|  |
| --- |
|  |

**Anlagen**

**Anlage 1 Anforderungen der datenschutzrechtlichen Einwilligung**

**Muster**

**Einwilligungserklärung**

**Einwilligung von Lehrlingen** (Vorlage in Rahmen von Schulungen)

Um Sie zeitnah, umfassend und individuell informieren zu können, benötigen wir folgende personenbezogene Daten:

Name:

Anschrift:

Geburtsdatum:

E-Mail:

Ausbildungsberuf:

Die mit Ihrer ausdrücklichen Einwilligung erhobenen und gespeicherten Daten werden ausschließlich vom Berufsbildungszentrum der Handwerkskammer und ausschließlich zum Zweck der Information über Weiterbildungs- und Veranstaltungshinweise genutzt. Eine Weitergabe Ihrer Daten an Dritte erfolgt nur, sofern das Berufsbildungszentrum hierzu gesetzlich verpflichtet ist.

Mir ist bekannt, dass ich zur Abgabe der Einwilligungserklärung nicht verpflichtet bin und ich diese Einwilligungserklärung jederzeit mit Wirkung für die Zukunft widerrufen kann. Der Widerruf ist

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

oder postalisch an: Handwerkskammer XY, Musterstraße 1, 12345 Musterstadt

Der Widerruf bewirkt, dass meine aufgrund dieser Einwilligungserklärung erfassten Daten gelöscht und mir keine Weiterbildungsangebote mehr unterbreitet werden.

**Mit der Verwendung der oben angegebenen Daten durch das Berufsbildungszentrum der Handwerkskammer zum Zwecke der Information über aktuelle Fort- und Weiterbildungsangebote aus dem Angebot des Berufsbildungszentrums erkläre ich mich hiermit einverstanden.**

Ort, Datum Unterschrift

Die Datenverarbeitung ist für die Zusendung von Informationen 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@hwk-xy.de oder unter Datenschutzbeauftragter c/o Handwerkskammer XY, Musterstraße 1, 12345 Musterstadt, erreichen. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

 **Anlage 2**

**Informationspflichten bei Erhebung personenbezogener Daten**

**Muster**

**Information bei Erhebung von Daten beim Betroffenen**

**Informationen zur Datenerhebung gemäß Artikel 13 DSGVO**

Die Handwerksinnung XY, Musterstraße 1, 12345 Musterstadt, Geschäftsführer Herr Mustermann, erhebt und verarbeitet Ihre Daten zur Erfüllung ihrer gesetzlichen Pflichten sowie zum Zweck der Wahrnehmung ihrer Aufgaben, die im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt erfolgen.

Die Datenerhebung und Datenverarbeitung ist für die Erfüllung unserer Pflichten und die Wahrnehmung unserer Aufgaben erforderlich und beruht auf Artikel 6 Abs. 1 c) und e) DSGVO. Eine Weitergabe Ihrer Daten erfolgt ausschließlich auf gesetzlicher Grundlage an andere öffentliche Stellen, die Ihre Daten zur Erfüllung ihrer gesetzlichen Aufgaben benötigen oder an private Personen, die ein berechtigtes Interesse an der Verwendung Ihrer Daten darlegen. Sofern keine besonderen gesetzlichen Aufbewahrungspflichten bestehen, werden die Daten gelöscht, sobald sie für den Zweck ihrer Verarbeitung nicht mehr erforderlich sind.

Sie haben das Recht, der Verwendung Ihrer Daten zum Zweck der Ausübung unserer Aufgaben, die im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt liegen, 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@handwerksinnung-xy.de oder unter Datenschutzbeauftragter c/o Handwerksinnung XY, Musterstraße 1, 12345 Musterstadt, erreichen.

Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

**Anlage 2 A**

**Informationspflicht bei Erhebung personenbezogener Daten auf Webseiten**

**Beispielsformulierungen**

**zur Ergänzung des Datenschutzhinweises**

Die Datenschutzerklärung auf Webseiten richtet sich danach, ob und inwieweit personenbezogene Daten auf der Webseite erhoben werden. Dies kann z.B. durch ein Tracking-Tool, Kontaktformulare oder Bestellungen von Newslettern der Fall sein und muss in jedem Einzelfall individuell angefertigt werden. Für typische Verarbeitungssituationen können Sie folgende Beispielformulierungen verwenden.

**Kontaktformular**

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Kontaktanfrage. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Unser berechtigtes Interesse ist, Ihre Anfrage zu beantworten. 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 Kontaktaufnahme jederzeit zu widersprechen.

**Newsletter**

Wir erheben Ihre Daten zum Zweck der Zusendung des von Ihnen gewünschten Informationsmaterials. Die Datenverarbeitung beruht auf Ihrer Einwilligung gemäß 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 haben das Recht, der Verwendung Ihrer Daten zum Zweck der Zusendung von Informationsmaterialien jederzeit zu widersprechen.

**Registrierung im Mitgliederbereich**

Wir erheben Ihre Daten zum Zweck der Durchführung Ihrer Anmeldung für den Mitgliederbereich von www…..de. Die Datenverarbeitung beruht auf Artikel 6 Abs. 1 f) DSGVO. Wir verfolgen das Interesse, sicherzustellen, dass nur Mitglieder Zugriff auf den Mitgliedern vorbehaltenen Informationen erhalten. 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 Registrierung jederzeit zu widersprechen.

**Ihre Rechte**

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. Ihnen steht des Weiteren ein Beschwerderecht bei der Aufsichtsbehörde zu.

**Datenschutzbeauftragter**

Wenn ein Datenschutzbeauftragter benannt werden muss, müssen dessen Kontaktdaten ebenfalls auf der Webseite genannt werden.

**Anlage 3**

**Die Erteilung von Auskünften**

**Es handelt es sich um ein Muster, das von der jeweiligen Handwerkskammer angepasst werden muss.**

**MUSTER**

**Auskunftserteilung an einen eingetragenen Betrieb**

**Datenspeicherung durch die Handwerkskammer**

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 und zu Ihrem Betrieb gespeichert haben. Sie sind bei uns mit Ihrem Betrieb erfasst.

**I.** Auf Grundlage von § 6 Abs. 1 und § 19 der Handwerksordnung (HwO) in Verbindung mit Anlage D zur Handwerksordnung haben wir die der Tabelle 1 zu entnehmenden Angaben zu Ihrer Person und zu Ihrem Betrieb gespeichert. Diese Daten haben wir von Ihnen oder auf Grundlage von § 14 Abs. 8 Satz 1 Nr. 2 der Gewerbeordnung (GewO) von der zuständigen Gewerbebehörde oder gemäß § 5a Abs. 2 HwO von einer anderen Handwerkskammer erhalten. Zweck der Speicherung dieser Daten ist die Erfüllung der uns nach der HwO übertragenen Aufgaben. Eine Weitergabe der Daten erfolgt ausschließlich auf gesetzlicher Grundlage. Bei der Weitergabe ist zu unterscheiden, ob es sich bei den Empfängern um eine öffentliche oder um eine nicht öffentliche Stelle handelt.

**a) Öffentliche Stellen**

An öffentliche Stellen werden von uns gem. § 6 Abs. 3 HwO die in der Tabelle 1 genannten Daten weitergegeben, sofern die Kenntnis dieser Daten zur Erfüllung der Aufgaben der anfragenden öffentlichen Stelle erforderlich ist (z.B. Deutsche Rentenversicherung, Gewerbeämter, Handwerkskammern, Kreishandwerkerschaften im jeweils satzungsmäßigen Zuständigkeitsbereich).

**b) Nicht öffentliche Stellen**

Hinsichtlich der Weitergabe von Daten an nicht öffentliche Stellen werden Einzelauskünfte

nach § 6 Abs. 2 HwO jedem erteilt, der ein berechtigtes Interesse glaubhaft darlegt. Eine listenmäßige Weitergabe von Daten wird nach § 6 Abs. 2 HwO erteilt, wenn sie zur Erfüllung

der Aufgaben der Handwerkskammer erforderlich ist oder wenn der Auskunftbegehrende ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und kein Grund zu der Annahme besteht, dass Sie ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben bzw. Sie keinen Widerspruch eingelegt haben. Ein Widerspruch liegt uns für ………………………….. vor.

**II.** Neben den oben angeführten Angaben haben wir für unsere internen Verwaltungszwecke weitere folgende Daten gespeichert:

* Zeitpunkt der letzten Änderung
* Betriebsnummer
* Grundsätzliche Beitragspflicht
* Beitreibgemeinde
* Wahlgruppe und -bezirk bezüglich der Kammerwahlen

Diese Daten wurden von uns selbst angelegt und werden ausschließlich zu Verwaltungszwecken verwendet. Eine Weitergabe an Dritte erfolgt nicht.

**III.** Gemäß § 106 Abs. 1 Nr. 5 und § 113 HwO sind wir berechtigt, zur Festsetzung der Beiträge Kammerzugehöriger die Bemessungsgrundlagen bei den Finanzbehörden zu erheben. Dementsprechend haben wir von Ihnen die in Tabelle 2 aufgeführten Daten gespeichert. Über diese Daten verfügen wir aufgrund der Übermittlung durch die Finanzämter. Diese Daten werden ausschließlich zum Zweck der Beitragsfestsetzung erhoben und gespeichert. Eine Weitergabe dieser Daten an Dritte erfolgt nicht.

**IV.** Ergänzend zu internen Verwaltungszwecken haben wir folgende Daten gespeichert:

* Zum Soll gestellte, d.h. veranlagte Grundbeiträge und Umlagen sowie das jeweilige Datum des Bescheids.
* Bezahlte Grundbeiträge und Umlagen sowie das jeweilige Datum der Zahlung sowie die Zahlungswege.

Diese Daten wurden von uns selbst angelegt und werden grundsätzlich ausschließlich zu internen Verwaltungszwecken verwendet. Eine Weitergabe solcher Daten an nicht öffentliche Stellen erfolgt nicht.

Lediglich Angaben über offene Beträge der von uns festgesetzten Beiträge werden gegebenenfalls an öffentliche Stellen weitergegeben, sofern dies zur Erfüllung unserer Aufgaben oder der anfragenden öffentlichen Stelle erforderlich ist. Namentlich sind hier die Fälle der Beitreibung oder Gewerbeuntersagung zu nennen. Andere der genannten Daten werden auch an öffentliche Stellen nicht weitergegeben.

**V.** Die Handwerkskammer gemäß § 23 HwO i. V. m. §§ 32, 76 BBiG berechtigt, u. a. die Berufsbildung zu überwachen. Zur Erfüllung dieser Aufgabe speichern wir bei Ausbildungsbetrieben zusätzlich die in Tabelle 3 aufgeführten Daten. Die Daten werden ausschließlich zur Erfüllung unserer gesetzlichen Pflichten gespeichert.

Die Handwerkskammer darf zur Verbesserung der Ausbildungsvermittlung, der Aktualität der Ausbildungsstatistik und der besseren Feststellung von Angebot und Nachfrage die folgenden Daten gemäß § 28 HwO an die Bundesagentur für Arbeit übermitteln:

* Namen, Vornamen und Geburtsdaten und Anschrift des Lehrlings
* Namen und Anschrift der Ausbildungsstätte
* Ausbildungsberuf
* Datum und Beginn der Berufsausbildung

**VI.** Bei ehrenamtlich für die Handwerkskammer tätigen Personen erfolgt eine Speicherung und Verarbeitung personenbezogener Daten, soweit dies für die Wahrung der ehrenamtlichen Tätigkeiten erforderlich ist.

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 die Handwerkskammer 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

Handwerkskammer ……..

**Anlagen**

Tabelle 1: Handwerksrollendaten

|  |  |  |  |
| --- | --- | --- | --- |
|  | Natürliche Person | Juristische Personen | Personengesellschaften |
|  | Betriebsinhaber | Gesetzliche Vertreter | Für die technische Betriebsleitung verantwortliche persönlich haftender Gesellschafter oder technischer Betriebsleiter  |
| Familienname |  |  |  |
| Vorname |  |  |  |
| Geburtsname |  |  |  |
| Geburtsdatum |  |  |  |
| Staatsangehörigkeit |  |  |  |
| Firma |  |  |  |
| Ort der Niederlassung |  |  |  |
| Straße der Niederlassung |  |  |  |
| Betriebene Handwerke |  |  |  |
| Eintragungsvoraussetzungen |  |  |  |
| Art, Ort und Zeitpunkt der Prüfung die zur Ausübung des Handwerks berechtigt |  |  |  |
| Eintragungszeitpunkt |  |  |  |
|  |  | Betriebsleiter | Weitere Gesellschafter |
| Familienname |  |  |  |
| Vorname |  |  |
| Geburtsname |  |  |
| Geburtsdatum |  |  |
| Staatsangehörigkeit |  |  |
| Vertretungsbefugnis |  |  |

Tabelle 2: Beitragsdaten

|  |  |
| --- | --- |
| Beitrag |  |
| Zeitpunkt der letzten Änderung |  |
| Betriebsnummer |  |
| Grundsätzliche Beitragspflichtigkeit |  |
| Beitreibgemeinde |  |
| Wahlgruppe und -bezirk bezüglich der Kammerwahlen |  |
| Finanzamt |
| Steuernummer |  |
| Bemessungsgrundlagen, d.h. Gewerbeerträge der Beitragsjahre |  |
| Vorläufige Bemessungsgrundlagen, d.h. Gewerbeerträge, die den vorläufigen Veranlagungen zugrunde liegen. |  |
| Zum Soll gestellte, d.h. veranlagte Grundbeiträge |  |
| Datum des Bescheids |  |
| Zum Soll gestellte Umlagen |  |
| Datum des Bescheids |  |
| Bezahlte Grundbeiträge und Umlagen |  |
| Datum der Zahlung |  |
| Zahlungsweg |  |

Tabelle 3: Ausbildungsbetrieb

|  |
| --- |
| Ausbildungsbetrieb |
| **Ausbilder** |
| Familienname |  |
| Vorname |  |
| Geburtsname |  |
| Geburtsdatum |  |
| Art der fachlichen Eignung |  |
| **Auszubildende** |
| Familienname |  |
| Vorname |  |
| Geburtsname |  |
| Geburtsdatum |  |
| Ausbildungsbeginn |  |
| Ausbildungsende |  |
| Prüfungstermine |  |

**Anlage 4**

**Die Erteilung von Auskünften**

**Es handelt es sich um ein Muster, das von der jeweiligen Handwerkskammer angepasst werden muss.**

**MUSTER**

**Auskunftserteilung an einen Auszubildenden**

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 Lehrling erfasst. Zur Datenverarbeitung durch die Handwerkskammer teilen wir Ihnen folgendes mit.

**I.** Die Datenerhebung erfolgt auf der Grundlage von § 28 der Handwerksordnung (HwO) in Verbindung mit Anlage D zur Handwerksordnung. Zweck der Speicherung dieser Daten ist die Erfüllung der uns nach der Handwerksordnung gesetzlich übertragenen Aufgaben. Entsprechend dieser Berechtigung haben wir die der beigefügten Tabelle zu entnehmenden Angaben zu Ihrer Person gespeichert.

Die Daten werden am Ende des Kalenderjahres, in dem das Berufsausbildungsverhältnis beendet wird, in der Lehrlingsrolle gelöscht und dann in einer gesonderten Datei höchstens 60 Jahre lang archiviert. Hinsichtlich der Weitergabe dieser Daten ist zwischen der Weitergabe an öffentliche und nicht öffentliche Stellen zu unterscheiden.

Die Daten dürfen an öffentliche und nicht öffentliche Stellen zur Regelung, Überwachung, Förderung und zum Nachweis der Berufsausbildung in anerkannten Ausbildungsberufen übermittelt werden.

**a) Öffentliche Stellen**

Gem. § 28 Abs. 7 HwO werden zur Regelung, Verbesserung der Ausbildungsvermittlung, zur Verbesserung der Zuverlässigkeit und Aktualität der Ausbildungsvermittlungsstatistik sowie zur Verbesserung der Feststellung von Angebot und Nachfrage auf dem Ausbildungsmarkt folgende Daten aus der Lehrlingsrolle an das statistische Bundesamt und die Bundesagentur für Arbeit übermittelt:

1.Name, Geburtsname, Vorname, Geburtsdatum und Anschrift des Lehrling (Auszubildenden),

2. Name und Anschrift der Ausbildungsstätte,

3. Ausbildungsberuf sowie

4. Datum des Beginns der Berufsausbildung.

Zur Regelung der Ausbildung werden die Daten an die zuständigen Prüfungsausschüsse der Handwerkskammer übermittelt. Die zuständige Innung und der Lehrlingswart erhalten die Daten zur Überwachung und Förderung der Ausbildung.

**b) Nicht öffentliche Stellen**

Hinsichtlich der Weitergabe von Daten an nicht öffentliche Stellen gilt, dass die Daten der Lehrlingsrolle ausschließlich an ein privatwirtschaftlich betriebenes Berufsbildungszentrum der Handwerkskammer weitergegeben werden.

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 die Handwerkskammer 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

Handwerkskammer ……..

**Anlage**

|  |
| --- |
| **Lehrling** |
| Familienname |  |
| Vorname |  |
| Geburtsname |  |
| Geschlecht |  |
| Geburtsdatum |  |
| Staatsangehörigkeit |  |
| Straße |  |
| PLZ |  |
| Wohnort |  |
| Allgemeinbildender Schulabschluss |  |
| Vorausgegangene Teilnahme an berufsvorbereitender Qualifizierung oder beruflicher Grundbildung |  |
| Berufliche Vorbildung |  |
| **Gesetzlicher Vertreter** (falls erforderlich) |
| Familienname |  |
| Vorname |  |
| Geburtsname |  |
| Straße |  |
| PLZ |  |
| Wohnort |  |
| **Ausbildungsverhältnis** |
| Ausbildungsberuf & Fachrichtung |  |
| Ausbildungsschwerpunkt |  |
| Datum Abschluss Ausbildungsvertrag |  |
| Ausbildungsdauer |  |
| Datum Beginn Berufsausbildung |  |
| Dauer der Probezeit |  |

**Anlage 5**

**Verzeichnis von Verarbeitungstätigkeiten**

**des Verantwortlichen**

Hauptblatt

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

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

|  |
| --- |
| **2. Gesetzlicher Vertreter (= Präsident, HGF, Obermeister, 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, ladungsfähige Anschrift |
| Nr. 2 | Vorstände, Geschäftsführer Angaben: Namen des Präsidenten, des Hauptgeschäftsführers, des Obermeisters und/oder des Geschäftsführers)*Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.* |
| Nr. 3 | Vom Verantwortlichen bestellter Datenschutzbeauftragter 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 in der Organisation 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, 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 Mitgliederverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
* Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Mitgliederbeziehungen, Marketing, 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 Tätigkeit 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 Mitglieder, Arbeitnehmer, Schuldner 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 „Mitgliederdaten“ oder Ähnliches.Beispiele: * Mitglieder: 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, Mitglieder, 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 die Organisation 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**

**Verzeichnis von Verarbeitungstätigkeiten**

**des Verantwortlichen**

Hauptblatt

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

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

|  |
| --- |
| **2. Gesetzlicher Vertreter (= Präsident, HGF, Obermeister, Geschäftsführung)***Herr Mustermann, Musterstraße 17-21, 12345 Musterstadt* |

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

**4. Zuständige Aufsichtsbehörde**

Landesbeauftragter für Datenschutz und Informationsfreiheit des Landes XY

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, ladungsfähige Anschrift |
| Nr. 2 | Vorstände, Geschäftsführer Angaben: Namen des Präsidenten, des Hauptgeschäftsführers, des Obermeisters und/oder des Geschäftsführers)*Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.* |
| Nr. 3 | Vom Verantwortlichen bestellter Datenschutzbeauftragter 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:** Führung der Handwerksrolle

**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**Führung der Mitgliederverzeichnisse der Handwerkskammer Musterstadt |

|  |
| --- |
| **5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit**§§ 6, 18, 19 HwO, Anlage D HwO |

|  |
| --- |
| **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** |
| Betriebsinhaber  | Name, Vorname, Adressdaten, Geburtsdatum, Geburtsort, Geschlecht, Qualifikation, Prüfungsdaten, (elektronische) Kontaktdaten, ggfs. Firma oder Etablissementbezeichnung |
| Technische Betriebsleiter | Siehe oben |
| Ausbilder? | Siehe oben (ohne Adressdaten) |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| **7. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, Art. 30 Abs. 1 d) DSGVO)** |
| **7.1. Interne Empfänger** | Mitarbeiter der Abteilung Handwerksrolle und Beitrag |
| **7.2. Externe Empfänger** | Partielle Offenlegung ggü. der DRV, den SOKAs der jeweiligen Handwerke, örtlich zuständigen Energieversorgern |
| **7.3. Vertragliche Dienstleister**(Vertrag der Auftragsdatenverarbeitung als Anlage beifügen) | Externer EDV-Dienstleister für die Führung der Datenbank, Dienstleister für die Führung der Betriebssuche. |

|  |
| --- |
| **8. Datenübermittlungen in Drittländer oder 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**Löschfristen ergeben sich aus § 13 Abs. 5 HwO, d.h. 30 Jahre nach der Löschung des Betriebes aus der Handwerksrolle. |

|  |
| --- |
| **10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO**IT-Sicherheitskonzept der HWK Musterstadt |
| **10.1.** **Art der eingesetzten Datenverarbeitungsanlagen und Software (optional)*** DV-Anlagen
* Software (und ggf. Unterprogramme)
* Schnittstellen
 |
| **10.2** **Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO***----------**(Siehe 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 in der Organisation 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, 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 Mitgliederverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
* Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Mitgliederbeziehungen, Marketing, 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 Tätigkeit 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 Mitglieder, Arbeitnehmer, Schuldner 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 „Mitgliederdaten“ oder Ähnliches.Beispiele: * Mitglieder: 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, Mitglieder, 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 die Organisation 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 7**

**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 8**

**Der behördliche Datenschutzbeauftragte (DSB)**

**MUSTER**

**Benennung eines/r behördlichen 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 a) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit § \_\_\_\_\_ Landesdatenschutzgesetz. In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Geschäftsführung unmittelbar unterstellt.

Zuständiges Mitglied der Geschäftsführung ist

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

Ihre Aufgaben als Datenschutzbeauftragte/r ergeben sich aus den Artikeln 37 bis 39 DSGVO sowie § \_\_\_\_\_Landesdatenschutzgesetz. 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 Geschäftsführung laufend Bericht erstatten.

Erforderliche Organisationsanweisungen schlagen Sie der Geschäftsführung vor.

Die Stellung des behördlichen Datenschutzbeauftragten ist in § \_\_\_ Landesdatenschutzgesetz geregelt.

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

Ort, Datum Unterschrift Hauptgeschäftsführer

Mit der Benennung bin ich einverstanden

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

Unterschrift, Datenschutzbeauftragte/r

**Anlage 9**

**Auftragsverarbeitung – Hinweise für Handwerksorganisationen**

**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 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.“