Handwerkskammer Koblenz

Was Betriebe künftig zu beachten haben

Neues Datenschutzrecht am 25. Mai 2018

Höchste Zeit zum Handeln!

Ab Mai 2018 tritt die neue EU-Datenschutzgrundverordnung als unmittelbar geltendes Recht in Kraft. Handwerksunternehmen müssen sicherstellen, dass unabhängig von ihrer Größe die erforderlichen Anpassungen vorgenommen werden. Bislang wurden Datenschutzverstöße und Datenpannen selten sanktioniert. Dies wird sich ab dem 25. Mai 2018 allerdings ändern. Beigefügt erhalten Sie für den Einsatz in Ihrem Betrieb eine

Mustersammlung[1]

Muster 1: Einwilligungserklärung
Muster 2: Information bei Erhebung von Daten beim Betroffenen
Muster 3: Auskunftserteilung eines Handwerksbetriebs an einen Kunden
Muster 4: Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen (blanko)
Muster 5: Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen (Beispiel)
Muster 6: Technische und organisatorische Maßnahmen
Muster 7: Benennung eines Datenschutzbeauftragten
Muster 8: Auftragsdatenverarbeitung
Muster 9: Unterrichtung und Verpflichtung von Beschäftigten

[1] Muster Leitfaden Datenschutzrecht Zentralverbands des Deutschen Handwerks
Gültig ab Mai 2018, Stand November 2017

Die Muster können Sie auch abrufen im Leitfaden Datenschutzrecht unter

https://t1p.de/datenschutzrecht

Daneben steht ein Online-Tool der EU-Kommission zu der ab Mai geltenden Datenschutz-Grundverordnung (DSGVO) für kleine und mittlere Unternehmen bereit. Das Online-Tool unterstützt die praktische Anwendung, indem es Bürgern, Organisationen und Unternehmen dabei hilft, die neuen Datenschutzbestimmungen einzuhalten und sie richtig zu nutzen.

Das Online-Tool finden Sie hier:

http://ec.europa.eu/justice/smedataprotect/index_de.htm

Muster 1
Anforderungen der datenschutzrechtlichen Einwilligung

Muster Einwilligungserklärung

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 Einwilligungen freiwillig und jederzeit widerruflich sind. 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 mehr nutzen und verarbeiten bzw. löschen.

.....

Ort, Datum Unterschrift

Muster 2
Informationspflichten bei Erhebung personenbezogener Daten

Muster Information bei Erhebung von Daten beim Betroffenen

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 erforderlich und beruht auf Artikel 6 Abs. 1 b) 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 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 datenschutz@musterbetrieb.de oder unter Datenschutzbeauftragter c/o Musterbetrieb GmbH, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

Muster 3
Die Erteilung von Auskünften

Muster Auskunftserteilung eines Handwerksbetriebs an einen Kunden

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

Sehr geehrte/r Frau/Herr ,

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.

Mit freundlichen Grüßen

Firma .....

Anlage

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	

Muster 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, Telefon

4. Zuständige Aufsichtsbhörde

Landesbeauftragter für Datenschutz und Informationsfreiheit Bundesland Rheinland-Pfalz

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 DSG- VO). 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 ☐ Ja

Wenn 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 Maß- nahmen, Art. 30 Abs. 1 g) i. V. m. Art. 32 Abs. 1 DSGVO

.....

– optionale Angaben –

Weitere Dokumentationen zur Verarbeitungstätigkeit

.....

.....

.....

.....

– Ende optionale Angaben –

Erläuterungen zum Verzeichnis von Verarbeitungstätigkeiten

Bezeichnung der Verarbeitungstätigkeit
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, Behör- den, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.

Nr. 8
Drittländer sind solche außerhalb der EU/des EWR
Beispiele für internationale Organisationen: Institutionen der UNO, der EU. 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 DSG- VO)
- Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen
- durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)

Muster 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)

Herr Otto Mustermann, Musterstraße 17-21, 12345 Musterstadt

3. Datenschutzbeauftragter

Frau Anja Mustermann, Musterstraße 17-21,12345 Musterstadt
Name, Anschrift

datenschutzbeauftragter@mustermann-gmbh.de
E-Mail, Telefon

4. Zuständige Aufsichtsbhörde
Landesbeauftragter für Datenschutz und Informationsfreiheit NRW

Verpflichtende Meldung des/der Datenschutzbeauftragten bereits erfolgt:
☒ ja ☐ nein

5. Regelungenzur Datensicherheit

datenschutzbeauftragter@mustermann-gmbh.de
IT-Sicherheitskonzept

(Verweis auf übergreifende IT-Sicherheitskonzepte, die grundsätzlich für alle Verarbeitungstätigkeiten gelten.

6. Sachverhalte zu Drittstaatenübermittlungen

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis Nr. 1

☒ Ersterstellung ☐ Änderung eines bestehenden Verzeichnisses

21.08.2017
Erstellungsdatum

Erstellung und Führung der Kundendatei
Bezeichnung der Verarbeitungstätigkeit

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 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 DSG- VO). Datenschutz-Folgenabschätzung als separate Anlage beifügen.

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

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

Kunden, Geschäftspartner

6.2 Kategorien personenbezogener Daten

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 ☐ Ja

Wenn ja, dann:

Name des Drittlandes / der internationalen Organisation

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

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 –

Muster 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

a) 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

b) Zugangs- und Benutzerkontrolle
Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

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

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

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

☐ Löschungskonzept für Daten
☐ Protokollierung der Vernichtung

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

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

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

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

3. Integrität

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

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

b) Dokumentationskontrolle

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

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

4. Verfügbarkeitskontrolle

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

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

5. Trennungsgebot

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

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

Muster 7
Der betriebliche Datenschutzbeauftragte (DSB)

Muster Benennung eines/r betrieblichen Datenschutzbeauftragten

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 (DSGVO) 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 DSGVO 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 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 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 Mitgliedsstaat 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 DSG- VO 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."

Muster 9[2]
Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen
a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen

[2] Bayerisches Landesamt für Datenschutzaufsicht Webseite: www.lda.bayern.de