

# Kostenlose Vorlage: Verzeichnis von Verarbeitungstätigkeiten

Bei diesem Dokument handelt es sich um eine kostenlose Vorlage bzw. Checkliste der activeMind AG zu den Themenbereichen Datenschutz und Datensicherheit. Die aktuellste Version finden Sie stets auf [im Downloadbereich unserer Website](https://www.activemind.de/datenschutz/dokumente/).

Sie können dieses Dokument an die Bedürfnisse in Ihrem Unternehmen anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass die activeMind AG keinerlei Haftung für etwaige Fehler übernimmt.

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der activeMind AG

Telefon: +49 (0)89 / 91 92 94 – 900  
E-Mail: [anfrage@activemind.de](mailto:anfrage@activemind.de)  
Web: <https://www.activemind.de>

# **Dokumentation der Verarbeitungstätigkeit**

|  |  |
| --- | --- |
| **Angaben zum Verantwortlichen** | |
| Verantwortlicher  (gemäß Art. 4 Nr. 7 DSGVO) | *(Name, Anschrift)* |
| Gesetzlicher Vertreter (= Geschäftsleitung) | *(Name, Kontaktdaten)* |
| Datenschutzbeauftragter  (gemäß Art. 37 ff. DSGVO) | *(Name, Kontaktdaten)*  *Soweit vorhanden entweder externen oder betrieblichen DSB angeben* |

|  |  |
| --- | --- |
| **Angaben nach Bedarf (soweit nicht zutreffend löschen)** | |
| Ggfs. Vertreter in der EU  (gemäß Art. 27 DSGVO) | *(Name, Anschrift)* |
| Ggfs. gemeinsamer Verantwortlicher  (gemäß Art. 26 DSGVO) | *(Name, Anschrift)*  *Bei gemeinsamer Verantwortlichkeit: Name*  *und Kontaktdaten des Leiters/der Leiter des/*  *der weiteren Verantwortlichen* |

|  |  |
| --- | --- |
| **Beschreibung der Verarbeitungstätigkeit** | |
| Allgemeine Beschreibung 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* * *Finanzbuchhaltung* * *Arbeitszeiterfassung* * *Betrieb Website* |

|  |  |
| --- | --- |
| **Angaben zur Verarbeitungstätigkeit nach Maßgabe des Art. 30 Abs. 1 DSGVO** | |
| Zwecke der Verarbeitung | * *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“* * *Etc. (Auch die Angabe mehrerer Zwecke ist möglich).* |
| Beschreibung der Kategorien  betroffener Personen | *Als betroffene Personengruppen kommen beispielsweise Kunden, Auftraggeber, Interessenten, Mandanten, Patienten, Beschäftigte, Bewerber, Mieter, Lieferanten usw. in Betracht.* |
| Beschreibung der Kategorien  personenbezogener Daten | * *Abrechnungsdaten* * *Bonitätsdaten* * *IT-Nutzungsdaten/Log Daten/Protokolldateien* * *Stammdaten* * *Lohn-und Gehaltsdaten* * *Qualifikationsdaten* * *Standortdaten, etc.* |

|  |  |
| --- | --- |
| **Empfänger oder Kategorien von Empfängern** | |
| Interne Empfänger (innerhalb des Verantwortlichen) | *Empfänger innerhalb des Verantwortlichen, z. B. Personalabteilung, IT-Abteilung, Einkauf, Produktion, Buchhaltung, Vertrieb, etc.* |
| Auftragsverarbeiter | *Beispielsweise IT-Support, Fernwartung, Hosting-Dienstleister, Lohnbüro, Webentwicklung, Mailingdienstleister, Poststelle, Callcenter, Clouddienstleister, Aktenvernichter, etc.* |
| Datenweitergabe an Dritte | *Z.B. Kunden, Behörden, Banken, Versicherungen, Unternehmen innerhalb der Unternehmensgruppe, Steuerkanzlei, Ärzte, Handelsvertreter, etc.* |

|  |  |
| --- | --- |
| **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 geeignete oder angemessene Garantie | * *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** | |
| Für die Löschung vorgesehene Fristen bzw. Speicherdauer oder Kriterien für deren Festlegung | *Es werden die konkreten Löschfristen angegeben. Wenn diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf Selbiges 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. 32 Abs. 1 DSGVO) | *Die Maßnahmen umfassen Folgendes:*   * *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;* * *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste 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 TOM zur Gewährleistung der Sicherheit der Verarbeitung.* |
| Nachweis | *Auch ein Verweis reicht aus, sofern sich die TOM schon aus vorhandenen Sicherheitsleitlinien oder Konzepten bzw. Zertifizierungen (z.B. ISO 27001) ergeben.* |
| 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 DSGVO ).* |

|  |  |
| --- | --- |
| **Angaben für eine weitergehende interne Dokumentation oder zur Erfüllung von Informationspflichten nach Art. 13 & 14 DSGVO (optional – nach Bedarf löschen)** | |
| Verarbeitungsart | *Analoge Verarbeitung, Teilautomatisierte Verarbeitung, Automatisierte Verarbeitung / Software.* |
| Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO | *Hinweis: im Folgenden handelt es sich nur um Beispiele:*   * *Einwilligung (Art. 6 Abs. 1 lit a, Art. 7 DSGVO)* * *Einwilligung eines Kindes (Art. 6 Abs. 1 lit a, Art. 8 DSGVO)* * *Vertrag oder Vertragsanbahnung (Art. 6 Abs. 1 lit b DSGVO)* * *Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit f DSGVO)* * *Verarbeitung besonderer Kategorien personenbezogener Daten, z.B. ausdrückliche Einwilligung (Art. 9 Abs. 2 lit a DSGVO)*   *Sonstige (etwa BDSG)*  *Hinweis: Die Nennung der Rechtsgrundlage ist Teil der notwendigen Informationen im Rahmen der Hinweispflicht nach Art. 13 & 14 DSGVO.* |
| Ort der Verarbeitung | *Wo werden die Daten verarbeitet bzw. gespeichert? Z. B. im Haus, in einem Rechenzentrum mit/ohne Fremdzugriff.* |
| Quelle der Daten | *Wo wurden die Daten erhoben? Vom Betroffenen selbst oder beispielsweise aus öffentlich zugänglichen Quellen, Adresshandel, Auskunftei etc.*  *Die Information dient der allgemeinen Dokumentation und erleichtert die Entscheidung, wonach sich die Informationspflicht richtet. Bei Ersterhebung nach Art. 13 DSGVO. Werden die Daten nicht bei dem Betroffenen selbst erhoben ist dieser nach Art. 14 Abs. 2 lit f DSGVO auch über die Quelle der Daten zu unterrichten.* |
| Verantwortlicher Ansprechpartner (inkl. Fachabteilung, Telefonnummer und E-Mail-Adresse): | *Nach der Unternehmensorganisation für diese Verarbeitungstätigkeit verantwortlicher Fachbereich bzw. Funktionsbezeichnung inkl. Name und Kontaktdaten* |
| 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.* |
| Grundsätze der Verarbeitung, Art. 5 DSGVO | *Die Rechtmäßigkeit orientiert sich an den Prinzipien:*  *„Zweckbindung“ (Art. 5 Abs. 1 lit. b DSGVO)*  *„Transparenz, Rechtmäßigkeit und Verarbeitung nach Treu und Glauben“ (Art. 5 Abs. 1 lit. a DSGVO)*  *„Datenminimierung“ (Art. 5 Abs. 1 lit. c DSGVO)*  *„Richtigkeit“ (Art. 5 Abs. 1 lit. d DSGVO)*  *„Speicherbegrenzung“ (Art. 5 Abs. 1 lit. e DSGVO)*  *„Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f DSGVO)* |

|  |  |
| --- | --- |
| **Stellungnahme des Datenschutzbeauftragten (optional – nach Bedarf löschen)** | |
| Prüfung durch den Datenschutzbeauftragten | *Erfolgt/nicht erfolgt* |
| Offene Maßnahmen | *Sofern Handlungsbedarf besteht, Auflistung der offenen Maßnahmen.* |
| Datum der Dokumentation |  |

|  |  |
| --- | --- |
| **Prüfung durch die Geschäftsleitung (optional – nach Bedarf löschen)** | |
| Prüfung durch die Geschäftsleitung | *Erfolgt/nicht erfolgt* |
| Datum, Unterschrift |  |

Im Grunde sind ausschließlich die „Angaben zur Verarbeitungstätigkeit nach Maßgabe des Art. 30 Abs. 1 DSGVO“ gesetzliche Pflicht. Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, die optionalen Angaben zur Verarbeitungstätigkeit ebenfalls 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: Auf Anfrage der Aufsichtsbehörde müssen ggfs. weitere Nachweise vorgelegt werden.