# Anlagen

## Anlage 1 - Einwilligungserklärung des Verbrauchers für SHK-Unternehmen (Muster)[[1]](#footnote-1)

In unserem Werbenewsletter informiert die **Mustermannbetrieb GmbH** ihre Kunden postalisch oder per E-Mail über Aktionsrabatte, aktuelle Leistungen und Neuigkeiten. Dies ist ein kostenloser Service für Sie.

□ **Ja, ich/wir bin/sind damit einverstanden**, dass meine/unsere Kontaktdaten

(Name, Adresse, Faxnummer und E-Mail-Adresse) zum Zweck der Produktwerbung und Informationen zum Leistungsspektrum des Betriebs gespeichert und zur Kontaktaufnahme genutzt werden.

Mir/uns ist dabei klar, dass diese Einwilligung freiwillig und jederzeit widerruflich ist. Der Widerruf ist

per E-Mail zu richten an: info@mustermannbetrieb.de

oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht zu den oben genannten Zwecken nutzen und verarbeiten bzw. löschen.

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

Ort, Datum, Unterschrift

Die Datenverarbeitung ist für die Zusendung der Produktwerbung per E-Mail erforderlich und beruht auf Artikel 6 Abs. 1 a) DSGVO. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie sind berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter datenschutz@mustermannbetrieb.de oder unter Datenschutzbeauftragter c/o Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

## Anlage 2 – Informationspflichten bei Erhebung personenbezogener Daten (Muster)

Informationen zur Datenerhebung gemäß Artikel 13 DSGVO

Die Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, Geschäftsführerin Frau Musterfrau, erhebt Ihre Daten zum Zweck der Vertragsdurchführung, zur Erfüllung ihrer vertraglichen und vorvertraglichen Pflichten sowie zur Direktwerbung.

Die Datenerhebung und Datenverarbeitung ist für die Durchführung des Vertrags und zur Direktwerbung erforderlich und beruht auf Artikel 6 Abs. 1 b), f) DSGVO. Mit der Direktwerbung wollen wir Sie über aktuelle Leistungen und Neuigkeiten unseres Betriebs informieren. Eine Weitergabe der Daten an Dritte findet nicht statt. Die Daten werden gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Direktwerbung jederzeit zu widersprechen. Zudem sind Sie berechtigt, Auskunft der bei uns über Sie gespeicherten Daten zu beantragen sowie bei Unrichtigkeit der Daten die Berichtigung oder bei unzulässiger Datenspeicherung die Löschung der Daten zu fordern. Sie können unseren Datenschutzbeauftragten unter daten-schutz@musterbetrieb.de oder unter Datenschutzbeauftragter c/o Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

## Anlage 3 - Erteilung von Auskünften (Muster)

Sie haben uns um Auskunft darüber gebeten, welche Daten wir zu Ihrer Person gespeichert haben. Sie sind bei uns als …………………(z.B. Kunde/Interessent) erfasst.

Zur Datenverarbeitung durch unser Unternehmen teilen wir Ihnen mit, dass die Datenerhebung zur Kommunikation mit Ihnen, Abgabe von Angeboten, Abrechnung von Leistungen oder zur Erfüllung von Verträgen erfolgt. Diese Daten haben Sie uns mitgeteilt. 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. Die Daten werden nicht an Dritte weitergeben. Die über Sie gespeicherten Daten entnehmen Sie bitte der beigefügten Tabelle.

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

Sie haben das Recht, sich bei der für uns zuständigen Datenschutzaufsichtsbehörde ………………..(Name, Adresse, E-Mail) zu beschweren, falls Sie der Meinung sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Für weitere Auskünfte stehen wir Ihnen selbstverständlich gerne zur Verfügung.

|  |
| --- |
| **Kunde** |
| Familienname |  |
| Vorname |  |
| Geburtsname |  |
| Geschlecht |  |
| Geburtsdatum |  |
| Staatsangehörigkeit |  |
| Straße |  |
| PLZ |  |
| Wohnort |  |
| UstID |  |
| **Kommunikationsdaten** |
| Telefon |  |
| Handy |  |
| E-Mail |  |
| **Bankverbindung** |
| Bankname |  |
| IBAN-Nummer |  |
| BIC |  |
| **Kundenspezifische Daten** |
| z.B. Wartungsverträge … |  |
|  |  |
|  |  |

## Anlage 4 – Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

**Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO**

|  |
| --- |
| **1. Verantwortlicher (= Firma/Legaleinheit)** |

|  |
| --- |
| **2. Gesetzlicher Vertreter (= Geschäftsführung)** |

|  |
| --- |
| **3. Datenschutzbeauftragter**Name:Anschrift:E-Mail:Tel.: |

**4. Zuständige Aufsichtsbehörde**

Landesbeauftragter für Datenschutz und Informationsfreiheit Bundesland XY

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

**□** Ja

**□** Nein

**5. Regelungen zur Datensicherheit**

*IT-Sicherheitskonzept*

*[Verweis auf übergreifende IT-Sicherheitskonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten]*

**6. Sachverhalte zu Drittstaatenübermittlungen**

**Erläuterungen zum Hauptblatt**

|  |  |
| --- | --- |
| 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 DSGVO)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*Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.* |
| Nr. 3 | Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde)Angaben: Name, Kontaktdaten |
| Nr. 4 | Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben  |
| Nr. 5 | Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle 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. 6 | Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR. |

**Verzeichnis von Verarbeitungstätigkeiten**

Verzeichnis Nr. \_\_\_\_\_

□ Ersterstellung

□ Änderung eines bestehenden Verzeichnisses

**Erstellungsdatum**:

**Bezeichnung der Verarbeitungstätigkeit:**

**I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO**

**1. Verantwortlicher Fachbereich/verantwortliche Führungskraft**

**2. Bei gemeinsamer Verantwortlichkeit:**

Name und Kontaktdaten des Leiters/der Leiter oder des/der weiteren Verantwortlichen

**II. Angaben zur Verarbeitungstätigkeit**

**3. Risikobewertung**

 **Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?**

□ Nein

□ Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSGVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

|  |
| --- |
| **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 c) DSGVO** |
| **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 d) DSGVO** |
| **7.1. Interne Empfänger** |  |
| **7.2. Externe Empfänger** |  |
| **7.3. Vertragliche Dienstleister**(Vertrag der Auftragsdatenverarbeitung als Anlage beifügen) |  |

|  |
| --- |
| **8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO**Übermittlung□ Nein□ JaWenn ja, dann: Name des Drittlandes / der internationalen Organisation |

|  |
| --- |
| **9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO** |

|  |
| --- |
| **10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO** |
| **10.1.** **Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)** |
| **10.2.** **Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO** |

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

Weitere Dokumentationen zur Verarbeitungstätigkeit

|  |
| --- |
|  |

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

**Erläuterungen zum Verarbeitungsverzeichnis**

|  |  |
| --- | --- |
| Nr. 1 | Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: * Allgemeine Kundenverwaltung
* Customer-Relationship-Management (CRM)
 |
| Nr. 1 | Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*) |
| Nr. 2 | 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 a) DSGVO, Art. 26 Abs. 1 DSGVO) |
| Nr. 3 | Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden. |
| 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 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 Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.  |
| Nr. 6 | Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO |
| 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 sind etwa Angaben wie „Kundendaten“ oder Ähnliches.Beispiele: * Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich 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 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. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO. |
| 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 Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.  |
| Nr. 10 | Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO. |
| 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. 5**) 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 d) DSGVO. 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 DSGVO)*
* *Verträge mit Dienstleistern (Art. 28 DSGVO)*
* *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)*
* *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen*
* *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*
 |

## Anlage 5 – Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Hauptblatt

**Angaben zum Verantwortlichen, Art. 30 Abs. 1 a) DSGVO**

|  |
| --- |
| **1. Verantwortlicher (=Firma/Legaleinheit)***Mustermann GmbH, Musterstraße 17-21, 12345 Musterstadt* |

|  |
| --- |
| **2. Gesetzlicher Vertreter (= Geschäftsführung/ Betriebsinhaber)***Herr Otto Mustermann, Musterstraße 17-21, 12345 Musterstadt* |

|  |
| --- |
| **3. Datenschutzbeauftragter****Name:** Frau Anja Mustermann**Anschrift:** Musterstraße 17-21,12345 Musterstadt**E-Mail:** datenschutzbeauftragter@mustermann-gmbh.de**Tel.:** 01234/ 123456-34 |

**4. Zuständige Aufsichtsbehörde**

*Landesbeauftragter für Datenschutz und Informationsfreiheit NRW*

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:

⌧ Ja

**□** Nein

**5. Regelungen zur Datensicherheit**

*IT-Sicherheitskonzept der HWK Musterstadt*

**6. Sachverhalte zu Drittstaatenübermittlungen**

*Findet nicht statt.*

**Erläuterungen zum Hauptblatt**

|  |  |
| --- | --- |
| 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 DSGVO)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*Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.* |
| Nr. 3 | Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde)Angaben: Name, Kontaktdaten |
| Nr. 4 | Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben.  |
| Nr. 5 | Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grds. alle Verarbeitungen* betreffen) Der Verweis auf übergreifende Regelungen an dieser Stelle 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. 6 | Ein Verweis zur Regelungen zur Drittstaatenübermittlung ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen hierdurch geregelt werden, z.B. durch BCR. |

**Verzeichnis von Verarbeitungstätigkeiten**

Verzeichnis Nr. 1

[ ]  Ersterstellung

[ ]  Änderung eines bestehenden Verzeichnisses

**Erstellungsdatum**: 21.8.2017

**Bezeichnung der Verarbeitungstätigkeit:** Erstellung und Führung der Kundendatei

**I. Angaben zur Verantwortlichkeit, Art. 30 Abs. 1 b) DSGVO**

**1. Verantwortlicher Fachbereich/verantwortliche Führungskraft**

Herr Mustermann

**2. Bei gemeinsamer Verantwortlichkeit:**

Name und Kontaktdaten des Leiters/der Leiter des/der weiteren Verantwortlichen

**II. Angaben zur Verarbeitungstätigkeit**

**3. Risikobewertung**

**Besteht bei der Verarbeitung ein hohes Risiko für die betroffenen Personen?**

⌧ Nein

**□** Ja

Wenn ja, dann Durchführung einer Datenschutz-Folgenabschätzung erforderlich (Art. 35 DSGVO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

|  |
| --- |
| **4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit**Organisation von Geschäftskontakten und Bestandskunden.Durchführung von Verträgen.Nutzung zur Direktwerbung.  |

|  |
| --- |
| **5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit**Art. 6 Abs. 1 b DSGVO |

|  |
| --- |
| **6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO** |
| **6.1. Betroffene Personengruppen**  | **6.2. Kategorien personenbezogener Daten** |
| Kunden, Geschäftspartner  | Name, Vorname, Adressdaten, (elektronische) Kontaktdaten, ggfs. Firma oder Etablissementbezeichnung, Datum des Auftrags, Gegenstand des Auftrags  |

|  |
| --- |
| **7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO** |
| **7.1. Interne Empfänger** | Vertriebsmitarbeiter, Mitarbeiter im Außendienst |
| **7.2. Externe Empfänger** | -------- |
| **7.3. Vertragliche Dienstleister**(Vertrag der Auftragsdatenverarbeitung als Anlage beifügen) | -------- |

|  |
| --- |
| **8. Datenübermittlungen in Drittländer oder an internationale Organisationen, Art. 30 Abs. 1 e) DSGVO**Übermittlung⌧ Nein**□** JaWenn ja, dann: Name des Drittlandes / der internationalen Organisation (DSGVO) |

|  |
| --- |
| **9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO**Die Datenwerden gelöscht, wenn sie für die Erfüllung des Zweck (siehe Nr. 4) nicht mehr erforderlich sind. |

|  |
| --- |
| **10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO**Siehe betriebsinternes IT-Sicherheitskonzept |
| * 1. **Art der eingesetzten DV-Anlagen und Software (optional)**

--------- (Siehe betriebsinternes IT-Sicherheitskonzept) |
| **10.2** **Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO***---------**(Siehe betriebsinternes IT-Sicherheitskonzept)* |

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

Weitere Dokumentationen zur Verarbeitungstätigkeit

|  |
| --- |
| ---------------------------- |

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

**Erläuterungen zum Verarbeitungsverzeichnis**

|  |  |
| --- | --- |
| Nr. 1 | Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: * Allgemeine Kundenverwaltung
* Customer-Relationship-Management (CRM)
 |
| Nr. 1 | Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*) |
| Nr. 2 | 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 a) DSGVO, Art. 26 Abs. 1 DSGVO) |
| Nr. 3 | Es ist zu bewerten, ob die Datenverarbeitung ein hohes Risiko für die Personen birgt, deren Daten verarbeitet werden. Ein hohes Risiko liegt u.a. dann vor, wenn sehr viele Personen von der Datenverarbeitung betroffen sind. Das gleiche gilt, wenn besonders schutzwürdige Daten (z.B. Gesundheitsdaten) umfangreich verarbeitet werden. |
| 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 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 Rechenschaftspflichten und die Gewährleistung von Transparenzpflichten ggü. den betroffenen Personen notwendig. Die Rechtsgrundlage können z.B. eine gesetzliche Vorschrift oder eine Einwilligung durch den Betroffenen sein.  |
| Nr. 6 | Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO |
| 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 sind etwa Angaben wie „Kundendaten“ oder Ähnliches.Beispiele: * Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließlich 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 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. Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren, Art. 49 Abs. 1. UAbs. 2 DSGVO. |
| 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 Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.  |
| Nr. 10 | Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO. |
| 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. 5**) 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 d) DSGVO. 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 DSGVO)*
* *Verträge mit Dienstleistern (Art. 28 DSGVO)*
* *Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO)*
* *Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen*
* *durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)*
 |

## Anlage 6 – Technische und organisatorische Maßnahmen

**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 DSGVO 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

## Anlage 7 – Der betriebliche Datenschutzbeauftragte (DSB)

**MUSTER**

**Benennung als Datenschutzbeauftragte/r**

[*Name des Verantwortlichen, Straße/Hausnummer, PLZ/Ort*]

benennt hiermit

[*Name des zu benennenden Datenschutzbeauftragten, Straße/Hausnummer, PLZ/Ort*]

mit sofortiger Wirkung zur/m Datenschutzbeauftragten gemäß Artikel 37 EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit § 38 Bundesdatenschutzgesetz (BDSG). Der/die Datenschutzbeauftragte ist in seiner/ihrer Funktion unmittelbar der Geschäftsleitung unterstellt.

Zuständiges Mitglied der Geschäftsleitung ist [*Name des Mitglieds der Geschäftsleitung*].

Die Stellung und die Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § 38 BDSG. Der/die Beauftragte unterliegt in Ausübung seines/ihres Amtes keinem Weisungsrecht. Bei der Erfüllung der Aufgaben ist er/sie an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden. Über seine/ihre Tätigkeit wird er/sie der Geschäftsleitung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlägt er/sie der Geschäftsleitung vor.

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

Ort, Datum Unterschrift Geschäftsleitung

Ich habe die vorstehende Benennung zur Kenntnis genommen:

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

Ort, Datum Unterschrift Datenschutzbeauftragte/r

## Anlage 8 - Auftragsverarbeitung

**Musterformulierungen**

**1.** **Gegenstand und Dauer des Auftrags**

* Der Gegenstand und die Dauer des Auftrags müssen individuell mit dem Auftragsverarbeiter verhandelt und festgelegt werden. Musterformulierungen sind insofern wegen der Individualität der Vereinbarungen nicht möglich.

**2. Umfang, Art und Zweck der Datenverarbeitung**

Formulierungsvorschlag:

„Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im sachlichen und zeitlichen Rahmen dieses Auftrages sowie nach Weisung des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

Die Verarbeitung der Daten auch durch Unterauftragnehmer findet

[ ]  ausschließlich im Gebiet der Bundesrepublik Deutschland,

[ ]  in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,

[ ]  in einem Drittstaat (Nennung des Drittstaats \_\_\_\_\_\_\_\_\_\_\_\_\_)

statt. In letzterem Fall weist der Auftragnehmer für die Rechtmäßigkeit entsprechende vertragliche oder sonstige, der DSGVO entsprechenden Rechtsgrundlagen nach.“

**3. Technische und organisatorische Maßnahmen**

Formulierungsvorschlag:

„Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den gesetzlichen Anforderungen genügen. Hierbei sind die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind gesondert zu diesem Vertrag festzulegen und sind Bestandteil des Vertrags.

Der Auftragnehmer gewährleistet ein Verfahren zur Überprüfung der technischen und organisatorischen Maßnahmen. Er ist verpflichtet, die technischen und organisatorischen Maßnahmen an den Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist. Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren. Die Änderungen sind schriftlich niederzulegen und werden Vertragsbestandteil. Vorschläge des Auftraggebers für Änderungen hat der Auftragnehmer zu prüfen. Der Auftraggeber ist über das Ergebnis zu informieren.

Beauftragt der Auftragnehmer zur Erfüllung seiner vertraglichen Pflichten einen Unterauftragnehmer, stellt er sicher, dass die erforderlichen technischen und organisatorischen Maßnahmen vom Unterauftragnehmer getroffen werden und dem Stand der Technik entsprechen.“

**4. Berichtigung, Sperrung und Löschung von Daten, Auskunft über Daten**

Formulierungsvorschlag:

„Der Auftragnehmer hat die Daten nach Weisung des Auftraggebers zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung, Sperrung oder Löschung seiner Daten wendet, leitet der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiter. Das gleiche gilt für Auskunftsersuche.“

**5. Kontrollen und sonstige Pflichten des Auftragnehmers**

Formulierungsvorschlag:

„Der Auftragnehmer ist verpflichtet, das Datengeheimnis sowie etwaige berufliche Verschwiegenheitsverpflichtungen zu wahren. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere sicherzustellen, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Datenschutzbestimmungen beachten und die vom Auftraggeber erlangten Informationen nicht unbefugt an Dritte weitergeben oder anderweitig verwerten.

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für sämtliche vertragsrelevanten Angelegenheiten des Datenschutzes. Der Auftragnehmer hat Frau/Herrn\_\_\_\_\_\_\_\_\_\_\_\_ als betrieblichen Datenschutzbeauftragten bestellt.

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen. Der Auftragnehmer gewährt dem Landesdatenschutzbeauftragten Zugang zu den Arbeitsräumen und unterwirft sich der Kontrolle nach Maßgabe des Landesdatenschutzgesetzes in seiner jeweiligen Fassung. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontroll- und Ermittlungshandlungen der Aufsichtsbehörde.“

**6. Unterauftragsverhältnisse**

Formulierungsvorschlag:

„Der Auftraggeber genehmigt die gesondert aufgelisteten Unterauftragsverhältnisse, die der Auftragnehmer vor Abschluss dieser Vereinbarung begründet hat. Über Änderungen hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Abschluss neuer Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.

Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten aufzuerlegen, die er selbst gegenüber dem Auftraggeber zu erfüllen hat. Der Unterauftragnehmer ist sorgfältig auszuwählen. Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer.“

**7. Kontrollrechte des Auftraggebers**

Formulierungsvorschlag:

„Der Auftraggeber hat das Recht, vor Beginn und während der Datenverarbeitung die Einhaltung der vom Auftragnehmer sowie von den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen zu kontrollieren oder von zu benennenden Prüfern kontrollieren zu lassen. Das Ergebnis ist zu dokumentieren.

Der Auftragnehmer gewährleistet die Möglichkeit zur Kontrolle. Hierzu weist er dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Der Nachweis kann durch Vorlage aktueller Testats oder durch Berichte unabhängiger Prüfer (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) erbracht werden.

Haben sich der Auftragnehmer und die von ihm beauftragten Unterauftragnehmer Verhaltensregeln unterworfen oder ein Zertifizierungsverfahren erfolgreich durchlaufen, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren.

Der Auftraggeber ist berechtigt, Stichprobenkontrollen durchzuführen. Diese sind anzukündigen. Würde die Ankündigung den Zweck der Prüfung gefährden oder besteht ein dringender Anlass zur Kontrolle, ist eine Ankündigung entbehrlich.“

**8. Mitteilung bei Verstößen**

Formulierungsvorschlag:

„Der Auftragnehmer meldet dem Auftraggeber unverzüglich sämtliche Verstöße gegen Pflichten aus diesem Vertrag. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen.“

**9. Weisungsbefugnis des Auftraggebers**

Formulierungsvorschlag:

„Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunkts der Verarbeitung von Daten. Die Weisungen des Auftraggebers erfolgen in Textform.

Erachtet der Auftragnehmer eine Weisung des Auftraggebers als rechtswidrig, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z.B. Änderungen der technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt.“

**10. Löschung von Daten und Rückgabe von Datenträgern**

„Der Auftragnehmer hat dem Auftraggeber sämtliche in seinen Besitz befindlichen personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, unverzüglich nach Erfüllung des Vertrags oder nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Zusammenarbeit auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind vom Auftragnehmer entsprechend der geltenden Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.“

## Anlage 9 - Datenschutz: Mitarbeiterinformation Datenschutz (Muster)

Sie werden heute über Ihre Pflichten im Umgang mit personenbezogenen Daten unterrichtet und unterzeichnen eine entsprechende Verpflichtung auf das Datengeheimnis. Dieses Merkblatt gibt Ihnen die Möglichkeit, das Wichtigste noch einmal nachzulesen. Sollten Sie Fragen haben – insbesondere wenn es darum geht, ob ein bestimmter Umgang mit personenbezogenen Daten erlaubt ist –, zögern Sie nicht, Ihren Vorgesetzten oder den betrieblichen Datenschutzbeauftragten zu fragen.

Datenschutz schützt das Persönlichkeitsrecht

Ihre Vertraulichkeitsverpflichtung dient – wie das gesamte Datenschutzrecht – dem Schutz des Persönlichkeitsrechts derjenigen Menschen, auf die sich die Daten beziehen. Diese Menschen nennt das Gesetz „betroffene Personen“. Das können unsere Kunden sein, Ihre Kollegen – oder auch Sie als unser Mitarbeiter.

Das Persönlichkeitsrecht gibt jedem Menschen das Recht, grundsätzlich selbst darüber zu entscheiden, wer was über ihn wissen darf. Beispielsweise darf jeder Kunde selbst entscheiden, wer seinen Wohnort erfahren soll, und Sie dürfen entscheiden, wer Ihren Gesundheitszustand kennen darf. Es ist Ihre Entscheidung, ob das geheim bleibt oder Sie es veröffentlichen.

Ausnahmen, in denen nicht nur der Wille des Betroffenen gilt, muss es natürlich geben – aber jede Ausnahme braucht nach dem Gesetz eine Rechtfertigung. Das kann nach der Regelung in Art. 6 Abs. 1 DS-GVO eine Einwilligung der betroffenen Person oder eine gesetzliche Erlaubnis sein. Die wichtigste gesetzliche Erlaubnis gilt für diejenigen Daten, die unbedingt benötigt werden, um einen Vertrag mit der betroffenen Person zu erfüllen. Deshalb darf Ihr Vermieter beispielsweise Ihren Namen speichern, ohne dass Sie einwilligen müssten.

Neben der DS-GVO, die in der gesamten Europäischen Union gilt, gibt es auch noch das Bundesdatenschutzgesetz (BDSG), das bestimmte Sonderfälle regelt, insbesondere den Beschäftigtendatenschutz.

Ihre Vertraulichkeitspflichten

Sie müssen personenbezogene Daten nicht nur vertraulich behandeln, Sie dürfen sie zum Beispiel nicht an Dritte weitergeben oder offen herumliegen lassen. Das Gesetz verpflichtet Sie vielmehr dazu, nur dann mit personenbezogenen Daten zu arbeiten, wenn dies erlaubt ist – unabhängig davon, ob Sie diese Daten beispielsweise lesen, notieren, löschen oder weitergeben. Diese Erlaubnis muss einerseits [*Unternehmen*] als Unternehmen haben, andererseits aber auch Sie persönlich nach unserer unternehmensinternen Aufgabenverteilung. Die gesetzlichen Vertraulichkeitspflichten einzuhalten, ist also auch Ihre ganz persönliche Verpflichtung. Diese Pflicht ergibt sich übrigens bereits aus dem Gesetz (unter anderem Art. 29 DS-GVO). Ihre heutige förmliche Verpflichtung zur Vertraulichkeit dient nur dazu, Ihnen deutlich zu machen, wie wichtig diese Pflicht ist.

Bitte beachten Sie: Ihre Vertraulichkeitsverpflichtung gilt zeitlich unbefristet, und zwar selbst dann, wenn Sie nicht mehr für uns tätig sind. Sie gilt gegenüber allen Personen, die nicht dienstlich für die jeweilige Sache zuständig sind – also auch gegenüber allen anderen Kollegen, Ihrer Familie und der Presse.

Wenn Sie mit personenbezogenen Daten arbeiten, müssen Sie sich dabei immer an die Weisungen Ihres Vorgesetzten halten. In ganz besonderen Fällen kann auch ein Gesetz vorschreiben, personenbezogene Daten z. B. an eine Behörde herauszugeben.

Der Begriff „personenbezogene Daten“

Das Datenschutzrecht gilt für alle „personenbezogenen Daten“. Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person, also einen Menschen, beziehen (Art. 4 Nr. 1 DS-GVO). Das kann die Angabe sein, dass jemand Mitglied in einem Verein ist, wo er wohnt oder wie viel Geld er auf dem Konto hat.

Personenbezogenes Datum kann aber auch die Angabe sein, dass die Kontonummer 123456 ihren Dispokredit überzogen hat. Denn obwohl hier kein Name genannt wird, ist einfach zu ermitteln, wer Inhaber dieses Kontos ist: Es handelt sich um Angaben zu einer „identifizierbaren“ Person. Eine Person ist identifizierbar, wenn man – eigene und fremde – Informationen kombinieren kann und dadurch erfährt, um wen es sich handelt.

Auch wenn Sie selbst denken, dass bestimmte Daten niemandem zuzuordnen sind, dürfen Sie diese deshalb nicht ohne Zustimmung Ihres Vorgesetzten und des betrieblichen Datenschutzbeauftragten an Dritte weitergeben oder veröffentlichen – abgesehen davon, dass es sich auch um Betriebsgeheimnisse handeln könnte, die Sie ebenfalls streng vertraulich behandeln müssen.

Für welche Daten das Datenschutzrecht gilt

Das Datenschutzrecht gilt einerseits für Computer-Daten (wozu auch die Daten vieler technischer Geräte zählen). Wichtig ist aber zu wissen, dass es auch für „die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“ (Art. 2 Abs. 1 DS-GVO) gilt, wobei unter Dateisystem jede geordnete Ablage zu verstehen ist (Art. 4 Nr. 6 DS-GVO) – etwa eine Kundenkartei auf Papier oder eine alphabetische Sammlung ausgefüllter Formulare. Das Datenschutzrecht gilt zudem auch dann, wenn die Daten später in eine Datei gespeichert werden sollen oder aus einer Datei stammen – etwa eine ausgedruckte Liste mit Kundendaten. Daten von Mitarbeitern oder Bewerbern werden in jeder Form durch das deutsche BDSG geschützt, auch wenn es sich um einen unsortierten Stapel handschriftlicher Notizen handelt, der weggeworfen werden soll.

Die Telefonnummern Ihrer Kinder auf Ihrem Handy dürfen Sie übrigens weiterhin speichern, ohne dass Sie eine Rechtsgrundlage benötigen: solche rein persönlichen oder familiären Tätigkeiten sind von der Geltung des Datenschutzrechts ausgenommen (Art. 2 Abs. 2 lit. c DS-GVO).

Unsere und Ihre Pflichten

Wir als Unternehmen und Sie als unser Mitarbeiter dürfen personenbezogene Daten nur dann verarbeiten, wenn es dafür eine Rechtsgrundlage gibt. Art. 4 Nr. 2 DS-GVO beschreibt den Begriff der Verarbeitung äußerst weit, so dass er letztlich jeden Kontakt mit personenbezogenen Daten umfasst: „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“. Als mögliche Rechtsgrundlage nennt Art. 6 Abs. 1 DS-GVO eine Einwilligung der betroffenen Person und verschiedene gesetzliche Erlaubnisse.

Für welche Daten es bei welchem Verfahren eine solche Rechtsgrundlage gibt, sagt Ihnen Ihr Vorgesetzter. Bitte beachten Sie: Andere Daten dürfen Sie nicht verwenden. Personenbezogene Daten dürfen zudem nur zu dem jeweils bestimmt festgelegten Zweck verwendet werden. Eine Zweckänderung braucht eine eigene Rechtsgrundlage. Das bedeutet, dass z. B. Kundendaten, die bisher nur für die Vertragsabwicklung verwendet wurden, nicht ohne weiteres für Werbung genutzt werden dürfen. Auch hier sagt Ihnen Ihr Vorgesetzter, ob eine Zweckänderung erlaubt ist.

Als wichtigste Regel sollten Sie sich hier merken, dass Sie personenbezogene Daten nie aus eigener Entscheidung heraus weitergeben oder für sich selbst nutzen (beispielsweise außerhalb dienstlicher Notwendigkeit lesen) dürfen.

Außerdem müssen personenbezogene Daten geschützt werden, so dass Unbefugte keine Kenntnis von ihnen nehmen und dass sie auch nicht versehentlich verloren gehen können. So sollten z. B. Ausdrucke mit personenbezogenen Daten oder Datenträger wie CDs, USB-Sticks oder Festplatten keinesfalls einfach weggeworfen oder weggegeben werden, sondern müssen ordnungsgemäß geschreddert oder durch die EDV-Abteilung sicher gelöscht werden.

Dass Sie Ihr Passwort nicht an Kollegen oder Dritte weitergeben oder gar auf einem Zettel an den Computer kleben dürfen, sollte sich von selbst verstehen – es ist Ihr persönliches Passwort, und wenn es jemand missbraucht, sind Sie persönlich dafür verantwortlich (siehe „Folgen von Verstößen“).

Rechte der betroffenen Personen

Einer der wichtigsten Aspekte des Persönlichkeitsrechts ist es, zu wissen, was andere über einen wissen. Wenn ein Unternehmen Daten über jemanden sammelt, muss es daher fast immer die betroffene Person informieren. Jeder Mensch kann zudem von jedem Unternehmen eine Kopie der Daten verlangen, die das Unternehmen über ihn gespeichert hat (Art. 15 DS-GVO). Dies bedeutet, dass alles, was Sie beispielsweise über einen Kunden notieren, auch schriftlich zu diesem Kunden gelangen kann. Achten Sie deshalb bitte darauf, dass Sie nur Angaben notieren, für die wir auch eine Erlaubnis zum Speichern haben – Ihr Vorgesetzter sagt Ihnen, welche Daten das in Ihrem konkreten Fall sind. Und achten Sie bitte auch darauf, wie Sie es aufschreiben: knapp, neutral und niemals beleidigend o. ä. Das Auskunftsrecht ist ein spezielles Recht des Betroffenen: An andere Personen und Stellen dürfen wir normalerweise keine Auskünfte geben – das wäre eine Übermittlung, für die wir eine Erlaubnis bräuchten.

Benötigen wir bestimmte Daten nicht mehr, müssen wir sie löschen (Art. 17 DS-GVO); falsche Daten müssen wir berichtigen (Art. 16 DS-GVO). Wenn Sie feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben, sprechen Sie bitte Ihren Vorgesetzten darauf an. Denn die Speicherung von Daten, die eigentlich zu löschen wären, kann mit Geldbußen bestraft werden. Zusätzlich haben betroffene Personen einen Anspruch auf Schadensersatz einschließlich Schmerzensgeld für die Verletzung ihres Rechts auf Datenschutz.

Jede betroffene Person kann uns zudem verbieten, ihre Daten für Werbezwecke zu benutzen (Art. 21 Abs. 2, 3 und 5 DS-GVO) und hat auch in bestimmten anderen Fällen ein Widerspruchsrecht (Art. 21 Abs. 1 DS-GVO). Betroffene Personen haben zudem weitere Rechte, die aber für Sie als Mitarbeiter normalerweise nicht von Bedeutung sind.

Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, leiten Sie ihn bitte sofort an [*den betrieblichen Datenschutzbeauftragten/die Geschäftsleitung*] weiter. Selbstständig dürfen Sie solche Dinge nur bearbeiten, wenn wir Ihnen diese Aufgabe ausdrücklich zugewiesen haben. In Zweifelsfällen fragen Sie [*den betrieblichen Datenschutzbeauftragten*/*die Geschäftsleitung*]. Beachten Sie bitte, dass auch Behörden oder die Polizei nicht ohne weiteres Daten von uns erhalten können. Wir benötigen hier einen förmlichen Beschlagnahmebeschluss. In bestimmten Fällen genügt ein förmliches Auskunftsersuchen. Wenn Sie von der Polizei oder einer anderen Behörde kontaktiert werden, informieren Sie bitte sofort Ihren Vorgesetzten und den betrieblichen Datenschutzbeauftragten.

Folgen von Verstößen

Verstöße gegen das Datenschutzrecht können für [*Unternehmen*] schwerwiegende Folgen haben – aber auch für Sie persönlich.

Fast alle Verstöße gegen das Datenschutzrecht können mit Geldbuße bestraft werden (Art. 83 DS-GVO). Diese Geldbuße kann bis zu 20.000.000 EUR pro Verstoß betragen oder für uns als Unternehmen bis zu vier Prozent des weltweiten Jahresumsatzes des gesamten Konzerns, je nachdem, was höher ist. Geldbußen können sogar gegen einzelne Mitarbeiter verhängt werden: Geben Sie beispielsweise ohne eine entsprechende Anweisung von [*Unternehmen*] personenbezogene Daten weiter oder nutzen Sie sie für Ihre eigenen Zwecke, können Sie persönlich mit einer Geldbuße bis zu 20.000.000 EUR bestraft werden. Zudem sind bestimmte Verstöße gegen das Datenschutzrecht Straftaten, die mit Gefängnis bestraft werden können (§ 42 BDSG): Beispiel: Jemand verkauft weisungswidrig eine Festplatte mit personenbezogenen Daten anstatt sie zu zerstören.

Verstöße gegen das Datenschutzrecht können zudem nach anderen Gesetzen strafbar sein, z. B. nach § 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen), § 202 a StGB (Ausspähen von Daten) oder § 263 a StGB (Computerbetrug).

Jede betroffene Person kann Schadensersatz für eine unzulässige Verarbeitung ihrer Daten verlangen, und zwar einschließlich Schmerzensgeld für die Persönlichkeitsrechtsverletzung (Art. 82 DS-GVO, §§ 823 ff. BGB). Unter Umständen müssen Sie persönlich diesen Schadensersatz ganz oder teilweise bezahlen, wenn Sie mittlere oder schwere Verstöße begangen oder personenbezogene Daten weisungswidrig verarbeitet haben, etwa für Ihre eigenen Zwecke genutzt haben. Fragen Sie daher lieber einmal zu viel als zu wenig.

Schwere Schäden für [*Unternehmen*] kann es verursachen, wenn eine so genannte Datenpanne öffentlich bekannt wird. Kunden verlieren das Vertrauen und schließen keine Verträge mehr bei uns, wenn sie nicht sicher sein können, dass ihre Daten bei uns in guten Händen sind. Hinzu kommt, dass wir nach Art. 34 Abs. 1 und Abs. 3 lit. c DS-GVO verpflichtet sein können, eine Datenpanne allen Betroffenen mitzuteilen oder gar öffentlich bekanntzumachen. Bitte helfen Sie mit, dass es niemals dazu kommt.

Nicht zuletzt können wir arbeitsrechtliche Konsequenzen ziehen, wenn Sie gegen Ihre Vertraulichkeitspflichten verstoßen. Denkbar sind je nach Schwere Ihres Fehlverhaltens insbesondere eine Abmahnung, eine fristgerechte Kündigung oder sogar eine fristlose Kündigung ohne vorherige Verwarnung.

Besondere Hinweise für Nutzer von Internet und E-Mail

Internet und E-Mail sind sehr praktisch, weil man innerhalb von Sekunden Daten ans andere Ende der Welt schicken kann. Gerade diese Geschwindigkeit macht sie aber auch so risikoreich. Hinzu kommt, dass das Internet als Medium zur Kommunikation zwischen Wissenschaftlern erfunden wurde, die sich gegenseitig absolut vertrauen konnten. Deshalb gibt es standardmäßig keine Sicherheitsmaßnahmen. Das ist heute nicht mehr angemessen und eine große Gefahr für vertrauliche Daten. Deshalb beachten Sie bitte folgende Grundregeln:

Bitte prüfen Sie vor Versand einer Mail, ob Sie die Daten überhaupt an den Empfänger weitergeben dürfen.

Bevor Sie eine E-Mail versenden, achten Sie bitte unbedingt darauf, ob der richtige Empfänger im Adressfeld steht. Hier liegt eine große Fehlerquelle, wenn mehrere Leute einen ähnlichen Namen oder eine ähnliche E-Mail-Adresse haben.

Beachten Sie den Unterschied zwischen „To:/An:“ (Empfänger), „CC:“ (Kopie) und „BCC:“ (Blindkopie): Jeder Empfänger der E-Mail sieht sämtliche anderen Empfänger, die im To:- bzw. CC:-Feld stehen. Soll ein Empfänger für die anderen nicht sichtbar sein, müssen Sie ihn ins BCC:-Feld schreiben. Die Daten aller To:-/CC:-Empfänger übermitteln Sie im rechtlichen Sinne an die anderen Empfänger. Und dafür benötigen Sie, wie Sie wissen, eine Erlaubnis.

Sie dürfen niemals vertrauliche Daten an Ihren privaten E-Mail-Account weiterleiten. Dies bedeutet unter anderem, dass Sie auch keinesfalls eine automatische Weiterleitung Ihres E-Mail-Accounts an Ihre private E-Mail-Adresse einrichten dürfen.

Bitte ändern Sie nicht die Einstellungen, insbesondere die Sicherheitseinstellungen, Ihrer Programme. Die EDV-Abteilung hat sich etwas bei der Konfiguration gedacht. Wenn Sie Änderungsvorschläge haben, sprechen Sie diese bitte mit der EDV-Abteilung ab – vielleicht können ja alle Mitarbeiter von Ihrer Idee profitieren.

## Anlage 10 - Verpflichtung auf das Datengeheimnis (Muster)

Über die einschlägigen datenschutzrechtlichen Vorschriften im Unternehmen wurde ich in Kenntnis gesetzt. Ich wurde mit den sich daraus ergebenden besonderen Anforderungen an Datensicherheit und Datenschutz bei der Ausübung meiner Tätigkeit vertraut gemacht. Personenbezogene Daten, also alle Informationen, die sich auf einen benannten oder identifizierbaren Menschen beziehen, dürfen nicht unbefugt erhoben, genutzt, weitergegeben oder sonst verarbeitet werden.

Ich verpflichte mich, personenbezogene Daten vertraulich zu behandeln und ausschließlich auf Weisung von [*Unternehmen*] zu verarbeiten. Diese Vertraulichkeitsverpflichtung besteht auch nach Beendigung meiner Tätigkeit für [*Unternehmen*] fort.

Eine Verletzung meiner Vertraulichkeitsverpflichtung kann zugleich eine Verletzung arbeitsvertraglicher Pflichten oder spezieller Geheimhaltungspflichten darstellen und beispielsweise zu Abmahnung, fristloser oder fristgerechter Kündigung und/oder Schadensersatzpflichten führen. Gesetzliche Folge von Verstößen gegen meine Vertraulichkeitsverpflichtung können auch Schadensersatzansprüche der Personen, auf die die Daten sich beziehen, gegen mich persönlich sein. Sonstige Geheimhaltungsverpflichtungen, etwa aus dem Arbeitsvertrag, bestehen neben dieser Vertraulichkeitsverpflichtung.

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

Ort, Datum Unterschrift Mitarbeiter/in

Ich bestätige, dass ich heute über die Bedeutung meiner Verpflichtung zur Verschwiegenheit über personenbezogene Daten belehrt wurde. Ein Exemplar dieses Formulars sowie ein Merkblatt mit Erläuterungen zum Datenschutzrecht habe ich erhalten.

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

Ort, Datum Unterschrift Mitarbeiter/in

## Anlage 11 - Datenschutzhinweis Internet (Muster)[[2]](#footnote-2)

I. Information über die Erhebung personenbezogener Daten

1. Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung unserer Website. Personenbezogene Daten sind alle Daten, die auf Sie persönlich beziehbar sind, z.B. Name, Adresse, E-Mail-Adresse, Nutzerverhalten.

2. Verantwortlicher gem. Art. 4 Abs. 7 EU-Datenschutz-Grundverordnung (DSGVO) ist: [*Verantwortlicher,* Adresse].

3. Unseren Datenschutzbeauftragten erreichen Sie unter [*datenschutz[at]musterbetrieb.de* *oder unter Datenschutzbeauftragter c/o Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt*].

4. Bei Ihrer Kontaktaufnahme mit uns per E-Mail oder über ein Kontaktformular werden die von Ihnen mitgeteilten Daten (wie z.B. Ihre E-Mail-Adresse, Ihr Name, etc.) von uns gespeichert, um Ihr Anliegen zu beantworten. Die in diesem Zusammenhang anfallenden Daten löschen wir, nachdem die Speicherung nicht mehr erforderlich ist, oder schränken die Verarbeitung ein, falls gesetzliche Aufbewahrungspflichten bestehen.

II. Ihre Rechte

1. Sie haben gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

 – Recht auf Auskunft,

 – Recht auf Berichtigung oder Löschung,

 – Recht auf Einschränkung der Verarbeitung,

 – Recht auf Widerspruch gegen die Verarbeitung,

 – Recht auf Datenübertragbarkeit.

2. Sie haben zudem das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten durch uns zu beschweren.

III. Erhebung personenbezogener Daten bei Besuch unserer Website

1. Bei der bloß informatorischen Nutzung der Website, also wenn Sie sich nicht registrieren oder uns anderweitig Informationen übermitteln, erheben wir nur die personenbezogenen Daten, die Ihr Browser an unseren Server übermittelt. Wenn Sie unsere Website betrachten möchten, erheben wir die folgenden Daten, die für uns technisch erforderlich sind, um Ihnen unsere Website anzuzeigen und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO):

 – IP-Adresse

 – Datum und Uhrzeit der Anfrage

 – Zeitzonendifferenz zur Greenwich Mean Time (GMT)

 – Inhalt der Anforderung (konkrete Seite)

 – Zugriffsstatus/HTTP-Statuscode

 – jeweils übertragene Datenmenge

 – Website, von der die Anforderung kommt

 – Browser

 – Betriebssystem und dessen Oberfläche

 – Sprache und Version der Browsersoftware.

*2. Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung unserer Website Cookies auf Ihrem Rechner gespeichert. Bei Cookies handelt es sich um kleine Textdateien, die auf Ihrer Festplatte dem von Ihnen verwendeten Browser zugeordnet gespeichert werden und durch welche der Stelle, die den Cookie setzt (hier durch uns), bestimmte Informationen zufließen. Cookies können keine Programme ausführen oder Viren auf Ihren Computer übertragen. Sie dienen dazu, das Internetangebot insgesamt nutzerfreundlicher und effektiver zu machen.*

*3. Einsatz von Cookies:*

*a. Diese Website nutzt folgende Arten von Cookies, deren Umfang und Funktionsweise im Folgenden erläutert werden:*

*– Transiente Cookies (dazu bb.)*

*– Persistente Cookies (dazu cc.).*

*b. Transiente Cookies werden automatisiert gelöscht, wenn Sie den Browser schließen. Dazu zählen insbesondere die Session-Cookies. Diese speichern eine sogenannte Session-ID, mit welcher sich verschiedene Anfragen Ihres Browsers der gemeinsamen Sitzung zuordnen lassen. Dadurch kann Ihr Rechner wiedererkannt werden, wenn Sie auf unsere Website zurückkehren. Die Session-Cookies werden gelöscht, wenn Sie sich ausloggen oder den Browser schließen.*

*c. Persistente Cookies werden automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann. Sie können die Cookies in den Sicherheitseinstellungen Ihres Browsers jederzeit löschen.*

*d. Sie können Ihre Browser-Einstellung entsprechend Ihren Wünschen konfigurieren und z.B. die Annahme von Third-Party-Cookies oder allen Cookies ablehnen. Wir weisen Sie darauf hin, dass Sie eventuell nicht alle Funktionen dieser Website nutzen können.*

*e. Wir setzen Cookies ein, um Sie für Folgebesuche identifizieren zu können, falls Sie über einen Account bei uns verfügen. Andernfalls müssten Sie sich für jeden Besuch erneut einloggen.*

*f. Die genutzten Flash-Cookies werden nicht durch Ihren Browser erfasst, sondern durch Ihr Flash-Plug-in. Weiterhin nutzen wir HTML5 storage objects, die auf Ihrem Endgerät abgelegt werden. Diese Objekte speichern die erforderlichen Daten unabhängig von Ihrem verwendeten Browser und haben kein automatisches Ablaufdatum. Wenn Sie keine Verarbeitung der Flash-Cookies wünschen, müssen Sie ein entsprechendes Add-On installieren, z.B. „Better Privacy“ für Mozilla Firefox (*[*https://addons.mozilla.org/de/firefox/addon/betterprivacy/*](https://addons.mozilla.org/de/firefox/addon/betterprivacy/)*) oder das Adobe-Flash-Killer-Cookie für Google Chrome. Die Nutzung von HTML5 storage objects können Sie verhindern, indem Sie in Ihrem Browser den privaten Modus einsetzen. Zudem empfehlen wir, regelmäßig Ihre Cookies und den Browser-Verlauf manuell zu löschen.*

IV. Widerspruch oder Widerruf gegen die Verarbeitung Ihrer Daten

1. Falls Sie eine Einwilligung zur Verarbeitung Ihrer Daten erteilt haben, können Sie diese jederzeit widerrufen. Ein solcher Widerruf beeinflusst die Zulässigkeit der Verarbeitung Ihrer personenbezogenen Daten, nachdem Sie ihn gegenüber uns ausgesprochen haben.

2. Soweit wir die Verarbeitung Ihrer personenbezogenen Daten auf die Interessenabwägung stützen, können Sie Widerspruch gegen die Verarbeitung einlegen. Dies ist der Fall, wenn die Verarbeitung insbesondere nicht zur Erfüllung eines Vertrags mit Ihnen erforderlich ist, was von uns jeweils bei der nachfolgenden Beschreibung der Funktionen dargestellt wird. Bei Ausübung eines solchen Widerspruchs bitten wir um Darlegung der Gründe, weshalb wir Ihre personenbezogenen Daten nicht wie von uns durchgeführt verarbeiten sollten. Im Falle Ihres begründeten Widerspruchs prüfen wir die Sachlage und werden entweder die Datenverarbeitung einstellen bzw. anpassen oder Ihnen unsere zwingenden schutzwürdigen Gründe aufzeigen, aufgrund derer wir die Verarbeitung fortführen.

3. Selbstverständlich können Sie der Verarbeitung Ihrer personenbezogenen Daten für Zwecke der Werbung und Datenanalyse jederzeit widersprechen. Über Ihren Werbewiderspruch können Sie uns unter folgenden Kontaktdaten informieren: [*datenschutz[at]musterbetrieb.*de].

Soweit Daten für abrechnungstechnische und buchhalterische Zwecke genutzt werden, sind sie von einer Kündigung beziehungsweise von einer Löschung nicht berührt.

V. Drittanbieter

Links zu Websites anderer Anbieter, die in unserem Angebot enthalten sind, werden von dieser Datenschutzerklärung nicht umfasst. Wir haben keinen Einfluss darauf, dass deren Betreiber die Datenschutzbestimmungen einhalten.

1. Das Original dieser Einwilligung ist für die Unterlagen des Unternehmens. Dem Kunden sollte eine Kopie ausgehändigt werden. [↑](#footnote-ref-1)
2. Die kursiv dargestellten Inhalte sind auszufüllen bzw. betreffen konkrete Sachverhalte; bei diesen ist zu prüfen, ob sie auf die eigenen Gegebenheiten zutreffen. Ggfs. enthält Ihre Webseite zusätzliche Funktionen, die ebenfalls in der Datenschutzerklärung abzubilden sind. [↑](#footnote-ref-2)