**Muster**

**Verarbeitungsverzeichnis**

Hauptblatt

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

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

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

|  |
| --- |
| **3. Datenschutzbeauftragter (soweit erforderlich; vgl. Information bei Erhebung Daten)**  **Name:** Frau Anja Mustermann  **Anschrift:** Musterstraße 17-21, 12345 Musterstadt  **E-Mail:** datenschutzbeauftragter@zahntechnik-mustermann.de  **Tel.:** 01234/ 123456-34 |
|  |
| **4. Zuständige Aufsichtsbehörde**  Landesbeauftragter für Datenschutz und Informationsfreiheit  Verpflichtende Meldung des Datenschutzbeauftragten bereits erfolgt  (soweit Datenschutzbeauftragter erforderlich)  ⌧ Ja  **□** Nein |
|  |
| **5. Regelungen zur Datensicherheit**  technische/organisatorische Maßnahmen (siehe Anlage) |
|  |
| **6. Sachverhalte zu Drittstaatenübermittlung**  *Findet nicht statt.* |

**Erläuterungen zum Hauptblatt**

|  |  |
| --- | --- |
| Nr. 1 | Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO)  Angaben: Name/Firma, ladungsfähige Anschrift |
| Nr. 2 | Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter  Angaben: Namen der geschäftsführenden Personen  *Gegebenenfalls kann hier einfach ein Link auf das Impressum der Webseite des Betriebs eingetragen werden.* |
| Nr. 3 | Vom Verantwortlichen bestellter Datenschutzbeauftragter (sofern ein Datenschutzbeauftragter bestellt wurde)  Angaben: Name, Kontaktdaten |
| Nr. 4 | Die Meldung der Kontakt-Informationen des Datenschutzbeauftragten  (Funktions-)E-Mail-Adresse und Telefonnummer sind Pflichtangaben. |
| Nr. 5 | Gegebenenfalls Verweise auf übergreifende Regelungen (*falls solche existieren, die grundsätzlich 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**

⌧ Ersterstellung

* Änderung eines bestehenden Verzeichnisses

**Erstellungsdatum**: xx.xx.2018

**Bezeichnung der Verarbeitungstätigkeit:** Führen eines zahntechnischen Labors

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

**1. Verantwortlicher Fachbereich/verantwortliche Führungskraft**

Herr Mustermann

**2. Bei gemeinsamer Verantwortlichkeit:**

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

**II. Angaben zur Verarbeitungstätigkeit**

**3. Risikobewertung**

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

⌧ Nein

**□** Ja

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

|  |
| --- |
| **4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit**  Organisation von Geschäftskontakten und Bestandskunden  Versorgung mit Zahnersatz  Durchführung von Verträgen |

|  |
| --- |
| **5. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit**  Art. 6 sowie Art. 9 DSGVO |

|  |  |
| --- | --- |
| **6. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Art. 30 Abs. 1 c) DSGVO** | |
| **6.1. Betroffene Personengruppen** | **6.2. Kategorien personenbezogener Daten** |
| Kunden, Geschäftspartner  Arbeitnehmer | Gesundheitsdaten  Name, Vorname, Adressdaten, (elektronische) Kontaktdaten, 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** | Mitarbeiter (Meister, Gesellen, Auszubildende, sonstige Mitarbeiter) |
| **7.2. Externe Empfänger** | Auftraggeber, Sozialversicherungsträger; Dienstleistungsträger der gesetzlichen Krankenkassen; Finanzbehörden |
| **7.3. Vertragliche Dienstleister**  (Vertrag der Auftragsdatenverarbeitung als Anlage beifügen) | Ggf. beauftragte Abrechnungsdienstleister; Rechenzentren; zahntechnische Labore; Fräszentren; Hersteller, etc. |

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

|  |
| --- |
| **9. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien, Art. 30 Abs. 1 f) DSGVO**  Die Daten werden gelöscht, wenn sie für die Erfüllung des Versorgungszwecks (siehe Nr. 4) nicht mehr erforderlich und die gesetzlichen Aufbewahrungsfristen erloschen sind. |

|  |
| --- |
| **10. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO**  Siehe Anlage „technische und organisatorische Maßnahmen“ (betriebsinternes IT-Sicherheitskonzept XY) |
| * 1. **Art der eingesetzten DV-Anlagen und Software**   ---------    (Siehe betriebsinternes IT-Sicherheitskonzept XY) |
| **10.2** **Konkrete Beschreibung der technischen und organisatorischen Maßnahmen, Art. 30 Abs. 1 g) i.V.m. Art. 32 Abs. 1 DSGVO**  *----------*    (Siehe betriebsinternes IT-Sicherheitskonzept XY) |

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

Weitere Dokumentationen zur Verarbeitungstätigkeit

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

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

**Erläuterungen zum Verarbeitungsverzeichnis**

|  |  |
| --- | --- |
| Nr. 1 | Eindeutige Bezeichnung der dokumentierten Verarbeitung/ Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden.  Beispiele: - Allgemeine Kundenverwaltung  - Customer-Relationship-Management (CRM) |
|  | 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. Die Erwägungsgründe der DSGVO bewerten die Verarbeitung von Patientendaten durch einen einzelnen Betrieb des Gesundheitswesens dabei nicht als „umfangreich“. |
| Nr. 4 | Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können. |
| 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 Sozialversicherungsträger und beauftragte Abrechnungsdienstleister sowie andere 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 Angehörige von Gesundheitsberufen, Vertragspartner, Kunden, Behörden, Versicherungen, sowie sonstige Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Hersteller, Reparaturfirmen, Otoplastiklabore, 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.  Es reicht in der Regel aus, darauf zu verweisen, dass die Daten gelöscht werden, wenn der Versorgungszweck erfüllt ist. |
| 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. |
| 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 (insb. Art. 13, 14 DSGVO) (Muster: Information bei Erhebung von Daten beim Betroffenen)* * *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)* |