**Muster zur Dokumentation einer Verarbeitungstätigkeit
gem. Artikel 30 DSGVO**

|  |  |
| --- | --- |
| **Bezeichnung der Verarbeitungstätigkeit** | *Der Name soll kurz und knapp beschreiben, welche Verarbeitung hiermit gemeint ist. Beispiele: Personalverwaltung, Buchhaltung, Verwaltung von Projektdaten, Umgang mit Bewerbungsdaten, Projektmanagement, Durchführung von Schulungen, etc.*  |
| **Zweck der Verarbeitung** | *Aus welchem Grund verarbeiten Sie die Daten? Was ist der Zweck der Verarbeitung?**Beispiele:* * *Datenverarbeitung im Beschäftigungskontext*
* *Sicherstellung des Betriebs der Organisation oder des Unternehmens*
* *Gewährleistung allgemeiner Sicherheitsmaßnahmen*
* *Bereitstellung von Infrastruktur für den Betrieb der Organisation oder des Unternehmens*
* *Begründung, Durchführung oder Beendigung von Kauf- oder Dienstleistungsverträgen*
* *Herstellung von Produkten und Dienstleistungen*
 |
| Verantwortliche Abteilung | *Welche Abteilung in Ihrer Organisation oder Ihrem Unternehmen ist für die Verarbeitung zuständig?*  |
| Ansprechperson | *Benennen Sie eine interne Ansprechperson bzw. die Person, die für den Prozess verantwortlich ist (Business Process Owner).* |
| Prozessbeschreibung | *Kurzbeschreibung der Verarbeitung. (optional)**Beschreibt den internen Prozess in Kurzform. Dies dient nur zur Veranschaulichung und zum besseren Verständnis.* |
| Betroffene Personengruppen | *Zählen Sie die Kategorien der Personen auf, die von der Verarbeitung betroffen sind. Mögliche Kategorien sind z.B.* * *Beschäftigte*
* *Interessenten*
* *Lieferanten*
* *Kunden*
* *…*
 |
| Betroffene Datenkategorien | *Zählen Sie die Kategorien der personenbezogenen Daten der betroffenen Personen auf, die im Rahmen dieser Verarbeitung verarbeitet werden.* *Hier sollten Sie sich Zeit nehmen und gut überlegen, welche Daten Sie von den betroffenen Personen verarbeiten. Das hängt stark von der jeweiligen Verarbeitung ab.* *z.B. (Bitte soweit wie möglich konkretisieren)** *Personenstammdaten (z.B. Name, Geburtsdatum, Familienstand, etc.)*
* *Kontaktdaten (z.B. Postadresse, E-Mail-Adresse, Telefonnummer, etc.)*
* *Stammdaten von Beschäftigten (z.B. Lohnsteuerklasse, Personalnummer, etc.)*
* *Nutzungsdaten (z.B. Surfverhalten, Kaufverhalten, Zugriffsdaten, etc.)*
* *Vertragsdaten (z.B. Vertragsnummer, Vertragsinhalte, Abrechnungsmodalitäten, etc.)*
* *Identifikationsmerkmale und Kennnummern (z.B. Personalausweisnummer, Reisepassnummer, Steuernummer, etc.)*
* *Abrechnungsdaten Personal (z.B. Lohn/Gehalt, Zuschläge, Krankenversicherungsbeiträge, sonstige Abzüge, etc.)*
* *Kundendaten (z.B. Konditionen, Auftragshistorie, Zahlungsverhalten, etc.)*
* *Zahlungsdaten (z.B. Bankverbindung, Kreditkartendaten, etc.)*
* *Bewerbungsspezifische Daten (z.B. Zeugnisse, Bewerbungsunterlagen, etc.)*
* *Lieferantendaten (Ansprechpartner und deren Kontaktdaten, etc.)*
* *Aufgedrängte Daten (Daten, die der Betroffene von sich aus übermittelt)*
* *….*
 |
| Besondere personenbezogene Daten | **Werden besondere Kategorien personenbezogener Daten nach Art. 9 verarbeitet?** *Ja / nein**Die DSGVO definiert in Artikel 9 besonders schützenswerte Daten. Sollten Sie solche Daten verarbeiten, empfehlen wir dringend die Durchführung einer Datenschutzfolgeabschätzung (DSFA). Ziehen Sie außerdem einen Datenschutzexperten oder rechtlichen Beistand hinzu.* *Anmerkung: Dies betrifft „Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ (Daten nach DSGVO Art. 9 (1))* |
| **Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden (gemäß Art. 30 Abs. 1 d) DSGVO)** |
| Interne Empfänger | *Liste der internen Empfänger (z.B. einzelne Abteilungen oder Personengruppen)**z.B.** *Buchhaltung*
* *Geschäftsleitung*
* *IT-Abteilung*
* *Sonstige Empfänger im Bedarfsfall*
* *…*
 |
| Externe Empfänger | *Externe Empfänger sind vor allem Dienstleister oder Behörden, die entweder Zugriff auf die Daten haben oder an die Daten übermittelt werden. Hier werden auch die Anbieter von Softwarelösungen aufgeführt, die theoretisch Zugriff auf die abgelegten Daten haben.* *z.B.** *Steuerberater*
* *Dienstleister XYZ (Namen und Art nennen)*
* *…*
 |
| Datenübermittlung an Drittländer (gemäß Art. 30 Abs. 1 e) DSGVO) | *Halten Sie hier fest, ob eine Übermittlung der Daten in ein Drittland stattfindet. Dies passiert häufig beim Einsatz von Dienstleistern (speziell von Internetdienstleistern und Softwarelösungen aus der Cloud).* *Halten Sie bei diesem Punkt entweder fest: „Datenübermittlung findet nicht statt und ist auch nicht geplant.“ oder „Datenübermittlung in ein Drittland erfolgt.“ und beschreiben Sie anschließend, welche Übermittlung stattfindet.* *Anmerkung: Hier sollte grundsätzlich immer das Drittland angegeben werden, sobald es sich nicht um das Land handelt, in dem Sie Ihren Sitz haben. Angeben werden kann auch der Ort der Datenverarbeitung sowie der Hauptsitz des Dienstleisters (sofern unterschiedlich).* *Eine Risikoeinschätzung des Drittlandes muss ebenfalls erfolgen.* *Unkritisch sind alle EU-Länder und Länder, denen die EU über einen Angemessenheitsbeschluss ein adäquates Datenschutzniveau zugesprochen hat. Bei allen anderen Ländern sollten weiterführende Maßnahmen durchgeführt werden.* *Die entsprechenden Garantien sollten ebenso an dieser Stelle aufgeführt sein. Zumindest sollte ein Vertrag zur Auftragsdatenverarbeitung mit dem jeweiligen Dienstleister abgeschlossen werden.*  |
| Fristen zur Löschung der Daten | *Halten Sie fest, wann Sie die erfassten Daten wieder löschen. Hier können Sie auch auf ein externes Löschkonzept verweisen, welches separat zu erstellen ist.*  |
| **Prüfung der Datenschutzkonformität für Verantwortliche** |
| Rechtsgrundlage der Verarbeitungstätigkeit  | *Eine Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn eine der Rechtsgrundlagen anwendbar ist, die in der DSGVO aufgeführt sind:** *Die Verarbeitung basiert auf einer Einwilligung der betroffenen Person (DSGVO Art. 6 Abs. 1 a)*
* *Die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich. (DSGVO Art. 6 Abs. 1 b)*
* *Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich. (DSGVO Art. 6 Abs. 1 c)*
* *Die Verarbeitung ist zum Schutz lebenswichtiger Interessen erforderlich. (DSGVO Art. 6 Abs. 1 d)*
* *Die Verarbeitung ist zur Wahrung des öffentlichen Interesses erforderlich. (DSGVO Art. 6 Abs. 1 e)*
* *Die Verarbeitung basiert auf dem berechtigten Interesse des Verantwortlichen. (DSGVO Art. 6 Abs. 1 f)*
 |
| Weitere Gesetze | *Sollte es weitere Gesetze in Ihrem Land geben, auf deren Grundlage Sie die hier beschriebenen Verarbeitung durchführen, können Sie diese an dieser Stelle dokumentieren.*  |
| **Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 30 Abs 1 g) i.V.m. Art. 32 Abs. 1 DSGVO***Um den Schutz von personenbezogenen Daten zu gewährleisten, müssen Sie in Ihrem Unternehmen technischen und organisatorischen Maßnahmen festlegen. Diese können auch separat dokumentiert werden.*  |