Datenschutz

DS-GVO und BDSG im Überblick

KRAFTFAHRZEUG GEWERBE

Herausgeber
Deutsches Kraftfahrzeuggewerbe e. V.
Zentralverband (ZDK)
Franz-Lohe-Straße 21, 53129 Bonn

Telefon: 0228 9127-0
Telefax: 0228 9127-150
E-Mail: zdk@kfzgewerbe.de
Internet: www.kfzgewerbe.de

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

Verfasser:
Abteilung Recht, Steuern, Tarife
Rechtsanwalt (Syndikusrechtsanwalt) Patrick Kaiser LL.M.
E-Mail: kaiser@kfzgewerbe.de

Erscheinungsdatum:
April 2019

Seite

1 Einleitung

Die **EU-Datenschutz-Grundverordnung (Verordnung (EU) 2016/679; kurz: DS-GVO)** gilt seit dem **25. Mai 2018** unmittelbar in allen europäischen Mitgliedstaaten. Ziel des europäischen Gesetzgebers war 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 gelangte. Mit diesem Gesetz wurde u.a. das neue Bundesdatenschutzgesetz (**BDSG**) in Kraft gesetzt.

Die neuen Datenschutzregelungen sind ausgesprochen umfangreich und komplex. Dies gilt insbesondere für die erweiterten **Informations- und Dokumentationspflichten**. Ebenfalls müssen die **Kontaktdaten** des betrieblichen (extern oder intern) **Datenschutzbeauftragten** den Landesdatenschutzbehörden **gemeldet** werden. Drastisch erhöht wurde zudem der **Bußgeldrahmen für Datenschutzverstöße**.

Für die praktische Umsetzung des neuen Datenschutzrechts soll dieser Leitfaden einen **ersten Überblick** geben. Der Leitfaden nimmt nicht für sich in Anspruch, das neue Recht vollumfänglich und im Detail darzustellen. Für eine vertiefende Auseinandersetzung mit einzelnen Themen enthält der Leitfaden in Abschnitt 3 nützliche Links auf öffentlich zugängliche Merkblätter und Praxisratgeber von Datenschutzbehörden und –organisationen.

Keinesfalls ersetzt der Leitfaden die Notwendigkeit einer individuellen Prüfung der Einhaltung der Datenschutzvorschriften im Einzelfall.

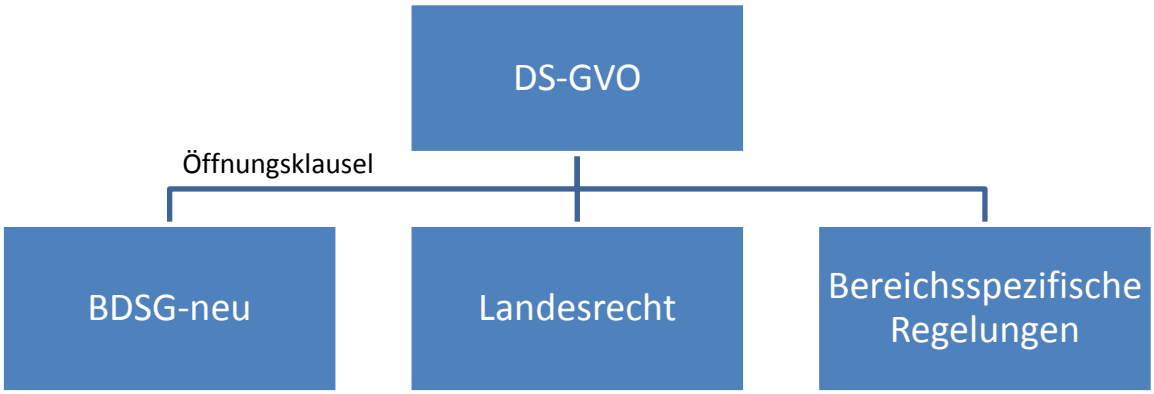
Der Leitfaden ist als **fortlaufendes, elektronisches Dokument** konzipiert.

2 Die Inhalte der DS-GVO und des BDSG

2.1 Zusammenspiel von europäischer DS-GVO und nationalen Datenschutzvorschriften

Die DS-GVO gilt seit dem 25. Mai 2018 unmittelbar in allen Mitgliedstaaten.

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, die allgemeinen Landesdatenschutzgesetze oder bereichsspezifischen Regelungen auf Bundes- und Landesebene zurückzugreifen. Es empfiehlt sich daher, die DS-GVO und z.B. das BDSG immer parallel zu lesen.



2.2 Zusammenspiel von DS-GVO und ePrivacy-Verordnung / Anpassungsbedarf von Internetseiten

Im Bereich der elektronischen Kommunikation soll die sogenannte ePrivacy-Verordnung der DS-GVO als Spezialgesetz vorgehen. Das Gesetzgebungsverfahren zur ePrivacy-Verordnung dauert derzeit noch an und mit einem Inkrafttreten wird nicht vor Mitte 2019 gerechnet. Im **Online-Bereich** finden daher bis auf weiteres und nach jetzigem Kenntnisstand die Regelungen der DS-GVO Anwendung.

2.3 Datenschutzrechtliche Grundsätze

Nachfolgend werden die wesentlichen Änderungen bzw. Grundsätze dargestellt, die insbesondere in der datenschutzrechtlichen Praxis von Kfz-Betrieben relevant sind. Auf eine Wiedergabe und Erläuterung sämtlicher neuen Vorgaben der DS-GVO wird verzichtet.

2.3.1 Begriffsbestimmungen, Artikel 4 DS-GVO

2.3.1.1 Personenbezogene Daten

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.

2.3.1.2 Verantwortlicher

Als Verantwortlicher im Sinne der DS-GVO gilt jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Beispiel: Kfz-Betriebe, Hersteller/Importeure, Dienstleister, Verbände, Innungen.

2.3.1.3 Verarbeitung

Neu ist, dass der Begriff **„Verarbeitung“** zukünftig alle bisherigen Nutzungsformen (Erhebung, Speicherung, Auslesen, Nutzung, Offenlegung durch Übermittlung, Bereitstellung u.a.) von personenbezogenen Daten umfasst. Es wird daher einheitlich nur noch von einer Verarbeitung von personenbezogenen Daten gesprochen.

2.3.2 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 **(Kompatibilitätstest**). 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 / Datensparsamkeit**

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

- **Richtigkeit, Integrität und zeitlich begrenzte Speicherung**

  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.

2.3.3 Datenschutz Management

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

Der Verantwortliche, z.B. die Geschäftsführung eines 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 erbringen zu können, dass eine datenschutzgerechte Verarbeitung der Daten erfolgt. Gegenüber Aufsichtsbehörden bedeutet dies eine **Umkehr der Beweislast**, d.h. in einem aufsichtsbehördlichen Verfahren oder Gerichtsprozess muss der Kfz-Betrieb sein datenschutzkonformes Verhalten darlegen. Gelingt der Nachweis nicht, drohen Bußgelder oder ein Prozessverlust.

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.

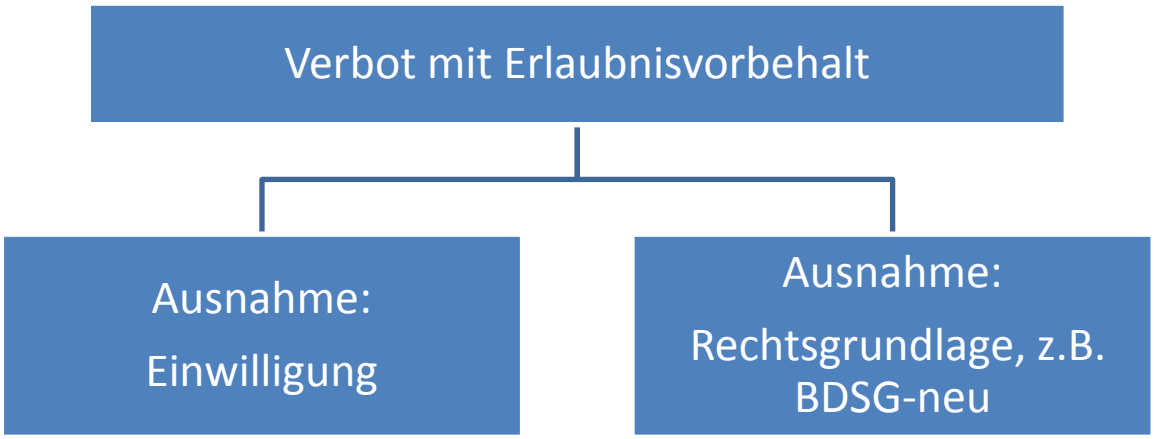
Bestandteile eines solches **Datenschutz-Managements** sind:

- Zuweisung von datenschutzrechtlichen Zuständigkeiten im Betrieb
- Sensibilisierung und regelmäßige Schulung der Mitarbeiter (siehe Ziffer 2.3.17.4)
- Regeln für Kontrollen, Optimierung und Anpassung aller Datenschutzmaßnahmen
- Einsatz „datenschutzfreundlicher“ Technologien (siehe Ziffer 2.3.8)
- IT-Sicherheit nach dem Stand der Technik (siehe Ziffer 2.3.10)

- Dokumentationspflichten, insbesondere
  - Verarbeitungsverzeichnis (siehe Ziffer 2.3.9)
  - Datenschutz-Organisation
  - Interne Datenschutzregeln und IT-Sicherheitsrichtlinien
  - Durchgeführte Datenschutz-Folgenabschätzungen
  - Datenschutzverstöße/-vorfälle
  - Zuständigkeiten

2.3.4 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 (Artikel 6 Abs. 1 S. 1 lit. a DS-GVO) nennt Artikel 6 DS-GVO insbesondere folgende Zulässigkeitstatbestände für die Verarbeitung von personenbezogenen Daten:

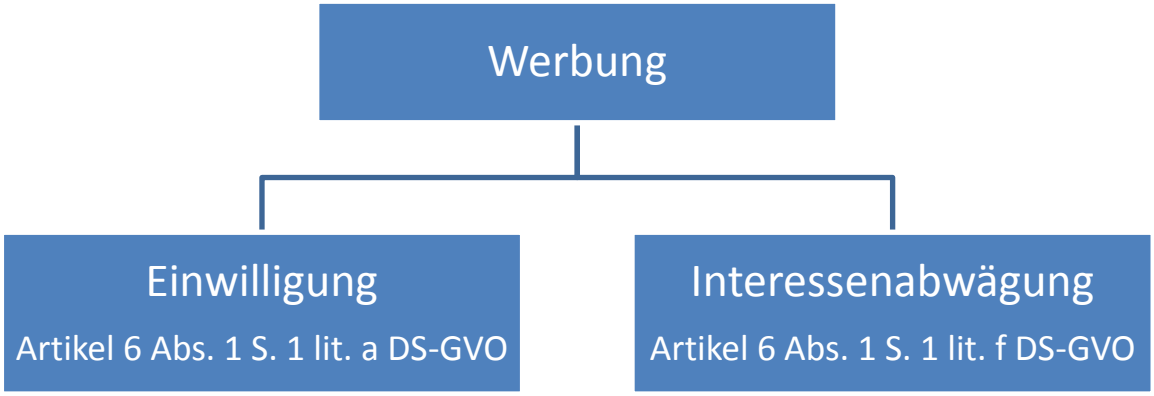
- **Verarbeitung zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen, Artikel 6 Abs. 1 S. 1 lit. b DS-GVO** (z.B. Abwicklung eines Kaufvertrags, Durchführung einer Fahrzeugreparatur, Übersendung von Prospekten)
- **Erfüllung rechtlicher Pflichten, Artikel 6 Abs. 1 S. 1 lit. c DS-GVO**
- **Interessenabwägung, Artikel 6 Abs. 1 S. 1 lit. f DS-GVO** (z.B. Werbemaßnahmen des Kfz-Betriebs ohne Einwilligung)

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

2.3.5 Verarbeitung personenbezogener Daten für Werbung

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.

Neben den datenschutzrechtlichen Vorgaben sind bei der Frage des Kontaktkanals der Werbung immer auch die Regelungen des UWG zu beachten, die für bestimmte Werbeformen, wie z.B. E-Mail, Telefon, Fax, SMS, regelmäßig eine vorherige ausdrückliche Einwilligung der betroffenen Person voraussetzen (siehe § 7 UWG). Noch nicht geklärt ist, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen für werbliche Ansprachen enthalten wird.



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

2.3.5.1 Interessenabwägung / Werbung ohne Einwilligung

Gemäß Artikel 6 Abs. 1 S. 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 bei 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.

Beispiel: Werbemaßnahmen gegenüber **Bestandskunden** des Kfz-Betriebs

Um dem Transparenzerfordernis und dem Grundsatz der Zweckbindung 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 S. 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, wird die Einholung von (möglichst) schriftlichen Einwilligungserklärungen zur Vermeidung von Rechtsunsicherheiten und Rechtsnachteilen empfohlen.

2.3.5.2 Werbung mit Einwilligung / Voraussetzungen einer Einwilligung

Die Einwilligung zur Verarbeitung personenbezogener Daten muss für einen oder mehrere bestimmte Zwecke abgegeben werden, Artikel 6 Abs. 1 S. 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.

a) Freiwilligkeit

Die Einwilligung muss freiwillig erfolgen. An der Freiwilligkeit fehlt es, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und dem Verantwortlichen besteht. Bislang

wurde ein solches Ungleichgewicht regelmäßig in **Arbeitsverhältnissen** zwischen Arbeitgeber und Arbeitnehmer angenommen. § 26 Abs. 2 BDSG differenziert nunmehr in derartigen Fällen und lässt es für eine Freiwilligkeit ausreichen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Die Einwilligung gilt **nicht als freiwillig** erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist (**Abkehr von Globaleinwilligungen**), oder wenn die Erfüllung eines Vertrages einschließlich der Erbringung einer Dienstleistung von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist, sogenanntes **Kopplungsverbot**, Artikel 7 Abs. 4 DS-GVO (Abkehr vom bisherigen „take it or leave it“-Prinzip).

b) Bestimmter Fall

Die Einwilligung muss sich auf einen konkreten Fall beziehen. Wenn die Verarbeitung der personenbezogenen Daten **mehreren Zwecken** dient, muss für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden.

c) In informierter Weise und unmissverständlich

Die betroffene Person muss wissen, dass und in welchem Umfang sie ihre Einwilligung erteilt. Als **Mindestinhalt** muss die Einwilligungserklärung daher die **Identität des Verantwortlichen** und die **Zwecke der Verarbeitung** der personenbezogenen Daten enthalten. Die Einwilligung muss zudem durch eine eindeutige bestätigende Handlung erfolgen, mit der unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine **Schriftform** ist hierfür **nicht erforderlich**. Die Einwilligung kann z.B. **auch elektronisch, mündlich** oder **konkludent** erklärt werden, wenn die betroffene Person eindeutig signalisiert, dass sie mit der Datenverarbeitung einverstanden ist. Durch das Anklicken eines Ankreuzkästchens (sogenannte Tickbox) kann z.B. auf einer Internetseite eine unmissverständliche Willensbekundung erfolgen. **Stillschweigen**, **bereits angekreuzte Kästchen** oder **Untätigkeit** der betroffenen Person stellen **keine Einwilligung** dar (siehe

Erwägungsgrund Nr. 32 DS-GVO). Aus diesem Grund dürfte die bisherige Rechtsprechung des BGH zur postalischen Werbung in Form von Opt-Out-Kästchen bzw. Opt-Out-Formulierungen keinen Bestand mehr haben. Die Muster-Einwilligungserklärung des ZDK (siehe Anlage 1) sieht daher auch für die postalische Werbung ein gesondertes Ankreuzkästchen vor.

d) Sonstige Bedingungen für eine wirksame Einwilligung

Ein Schriftformerfordernis enthält die DS-GVO nicht. Die ausdrückliche Einwilligungserklärung kann daher auch elektronisch oder mündlich erklärt werden. Der Verantwortliche muss jedoch **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. **Es wird daher empfohlen, möglichst immer schriftlich erteilte Einwilligungserklärungen einzuholen.**

Sofern die Einwilligungserklärung zusammen mit anderen Erklärungen abgegeben werden soll, muss sie gemäß Artikel 7 Abs. 2 DS-GVO **besonders hervorgehoben** werden. Sie muss zudem in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfasst sein.

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

e) Fortbestand von Alt-Einwilligungserklärungen

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. **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 2.3.6), anzupassen. Eine Muster-Einwilligungserklärung nach neuem Recht ist der Anlage beigefügt. Diese kann schon jetzt für die Einholung von Einwilligungen verwendet werden.

f) Wirksamkeitsdauer von Einwilligungserklärungen

Die Muster-Einwilligungserklärung des ZDK sieht vor, dass die Einwilligung der betroffenen Person **bis auf Widerruf** gilt. In der Praxis wird jedoch teilweise davon ausgegangen, dass Einwilligungserklärungen nicht unbeschränkt gültig sind. Zu dieser Fragestellung muss die weitere Rechtsprechung abgewartet werden. In Zweifelsfällen sollte ein Kfz-Betrieb darauf abstellen, ob ein Kunde, der eine Einwilligungserklärung abgegeben hat, auch nach einem längeren Zeitablauf noch mit einer Verarbeitung seiner Daten, z.B. in Form von Werbung, rechnen muss (**vernünftige Erwartungshaltung des Betroffenen**). Die relevanten Zeiträume sind in Abhängigkeit vom jeweiligen Einzelfall zu beurteilen (z.B. Ablauf von langjährigen Finanzierungs- oder Leasingverträgen, Garantiezeiträumen etc.).

2.3.5.3 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.

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

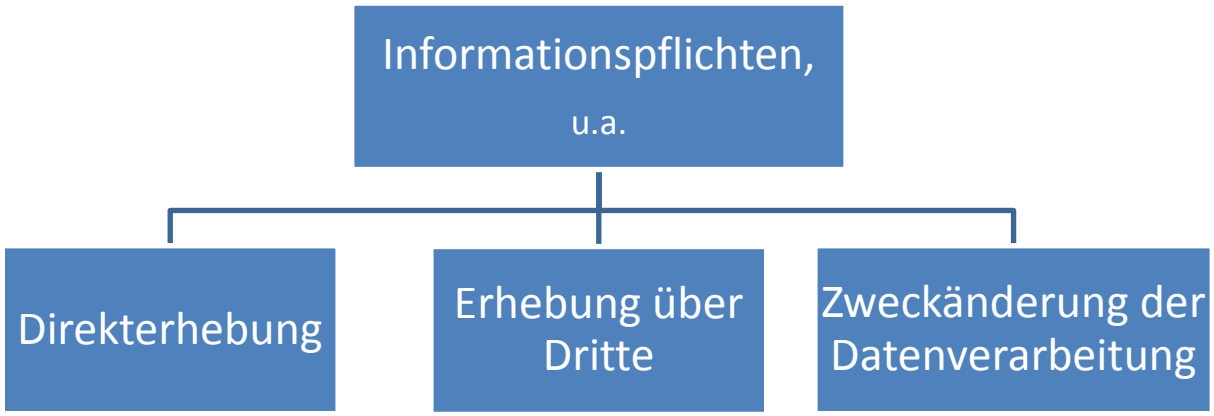
Medium		UWG
Brief		➔ UWG: kein hartnäckiges Ansprechen, obwohl erkennbar nicht erwünscht
Telefon	**Verbraucher**	➔ vorherige ausdrückliche Einwilligung
	Geschäftskunde	➔ mutmaßliche Einwilligung

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

ANLAGE 1
➔ **Muster einer datenschutzrechtlichen Einwilligungserklärung**

2.3.6 Informationspflichten gegenüber dem Betroffenen

Die Informationspflichten des Verantwortlichen gegenüber der betroffenen Person werden durch die DS-GVO deutlich erweitert. Relevante Informationspflichten existieren insbesondere in folgenden Fällen:



2.3.6.1 Direkterhebung, Artikel 13 DS-GVO, § 32 BDSG-neu

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:

- Namen und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (wenn dieser erforderlich ist)
- Zweck und Rechtsgrundlage der Verarbeitung
- Wenn die Verarbeitung auf Artikel 6 Abs. 1 S. 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 S. 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 oder Erforderlichkeit für einen Vertragsabschluss und Folgen der Nichtbereitstellung
- Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling

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.

2.3.6.2 Erhebung über Dritte, Artikel 14 DS-GVO, § 33 BDSG

Werden die personenbezogenen Daten nicht bei der betroffenen Person, sondern bei einem Dritten oder aus öffentlichen Quellen erhoben, sind die Informationen gemäß Ziffer 2.3.6.1 um folgende Angaben zu ergänzen:

- Welche Kategorien von personenbezogenen Daten werden erhoben?
- Aus welcher Quelle die Daten stammen und ggf. ob sie aus öffentlich zugänglichen Quellen stammen

Die Informationen sind innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, spätestens jedoch **innerhalb eines Monats**, bei Nutzung zur Kommunikation mit der betroffenen Person spätestens **zum Zeitpunkt der ersten Mitteilung** an sie oder bei einer Offenlegung an einen anderen Empfänger, spätestens zum Zeitpunkt der **ersten Offenlegung** zu erteilen.

Die Informationspflicht entfällt u.a., wenn

- die betroffene Person bereits über die Informationen verfügt oder
- die Erteilung der Information unmöglich oder nur mit einem unverhältnismäßigen Aufwand durchführbar ist
- die Vorgaben des § 33 BDSG-neu erfüllt sind

2.3.6.3 Zweckänderung der Datenverarbeitung, Artikel 13 Absatz 3, Artikel 14 Absatz 4 DS-GVO

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:**

- Neuer Zweck der Verarbeitung
- Dauer der Verarbeitung bzw. Kriterien für die Fertigstellung dieser Daten
- Rechte der Betroffenen
- Beschwerderecht bei einer Aufsichtsbehörde
- ggf. gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der personenbezogenen Daten oder Erforderlichkeit für einen Vertragsabschluss und Folgen der Nichtbereitstellung
- ggf. Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling.

2.3.6.4 Form der Informationserteilung, Artikel 12 DS-GVO

Die Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden. Die Informationen werden grundsätzlich **unentgeltlich** zur Verfügung gestellt.

Um die Informationspflichten fristgerecht umzusetzen, sollten die bislang verwendeten Datenschutzerklärungen, insbesondere auch auf Internetseiten (siehe Ziffer 2.2), geprüft und an die neuen Vorgaben angepasst werden.

2.3.7 Rechte der betroffenen Person

Die DS-GVO räumt betroffenen Personen, deren personenbezogenen Daten verarbeitet werden, zahlreiche Rechte ein. Hierzu zählen:

2.3.7.1 Auskunftsrecht, Artikel 15 DS-GVO, §§ 29, 34 BDSG

Die betroffene Person kann von dem Verantwortlichen (formfrei) Auskunft darüber verlangen, ob sie betreffende personenbezogenen Daten verarbeitet werden. Ist dies der Fall muss die Auskunft gemäß Artikel 15 Abs. 1 DS-GVO folgende Informationen enthalten:

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden
- die Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt wurden
- falls möglich, die Dauer der Speicherung bzw. die Kriterien für die Festlegung der Dauer
- die Rechte des Betroffenen
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen über die Herkunft der Daten
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- sofern eine Datenübermittlung an ein Drittland oder eine internationale Organisation erfolgt, ist über die Garantien gemäß Artikel 46 DS-GVO zu unterrichten

a) Prüfung der Identität des Antragstellers

Um missbräuchliche Auskunftsverlangen zu vermeiden, ist es erforderlich, sich vorab von der Identität des Antragstellers zu überzeugen (**Identitätsprüfung**). Der Antragsteller und die betroffene Person, deren Daten verarbeitet werden, müssen identisch sein. Hat z.B. ein Kfz-

Betrieb Zweifel an der Identität des Antragstellers, kann er weitere Informationen anfordern, bevor er eine Auskunft erteilt.

b) Form, Fristen und Kosten der Auskunftserteilung

Die Auskunft soll in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Hierzu stellt die verantwortliche Stelle eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Stellt die betroffene Person den Antrag elektronisch, sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

Ein **Muster einer Auskunftserteilung** ist als **Anlage 2** beigefügt.

Die Auskunftserteilung hat **unverzüglich**, in jedem Fall aber **innerhalb eines Monats** nach Eingang des Antrags zu erfolgen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist.

Die Auskunftserteilung erfolgt **unentgeltlich**. Beantragt die betroffene Person mehr als eine Kopie der personenbezogenen Daten, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.

c) Ablehnung der Auskunftserteilung

Sofern der Verantwortliche glaubhaft macht, dass er **nicht in der Lage** ist, den Antragsteller **zu identifizieren** (s.o.), kann er die Auskunftserteilung ablehnen. Entsprechendes gilt bei offenkundig **unbegründeten** oder **exzessiven Anträgen** einer betroffenen Person. Gemäß § 34 Absatz 1 BDSG-neu besteht ein Auskunftsrecht zudem dann nicht, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund **gesetzlicher oder satzungsmäßiger Aufbewahrungsfristen** nicht gelöscht werden dürfen oder ausschließlich Zwecken der **Datensicherung** oder der **Datenschutzkontrolle** dienen und die Auskunftserteilung einen **unverhältnismäßigen Aufwand** erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Die Gründe der Auskunftsverweigerung sind vom Verantwortlichen zu dokumentieren und dem Betroffenen ohne Verzögerung, spätestens innerhalb eines Monats nach Eingang des

Antrags, mitzuteilen. Der Betroffene ist gleichzeitig über die Möglichkeit zu informieren, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

2.3.7.2 Recht auf Berichtigung, Artikel 16 DS-GVO

Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, hat die betroffene Person ein Recht auf Berichtigung. Der Verantwortliche muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.

2.3.7.3 Recht auf Löschung („Recht auf Vergessenwerden"), Artikel 17 DS-GVO, § 35 BDSG

Betroffene Personen können die Löschung ihrer personenbezogenen Daten u.a. dann verlangen, wenn

- sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
- der Betroffene seine Einwilligung widerrufen hat,
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Eine Löschung der personenbezogenen Daten hat u.a. dann zu unterbleiben, wenn gesetzliche Aufbewahrungsfristen bestehen (z.B. rentenrelevante Unterlagen von Mitarbeitern des Kfz-Betriebs). Anstelle einer Löschung tritt die sogenannte Einschränkung der Verarbeitung gemäß § 35 BDSG, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse des Betroffenen an der Löschung als gering anzusehen ist.

Ein Unterfall des Löschungsanspruchs ist das sogenannte **Recht auf Vergessenwerden.** Es verpflichtet den Verantwortlichen, der die Daten veröffentlicht hat, allen anderen Verantwortlichen, die die Daten verarbeiten, mitzuteilen, alle Links zu diesen Daten oder Kopien davon zu löschen.

2.3.7.4 Recht auf Einschränkung der Verarbeitung, Artikel 18 DS-GVO, § 35 BDSG

Das Recht auf Einschränkung der Verarbeitung ermöglicht es dem Betroffenen, eine Sperrung der Datenverarbeitung von einem Verantwortlichen u.a. dann zu verlangen, wenn

- die Richtigkeit gespeicherter Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll
- die Datenverarbeitung unrechtmäßig ist und der Betroffene anstatt der Löschung die Nutzungsbeschränkung wünscht.

2.3.7.5 Recht auf Datenübertragbarkeit, Artikel 20 DS-GVO

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Dieses Recht soll insbesondere Anbieterwechsel erleichtern, wie z.B. eine Übertragung von Profilen in sozialen Netzwerken.

2.3.7.6 Widerspruchsrecht, Artikel 21 DS-GVO, § 36 BDSG

Der betroffenen Person steht ein jederzeitiges Widerspruchsrecht gegen eine Verarbeitung ihrer personenbezogenen Daten, z.B. in Form einer Direktwerbung, zu. Auf dieses Recht ist spätestens zum Zeitpunkt der ersten Kommunikation hinzuweisen. Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zur Direktwerbung genutzt werden.

Die betroffene Person ist über seine vorgenannten Rechte **zu informieren** (siehe Ziffer 2.3.6).

Im Falle der **Berichtigung oder Löschung** personenbezogener Daten oder **der Einschränkung der Verarbeitung** ist der Verantwortliche gemäß Artikel 19 DS-GVO 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.

ANLAGE 2
Muster einer Auskunftserteilung

2.3.8 Datenschutz durch Technik, Artikel 25 DS-GVO

Bereits bei der Einführung von Systemen oder der Gestaltung von Prozessen und bei der späteren Verarbeitung sind geeignete technische und organisatorische Maßnahmen, wie z.B. Pseudonymisierung von Daten, vorzusehen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen (**„Privacy by Design“).**

Im Alltag eines Kfz-Betriebs ist z.B. systemseitig sicherzustellen, dass personenbezogene Daten jederzeit gelöscht werden können.

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. Unzulässig wäre es demnach, wenn die Voreinstellungen bereits eine Einwilligung zum Erhalt verschiedener Werbeangebot beinhalten würde (Opt-out).

Die Einhaltung dieser Prinzipien muss nachgewiesen werden können. Artikel 25 Abs. 3 DS-GVO geht davon aus, dass sich zur Nachweiserbringung Zertifizierungsverfahren etablieren werden.

2.3.9 Verarbeitungsverzeichnis, Artikel 30 DS-GVO

Die 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 zu erstellen und zu führen. Diese Pflicht trifft auch den Auftragsverarbeiter.

Es sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Der Umfang des Verzeichnisses von Verarbeitungstätigkeiten ist dabei 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:

- den Namen und die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der personenbezogener Daten
- die Kategorien von Empfängern der personenbezogenen Daten
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation
- wenn möglich, Löschfristen für die Datenkategorien
- wenn möglich, eine allgemeine 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 z.B. 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. Eine Einsichtnahme des Verarbeitungsverzeichnisses durch die Öffentlichkeit sieht die DS-GVO hingegen nicht vor.

ANLAGE 3
Muster-Verarbeitungsverzeichnis

2.3.10 Sicherheit der Datenverarbeitung, § 32 DS-GVO

Artikel 32 DS-GVO verpflichtet verantwortliche Stellen 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
- ein 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 Geeignetheit und Effektivität in der Praxis bewiesen haben und einen ausreichenden Sicherheitsstandard gewährleisten.

Verantwortliche Stellen, wie z.B. Kfz-Betriebe, müssen auch in Bezug auf die ergriffenen Sicherheitsmaßnahmen einen **Nachweis** erbringen können (**Rechenschaftspflicht**).

ANLAGE 4
→ **Checkliste „Technische und organisatorische Maßnahmen“**

2.3.11 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 (bloßen) **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. Der Inhalt der Meldung beinhaltet folgende Mindestangaben:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der Datenkategorien und der ungefähren Zahl der betroffenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

- eine Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Eine ausführliche Aufzählung möglicher Risiken findet sich in Erwägungsgrund 75 der DS-GVO. Es muss daher eine **Risikoprognose** durchgeführt und im Zweifel die Aufsichtsbehörde informiert werden.

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.

2.3.12 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. Entsprechendes gilt regelmäßig für den Einsatz von **Videoüberwachungsanlagen** gemäß Artikel 35 Abs. 3 lit. c DS-GVO.

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.

Inhaltlich umfasst die Datenschutz-Folgenabschätzung folgende Mindestangaben:

- eine Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung sowie der vom Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen

Sofern ein hohes Risiko festgestellt wird und der Verantwortlich keine Maßnahmen zur Eindämmung des Risikos trifft, ist vor der Verarbeitung die Aufsichtsbehörde zu konsultieren.

2.3.13 Der Datenschutzbeauftragte, Artikel 37 ff DS-GVO, § 38 BDSG

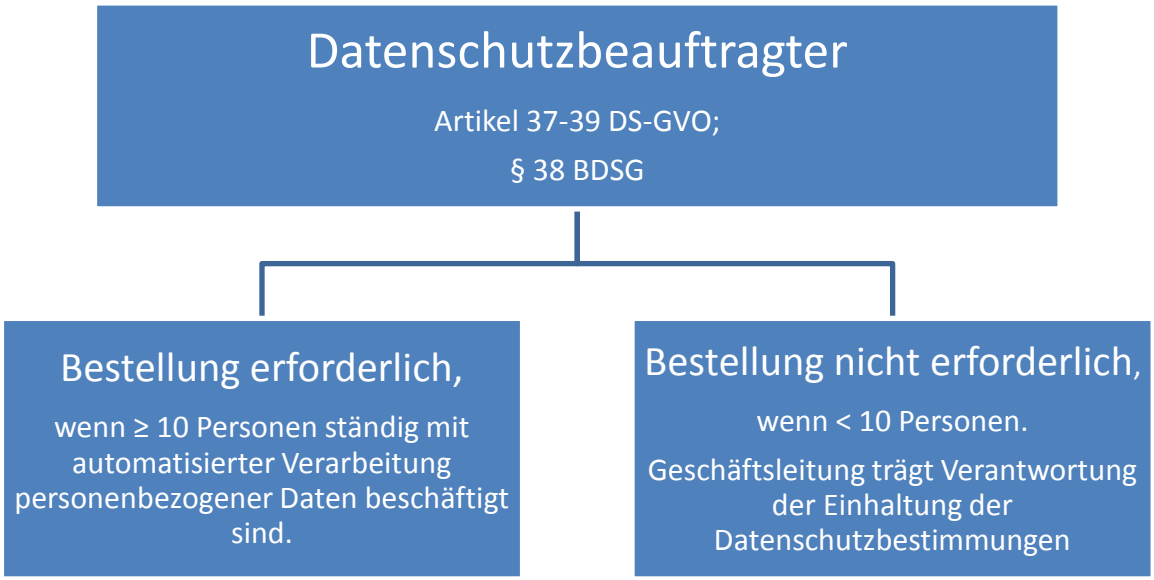
Die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten bleibt für die meisten verantwortlichen Stellen bestehen. Die DS-GVO sieht in Artikel 37 eine Pflicht zur Bestellung eines Datenschutzbeauftragten vor, wenn entweder die Kerntätigkeit des Unternehmens

- 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 eine Regelung zur Bestellung des Datenschutzbeauftragten, die der bisherigen Vorgabe im BDSG entspricht.

Hiernach ist ein Datenschutzbeauftragter zu bestellen, wenn z.B. Kfz-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“ 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. Ebenso müssen Behörden oder **öffentliche Stellen** einen betrieblichen Datenschutzbeauftragten unabhängig von ihrer Personenzahl benennen.

2.3.13.1 Interner, externer sowie Konzern-Datenschutzbeauftragter

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 der Datenschutzbeauftragte von jeder

Niederlassung aus leicht erreicht werden kann, Artikel 37 Abs. 2 DS-GVO. Die leichte Erreichbarkeit liegt dann vor, wenn sowohl die persönliche, als auch die sprachliche Erreichbarkeit des Datenschutzbeauftragten gewährleistet ist. Innerhalb des jeweiligen Unternehmens sind Vorkehrungen zu treffen, die es den Betroffenen oder anderen Stellen ermöglichen, den Datenschutzbeauftragten zu erreichen. **Beispiele**: Einrichtung einer Hotline, Kontaktformular auf der Homepage, Sprechstunde für Beschäftigte im Unternehmen etc..

2.3.13.2 Stellung des Datenschutzbeauftragten

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. Eine gesetzlich vorgeschriebene Ausbildung o.ä. für die Tätigkeit des Datenschutzbeauftragten existiert nicht. Der sogenannte Düsseldorfer Kreis stellt jedoch an die Fachkunde des Datenschutzbeauftragten Anforderungen, die den vertiefenden Hinweisen entnommen werden können. Eine **Abberufung** des Datenschutzbeauftragten ist nur aus wichtigem Grund in entsprechender Anwendung des § 626 BGB zulässig. Nach dem Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig.

2.3.13.3 Aufgaben des Datenschutzbeauftragten

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**

2.3.13.4 Bestellung des Datenschutzbeauftragten

Die Bestellung eines Datenschutzbeauftragten sollte aus Nachweis- und Dokumentationsgründen schriftlich erfolgen. Ein entsprechendes Muster ist als Anlage 5 beigefügt.

2.3.13.5 Neu: Veröffentlichung der Kontaktdaten und Meldung an die Aufsichtsbehörde

Anders als bisher müssen Verantwortliche und Auftragsverarbeiter die Kontaktdaten ihres Datenschutzbeauftragten

- **veröffentlichen und**
- **diese der zuständigen Aufsichtsbehörde mitteilen (Artikel 37 Abs. 7 DS-GVO)**

Daher sind seine Kontaktdaten sowohl **innerhalb der Organisation** des Verantwortlichen (Intranet, Organisationspläne), als auch z.B. auf der **Homepage** für außenstehende Dritte zu veröffentlichen.

Zu den zu veröffentlichenden Kontaktdaten des Datenschutzbeauftragten gehören mindestens folgende Informationen:

- Adresse
- Telefon-Nummer und
- E-Mail-Adresse des Datenschutzbeauftragten.

Artikel 37 Abs. 7 DS-GVO gibt nicht verpflichtend vor, dass auch der Name des Datenschutzbeauftragten zu den zu veröffentlichenden Daten gehört. Die Kontaktdaten sollten Angaben erhalten, die Betroffene in die Lage versetzen, den Datenschutzbeauftragten auf einfachem Wege (postalisch, persönliche Telefonnummer und/oder eine persönliche E-Mail Adresse) zu erreichen (vgl. WP 243 der Artikel 29 Datenschutzgruppe, „Leitlinien in Bezug auf Datenschutzbeauftragte“)

Zur Erfüllung der Mitteilungspflicht sehen die Internetseiten der Landesdatenschutzbehörden regelmäßig Eingabemasken bzw. Hinweise vor.

ANLAGE 5
Muster „Benennung eines/r betrieblichen Datenschutzbeauftragten“

2.3.14 Beschäftigtendatenschutz, § 26 BDSG

Die bisherige Regelung zum Beschäftigtendatenschutz gemäß § 32 BDSG-alt wurde durch die neue Regelung des § 26 BDSG nur marginal verändert. § 26 Abs. 1 BDSG 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 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.

2.3.15 Befugnisse der Aufsichtsbehörden und Sanktionen

Die Aufsichtsbehörden sind befugt, von einem Verantwortlichen die Bereitstellung aller Informationen zu verlangen, die für die Erfüllung ihrer Aufgaben, d.h. insbesondere die Überwachung und Durchsetzung der DS-GVO, erforderlich sind. Sie können Datenschutzprüfungen vornehmen und Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und –geräte z.B. des Kfz-Betriebs und des Auftragsverarbeiters verlangen.

2.3.15.1 Abhilfemaßnahmen der Aufsichtsbehörden

Die Aufsichtsbehörden verfügen gemäß Artikel 58 DS-GVO über sämtliche Abhilfemaßnahmen, die es ihr u.a. gestatten,

- einen Verantwortlichen oder Auftragsverarbeiter zu **warnen**, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen,
- einen Verantwortlichen oder Auftragsverarbeiter zu **verwarnen**, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstoßen hat,

- den Verantwortlichen oder den Auftragsverarbeiter **anzuweisen**, Verarbeitungsvorgänge ggf. auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen

Die letztgenannte Maßnahme wird in der Praxis sicherlich am häufigsten zur Anwendung kommen, sofern keine schwerwiegenden Datenschutzverstöße vorliegen. Die Aufsichtsbehörden sind jedoch befugt, **zusätzlich oder anstelle der o.g. Maßnahmen in Abhängigkeit der Umstände im Einzelfall**, **Geldbußen** gemäß Artikel 83 DS-GVO zu verhängen.

Bei der **Entscheidung über die Verhängung einer Geldbuße und über deren Betrag** sind in jedem Einzelfall gemäß Artikel 83 Absatz 2 DS-GVO u.a. folgende Umstände gebührend zu berücksichtigen:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- Jegliche von dem Verantwortlichen oder des Auftragsverarbeiters getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern.

Im Falle einer entsprechenden Kontaktaufnahme durch eine datenschutzrechtliche Aufsichtsbehörde sollten sich die Verantwortlichen daher in hohem Maße kooperativ zeigen.

2.3.15.2 Höhe der Bußgelder

Die **Bußgeldtatbestände** wurden durch die DS-GVO **massiv erhöht**. 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. Die Höhe der Bußgelder zielen vornehmlich auf international tätige Großkonzerne ab.

2.3.16 Auftragsverarbeitung, Artikel 28 DS-GVO

Werden personenbezogene Daten im Auftrag, z.B. von Dienstleistern, verarbeitet, liegt regelmäßig eine sogenannte Auftragsverarbeitung (ehem. Auftragsdatenverarbeitung) vor, sofern die betroffene Person nicht ausdrücklich in die Datenverarbeitung durch den Dienstleister eingewilligt hat.

Beispiele: Einsatz von Rechenzentren, Call-Centern, Werbeagenturen, Entsorger etc.

Der Abschluss eines Auftragsverarbeitungsvertrags, dessen Inhalt Artikel 28 Absatz 3. DS-GVO entsprechen muss, bleibt weiterhin erforderlich. 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.

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.

ANLAGE 6
Muster eines Datenverarbeitungsvertrages

2.3.17 Sonstiges

2.3.17.1 Videoüberwachung nach der DS-GVO

Siehe vertiefende Hinweise (Orientierungshilfen)

2.3.17.2 Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer oder international tätige Organisationen kann insbesondere bei Fabrikatsbetrieben von Belang sein, deren Vertragspartner/Hersteller ihren Sitz in Nicht-EU-Staaten haben und an diese eine Übertragung von personenbezogenen Daten erfolgen soll.

2.3.17.3 Verpflichtungserklärung von Beschäftigten auf die Vertraulichkeit

Beschäftigte sind auf die Einhaltung der Datenschutzvorschriften zu verpflichten. Eine **Verpflichtungserklärung ist als Anlage 7** beigefügt.

3 Vertiefende Hinweise / Nützliche Links

Zum Datenschutzrecht und dessen Umsetzung werden regelmäßig Muster und Orientierungshilfen veröffentlicht, die insbesondere auf den Internetseiten der Landesdatenschutzbehörden zur Verfügung stehen. Es wird empfohlen, diese Seite regelmäßig zu besuchen. Hervorzuheben ist insbesondere die Seite des Bayerischen Landesamtes für Datenschutzaufsicht unter www.lda.bayern.de.

- **Gesetzestext DS-GVO**
  https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE
- **Gesetzestext BDSG**
  https://www.gesetze-im-internet.de/bdsg_2018/
- **Praxishilfen zur DS-GVO**
  https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- **Orientierungshilfen zur DS-GVO**
  Siehe www.lda.bayern.de
- **Kurzpapiere der Deutschen Datenschutzkonferenz**
  https://www.datenschutzkonferenz-online.de/kurzpapiere.html
- **Leitlinien der Artikel-29-Gruppe**
  https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/Artikel-29-Gruppe.html
- **Anforderungen der DS-GVO an kleine Unternehmen, Vereine etc., hier: Kfz-Werkstatt**
  https://www.lda.bayern.de/media/muster_2_kfz-werkstatt.pdf
- **Muster-Verarbeitungsverzeichnis für Kfz-Werkstätten**
  https://www.lda.bayern.de/media/muster_2_kfz-werkstatt_verzeichnis.pdf

4 Anlagen

ÜBERSICHT

4.1 Muster-Datenschutzrechtliche Einwilligungserklärung (Anlage 1)

Muster-Datenschutzhinweise und Muster-Einwilligungserklärung

Die nachfolgenden Muster-Erklärungen beinhalten jeweils

- Datenschutzhinweise gemäß **Artikel 13 Datenschutzgrundverordnung** (DS-GVO) sowie
- eine **freiwillige Einwilligungserklärung** des Kunden zu Werbezwecken.

Die Muster setzen voraus, dass die personenbezogenen Daten bei der betroffenen Person direkt erhoben werden, z.B. im Rahmen eines Vertragsschlusses.

Für die Verwendung der Muster ist zu berücksichtigen, dass es sich um Muster handelt, die auf die konkrete Ausgestaltung der Datenverarbeitung von Kundendaten durch den Kfz-Betrieb angepasst werden müssen. Hilfestellungen bieten hierfür die Fußnoten in den Mustern sowie der Leitfaden des ZDK zum neuen Datenschutzrecht.

Die Muster differenzieren grundsätzlich danach, ob die Kundendaten - neben der eigentlichen Vertragsabwicklung - für weitergehende Zwecke, z.B. Werbung,

- **nur vom Kfz-Betrieb** (z.B. Werkstatt, Gebrauchtwagenhändler) ohne Übermittlung an einen Dritten (**Muster 1**)

  oder

- **vom Kfz-Betrieb und zusätzlich von einem Dritten** (z.B. Hersteller / Importeur / Bank / sonstigen Dritten) (**Muster 2**)

erhoben, genutzt und verarbeitet werden.

Je nach Einzelfall und der konkreten Nutzung der Daten ist daher ein entsprechendes Muster zu wählen und auf die individuellen Anforderungen anzupassen.

4.1.1 Muster 1: Einwilligungserklärung des Kunden gegenüber einem Kfz-Betrieb

Datenschutzhinweis gemäß Artikel 13 Datenschutzgrundverordnung (DS-GVO) und Einwilligungserklärung des Kunden zu Werbezwecken

- Unverbindliche Empfehlung des Zentralverband Deutsches Kraftfahrzeuggewerbe (ZDK) -

Unser Unternehmen nimmt den Schutz der Kundendaten ernst und möchte, dass sich jeder Kunde beim Besuch unserer Geschäftsräume wohl fühlt. Der Schutz der individuellen Privatsphäre bei der Verarbeitung persönlicher Daten ist für uns ein wichtiges Anliegen, das wir bei unseren Geschäftsprozessen mit hoher Aufmerksamkeit berücksichtigen. [1]

A. Datenverarbeitung zur Vertragsabwicklung und aufgrund gesetzlicher Verpflichtungen [2]

Die Verarbeitung der von Ihnen angegebenen personenbezogenen Daten in Verbindung mit den technischen Daten Ihres Fahrzeugs durch uns (oder einen von uns beauftragten Dienstleister [3]), ist zur ordnungsgemäßen Abwicklung des zugrunde liegenden Vertragsverhältnisses (Probefahrt, Kaufvertrag, Werkvertrag, Übermittlung an Garantiegeber, Leasinggeber und Finanzierungsinstitute, Mietwagenfirmen [4]) und soweit wir zu deren Erhebung gesetzlich verpflichtet sind, z.B. zur Einhaltung von Vorhaltefristen gegenüber dem Finanzamt, erforderlich. Die Verarbeitung der personenbezogenen Daten beruht auf Art. 6 Abs. 1 S. 1 lit. b und c DS-GVO. Die Daten werden gelöscht, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind.

Eine darüber hinausgehende, unter Abschnitt B. beschriebene Verarbeitung Ihrer personenbezogenen Daten erfolgt nur mit Ihrer Einwilligung (**freiwillig**).

B. Einwilligung in die Datenverarbeitung durch *(Name des Kfz-Betriebs angeben)* zu Werbezwecken

[5]

[ ] Ich bin damit einverstanden, dass das Autohaus (ggf. unter Einschaltung eines beauftragten Dienstleisters **[6]**), meine personenbezogenen Daten **[7]** in Verbindung mit den technischen Daten meines Fahrzeugs zum Zwecke der **Werbung** **[8]** (z.B. Kundeninformation und -betreuung, Einladungen zu Produktvorstellungen, Mitteilung über technische Neuerungen zu meinem Fahrzeug, Reifenwechsel, Serviceinformationen und Serviceaktionen, Anschlussangebote bei Auslauf des Leasing- /Finanzierungsvertrages, Neukaufoption für mein aktuelles Fahrzeug, Versendung von Kundenmagazinen, Befragung meiner Zufriedenheit mit den Leistungen des Autohauses), **bis auf Widerruf** **[9]** verwendet.

Zu den vorgenannten Zwecken möchte ich per

[ ] Post
[ ] E-Mail unter der E-Mail-Adresse _____ **[10]**
[ ] Telefon unter der Telefonnummer _____
[ ] SMS unter der Mobilnummer _____
(Zutreffendes bitte ankreuzen. Mehrfachnennungen sind möglich)

kontaktiert werden. Mir ist bewusst, dass diese Einwilligung **freiwillig** erfolgt und **jederzeit widerruflich** ist.

_____ _____

(Ort, Datum) (Unterschrift des Kunden) **[11]**

C. Datenschutzrechte des Kunden und Kontaktdaten [12]

Sie können von uns jederzeit **Auskunft** über Ihre gespeicherten personenbezogenen Daten erhalten (Artikel 15 DS-GVO), deren **Berichtigung** (Artikel 16 DS-GVO), **Löschung** (Artikel 17 DS-GVO) oder **Einschränkung der Verarbeitung** (Artikel 18 DS-GVO) verlangen sowie Ihr **Recht auf Datenübertragbarkeit** (Artikel 20 DS-GVO) geltend machen. Ebenfalls können Sie Ihre in Abschnitt B. erteilte Einwilligungserklärung jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft **ändern oder widerrufen** (Artikel 7 Abs. 3 DS-GVO). Durch den

Widerruf Ihrer Einwilligungserklärung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Zu den vorgenannten Zwecken wenden Sie sich bitte an eine der nachfolgenden Kontaktadressen.

Sie erreichen unseren **Datenschutzbeauftragten** unter:

Autohaus Mustermann
-Datenschutzbeauftragter-
Musterstrasse 21
53129 Bonn
Tel: xxxx
Mail: datenschutz@autohausmustermann.de

Für die Datenverarbeitung **verantwortlich**:

Autohaus Mustermann
Geschäftsführer: Max Mustermann
Musterstrasse 21
53129 Bonn
Tel: xxxx
E-Mail: xy@autohausmustermann.de

Ihnen steht des Weiteren ein **Beschwerderecht bei einer Aufsichtsbehörde** zu.

Die in den Abschnitten A. und C. genannten Datenschutzhinweise habe ich zur Kenntnis genommen.

_____ _____

(Ort, Datum) (Unterschrift des Kunden)

Das Original dieser Erklärung verbleibt beim Kfz-Betrieb. Der Kunde erhält eine Kopie.

Anmerkungen zum Muster 1

[1] Die Einleitung ist **optional** und kann **individuell formuliert** werden. Die nachfolgenden **Datenschutzhinweise** sind der betroffenen Person (Kunde) **zum Zeitpunkt der Erhebung** der Daten mitzuteilen, d.h. regelmäßig bei Vertragsabschluss.

[2] In Abschnitt A. ist dem Kunden die **Verwendung seiner Daten** zur Abwicklung des zugrunde liegenden Vertrages und zur Erfüllung gesetzlicher Verpflichtungen (z.B. Aufbewahrungspflichten) so **transparent und ausführlich** wie möglich zu beschreiben. Es müssen **alle Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage für jede einzelne Verarbeitung** genannt werden. Vom Kunden sollten zudem nur diejenigen personenbezogenen Daten erfragt und verarbeitet werden, die für die konkrete Vertragsabwicklung tatsächlich erforderlich sind (**Grundsatz der Datensparsamkeit**).

Ergänzungen des Musters in Abschnitt A.:

Sofern personenbezogene Daten auf Grundlage einer Interessenabwägung gemäß Artikel 6 Abs. 1 S.1 lit. f DS-GVO verarbeitet werden sollen, sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, zusätzlich zu benennen. Sollen die Daten zudem an ein Drittland außerhalb der EU oder eine internationale Organisation übermittelt werden, ist darauf unter Berücksichtigung der Vorgaben gemäß Artikel 13 Abs. 1 S. 1 lit. f DS-GVO ergänzend hinzuweisen. Ebenso ist zusätzlich darüber zu informieren, sofern eine automatisierte Entscheidungsfindung, einschließlich Profiling, vorgenommen wird.

[3] Sofern **externe Dienstleister** mit der Verarbeitung beauftragt werden, wie z.B. Auftragsverarbeiter, sind diese - sofern namentlich schon bekannt - **konkret und ansonsten in Form von Kategorien zu benennen**. Der Klammerinhalt ist entsprechend anzupassen. Er kann entfallen, wenn die Datenverarbeitung allein durch das Autohaus durchgeführt wird.

[4] Der Klammerzusatz ist in Abhängigkeit des Zwecks bzw. der Zwecke der Datenverarbeitung ggf. anzupassen.

[5] Die **Einwilligung des Kunden muss aktiv erfolgen**. Ob unter der DS-GVO auch weiterhin eine Opt-Out Variante bei der postalischen Werbung zulässig ist, kann

derzeit nicht beurteilt werden. Das Muster stellt daher darauf ab, dass der Kunde aktiv erklärt, ob er Werbung erhalten möchte und auf welchem Wege dies erfolgen soll (Post, E-Mail etc.). Der Einwilligungstext kann entsprechend angepasst werden, wenn der Kfz-Betrieb z.B. nur postalische und/oder E-Mail Werbung betreiben möchte. Der Einwilligungstext könnte dann um den Passus „…zum Zwecke der postalischen und E-Mail Werbung“ ergänzt werden. In diesem Fall macht der Kunde also nur ein Kreuz; die zusätzlichen Ankreuzoptionen können entfallen. Ebenso können weitere Ankreuzoptionen eingefügt werden, wenn der Kfz-Betrieb Kontaktkanäle anbietet, die im Muster nicht genannt sind.

[6] siehe Fußnote 3

[7] Aus Gründen der Transparenz kann dem Kunden an dieser Stelle mitgeteilt werden, welche konkreten **Daten für die Werbung genutzt werden**. Das Muster verweist insoweit nur auf die personenbezogenen Daten. Alternativ können auch Datenfelder in das Muster aufgenommen werden, die der Kunde zwecks Erhalt von Werbung ausfüllen muss. Eine Werbung erfolgt dann nur auf der Grundlage der vom Kunden in diesen Feldern angegeben Daten.

[8] Die **Zweckbestimmung(en)** der Nutzung der Kundendaten ist/sind zu **benennen und möglichst konkret zu beschreiben**. **Die Auflistung der Werbeformen im Klammerzusatz ist daher auf den konkreten Einzelfall anzupassen**.

[9] Die Einwilligung des Kunden gilt grundsätzlich bis auf Widerruf und muss nicht bei jedem Folgekontakt neu eingeholt werden. Obwohl die gesetzlichen Vorschriften keine zeitliche Geltungsdauer vorsehen, wird in der Praxis jedoch teilweise davon ausgegangen, dass Einwilligungserklärungen nicht unbeschränkt gültig sind. Eine vom Kunden erklärte Einwilligungserklärung sollte daher trotz der Musterformulierung „bis auf Widerruf“ nur herangezogen werden, solange der Kunde vernünftigerweise mit einer Verarbeitung seiner Daten rechnen muss. **Im Zweifelsfall wird empfohlen, von diesen Kunden vorsorglich eine erneute Einwilligungserklärung einzuholen**.

[10] Sofern der Kunde die E-Mail Adresse, Mobilnummer etc. bereits anderweitig angegeben hat, kann darauf Bezug genommen werden. Beispiel: „siehe Verbindliche Bestellung“

[11] Die Unterschrift des Kunden legitimiert die Werbung in Form der in Abschnitt B. beschriebenen und ausgewählten Kontaktarten. Erfolgt keine Unterschrift, ist eine Kontaktaufnahme des Kunden zu Zwecken der Werbung unzulässig.

[12] Der Kunde ist bereits bei der Datenerhebung auf sein Widerrufsrecht unter Angabe der hierfür erforderlichen Kontaktadresse(n) hinzuweisen. Macht der Kunde von seinen in Abschnitt C. genannten Rechten Gebrauch, ist vom Autohaus sicherzustellen, dass es sich auch wirklich um den betreffenden Kunden handelt (**Identitätsfeststellung**). Das Autohaus muss sich also von der Identität des Anfragenden überzeugen und darf ggf. weitere Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. **In Zweifelsfällen sollte der Kunde daher gebeten werden, schriftliche Informationen nachzureichen oder bereits seine Anfrage schriftlich zu stellen**.

Das Autohaus stellt die Informationen, wie z.B. beim Auskunftsrecht, grundsätzlich **unentgeltlich** zur Verfügung. Ausnahmen regelt Art. 12 Abs. 5 DS-GVO.

Die Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters und die Kontaktdaten des Datenschutzbeauftragten, sofern dieser erforderlich ist, sind zu nennen.

Es wird empfohlen, die zuständige Datenschutz-Aufsichtsbehörde mit Namen und Anschrift zu benennen.

4.1.2 Muster 2: Einwilligungserklärung gegenüber einem Kfz-Betrieb und dessen Hersteller/Importeur (sofern nicht dessen Einwilligungserklärung verwendet wird)

Datenschutzhinweis gemäß Artikel 13 Datenschutzgrundverordnung (DS-GVO) und Einwilligungserklärung des Kunden zu Werbezwecken

- Unverbindliche Empfehlung des Zentralverband Deutsches Kraftfahrzeuggewerbe (ZDK) -

Unser Unternehmen nimmt den Schutz der Kundendaten ernst und möchte, dass sich jeder Kunde beim Besuch unserer Geschäftsräume wohl fühlt. Der Schutz der individuellen Privatsphäre bei der Verarbeitung persönlicher Daten ist für uns ein wichtiges Anliegen, das wir bei unseren Geschäftsprozessen mit hoher Aufmerksamkeit berücksichtigen. [1]

A. Datenverarbeitung zur Vertragsabwicklung und aufgrund gesetzlicher Verpflichtungen [2]

Die Verarbeitung der von Ihnen angegebenen personenbezogenen Daten in Verbindung mit den technischen Daten Ihres Fahrzeugs durch uns (oder einen von uns beauftragten Dienstleister [3]), ist zur ordnungsgemäßen Abwicklung des zugrunde liegenden Vertragsverhältnisses (Probefahrt, Kaufvertrag, Werkvertrag, Übermittlung an Garantiegeber, Leasinggeber und Finanzierungsinstitute, Mietwagenfirmen [4]) und soweit wir zu deren Erhebung gesetzlich verpflichtet sind, z.B. zur Einhaltung von Vorhaltefristen gegenüber dem Finanzamt, erforderlich. Die Verarbeitung der personenbezogenen Daten beruht auf Art. 6 Abs. 1 S. 1 lit. b und c DS-GVO. Die Daten werden gelöscht, sobald sie für die vorgenannten Zwecke nicht mehr erforderlich sind.

Eine darüber hinausgehende, unter Abschnitt B. und C. beschriebene Verarbeitung Ihrer personenbezogenen Daten erfolgt nur mit Ihrer Einwilligung (**freiwillig**).

B. Einwilligung in die Datenverarbeitung durch *(Name des Kfz-Betriebs angeben)* zu Werbezwecken

[5]

[ ] Ich bin damit einverstanden, dass das Autohaus (ggf. unter Einschaltung eines beauftragten Dienstleisters **[6]**), meine personenbezogenen Daten **[7]** in Verbindung mit den technischen Daten meines Fahrzeugs zum Zwecke der **Werbung** **[8]** (z.B. Kundeninformation und -betreuung, Einladungen zu Produktvorstellungen, Mitteilung über technische Neuerungen zu meinem Fahrzeug, Reifenwechsel, Serviceinformationen und Serviceaktionen, Anschlussangebote bei Auslauf des Leasing- /Finanzierungsvertrages, Neukaufoption für mein aktuelles Fahrzeug, Versendung von Kundenmagazinen, Befragung meiner Zufriedenheit mit den Leistungen des Autohauses), **bis auf Widerruf** **[9]** verwendet.

Zu den vorgenannten Zwecken möchte ich per

[ ] Post
[ ] E-Mail unter der E-Mail-Adresse _____ **[10]**
[ ] Telefon unter der Telefonnummer _____
[ ] SMS unter der Mobilnummer _____
(Zutreffendes bitte ankreuzen. Mehrfachnennungen sind möglich)

kontaktiert zu werden. Mir ist bewusst, dass diese Einwilligung **freiwillig** erfolgt und **jederzeit widerruflich** ist.

_____ _____

(Ort, Datum) (Unterschrift des Kunden) **[11]**

C. Einwilligung in die Übermittlung Ihrer Daten an den Hersteller/Importeur [12]

[ ] Ich bin damit einverstanden, dass das Autohaus die unter B. genannten Daten für folgende Zwecke

- Werbung und
- Kundenzufriedenheitsbefragungen **[13]**

an den *Hersteller/Importeur, Anschrift*, übermittelt. Hierfür kann der Hersteller/Importeur ggf. auch Agenturen oder Meinungsforschungsinstitute (*möglichst namentlich angeben*) beauftragen.

Zu den vorgenannten Zwecken möchte ich per

[ ] Post
[ ] E-Mail unter der E-Mail-Adresse _____
[ ] Telefon unter der Telefonnummer _____
[ ] SMS unter der Mobilnummer _____
(Zutreffendes bitte ankreuzen. Mehrfachnennungen sind möglich)

kontaktiert werden. Mir ist bewusst, dass diese Einwilligung **freiwillig** erfolgt und **jederzeit widerruflich** ist.

_____ _____

(Ort, Datum) (Unterschrift des Kunden)

D. Datenschutzrechte des Kunden und Kontaktdaten[14]

Sie können von uns jederzeit **Auskunft** über Ihre gespeicherten personenbezogenen Daten erhalten (Artikel 15 DS-GVO), deren **Berichtigung** (Artikel 16 DS-GVO), **Löschung** (Artikel 17 DS-GVO) oder **Einschränkung der Verarbeitung** (Artikel 18 DS-GVO) verlangen sowie Ihr **Recht auf Datenübertragbarkeit** (Artikel 20 DS-GVO) geltend machen. Ebenfalls können Sie Ihre in Abschnitt B. und C. erteilte(n) Einwilligungserklärung(en) jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft **ändern oder widerrufen** (Artikel 7 Abs. 3 DS-GVO). Durch den Widerruf Ihrer Einwilligungserklärung(en) wird die Rechtmäßigkeit der aufgrund der Einwilligung(en) bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Zu den vorgenannten Zwecken wenden Sie sich bitte an eine der nachfolgenden Kontaktadressen.

Kontaktdaten des Autohauses

Sie erreichen unseren **Datenschutzbeauftragten** unter:

Autohaus Mustermann
-Datenschutzbeauftragter-
Musterstrasse 21
53129 Bonn
Tel: xxxx
Mail: datenschutz@autohausmustermann.de

Für die Datenverarbeitung **verantwortlich**:

Autohaus Mustermann
Geschäftsführer: Max Mustermann
Musterstrasse 21
53129 Bonn
Tel: xxxx
E-Mail: xy@autohausmustermann.de

Kontaktdaten des Herstellers/Importeurs

Angabe der Kontaktdaten des Datenschutzbeauftragten des Herstellers/Importeurs

und

Angabe der Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreters des Herstellers/Importeurs

Ihnen steht des Weiteren ein **Beschwerderecht bei einer Aufsichtsbehörde** zu.

Die in den Abschnitten A. und D. genannten Datenschutzhinweise habe ich zur Kenntnis genommen.

_____ _____

(Ort, Datum) (Unterschrift des Kunden)

Das Original dieser Erklärung verbleibt beim Kfz-Betrieb. Der Kunde erhält eine Kopie.

Anmerkungen zu Muster 2

[1] Die Einleitung ist **optional** und kann **individuell formuliert** werden. Die nachfolgenden **Datenschutzhinweise** sind der betroffenen Person (Kunde) **zum Zeitpunkt der Erhebung** der Daten mitzuteilen, d.h. regelmäßig bei Vertragsabschluss.

[2] In Abschnitt A ist dem Kunden die **Verwendung seiner Daten** zur Abwicklung des zugrunde liegenden Vertrages und zur Erfüllung gesetzlicher Verpflichtungen (z.B. Aufbewahrungspflichten) so **transparent und ausführlich** wie möglich zu beschreiben. Es müssen **alle Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage für jede einzelne Verarbeitung** genannt werden. Vom Kunden sollten zudem nur diejenigen personenbezogenen Daten erfragt und verarbeitet werden, die für die konkrete Vertragsabwicklung tatsächlich erforderlich sind (**Grundsatz der Datensparsamkeit**).

Ergänzungen des Musters in Abschnitt A.:

Sofern personenbezogene Daten auf Grundlage einer Interessenabwägung gemäß Artikel 6 Abs. 1 S. 1 lit. f DS-GVO verarbeitet werden sollen, sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, zusätzlich zu benennen. Sollen die Daten zudem an ein Drittland außerhalb der EU oder eine internationale Organisation übermittelt werden, ist darauf unter Berücksichtigung der Vorgaben gemäß Artikel 13 Abs. 1 S. 1 lit. f DS-GVO ergänzend hinzuweisen. Ebenso ist zusätzlich darüber zu informieren, sofern eine automatisierte Entscheidungsfindung, einschließlich Profiling, vorgenommen wird.

[3] Sofern **externe Dienstleister** mit der Verarbeitung beauftragt werden, wie z.B. Auftragsverarbeiter, sind diese - sofern namentlich schon bekannt - **konkret und ansonsten in Form von Kategorien zu benennen**. Der Klammerinhalt ist entsprechend anzupassen. Er kann entfallen, wenn die Datenverarbeitung allein durch das Autohaus durchgeführt wird.

[4] Der Klammerzusatz ist in Abhängigkeit des Zwecks bzw. der Zwecke der Datenverarbeitung ggf. anzupassen.

[5] Die **Einwilligung des Kunden muss aktiv erfolgen**. Ob unter der DS-GVO auch weiterhin eine Opt-Out Variante bei der postalischen Werbung zulässig ist, kann

derzeit nicht beurteilt werden. Das Muster stellt daher darauf ab, dass der Kunde aktiv erklärt, ob er Werbung erhalten möchte und auf welchem Wege dies erfolgen soll (Post, E-Mail etc.). Der Einwilligungstext kann entsprechend angepasst werden, wenn der Kfz-Betrieb z.B. nur postalische und/oder E-Mail Werbung betreiben möchte. Der Einwilligungstext könnte dann um den Passus „…zum Zwecke der postalischen und E-Mail Werbung“ ergänzt werden. In diesem Fall macht der Kunde also nur ein Kreuz; die zusätzlichen Ankreuzoptionen können entfallen. Ebenso können weitere Ankreuzoptionen eingefügt werden, wenn der Kfz-Betrieb Kontaktkanäle anbietet, die im Muster nicht genannt sind.

[6] siehe Fußnote 3

[7] Aus Gründen der Transparenz kann dem Kunden an dieser Stelle mitgeteilt werden, welche konkreten **Daten für die Werbung genutzt werden**. Das Muster verweist insoweit nur auf die personenbezogenen Daten. Alternativ können auch Datenfelder in das Muster aufgenommen werden, die der Kunde zwecks Erhalt von Werbung ausfüllen muss. Eine Werbung erfolgt dann nur auf der Grundlage der vom Kunden in diesen Feldern angegeben Daten.

[8] Die **Zweckbestimmung(en)** der Nutzung der Kundendaten ist/sind zu **benennen und möglichst konkret zu beschreiben**. **Die Auflistung der Werbeformen im Klammerzusatz ist daher auf den konkreten Einzelfall anzupassen**.

[9] Die Einwilligung des Kunden gilt grundsätzlich bis auf Widerruf und muss nicht bei jedem Folgekontakt neu eingeholt werden. Obwohl die gesetzlichen Vorschriften keine zeitliche Geltungsdauer vorsehen, wird in der Praxis jedoch teilweise davon ausgegangen, dass Einwilligungserklärungen nicht unbeschränkt gültig sind. Eine vom Kunden erklärte Einwilligungserklärung sollte daher trotz der Musterformulierung „bis auf Widerruf“ nur herangezogen werden, solange der Kunde vernünftigerweise mit einer Verarbeitung seiner Daten rechnen muss. **Im Zweifelsfall wird empfohlen, von diesen Kunden vorsorglich eine erneute Einwilligungserklärung einzuholen**.

[10] Sofern der Kunde die E-Mail Adresse, Mobilnummer etc. bereits anderweitig angegeben hat, kann darauf Bezug genommen werden. Beispiel: „siehe Verbindliche Bestellung“

[11] Die Unterschrift des Kunden legitimiert die Werbung in Form der in Abschnitt B. beschriebenen und ausgewählten Kontaktarten. Erfolgt keine Unterschrift, ist eine Kontaktaufnahme des Kunden zu Zwecken der Werbung unzulässig.

[12] Die Trennung zwischen der Verarbeitung der Kundendaten durch den Kfz-Betrieb und dessen Hersteller/Importeur dient der besseren Übersichtlichkeit und dem besseren Verständnis für den Kunden. Wir halten es grundsätzlich für möglich, die Abschnitte B. und C. auch zusammen zu fassen.

Werden die Daten zusätzlich an Dritte, wie z.B. **Banken und Leasinggesellschaften** übermittelt, so ist für diese Übermittlung ein zusätzlicher Abschnitt einzufügen, der dem Aufbau des Abschnitt C. entspricht und inhaltlich an die entsprechenden Datenempfänger und deren Nutzung der Daten angepasst wird.

In jedem Fall ist zu prüfen, ob zwischen dem Kfz-Betrieb und dem Hersteller/Importeur oder sonstigen Dritten ggf. ein Auftragsverarbeitungsverhältnis besteht. Sofern ein solches Verhältnis besteht und der Hersteller/Importeur oder sonstige Dritte die Daten ausschließlich für den Kfz-Betrieb nutzen, ist Abschnitt C überflüssig.

Im Übrigen gelten für Abschnitt C. die Anmerkungen zu Abschnitt B. entsprechend.

[13] Die Zwecke der Datenverarbeitung durch den Hersteller/Importeur sind anzugeben.

[14] Der Kunde ist bei der Datenerhebung auf sein Widerrufsrecht unter Angabe der hierfür erforderlichen Kontaktadresse(n) hinzuweisen. Macht der Kunde von seinen in Abschnitt D. genannten Rechten Gebrauch, ist vom Autohaus sicherzustellen, dass es sich auch wirklich um den betreffenden Kunden handelt (**Identitätsfeststellung**). Das Autohaus muss sich also von der Identität des Anfragenden überzeugen und darf ggf. weitere Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. **In Zweifelsfällen sollte der Kunde daher gebeten werden, schriftliche Informationen nachzureichen oder bereits seine Anfrage schriftlich zu stellen**.

Das Autohaus stellt die Informationen, wie z.B. beim Auskunftsrecht, grundsätzlich **unentgeltlich** zur Verfügung. Ausnahmen regelt Art. 12 Abs. 5 DS-GVO.

Die Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters und die Kontaktdaten des Datenschutzbeauftragten des Autohauses sowie des Herstellers/Importeurs sind zu nennen.

Es wird empfohlen, die zuständige Datenschutz-Aufsichtsbehörde mit Namen und Anschrift zu benennen.

4.2 Muster – Auskunftserteilung an einen Kunden (Anlage 2)

Auskunftserteilung eines Kfz-Betriebs an einen Kunden gemäß Artikel 15 Datenschutzgrundverordnung (DS-GVO)

(Unverbindliches Muster)

Sehr geehrte/r Frau/Herr _____,

Sie haben um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person gespeichert haben. Hierzu möchten wir Ihnen gerne folgende Informationen geben:

Sie sind bei uns als ……*(z.B. Kunde/Interessent)* erfasst. Eine Kopie der von uns über Sie gespeicherten personenbezogenen Daten entnehmen Sie bitte der Anlage. *[Falls keine Kopie erstellt werden kann, bietet es sich an, die Kundendaten mit Hilfe einer Tabelle darzustellen. In diesem Fall könnte der Satz lauten: „Die über Sie gespeicherten Daten entnehmen Sie bitte der beigefügten Tabelle“]*

Eine Datenverarbeitung Ihrer personenbezogenen Daten durch unser Unternehmen dient den folgenden Zwecken *[die einzelnen Verarbeitungszwecke sind anzugeben]*:

- *Ordnungsgemäße Abwicklung des zugrundeliegenden Vertragsverhältnisses*
- *Kommunikation mit Ihnen, z.B. in Form von Werbung*

Zur ordnungsgemäßen Vertragsabwicklung haben wir Ihre Daten an folgende Empfänger übermittelt: Hersteller/Importeur,…. [*wenn eine Weitergabe erfolgte, sind die Empfänger anzugeben. Falls keine Weitergabe erfolgte bzw. auch nicht geplant ist, kann der Satz entfallen und der Hinweis „Eine Offenlegung ihrer Daten gegenüber Dritten erfolgt nicht*“ aufgenommen werden].

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung erforderlich sind. Sofern Daten hiervon nicht erfasst sind, werden

sie gelöscht, sobald sie für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden. Eine automatisierte Entscheidungsfindung einschließlich Profiling findet nicht statt.

Sie haben das Recht auf Berichtigung (Artikel 16 DS-GVO) oder Löschung (Artikel 17 DS-GVO) der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung (Artikel 18 DS-GVO). Ihnen steht zudem ein Widerspruchsrecht gegen die Verarbeitung (Artikel 17 DS-GVO) zu. In diesen Fällen wenden Sie sich gerne an uns. Ebenfalls steht Ihnen ein Beschwerderecht bei einer Aufsichtsbehörde (Artikel 15 Abs. 1 f) DS-GVO) zu.

Wir hoffen, dass wir Ihre Fragen mit den vorstehenden Ausführungen hinreichend beantworten konnten. Informieren Sie uns bitte, falls Daten unrichtig sind.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

Anlage

Muster einer Tabelle zur Darstellung der gespeicherten Kundendaten. Diese Tabelle ist auf den konkreten Einzelfall anzupassen.

Kunde	
Familienname	
Vorname	
Geburtsname	
Geschlecht	
Geburtsdatum	
Staatsangehörigkeit	
Straße	
PLZ	
Wohnort	
UstID	
Kommunikationsdaten	
Telefon	
Handy	
E-Mail	

Bankverbindung	
Bankname	
IBAN-Nummer	
BIC	
Fahrzeugdaten	
Angaben zum Fahrzeug	
FIN	
etc.	

4.3 Muster - Verarbeitungsverzeichnis (Anlage 3)

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DS-GVO)

1. Verantwortlicher (=Firma/Legaleinheit) *[Name/Ladungsfähige Anschrift]*

2. Gesetzlicher Vertreter (= Geschäftsführung) *[Name/Kontaktdaten]*

3. Vertreter in der EU (gemäß Art. 27 DS-GVO) [Name / Ladungsfähige Anschrift]

4. Datenschutzbeauftragter *[Name/Kontaktdaten]*

Optionale Inhalte / Übergreifende Regelungen und Sachverhalte

5. Zuständige Aufsichtsbehörde

[Name]

Meldung des/der Datenschutzbeauftragten erfolgt:

[ ] Ja

[ ] Nein

6. Regelungen zur Datensicherheit

[Verweis auf übergreifende IT-Sicherheitskonzepte, die grunds. für alle Verarbeitungstätigkeiten gelten]

7. Regelungen zur Datenlöschung

[Verweis auf übergreifende Löschkonzepte, die grunds. für alle Verarbeitungstätigkeiten gelten]

8. Sachverhalte zu Drittstaatenübermittlungen

[Verweis auf übergreifende Punkte wie BCR, die grunds. für alle Verarbeitungstätigkeiten gelten]

Erläuterungen

Nr. 1	Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO) Angaben: Name/Firma, ladungsfähige Anschrift
Nr. 2	Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter Angaben: Namen der geschäftsführenden Personen *Ggf. kann hier einfach ein Link auf das Web-Impressum eingetragen werden.*
Nr. 3	Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DS-GVO, Art. 27 Abs. 1 DS-GVO) anzugeben.
Nr. 4	Vom Verantwortlichen bestellter Datenschutzbeauftragter* [Name, Kontaktdaten
Nr. 5	Die Meldung der Kontakt-Informationen des DSB – z.B. (Funktions-)e-mail-Adresse, Telefonnummer – ist verpflichtend.
Nr. 6	Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) – Der Verweis an dieser Stelle auf übergreifende Regelungen entbindet nicht von der Dokumentation von ggf. erforderlichen Abweichungen zu den einzelnen Verarbeitungstätigkeiten. Verweis z.B. auf ein IT-Sicherheitskonzept, das alle Verarbeitungstätigkeiten einschließt. Eventuell auch Verweise auf relevante Dokumente eines ISMS nach ISO27001.

Nr. 7	Verweis auf Löschkonzepte, die grds. für alle Verarbeitungen gelten.
Nr. 8	Ein Verweis Regelungen zur Drittstaatenübermittlung sind hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR.
--------	*Ende optional* -------

Verzeichnis von Verarbeitungstätigkeiten

Anlage Nr. _____

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DS-GVO)

1. Bezeichnung der Verarbeitungstätigkeit

2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (optionaler Inhalt)

3. Bei gemeinsamer Verantwortlichkeit:
   Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

Angaben zur Verarbeitungstätigkeit

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

6.1 Betroffene Personengruppen	6.2 Kategorien personenbezogener Daten

7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

[interne, externe – auch im Konzern, eingebundene Dienstleister]

8. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 e DS-GVO)

Übermittlung

□ Ja
□ Nein

Name des Drittlandes / der internationalen Organisation (DS-GVO)

--- *Optionale Angaben* ---

Ggf. vereinbarte Garantien

□ Anerkannter Drittstaat

□ EU-Standardvertrag C/C

□ EU-Standardvertrag C/P

□ Aufsichtsbehördlich genehmigter Vertrag

□ BCR

□ Andere:

--- *Ende optionale Angaben* ---

Garantien zum Schutz der personenbezogenen Daten im Drittland, soweit weder eine Anerkennung des Datenschutzniveaus, EU-Standardverträge noch BCR vorliegen:

9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

10.1 Art der eingesetzten DV-Anlagen und Software (optional)

- DV-Anlagen

- Software (und ggf. Unterprogramme) - Schnittstellen
10.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO) - [Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen] *oder: Link auf TOM (Processor) hier anführen* *oder: Verweis auf Datenschutz-Zertifizierung etc.*

----- *Optionale Angaben* ----

Weitere Dokumentationen zur Verarbeitungstätigkeit

z. B.: - *Zu Informationspflichten* - *Zu Verträgen mit Dienstleistern* - *Zu Vereinbarungen zur gemeinsamen Verantwortung* - *Zu durchgeführten Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten*

----- *Ende optionale Angaben*----

Erläuterungen

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: - Allgemeine Kundenverwaltung - Customer-Relationship-Management (CRM)
Nr. 2	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 3	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 Lit. a DS-GVO, Art. 26 Abs. 1 DS-GVO)
Nr. 4	Beispiele: - Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ - Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“ Eine Verarbeitungstätigkeit (aus der Anwendung des BDSG als „Verfahren“ vertraut) kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so

	dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-Einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung, oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Accountability-Pflichten und die Gewährleistung von transparenzpflichten ggü. betroffenen Personen notwendig.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, so müssen diese so konkret wie möglich sein. Nicht ausreichend, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder Ähnliches. Beispiele: - Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten,

	Bankverbindung - Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU -------- *Start optional* ------- - Geeignete Garantien beim Empfänger sind grds. erforderlich, falls für den kein - Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DS-GVO - vorliegt. Solche Garantien können gem. Art. 46 DS-GVO durch verbindliche - interne Datenschutzvorschriften (BCR) oder EU-Standardverträge erbracht werden. -------- *Ende optional* ------- Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO)

Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept (**siehe Hauptblatt Nr. 6**) zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, so sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren. (Art. 35 Abs. 7 lit. d DS-GVO). Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).

Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • *Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DS-GVO)* • *Verträge mit Dienstleistern (Art. 28 DS-GVO)* • *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DS-GVO)* • *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen* • *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DS-GVO)*

Quelle: gdd

4.4 Checkliste „Technische und organisatorische Maßnahme“ (Anlage 4)

1. Organisatorische Maßnahmen

☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
☐ Nein
☐ Ja
Name: …….
Funktion: ……
E-Mail: ……
Telefon: …….
☐ Mitarbeiter wurden nachweislich über Datenschutzrecht und Datensicherheit geschult.
☐ Alle Mitarbeiter sind nachweislich auf das Datengeheimnis, ggf. auf das Fernmeldegeheimnis, verpflichtet.
☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z.B. technisch unterstützt oder durch Externe).
☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden.
☐ Ein Datenschutzkonzept ist vorhanden.
☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am _____und Bestätigung s. Anlage ____).
☐ Verhaltensregeln nach Art. 40 DS-GVO sind vorhanden (Unterwerfung am _____und Bestätigung s. Anlage ____).

2. Vertraulichkeit

a) <u>Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle</u>

Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet werden.

☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
☐ Alarmanlage
☐ Automatisches Zutrittskontrollsystem, Ausweisleser
☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)

- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☐ Sicherheitsschlösser
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Biometrie (Fingerabdrücke o. ä.)
- ☐ Manuelles Schließsystem
- ☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
- ☐ Magnetschleusen
- ☐ Werkschutz/Pförtner
- ☐ Empfang mit Anmeldung
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

b) ***Zugangs- und Benutzerkontrolle***

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
  Länge des Passworts: … Zeichen
  Wechselfristen … Wochen/Monate
  Anzahl der Fehleingaben …
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern

c) ***Zugriffskontrolle***

Maßnahmen, die gewährleisten, dass Personen nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ Schriftliches Berechtigungskonzept vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand: ….
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern
- ☐ Löschungskonzept für Daten
- ☐ Protokollierung der Vernichtung

d) Transport- und Übertragungskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen *Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall: Die nach dem Stand der Technik erforderlichen Firewall-Technologien sind implementiert und werden auf dem aktuellen Stand gehalten
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschließbarer Transportbehälter), auch für Papier

e) ***Auftragskontrolle***

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☐ Vorhandene Vereinbarungen zur Auftragsverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

3. Integrität

a) *Eingabekontrolle/Verarbeitungskontrolle*

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

b) ***Dokumentationskontrolle***

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verarbeitungsverzeichnisses
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Zulässigkeit eines Datentransfers in Drittländer ist gegeben

4. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und im Störfall wieder hergestellt werden können.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

5. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

4.5 Muster – Benennung eines Datenschutzbeauftragten (Anlage 5)

Benennung eines/r betrieblichen Datenschutzbeauftragten

(Unverbindliches Muster)

Herrn/Frau
Michael(a) Muster
Mustergasse 1
33333 Musterstadt

Sehr geehrte/r Frau/Herr _____,

ich/wir benennen Sie mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 Abs. 1 b) und c) EU-Datenschutzgrundverordnung (DS-GVO) in Verbindung mit

§ 38 Bundesdatenschutzgesetz (BDSG). In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsleitung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsleitung ist

_____

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DS-GVO sowie § 38 BDSG. In Anwendung Ihrer Fachkunde auf dem Gebiet des Datenschutzes sind Sie weisungsfrei. Bei der Erfüllung Ihrer Aufgaben sind Sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über Ihre Tätigkeit werden Sie der Geschäftsleitung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsleitung vor.

_____ _____

Ort, Datum Unterschrift Geschäftsleitung

Mit der Benennung bin ich einverstanden.

_____

Unterschrift, Datenschutzbeauftragte/r

4.6 Muster – Auftragsverarbeitungsvertrag (Anlage 6)

MUSTERVERTRAG ZUR AUFTRAGSVERARBEITUNG GEMÄß ART. 28 DS-GVO

[Stand: Mai 2017]

Vereinbarung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO:

.....]

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DS-GVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen. Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/..... vom ....., auf die hier verwiesen wird (im folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ……
(Definition der Aufgaben)

(2) Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in …….

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

☐ wird hergestellt durch sonstige Maßnahmen: ……. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

(2) Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ...

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zutreffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

   ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

   ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

   ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat,

dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu

gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

c) ☐ Die Auslagerung auf Unterauftragnehmer oder

☐ der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen

Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

ANLAGE - TECHNISCH-ORGANISATORISCHE MAßNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer

Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;

- Incident-Response-Management;

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Quelle: gdd

4.7 Muster – Verpflichtung von Beschäftigten auf Vertraulichkeit (Anlage 7)

Verpflichtungserklärung auf Vertraulichkeit

(Unverbindliches Muster)

Das Datenschutzrecht verlangt, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität

ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Es ist Ihnen gesetzlich untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugter Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses fort.

Frau/Herr	Abteilung/Tätigkeit
_____	_____

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten. Weitergehende Informationen zum geltenden Datenschutzrecht entnehmen Sie bitte dem ZDK Leitfaden zum Datenschutz.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift.

_____,	_____
Ort, Datum	Verpflichtete(r)

4.8 Fragebogen (Checkliste) zur Umsetzung des DS-GVO (Anlage 8)

Fragen/Checkliste zur Vorbereitung auf die DS-GVO

1. Datenschutz ist Chefsache

[ ] Haben Sie sich als Geschäftsleitung schon mit den neuen Anforderungen der DS-GVO und des BDSG (neu) befasst? Kennen Sie insbesondere die neuen Regelungen

- [ ] zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Art. 5 Absatz 2 DS-GVO)?
- [ ] zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten (Art. 12 - 14 DS-GVO)?
- [ ] zu den Rechten der Betroffenen auf Datenübertragbarkeit (Art. 20 DS-GVO)?
- [ ] zur technischen und organisatorischen Sicherheit der Datenverarbeitung Art. 32 DS-GVO?
- [ ] zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)?
- [ ] zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO)?

[ ] Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten bestellt (Art. 37 DS-GVO, § 38 BDSG neu)?

[ ] Wurden Ihre Beschäftigen über die neuen Datenschutzregelungen informiert und/oder geschult?

Anmerkungen:

_____

_____

_____

2. Bestandsaufnahme

[ ] Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)? Denken Sie hierbei insbesondere an die

  [ ] Verarbeitung von Kundendaten

  [ ] Verarbeitung von Beschäftigtendaten

  [ ] Verarbeitung von Daten für Dritte als Auftragsverarbeiter

[ ] Wird dieses Verzeichnis regelmäßig aktualisiert? Wer ist hierfür in Ihrem Unternehmen zuständig?

Anmerkungen:

_____
_____
_____
_____
_____

3. Zulässigkeit der Verarbeitung

Auch nach neuem Recht benötigen Sie für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

[ ] Haben Sie für alle Verarbeitungen eine Rechtsgrundlage nach der neuen Rechtslage (Art. 6 bis 11 DS-GVO sowie § 26 BDSG neu)?

[ ] Haben Sie dies dokumentiert?

[ ] Haben Sie Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten usw. an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)? Siehe

hierzu die Muster-Einwilligungserklärung des ZDK bzw. Muster der Hersteller/Importeure.

Anmerkungen:

_____
_____
_____
_____
_____

4. Betroffenenrechte und Informationspflichten

[ ] Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DS-GVO). Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher?

Besonders wichtig sind in diesem Zusammenhang folgende Informationen:

[ ] Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)

[ ] Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten

[ ] Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer

[ ] Hinweis auf Betroffenenrechte

[ ] Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Widerruf der Einwilligung

[ ] Recht auf Beschwerde bei der Aufsichtsbehörde

[ ] Herkunft der Daten

[ ] Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15-22 DS-GVO)? Denken Sie dabei insbesondere an folgende Rechte:

[ ] Recht auf Auskunft

[ ] Recht auf Berichtigung

[ ] Recht auf fristgemäße Löschung der verarbeiteten Daten

[ ] Recht auf Einschränkung der Verarbeitung

[ ] Recht auf Datenübertragbarkeit

Anmerkungen:

_____
_____
_____
_____
_____

5. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

[ ] Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DS-GVO)? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung4 dokumentiert?

[ ] Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? In welchen Fällen?

[ ] Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?

[ ] Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Art. 25 DS-GVO)?

Anmerkungen:

_____
_____
_____
_____
_____

6. Verträge prüfen

[ ] Entsprechen die bestehenden Verträge mit Ihrem Hersteller/Importeur den neuen Datenschutzvorgaben?

[ ] Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d.h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 26 – 28 DS-GVO) angepasst?

[ ] Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

[ ] Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist, entsprechende zusätzliche Garantien/Vereinbarungen?

  [ ] EU-Standardvertragsklauseln

  [ ] Binding Corporate Rules

  [ ] Privacy Shield (nur für die USA)

Anmerkungen:

_____
_____
_____
_____
_____

7. Datenschutz-Folgenabschätzung

[ ] Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Art. 35 DS-GVO)? Dies gilt z.B. bei einer Videoüberwachung.

[ ] Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?

[ ] Wer ist für diesen Prozess zuständig?

Anmerkungen:

_____
_____
_____
_____
_____

8. Meldepflichten

[ ] Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)?

[ ] Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet?

[ ] Wer ist in Ihrem Unternehmen für die Meldung zuständig?

[ ] Falls Sie einen Datenschutzbeauftragten bestellt haben, denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde. Ebenso sind dessen Kontaktdaten zu veröffentlichen, z.B. auf der Homepage.

Anmerkungen:

_____
_____
_____
_____
_____

9. Dokumentation

[ ] Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen?

[ ] Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

Anmerkungen:

_____
_____
_____
_____
_____

4.9 Kontaktdaten der Landesdatenschutzbehörden (Anlage 9)

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/


KRAFTFAHRZEUG
GEWERBE