# Anlagen

|  |
| --- |
| Übersicht |
| * **Anlage 1** Muster - Datenschutzrechtliche Einwilligungserklärung
* **Anlage 2** Muster - Auskunftserteilung an einen Kunden
* **Anlage 3** Muster - Verarbeitungsverzeichnis
* **Anlage 4** Checkliste „Technische und organisatorische Maßnahme“
* **Anlage 5** Muster - Benennung eines Datenschutzbeauftragten
* **Anlage 6** Muster - Auftragsverarbeitungsvertrag
* **Anlage 7** Muster - Verpflichtung von Beschäftigten auf Vertraulichkeit
* **Anlage 8** Fragebogen (Checkliste) zur Umsetzung des DS-GVO
* **Anlage 9** Kontaktdaten der Landesdatenschutzbehörden
 |

## 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.

### 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.

### 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.

## 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. |  |

## 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**

|  |
| --- |
| 1. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit
 |

|  |
| --- |
| 1. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit
 |

|  |
| --- |
| 1. 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 |
|  |  |
|  |  |

|  |
| --- |
| 1. 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]* |

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

Übermittlung□ Ja□ NeinName 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: |

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

|  |
| --- |
| 1. 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 EWRBeispiele 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

## 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**

1. ***Zutritts-, Zugangs-, Speicher- und Datenträgerkontrolle***

*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

1. ***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

1. ***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

1. ***Transport- und Übertragungskontrolle***

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektroni*schen 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

1. ***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**

1. ***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

1. ***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

## 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

## 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.
1. **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
* ...
1. **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.

1. **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.

1. **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:

1. [ ]  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.
1. [ ]  Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
2. [ ]  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].

1. 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.
2. 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].
3. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
4. 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.
5. 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.
6. 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.
7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
8. **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.

1. [ ]  Eine Unterbeauftragung ist unzulässig.
2. [ ]  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 |
|  |  |  |

1. [ ]  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.

1. **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.

1. **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.

1. 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
2. die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
3. 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
4. die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
5. 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.

1. **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.

1. **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;
1. **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;
1. **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);
1. **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

## 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)

## 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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 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](http://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/>