Dokumentation der Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	*(Name, Anschrift)*
Ggf. gemeinsamer Verantwortlicher	*(Name, Anschrift)*
Gesetzlicher Vertreter (= Geschäftsführung)	*(Name, Kontaktdaten)*
Ggf. Vertreter in der EU (gemäß Art. 27 DSGVO)	*(Name, Anschrift)*
Datenschutzbeauftragter	*(Name, Kontaktdaten)*

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	*(Eindeutige Bezeichnung der dokumentierten Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen alltägliche Bezeichnung des Fachprozesses gewählt werden.* *Beispiele:* • *E-Mailverarbeitung* • *Allgemeine Kundenverwaltung* • *Lohn- und Gehaltsabrechnung*
Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse):	*Nach der Unternehmensorganisation für diese Verarbeitungstätigkeit verantwortlicher Fachbereich bzw. Funktionsbezeichnung inkl. Name und Kontaktdaten*
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des Leiters/der Leiter des/ der weiteren Verantwortlichen	*s. o.*
Status: (optionale Angabe)	*In Betrieb, geplant?*
Art der Verarbeitung / Name der Software: (optionale Angabe)	*Eigenentwickelte Software, Standardsoftware, Auftragsdatenverarbeitung, etc.?*
Ort der Verarbeitung: (optionale Angabe)	*Wo werden die Daten verarbeitet und gespeichert? Z. B. im Haus, in einem Rechenzentrum in Deutschland oder Ausland.*

Allgemeine datenschutzrechtliche Anforderungen DSGVO

Zweckbestimmung:	*Beispiele:* • *Verarbeitungstätigkeit: „E-Mailverarbeitung“ → verfolgte Zweckbestimmungen: „Durchführung der elektronischen Kommunikation“* • *Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“ → verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung, Inkasso“* • *Verarbeitungstätigkeit: „Lohn- und Gehaltsabrechnung“ → verfolgte Zweckbestimmungen: „zur Erstellung der Lohnabrechnung; Erfüllung gesetzl. Anforderungen“* *Eine Verarbeitung kann auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.*
Zweckänderung: (optionale Angabe)	*Wenn eine Zweckänderung durchgeführt werden soll/ wurde, sollte hier der Grund für die Zweckänderung benannt werden.*
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	*Hinweis: im Folgenden handelt es sich nur um Beispiele:* • *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)* • *Einwilligung eines Kindes (Art. 6 Abs. 1 lit. a, Art. 8)* • *Vertrag oder Vertragsanbahnung (Art. 6 Abs. 1 lit. b)* • *Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f)* • *Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs.)* • *Sonstige (etwa DSAnpUG-EU)*
Erforderlichkeit und Verhältnismäßigkeit, Art. 5 DSGVO (optionale Angabe)	*Die Rechtmäßigkeit orientiert sich neben den Prinzipien „Verhältnismäßigkeit“ (Art. 5 Abs. 1 lit. b), „Transparenz“ (Art. 5 Abs. 1 lit. a), „Datenminimierung“ (Art. 5 Abs. 1 lit. c), „Richtigkeit“ (Art. 5 Abs. 1 lit. d), „Speicherbegrenzung“ (Art. 5 Abs. 1 lit. c) und „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f), insbesondere an dem Prinzip der Zweckbindung (Art. 5 Abs. 1 lit. b).*
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	*Hier sollte eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen auf Basis von Art. 35 DSGVO durchgeführt werden, um festzustellen ob die Durchführung einer Datenschutz-Folgenabschätzung notwendig ist.*

Erhebung der Daten

Kreis der betroffenen Personengruppen	*Als betroffene Personengruppen kommen beispielsweise Kunden, Auftraggeber, Interessenten, Mandanten, Patienten, Arbeitgeber, Mitarbeiter, Bewerber, Mieter, Lieferanten usw. in Betracht.*
Art der gespeicherten Daten bzw. Datenkategorien:	*Beispiele:* • *Abrechnungsdaten* • *Adressdaten* • *Bankverbindungsdaten/Kreditkartendaten* • *Bonitätsdaten* • *Geburtsdatum* • *IT-Nutzungsdaten/Log Daten/Protokolldateien* • *IP-Adresse* • *Interessen/Präferenzen* • *Kontaktdaten* • *Lohn-und Gehaltsdaten* • *Lebenslauf* • *Name/Vorname/Anrede/Titel* • *Qualifikationsdaten/Leistungs- und/oder Potenzialbeurteilung* • *Sozialversicherungsdaten* • *Standortdaten* • *Vertragsdaten* • *Vertragsstammdaten* • *Zahlungsdaten* • *Zeiterfassungsdaten*
Herkunft der Daten:	*Woher stammen die Daten? Von Betroffenen selbst oder von einem Dritten?*

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

Interne Empfänger (innerhalb der verantwortlichen Stelle)	*Empfänger innerhalb des Verantwortlichen, z. B. Personalabteilung, IT-Abteilung, Einkauf, Produktion, Buchhaltung, Auftragsverarbeiter*
Externe Empfänger und Dritte: (jeder andere Empfänger, auch in Konzernunternehmen soweit nicht Auftragsverarbeiter)	*Dritte, die nicht Auftragsverarbeiter sind, z. B. Konzerngesellschaft, Geschäftskunde, Finanzamt, Polizei, Staatsanwaltschaft.* *Das Datenschutzrecht kennt kein Konzernprivileg. Werden personenbezogene Daten innerhalb des Konzerns von einer Konzerngesellschaft zur anderen Konzerngesellschaft weitergegeben oder übermittelt, so handelt es sich bei der empfangenden Konzerngesellschaft um einen Dritten und nicht um einen Empfänger innerhalb des Verantwortlichen.*

Zugriffsberechtigte Personen (optionale Angaben)

Zugriffsberechtigte Personen	*Benennung der berechtigten Gruppen z. B. Personalabteilung, IT-Abteilung, Einkauf, Produktion, Buchhaltung, Auftragsverarbeiter*
Nachweis	*Skizzierung des Berechtigungsverfahrens: z. B. Active-Directory, Berechtigungskonzept*

Auftragsverarbeitung als Auftraggeber (optionale Angabe)

Auftragsverarbeiter	*Dieser Abschnitt ist auszufüllen, falls von dem Verantwortlichen bei der Verarbeitungstätigkeit Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter eingesetzt werden (Art. 28 DSGVO).* *Bei mehr als einem Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter ist jeweils eine neue Tabelle anzulegen, welche nummerisch fortlaufend zu kennzeichnen ist*
Schriftlicher datenschutzkonformer Vertrag	*Ist ein Auftragsverarbeitungsvertrag vorhanden? (Nach BDSG oder bereits nach DSGVO?)*
Geeignetheit des Auftragsverarbeiters	*Hier sollte das Ergebnis der Erstkontrolle angeführt werden.*
Standort der Verarbeitung	*In der EU oder im Drittland (d.h. außerhalb der EU/des EWR)?*

Datenübermittlung in Drittstaaten / internationale Organisationen

Datenübermittlung in Drittstaaten:	*Die Übermittlung von personenbezogenen Daten in Drittländer ist ausschließlich zulässig, wenn neben der Rechtmäßigkeit der Datenverarbeitung weiterführend das durch die DSGVO gewährleistete Schutzniveau in dem jeweiligen Drittland nicht untergraben wird (Art. 44).*
Drittstaaten / internationale Organisationen	*Drittländer sind Länder außerhalb der EU/des EWR.* *Beispiele für internationale Organisationen: Institutionen der UNO, der EU, usw.*

Angemessenes Datenschutzniveau durch:	*Wählen Sie hier ein Element aus:*
	• *Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO*
	• *Garantien gem. Art. 46 DSGVO*
	  - *Verbindliche interne Datenschutzvorschriften (BCR)*
	  - *EU-Standardvertrag*
	Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. Abs. 2 DSGVO)

Regelfristen für die Löschung der Daten

Speicherdauer	*Anzugeben sind hier die konkreten Aufbewahrungs- und Löschfristen, die in Verarbeitungstätigkeiten implementiert sind.* *Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene (und in der Verarbeitungstätigkeit umgesetzte) Löschkonzept aus.*
Nachweis	*Dokument in dem der Nachweis zur Löschung geschaffen wird, z. B. Löschkonzept*

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DSGVO)	*Maßnahmen müssen unter anderem Folgendes einschließen:* • *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;* • *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen;* • *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;* • *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.* *Optional kann hier eine knappe Beschreibung der TOM angegeben werden, sofern sich die TOM schon aus vorhandenen Sicherheitsleitlinien oder (Datenschutz-) Konzepten bzw. Zertifizierungen (z.B. ISO 27001) ergeben. Sollte dies der Fall sein, ist ein konkreter Verweis hierauf ausreichend. Abweichungen sind jedoch zu dokumentieren.*
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	*Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche (und der Auftragsverarbeiter) geeignete TOM, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1).*

Stellungnahme des Datenschutzbeauftragten	
Prüfung durch den Datenschutzbeauftragten	*Erfolgt/nicht erfolgt*
Besteht weiterer Handlungsbedarf?	*Ja/nein*
Offene Maßnahmen	*Sofern Handlungsbedarf besteht, Auflistung der offenen Maßnahmen.*
Datum der Dokumentation	

Prüfung durch die Geschäftsleitung	
Prüfung durch die Geschäftsleitung	*Erfolgt/nicht erfolgt*

Datum, Unterschrift	

Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren.

Hierzu gehören z. B. Angaben zu:

- Informationspflichten (Art. 13 und 14 DSGVO);
- Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO);
- durchgeführten Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit (Art. 35 DSGVO).

Hinweis: Bei einer Anfrage der Aufsichtsbehörde müssen ggfs. weitere Nachweise vorgelegt werden.

Quelle: activeMind AG