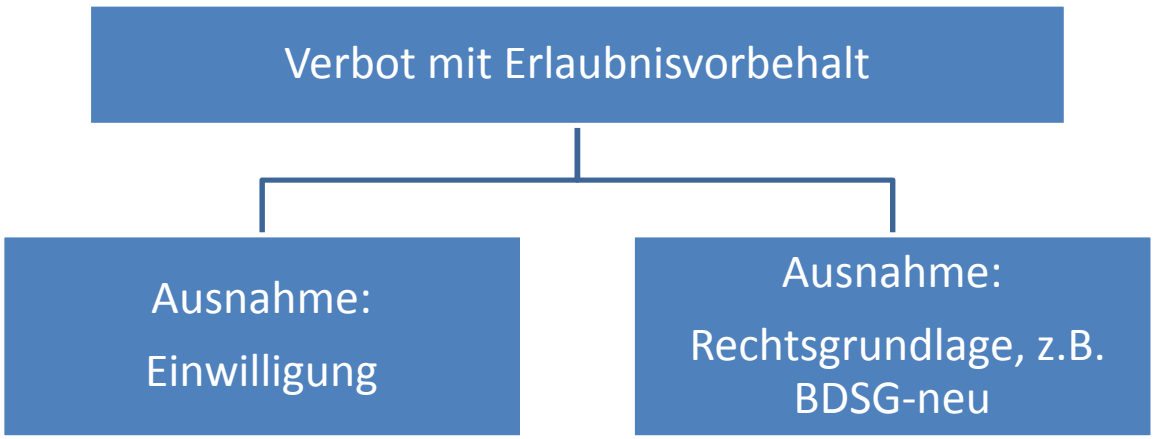
  Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

- **Richtigkeit:**

  Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

3. Rechtmäßigkeit der Datenverarbeitung, Artikel 6 DS-GVO

Der bisherige Grundsatz des **Verbots mit Erlaubnisvorbehalt** bleibt erhalten. Personenbezogene Daten dürfen also auch zukünftig nur verarbeitet werden, wenn die betroffene Person eingewilligt hat oder eine Rechtsgrundlage dies erlaubt.



Neben der Einwilligung des Betroffenen nennt Artikel 6 DS-GVO insbesondere folgende Zulässigkeitstatbestände für die Verarbeitung von personenbezogenen Daten:

- Verarbeitung zur Erfüllung eines Vertrags (z.B. im Rahmen einer Fahrzeugreparatur)
- Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen (z.B. Übersendung von Prospekten)
- Erfüllung rechtlicher Pflichten

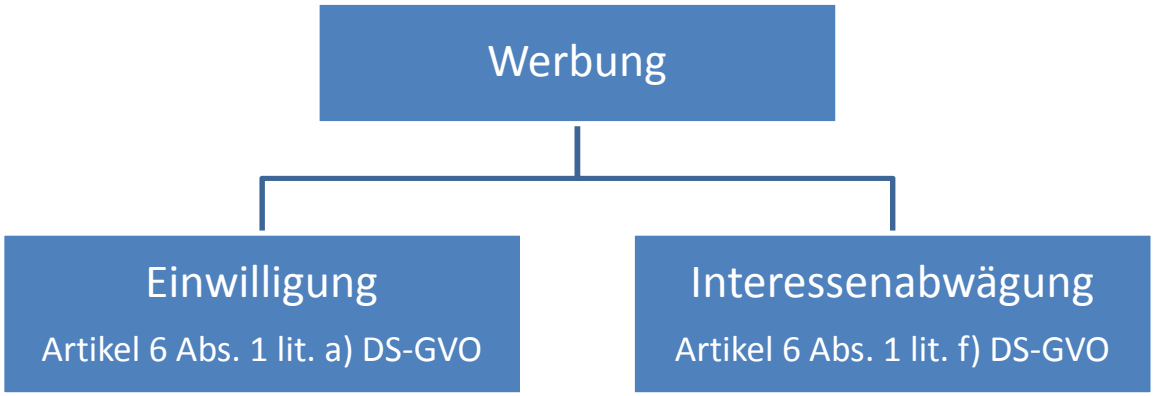
- Interessenabwägung (z.B. Werbemaßnahmen)

Für die Beurteilung der Rechtmäßigkeit einer Datenverarbeitung sind die Anforderungen der Artikel 5 und 6 DS-GVO kumulativ zu erfüllen.

4. Verarbeitung personenbezogener Daten für Werbung

Die bisherigen Regelungen im BDSG zur Werbung werden vollständig durch die DS-GVO ersetzt. Das bisherige Listenprivileg oder eine Privilegierung von Daten aus öffentlichen Verzeichnissen oder Quellen kennt die DS-GVO nicht. **Unangetastet bleiben hingegen die Regelungen des UWG, die für bestimmte Werbeformen, wie z.B. E-Mail, Telefon, Fax, SMS, regelmäßig eine vorherige ausdrückliche Einwilligung der betroffenen Person voraussetzen.** Noch nicht geklärt ist, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen für werbliche Ansprachen enthalten wird.

Grundsätzlich wird zukünftig jede Verarbeitung personenbezogener Daten zu Werbezwecken an den allgemeinen Zulässigkeitstatbeständen des Artikel 6 Abs. 1 DS-GVO zu messen sein. Eine Datenverarbeitung zu Werbezwecken ist hiernach zulässig, wenn eine **Einwilligung** des Betroffenen vorliegt **oder** das Ergebnis einer **Interessenabwägung** zugunsten des Werbenden ausfällt.



Beachte: Alle Werbemaßnahmen müssen **zusätzlich** die Vorgaben des **§ 7 UWG** erfüllen.

a) Interessenabwägung

Gemäß Artikel 6 Abs. 1 lit. f) DS-GVO ist eine Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich der betreffenden Person um ein Kind handelt.

Erwägungsgrund 47 DS-GVO konkretisiert ein berechtigtes Interesse des Verantwortlichen und stellt grundsätzlich klar, **dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann**. Hierbei sind u.a. die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen (z.B. die betroffene Person ist ein Kunde des Kfz-Betriebs). Um dem Transparenzerfordernis der DS-GVO zu genügen, sollte der Kunde bei **erstmaliger Datenerhebung allerdings auf die Möglichkeit einer späteren Direktwerbung hingewiesen werden**.

Da die DS-GVO das bislang im BDSG geregelte **Listenprivileg** nicht kennt, ist die Zulässigkeit der Datennutzung zu Werbezwecken zukünftig nicht mehr auf die Nutzung abschließend gesetzlich vorgegebener Datenkategorien beschränkt. Ebenso ist der sogenannte **Adresshandel** nicht mehr explizit in der DS-GVO geregelt. Für diesen gilt ebenfalls Artikel 6 Abs. 1 lit. f) DS-GVO. Für beide Fallkonstellationen gilt es, die weitere rechtliche Entwicklung abzuwarten.

Wird auf Grundlage einer Interessenabwägung Werbung betrieben, hat die betroffene Person das Recht, jederzeit **Widerspruch** gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke der Werbung einzulegen, § 21 Abs. 2 DS-GVO. Über dieses Recht ist die betroffene Person **spätestens zum Zeitpunkt der ersten Kommunikation**, also der Werbemaßnahme, **zu informieren**, § 21 Abs. 4 DS-GVO.

Trotz der Möglichkeit zur Durchführung von Werbemaßnahmen auf Grundlage einer Interessenabwägung, sollten Kfz-Betriebe zur Vermeidung von Rechtsunsicherheiten und Rechtsnachteilen die Einholung von (möglichst) schriftlichen Einwilligungserklärungen ihrer Kunden vorziehen.

b) Einwilligung

Die Einwilligung zur Verarbeitung personenbezogener Daten muss für einen oder mehrere bestimmte Zwecke abgegeben werden, Artikel 6 Abs. 1 lit. a) DS-GVO.

Gemäß der Definition in Artikel 4 Nr. 11 DS-GVO ist die Einwilligung jede

- freiwillig,
- für einen bestimmten Fall,
- in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Stillschweigen, **bereits angekreuzte Kästchen** oder **Untätigkeit** der betroffenen Person stellen **keine Einwilligung** dar (siehe Erwägungsgrund Nr. 32 DS-GVO). Wenn die Verarbeitung

der personenbezogenen Daten **mehreren Zwecken** dient, muss für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.

Die Einwilligung muss **nicht** mehr in **Schriftform** abgegeben werden. Sie kann z.B. auch elektronisch oder mündlich erklärt werden. Der Verantwortliche muss allerdings **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. **Für Kfz-Betriebe empfiehlt es sich daher auch zukünftig, möglichst schriftlich erteilte Einwilligungserklärungen ihrer Kunden einzuholen.**

Sofern die Einwilligungserklärung zusammen mit anderen Erklärungen abgegeben werden soll, muss sie gemäß Artikel 7 Abs. 2 DS-GVO **besonders hervorgehoben** werden.

Die betroffene Person kann ihre Einwilligung jederzeit **widerrufen** und ist in der Einwilligungserklärung auf diese Widerrufsmöglichkeit hinzuweisen, Artikel 7 Abs. 3 DS-GVO.

Es gilt ein **Kopplungsverbot.** Sofern die Einwilligung für einen Vertrag oder eine Dienstleistung verlangt wird, die für die Erfüllung des Vertrags nicht erforderlich ist, so gilt diese als im Zweifel nicht freiwillig erteilt, Artikel 7 Abs. 4 DS-GVO (Abkehr vom bisherigen „take it or leave it“-Prinzip).

Bislang erteilte Einwilligungserklärungen gelten fort, sofern sie der Art nach den Bedingungen der DS-GVO entsprechen (Erwägungsgrund Nr. 171). Dies dürfte bei den bisher von den Kfz-Betrieben eingeholten Einwilligungserklärungen regelmäßig der Fall sein (zum Bestandsschutz siehe die nachfolgenden vertiefenden Hinweise). Es empfiehlt sich jedoch, die bisherigen Einwilligungserklärungen sukzessive gegen Erklärungen nach neuem Recht auszutauschen. Hierzu sind die verwendeten Datenschutzerklärungen inhaltlich an die neuen Vorgaben der DS-GVO, insbesondere an die Informationspflichten gegenüber den Betroffenen (siehe nachfolgende Ziffer 5), anzupassen. Eine Muster-Einwilligungserklärung nach neuem Recht liegt noch nicht vor.

c) Übersicht der Werbeformen gemäß § 7 UWG

Neben den Voraussetzungen der DS-GVO zur Verarbeitung von personenbezogenen Daten zu Werbezwecken, sind auch weiterhin die Vorgaben des UWG zu beachten. Hierzu kann weiterhin auf den ZDK-Leitfaden „Nutzung von Kundendaten zu Werbezwecken“ zurückgegriffen werden.

Die nachfolgende Übersicht zeigt die Anforderungen des § 7 UWG an die unterschiedlichen Werbeformen auf:

Medium	UWG
Brief	➔ UWG: kein hartnäckiges Ansprechen, obwohl erkennbar nicht erwünscht
Telefon → Verbraucher	➔ vorherige ausdrückliche Einwilligung
Telefon → Geschäftskunde	➔ mutmaßliche Einwilligung
E-Mail	➔ vorherige ausdrückliche Einwilligung des Adressaten ➔ Ausnahme: keine Einwilligung, wenn • Mailadresse mit Vertrag erhalten • Werbung für eigene, ähnliche Produkte • kein Widerspruch • Hinweis auf Widerspruchsrecht ohne Zusatzkosten

Vertiefende Hinweise:

Verarbeitung personenbezogener Daten für Werbung:
https://www.lda.bayern.de/media/dsk_kpnr_3_werbung.pdf
https://www.lda.bayern.de/media/baylda_ds-gvo_12_advertising.pdf

Merkblatt zur Einwilligung nach der DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_9_consent.pdf

Beschluss des Düsseldorfer Kreises zur Fortgeltung bisher erteilter Einwilligungen:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/FortgeltungBisherErteilterEinwilligungen.html?nn=5217228

5. Informationspflichten gegenüber dem Betroffenen, Artikel 13 DS-GVO, § 32 BDSG-neu

Die Informationspflichten des Verantwortlichen gegenüber der betroffenen Person werden durch die DS-GVO deutlich erweitert.

Im Falle der **Direkterhebung** von personenbezogenen Daten **bei der betroffenen Person**, müssen gemäß Artikel 13 DS-GVO zum Zeitpunkt der Erhebung folgende Informationen gegeben werden (wesentliche Erweiterungen zum bisherigen Recht sind hervorgehoben):

- Namen und Kontaktdaten des Verantwortlichen
- ggf. Kontaktdaten des Datenschutzbeauftragten (wenn dieser erforderlich ist)
- Zweck und **Rechtsgrundlage der Verarbeitung**
- Wenn die Verarbeitung auf Artikel 6 Abs. 1 lit. f) DS-GVO beruht, die berechtigten Interessen des Verantwortlichen oder eines Dritten
- ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- ggf. Absicht des Verantwortlichen, die Daten an ein Drittland/eine internationale Organisation zu übermitteln
- **Dauer der Datenspeicherung, falls nicht möglich: Kriterien für die Festlegung dieser Dauer**
- Bestehen **eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht und Recht auf Datenübertragbarkeit**
- Bei einer Verarbeitung nach Artikel 6 Abs. 1 lit. a) oder Artikel 9 Absatz 2 lit. a) DS-GVO: Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen
- **Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde**
- Gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der personenbezogenen Daten und Folgen der Nichtbereitstellung
- Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling

Beabsichtigt der Verantwortliche, personenbezogene Daten für einen **anderen Zweck** weiterzuverarbeiten als den, für den die Daten erhoben wurden, **so hat er der betroffenen Person vor dieser Weiterverarbeitung die maßgeblichen Informationen über die geplante Zweckänderung zur Verfügung zu stellen,** Artikel 13 Abs. 3 DS-GVO. Ausnahmen von dieser Verpflichtung regelt § 32 BDSG-neu. Hiernach besteht die Informationsverpflichtung für eine beabsichtigte Weiterverarbeitung u.a. dann nicht, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Die Informationspflichten gegenüber dem Betroffenen **entfallen** nur dann, wenn die betroffene Person bereits **über die Informationen verfügt**, Artikel 13 Abs. 4 DS-GVO.

Die Informationen müssen der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer **klaren und einfachen Sprache** übermittelt werden, Artikel 12 Abs. 1 DS-GVO. Die Übermittlung der Informationen erfolgt grundsätzlich **kostenlos**, Artikel 12 Abs. 5 DS-GVO. Die Informationen können **schriftlich oder in anderer Form**, ggf. auch elektronisch vorgenommen werden. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Sofern personenbezogene Daten **nicht direkt bei der betroffenen Person** erhoben werden sollen, gelten gemäß Artikel 14 DS-GVO, §§ 29, 33 BDSG-neu gesonderte Informationspflichten.

Um die Informationspflichten fristgerecht umzusetzen, sollten Kfz-Betriebe ihre bislang verwendeten Datenschutzerklärungen prüfen und an die neuen Vorgaben anpassen.

Vertiefende Hinweise:

GDD-Praxishilfe: Transparenzpflichten bei der Datenverarbeitung
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

Kurzpapier zu den Informationspflichten bei Dritt- und Direkterhebung:
https://www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

6. Rechte der betroffenen Person

Den betroffenen Personen stehen folgende Rechte zu:

- **Auskunftsrecht**, Artikel 15 DS-GVO, §§ 29,34 BDSG-neu
- **Recht auf Berichtigung**, Artikel 16 DS-GVO
- **Recht auf Löschung** („Recht auf Vergessenwerden“), Artikel 17 DS-GVO, § 35 BDSG-neu
- **Recht auf Einschränkung der Verarbeitung**, Artikel 18 DS-GVO, § 35 BDSG-neu
- **Recht auf Datenübertragbarkeit**, Artikel 20 DS-GVO

  Hiernach müssen Daten, die die betroffene Person selbst zur Verfügung gestellt hat, in einem gängigen Format zur Verfügung gestellt und ggf. auf Wunsch direkt an Dritte weitergeleitet werden.
- **Widerspruchsrecht**, Artikel 21 DS-GVO, § 36 BDSG-neu

Die betroffene Person ist über seine Rechte zu informieren (siehe Ziffer 5).

Im Falle der **Berichtigung oder Löschung** personenbezogener Daten oder der Einschränkung der Verarbeitung ist der Verantwortliche verpflichtet, **allen Empfängern**, denen personenbezogene Daten offengelegt wurden, eine entsprechende **Information darüber zukommen zu lassen**. Eine Ausnahme gilt nur dann, wenn sich die Mitteilung als unmöglich erweist oder nur mit einem unverhältnismäßigen Aufwand verbunden ist. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt, Artikel 19 DS-GVO.

Vertiefende Hinweise:

Kurzpapier zum Auskunftsrecht der betroffenen Person:
https://www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf

Merkblatt und Kurzpapier zum Recht auf Löschung („Vergessenwerden") – Artikel 17 DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_4_right_to_be_forgotten.pdf
https://www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf

7. Auftragsverarbeitung, Artikel 28 DS-GVO

Werden personenbezogene Daten im Auftrag, z.B. von Dienstleistern, verarbeitet, liegt regelmäßig eine sogenannte Auftragsverarbeitung (ehem. Auftragsdatenverarbeitung) vor. Datenschutzrechtlich gilt der Auftragnehmer in diesen Fällen lediglich als **verlängerter Arm des Auftraggebers**, so dass keine Datenübermittlung an einen Dritten vorliegt. Dieser Grundsatz gilt auch unter der DS-GVO fort, Artikel 4 Nr. 10 DS-GVO. Ebenso bleibt der Abschluss eines **Auftragsverarbeitungsvertrags**, dessen Inhalt Artikel 28 Abs. 3 DS-GVO entsprechen muss, für die Verarbeitung personenbezogener Daten im Auftrag weiterhin erforderlich.

Unter dem Regime der DS-GVO werden Auftragnehmer für ihren Verantwortungsbereich jedoch stärker in die Pflicht genommen. So darf gemäß Artikel 28 Abs. 1 DS-GVO nur mit solchen Auftragsverarbeitern zusammengearbeitet werden, die hinreichend Garantien dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** zur Einhaltung des Datenschutzes durchgeführt werden. **Subunternehmer** dürfen vom Auftragnehmer **nur mit Zustimmung** des Auftraggebers eingesetzt werden.

Neu ist zudem, dass der Auftragnehmer ein eigenes Verarbeitungsverzeichnis führen und auf Verlangen der Aufsichtsbehörde zur Verfügung stellen muss. Artikel 82 Abs. DS-GVO sieht zudem eine eigene Haftung des Auftragnehmers bei Datenschutzverletzungen vor.

Vertiefende Hinweise:

Merkblatt zur Auftragsverarbeitung nach der DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_10_processor.pdf

Vertragsmuster zur Auftragsdatenverarbeitung:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

8. Verarbeitungsverzeichnis, Artikel 30 DS-GVO

Die derzeit geltende Verpflichtung zum Führen eines öffentlichen Verfahrensverzeichnisses und einer internen Verarbeitungsübersicht werden mit der DS-GVO abgelöst durch **ein einziges (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten** mit personenbezogenen Daten. Das Verarbeitungsverzeichnis ist vom Verantwortlichen, d.h. der Unternehmensleitung des Kfz-Betriebs, (nicht hingegen vom Datenschutzbeauftragten) zu erstellen und zu führen. Diese Pflicht trifft auch den Auftragsdatenverarbeiter.

Der Umfang des Verzeichnisses von Verarbeitungstätigkeiten ist sehr weit: Erfasst sind z.B. die Personaldatenverwaltung, Kundendatenbanken, CRM-Systeme, E-Mail und Internetanschlüsse sowie Videoüberwachungssysteme.

Der **Inhalt des Verzeichnisses** wird von Artikel 30 Absatz 1 S. 2 DS-GVO vorgegeben:

- Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der personenbezogener Daten
- Kategorien von Empfängern der personenbezogenen Daten
- ggf. Übermittlung von personenbezogenen Daten an ein Drittland
- wenn möglich, Löschfristen für die Datenkategorien
- wenn möglich, Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO

Die Pflicht zur Führung des Verzeichnisses gilt gemäß Artikel 30 Abs. 5 DS-GVO nicht für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen. Eine Ausnahme besteht jedoch dann, wenn Kunden- oder Beschäftigtendaten regelmäßig und nicht nur gelegentlich verarbeitet werden. **Da Kfz-Betriebe fortlaufend personenbezogene Daten ihrer Mitarbeiter und Kunden verarbeiten, muss nach derzeitigem Stand ein Verfahrensverzeichnis geführt werden.**

Zur Überprüfung der Einhaltung des Datenschutzes können die Aufsichtsbehörden Einsicht in das Verfahrensverzeichnis verlangen, Artikel 30 Abs. 4 DS-GVO. **Es ist daher nicht auszuschließen, dass die Aufsichtsbehörden zukünftig an Kfz-Betriebe herantreten und eine**

Übersendung des Verzeichnisses verlangen. Diese Möglichkeit bestand jedoch auch schon unter dem bisherigen Recht.

Die Pflicht zur Führung eines öffentlichen Verfahrensverzeichnisses entfällt unter der DS-GVO.

Vertiefende Hinweise:

GDD Praxishilfe: Verzeichnis von Verarbeitungstätigkeiten nebst Muster:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

Bitkom Leitfaden: Das Verarbeitungsverzeichnis nebst Mustern:
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Verarbeitungsverzeichnis-online.pdf

Kurzpapier: Verzeichnis von Verarbeitungstätigkeiten – Artikel 30 DS-GVO:
https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf
https://www.lda.bayern.de/media/baylda_ds-gvo_5_processing_activities.pdf

9. Meldepflicht bei Datenpannen, Artikel 33 DS-GVO

Der Anwendungsbereich der Meldepflicht bei Datenpannen wird unter der DS-GVO deutlich erweitert. Bislang musste eine derartige Meldung nur erfolgen, wenn die Datenpanne besonders sensible Daten betraf und nur bei schwerwiegenden Beeinträchtigungen des Betroffenen.

Zukünftig muss der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten dies **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, der **zuständigen Aufsichtsbehörde** melden, Artikel 33 Abs. 1 DS-GVO. Die **Meldepflicht entfällt nur dann**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich **nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen** führt. Den Inhalt der Meldung regelt Artikel 33 Abs. 3 DS-GVO.

Eine ausführliche Aufzählung möglicher Risiken findet sich in Erwägungsgrund 75 der DS-GVO. Ein Kfz-Betrieb muss daher eine **Risikoprognose** durchführen und im Zweifel die Aufsichtsbehörde informieren.

Sofern die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, ist der Verantwortliche zusätzlich verpflichtet, **die betroffene Person unverzüglich von der Verletzung in Kenntnis zu setzen**. Den Inhalt der Meldung an den Betroffenen regelt Artikel 34 Abs. 2 DS-GVO. Eine **Ausnahme** von der Benachrichtigungspflicht der Betroffenen besteht nur dann, wenn eine der folgenden Bedingungen erfüllt ist:

- Geeignete technische und organisatorische Sicherheitsvorkehrungen wurden vom Verantwortlichen getroffen und diese wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt.
- Sicherstellung durch nachfolgende Maßnahmen, dass das hohe Risiko für die Rechte und Freiheiten des Betroffenen aller Wahrscheinlichkeit nicht mehr besteht,
- Die Benachrichtigung würde einen unverhältnismäßigen Aufwand darstellen. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Gemäß Artikel 33 Abs. 5 DS-GVO muss der Verantwortliche zudem jede Datenschutzverletzung **dokumentieren**, einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.

Vertiefende Hinweise:

Merkblatt: Umgang mit Datenpannen – Art. 33 und 34 DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

10. Datenschutz-Folgenabschätzung, Artikel 35 DS-GVO

Die Datenschutz-Folgenabschätzung ersetzt die bislang im deutschen Recht vorgesehene „Vorabkontrolle“. Artikel 35 Abs. 1 DS-GVO schreibt die Durchführung einer Datenschutz-Folgenabschätzung generell für alle Verarbeitungsformen vor, die voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge haben können. Dies ist z.B. bei umfassenden automatisierten Persönlichkeitsbewertungen (einschließlich Profiling) oder bei einer umfangreiche Verarbeitung sensibler Daten der Fall.

Die nationalen Aufsichtsbehörden sollen Listen mit weiteren Verarbeitungstätigkeiten erstellen, für die zwingend eine Folgenabschätzung durchzuführen ist, Artikel 35 Abs. 4 DS-GVO. Diese Listen liegen derzeit noch nicht vor.

Vertiefende Hinweise:

Merkblatt zur Datenschutz-Folgenabschätzung – Art. 35 DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf

Leitfaden der bitkom zum Risk-Assessment & Datenschutz-Folgenabschätzung:
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf

11. Der Datenschutzbeauftragte, Artikel 37 ff DS-GVO, § 38 BDSG-neu

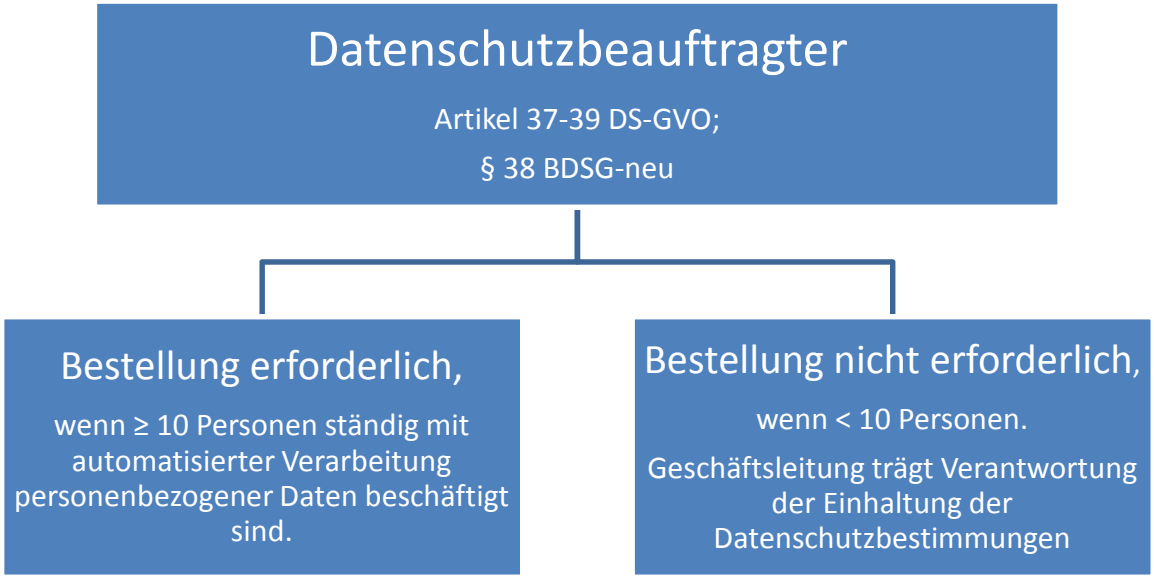
Die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten bleibt für die meisten Kfz-Betriebe bestehen. Die DS-GVO sieht in Artikel 37 eine Pflicht zur Bestellung eines Datenschutzbeauftragten vor, wenn entweder die Kerntätigkeit des Unternehmens

- in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen oder
- in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht.

Diese Fallgruppen dürften zwar für die Kfz-Betriebe keine Rolle spielen. Das BDSG-neu enthält aber in § 38 BDSG-neu eine Regelung zur Bestellung des Datenschutzbeauftragten, die der bisherigen Vorgabe im BDSG entspricht.

Hiernach ist ein Datenschutzbeauftragter zu bestellen, wenn Betriebe in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Diese Personenzahl dürfte von vielen Kfz-Betrieben überschritten werden. Sollte dies nicht der Fall sein, obliegt es der **Geschäftsleitung des Betriebs**, die Einhaltung der Datenschutzbestimmungen als „Verantwortlicher“ gemäß DS-GVO zu erfüllen.



Eine Bestellung eines Datenschutzbeauftragten hat **unabhängig von der Personenzahl** auch dann zu erfolgen, wenn der Verantwortliche oder ein Auftragsdatenverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO unterliegen oder geschäftsmäßig zum Zwecke der Übermittlung erfolgen.

Wie bisher auch, kann gemäß Artikel 37 Abs. 6 DS-GVO **sowohl ein Beschäftigter des Unternehmens als auch ein externer Experte zum Datenschutzbeauftragten bestellt werden**.

Neu ist hingegen die Möglichkeit für **Unternehmensgruppen, einen gemeinsamen Datenschutzbeauftragten** zu ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann, Artikel 37 Abs. 2 DS-GVO.

Der Datenschutzbeauftragte übt seine Tätigkeit gemäß Artikel 38 Abs. 3 DS-GVO **weisungsfrei** aus und **berichtet unmittelbar der höchsten Managementebene** des Unternehmens. Das Unternehmen ist gemäß Artikel 38 Abs. 1 DS-GVO verpflichtet, den Datenschutzbeauftragten ordnungsgemäß und **frühzeitig** in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **einzubinden**. Zur Unterstützung gehören zudem die Bereitstellung der erforderlichen **personellen und sachlichen Infrastruktur** und die Möglichkeit, an **Fortbildungsveranstaltungen** teilzunehmen, um seine Fachkunde aktuell zu halten. Zu den Anforderungen des Düsseldorfer Kreises an die erforderliche Fachkunde des Datenschutzbeauftragten siehe die vertiefenden Hinweise.

Dem Datenschutzbeauftragten obliegen gemäß Artikel 39 DS-GVO u.a. folgende **Aufgaben**:

- **Unterrichtung und Beratung im Hinblick auf die Datenschutzpflichten des Unternehmens und der Beschäftigten**
- **Überwachung der Einhaltung der DS-GVO im Unternehmen**
- **Sensibilisierung und Schulung von Mitarbeitern**
- **Zusammenarbeit mit der Aufsichtsbehörde**

Verstöße gegen die Pflichten aus Artikel 37-39 DS-GVO können gemäß Artikel 83 Abs. 4a DS-GVO mit einem Bußgeld geahndet werden.

Vertiefende Hinweise:

Merkblatt zum betrieblichen Datenschutzbeauftragten nach altem Recht:
https://www.datenschutz.hessen.de/download.php?download_ID=298

Merkblatt zu den Aufgaben und zur Stellung des betrieblichen Datenschutzbeauftragten nach neuem Recht:
https://www.lda.bayern.de/media/baylda_ds-gvo_19_data_protection_officer.pdf

Praxishilfe: Der Datenschutzbeauftragte nach der DS-GVO:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_1.pdf

Anforderungen an die Fachkunde des Datenschutzbeauftragten nach altem Recht:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.html

12. Beschäftigtendatenschutz, § 26 BDSG-neu

Die bisherige Regelung zum Beschäftigtendatenschutz gemäß § 32 BDSG-alt wurde durch die neue Regelung des § 26 BDSG-neu nur marginal verändert. § 26 Abs. 1 BDSG-neu stellt klar, dass – wie bisher auch - Kollektivvereinbarungen (Tarifvertrag, Betriebs- oder Dienstvereinbarung) als Legitimationsgrundlage für eine Datenverarbeitung herangezogen werden können.

Zur **Freiwilligkeit einer Einwilligungserklärung im Beschäftigungsverhältnis** führt § 26 Abs. 2 BDSG-neu aus, dass eine Freiwilligkeit insbesondere dann vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Als Beispiele für die Erreichung eines Vorteils nennt die Gesetzesbegründung die Einführung eines betrieblichen Gesundheitsmanagements und die Erlaubnis zur Privatnutzung der betrieblichen IT-Systeme. An der **Schriftform** der Einwilligung im Beschäftigungsverhältnis wird grundsätzlich festgehalten.

Vertiefende Hinweise:

Merkblatt: Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu:
https://www.lda.bayern.de/media/baylda_ds-gvo_20_employment.pdf

13. Sanktionen, Artikel 83 f DS-GVO

Die **Bußgeldtatbestände** wurden durch die DS-GVO **massiv erhöht**. Zukünftig haben die Aufsichtsbehörden neben ihren in Artikel 58 DS-GVO normierten Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen die Möglichkeit zur Verhängung von Bußgeldern, die in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** sein sollen, Artikel 83 DS-GVO. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag sind in jedem Einzelfall u.a. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens sowie die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes zu berücksichtigen. Die absolute Bußgeldhöhe beträgt **20. Mio. Euro** und kann sich bei Unternehmen auf **bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Jahres** belaufen, Artikel 83 Abs. 5 DS-GVO. Verstöße gegen **weniger zentrale Vorgaben** der DS-GVO unterliegen einer Bußgeldandrohung in Höhe von bis zu **10 Mio. Euro** bzw. im Falle eines Unternehmens von bis zu **2 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres**, Artikel 83 Abs. 4 DS-GVO.

14. Datenschutz Management

Ein deutlich höheres Gewicht erhalten die sogenannten **Organisations- und Dokumentationspflichten** sowie das **Prinzip der „Accountability**“ (Rechenschaftspflicht) für Kfz-Betriebe.

Der Verantwortliche, d.h. die Geschäftsführung des Kfz-Betriebs, ist gemäß Artikel 5 Abs. 2 DS-GVO für die Einhaltung der Datenschutz-Grundsätze verantwortlich und muss deren Einhaltung nachweisen können (**Rechenschaftspflicht)**. Zugleich ist er gemäß Artikel 24 Abs. 1 DS-GVO verpflichtet, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete **technische und organisatorische Maßnahmen** umzusetzen, um sicherzustellen und den Nachweis dafür zu erbringen zu können, dass eine datenschutzgerechte Verarbeitung der Daten erfolgt.

Kfz-Betriebe müssen also jederzeit die Rechtskonformität der Datenverarbeitung in rechtlicher wie in technischer und organisatorischer Sicht nachweisen können. Hierzu ist es unerlässlich, alle datenschutzrelevanten Vorgänge im Unternehmen **sorgfältig zu dokumentieren.** Kfz-Betriebe sollten daher ein Datenschutz-Managementsystem in ihren Unternehmen etablieren.

Bestandteile eines solches Datenschutz-Managements sind:

- Zuweisung von datenschutzrechtlichen Zuständigkeiten im Betrieb
- Sensibilisierung und regelmäßige Schulung der Mitarbeiter
- Regeln für Kontrollen, Optimierung und Anpassung aller Datenschutzmaßnahmen
- Einsatz „datenschutzfreundlicher“ Technologien (siehe Ziffer 15)
- IT-Sicherheit nach dem Stand der Technik (siehe Ziffer 16)
- Dokumentationspflichten, insbesondere
    - Verarbeitungsverzeichnis
    - Datenschutz-Organisation
    - Interne Datenschutzregeln und IT-Sicherheitsrichtlinien
    - Durchgeführte Datenschutz-Folgenabschätzungen
    - Datenschutzverstöße/-vorfällen
    - Zuständigkeiten

15. Datenschutz durch Technik, Artikel 25 DS-GVO

Die umzusetzenden technischen Maßnahmen müssen **im Hinblick auf das Risiko** der Datenverarbeitung **verhältnismäßig** sein. Konkrete Vorgaben zum Datenschutz durch Technikgestaltung enthält Artikel 25 DS-GVO. Hiernach müssen Kfz-Betriebe ihre datenverarbeitenden Systeme und Verfahren derart gestalten, dass sie die Datenschutzgrundsätze, wie etwa den Grundsatz der Datenminimierung und der schnellstmöglichen Pseudonymisierung von personenbezogenen Daten, wirksam umsetzen (sog. „**Privacy by Design**“, **Datenschutz durch Technikgestaltung**). Insbesondere für Onlinedienste ist das Prinzip des „**Privacy by Default**“ (**Datenschutzfreundliche Voreinstellungen**) von Bedeutung. Voreinstellungen in datenschutzverarbeitenden Systemen sind demnach so zu regeln, dass jeweils nur die für den jeweiligen Verarbeitungszweck erforderlichen Daten erhoben und gespeichert werden. Die Einhaltung dieser Prinzipien ist vom Kfz-Betrieb nachzuweisen. Artikel 25 Abs. 3 DS-GVO geht davon aus, dass sich zur Nachweiserbringung Zertifizierungsverfahren etablieren werden.

16. Sicherheit der Datenverarbeitung, § 32 DS-GVO

Artikel 32 DS-GVO verpflichtet Kfz-Betriebe zur Implementierung **geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines risikoangemessenen Datenschutzniveaus.** Zu diesen Maßnahmen zählen gemäß Artikel 32 DS-GVO insbesondere

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- IT-Sicherheit wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
- Sicherstellung, dass Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur weisungsgebunden, z.B. im Rahmen ihrer Aufgabenerfüllung, verarbeiten.

Die Maßnahmen müssen unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art, des Umfangs**, der **Umstände** und der **Zwecke** der Verarbeitung sowie der **Schwere** der unterschiedlichen Eintrittswahrscheinlichkeit und **Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen** geeignet sein, **um ein dem Risiko angemessenes Schutzniveau zu gewährleisten**. Es gilt also auch hier – wie schon unter § 9 BDSG-alt - der **Verhältnismäßigkeitsgrundsatz**. Neu ist hingegen der Verweis auf den Stand der Technik. Dies bedeutet jedoch nicht, dass nur solche Techniken zum Einsatz kommen dürfen, die gerade neu entwickelt wurden. Vielmehr muss die jeweilige Maßnahme ihre Ge-

eignetheit und Effektivität in der Praxis bewiesen haben und einen ausreichenden Sicherheitsstandard gewährleisten.

Kfz-Betriebe müssen auch in Bezug auf die ergriffenen Sicherheitsmaßnahmen einen **Nachweis** erbringen können (Rechenschaftspflicht).

Vertiefende Hinweise:

Leitfaden der bitkom zum Risk-Assessment & Datenschutz-Folgenabschätzung:
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf

Merkblatt: Sicherheit der Verarbeitung – Art. 32 DS-GVO:
https://www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf

III. Anlagen

1. Kontaktdaten der Landesdatenschutzbehörden

Baden Württemberg:	https://www.baden-wuerttemberg.datenschutz.de/
Bayern:	https://www.lda.bayern.de/de/index.html
Berlin:	https://datenschutz-berlin.de/
Bremen:	www.datenschutz-bremen.de
Brandenburg:	http://www.lda.brandenburg.de/
Hamburg:	https://www.datenschutz-hamburg.de/
Hessen:	https://www.datenschutz.hessen.de/
Mecklenburg-Vorpommern:	https://www.datenschutz-mv.de/
Niedersachsen:	http://www.lfd.niedersachsen.de/startseite/
Nordrhein-Westfalen:	https://www.ldi.nrw.de/
Rheinland-Pfalz:	https://www.datenschutz.rlp.de/de/startseite/
Saarland:	https://datenschutz.saarland.de/
Sachsen:	https://www.saechsdsb.de/
Sachsen-Anhalt:	https://datenschutz.sachsen-anhalt.de/nc/datenschutz-sachsen-anhalt/
Schleswig-Holstein:	https://www.datenschutzzentrum.de/
Thüringen:	https://www.tlfdi.de/tlfdi/

IMPRESSUM

Herausgeber:

Deutsches Kraftfahrzeuggewerbe
Zentralverband (ZDK)
Franz-Lohe-Str. 21
53129 Bonn
Telefon: 0228-9127-0
www.kfzgewerbe.de

Verantwortlich:

Abteilung Recht, Steuern, Tarife
Rechtsanwalt Ulrich Dilchert
E-Mail: dilchert@kfzgewerbe.de

Verfasser:

Abteilung Recht, Steuern, Tarife
Rechtsanwalt Patrick Kaiser
E-Mail: kaiser@kfzgewerbe.de

Stand:

Oktober 2017

Deutsches Kraftfahrzeuggewerbe
Zentralverband