Muster (Vorblatt) zum Verzeichnis von Verarbeitungstätigkeiten (VVT)

Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Vorblatt 1

**Angaben zum Verantwortlichen
(Art. 30 Abs. 1 lit. a DS-GVO)**

1. Verantwortlicher (= Unternehmen/Legaleinheit)

*[Name/ladungsfähige Anschrift]*

2. Gesetzlicher Vertreter (= Geschäftsführung)

*[Name/Kontaktdaten]*

3. Vertreter in der EU (gemäß Art. 27 DS-GVO)

*[Name/ladungsfähige Anschrift]*

4. Datenschutzbeauftragter

*[Name/Kontaktdaten]*

Vorblatt 2 (*optional*)

**Übergreifende Regelungen und Sachverhalte**

**5. Regelungen zur Datensicherheit**

*[Verweis auf übergreifende IT-Sicherheitskonzepte, die grds. für alle Verarbeitungstätigkeiten gelten.]*

6. Regelungen zur Datenlöschung

*[Verweis auf übergreifende Löschkonzepte, die grds. für alle Verarbeitungstätigkeiten gelten.]*

7. Sachverhalte zu Drittlandübermittlungen

*[Verweis auf übergreifende Drittlandübermittlungen, die grds. alle oder mehrere Verarbeitungstätigkeiten betreffen.]*

Erläuterungen

**1. Verantwortlicher**

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 DS-GVO).

[Angaben: Name/Firma, ladungsfähige Anschrift]

**2. Gesetzlicher Vertreter**

Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter

[Angaben: Namen der geschäftsführenden Personen]

Ggf. kann hier einfach ein Link auf das Web-Impressum eingetragen werden.

**3. Vertreter in der EU**

Bei Unternehmen ohne Niederlassung in der Europäischen Union ist hier der benannte Vertreter des Verantwortlichen (Art. 4 Nr. 17 DS-GVO, Art. 27 Abs. 1 DS-GVO) anzugeben.

**4. Datenschutzbeauftragter**

Vom Verantwortlichen bestellter Datenschutzbeauftragter *[Name, Kontaktdaten]*.

**5. Regelungen zur Datensicherheit**

Gegebenenfalls Verweise auf übergreifende Regelungen (falls solche existieren, die grds. alle Verarbeitungen betreffen) - Der Verweis an dieser Stelle auf übergreifende Regelungen 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 Informations-Sicherheits-Management-Systems (ISMS) nach ISO27001.

**6. Regelungen zur Datenlöschung**

Verweis auf Löschkonzepte, die grds. für alle Verarbeitungen gelten.

**7. Sachverhalte zu Drittlandübermittlungen**

Ein Verweis auf Drittlandübermittlungen ist hier sinnvoll, wenn alle oder die Mehrzahl der Verarbeitungen betroffen sind.

Muster (Hauptblatt) für ein VVT für Angaben zu den einzelnen Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten

**Hauptblatt Nr. \_\_\_\_\_**

**Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit**

**(Art. 30 Abs. 1 lit. b ff. DS-GVO)**

1. Bezeichnung der Verarbeitungstätigkeit

2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen (optionaler Inhalt)

3. Bei gemeinsamer Verantwortlichkeit:

*[Name und Kontaktdaten (ladungsfähige Anschrift) des/der weiteren Verantwortlichen]*

4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

|  |  |
| --- | --- |
| Betroffene Personengruppen | Kategorien personenbezogener Daten |

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)

*[interne, externe – auch im Konzern, eingebundene Dienstleister]*

7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Übermittlung □ Ja / □ Nein

*[Name des Drittlandes/der internationalen Organisation (DS-GVO)]*

*[Falls zutreffend, Angaben zu geeigneten Garantien bei Datenübermittlungen auf der Grundlage von Art. 49 Abs. 1 UAbs. 2 DS-GVO]*

8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
(Art. 30 Abs. 1 lit. f DS-GVO)

9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(TOM; Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

*[Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen*

*oder (soweit zutreffend): Link auf TOM (des Auftragsverarbeiters) hier anführen*

*oder (soweit zutreffend): Verweis auf Datenschutz-Zertifizierung etc.]*

Erläuterungen

**1. Bezeichnung der Verarbeitungstätigkeit**

Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden.

Empfehlung: Der Name der Verarbeitung sollte unabhängig von einzelnen IT-Tools sein, die ggfs. im Rahmen der Verarbeitung / des Prozesses zum Einsatz kommen.

Beispiele:

* Allgemeine Kundenverwaltung
* Customer-Relationship-Management (CRM)

**2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen**

Dies ist bezogen auf die Pflichtangaben des Art. 30 Abs. 1 DS-GVO eine optionale Angabe, um unternehmensintern die Zuordnung der dokumentierten Verarbeitungstätigkeit im VVT zu einem bestimmten Fachbereich und dessen erweiterter Dokumentation herstellen zu können.

Dies kann z.B. mittels der Funktionsbezeichnung des Fachbereiches, oder eines sonstigen Zuordnungskennzeichens (z.B. eine eindeutige Identifikationsnummer) erfolgen.

**3. Bei gemeinsamer Verantwortlichkeit**

Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten (ladungsfähige Anschrift) des oder der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 lit. a DS-GVO, Art. 26 Abs. 1 DS-GVO)

**4. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit**

Beispiele:

* Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“
* Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“

Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse (der EuGH spricht von „Vorgängen“) zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.

Die Detailtiefe hängt von der Geschäftstätigkeit des Unternehmens 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.

**5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)**

Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.

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, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder Ähnliches.

Beispiele:

* Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax- und E-Mail-Daten), Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung
* Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.

**6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DS-GVO)**

Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten - ggf. über Schnittstellen - erhalten, z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.

Laut Gesetz sind nur die Kategorien von Empfängern anzugeben. Bei genauerer Darstellung sind spätere Änderungen zu berücksichtigen und die regelmäßige Pflege der Angaben ist zu gewährleisten.

**7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)**

Drittländer sind solche außerhalb der EU/des EWR.

Beispiele für internationale Organisationen: Institutionen der UNO, der EU

Lediglich in Ausnahmefällen wird es erforderlich sein, Angaben zu geeigneten Garantien anzugeben, nämlich dann, wenn keine der genannten Garantien vorliegt, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO) .

D.h. falls es sich bspw. um ein Drittland mit Angemessenheitsbeschluss der EU-Kommission handelt, EU-Standarddatenschutzklauseln abgeschlossen wurden oder verbindliche interne Datenschutzvorschriften vorliegen, sind nähere Angaben zu den Garantien nicht erforderlich.

**8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)**

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 konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.

**9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)**

* Soweit für die Verarbeitung die Vorgaben des übergreifenden Sicherheitskonzepts (siehe Vorblatt 2 Nr. 5) Anwendung finden, kann hierauf verwiesen werden. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.
* Soweit sich die technischen und organisatorischen Maßnahmen aus anderen vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen, z.B. aus dem Sicherheitskonzept eines eingebundenen Auftragsverarbeiters, ergeben, ist ein konkreter Verweis hierauf ausreichend. Eventuelle Abweichungen sind zusätzlich zum Verweis zu dokumentieren.
* Soweit für die technischen und organisatorischen Maßnahmen keine der vorgenannten Dokumentationen vorliegen, sind sie hier im Einzelnen zu dokumentieren.
* Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe, um darüber aufzuzeigen, dass eine individuelle Betrachtung der Risiken erfolgt ist und angemessene Sicherheitsvorkehrungen ergriffen und dokumentiert wurden.

Anlage Muster zum VVT von
EU-Aufsichtsbehörden

Aufsichtsbehörde (Staat) mit Hinweisen und/oder Muster und entsprechendem Link

Deutschland

**DSK**

https://www.datenschutzkonferenz-online.de/media/kp/dsk\_kpnr\_1.pdf

https://www.datenschutzkonferenz-online.de/media/ah/201802\_ah\_verzeichnis\_
verarbeitungstaetigkeiten.pdf

**LDA Bayern**

https://www.lda.bayern.de/de/muster.html

https://www.lda.bayern.de/media/muster/muster\_5\_arztpraxis\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_11\_beherbergungsbetrieb\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_12\_einzelhaendler\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_2\_kfz-werkstatt\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_9\_online-shop\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_1\_verein\_verzeichnis.pdf

https://www.lda.bayern.de/media/muster/muster\_6\_weg-verwaltung\_verzeichnis.pdf

Belgien

https://www.autoriteprotectiondonnees.be/canevas-de-registre-des-activites-de-traitement

https://www.autoriteprotectiondonnees.be/node/20442

auch unter

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/canevas%20registre%20des%20activit%C3%A9s%20de%20traitement\_version19072017.xls

Dänemark

 https://www.datatilsynet.dk/media/6567/fortegnelse.pdf

Finnland

 https://tietosuoja.fi/en/record-of-processing-activities

https://tietosuoja.fi/en/controller-s-record-of-processing-activities

https://tietosuoja.fi/documents/6927448/8323207/Template+for+controllers+-+record+of+processing+activities.xlsx/696390cb-00ae-4780-884a-668d0f8dd655

Frankreich

https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

https://www.cnil.fr/sites/default/files/atoms/files/registre-traitement-simplifie.ods

Griechenland

https://www.dpa.gr/portal/page?\_pageid=33,211400&\_dad=portal&\_schema=PORTAL

http://www.dpa.gr/pls/portal/url/ITEM/6CDCE1FFFC42A14AE050A8C07C243BD0

Großbritannien

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/#how5

https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx

Italien

https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048327

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048348

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048395

Liechtenstein

 https://www.datenschutzstelle.li/index.php?cID=319

https://www.datenschutzstelle.li/download\_file/300/319

Luxemburg

 https://cnpd.public.lu/en/professionnels/obligations/registre.html

https://cst.cnpd.lu/portal/

Polen

 https://uodo.gov.pl/pl/file/708

Spanien

https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/actividades-tratamiento

https://www.aepd.es/es/prensa-y-comunicacion/blog/elaborar-el-registro-de-actividades-de-tratamiento

*\* “GDPR Compliance Support Tool“ mit der Möglichkeit, das VVT hier anzulegen*

Auf den Webseiten folgender Aufsichtsbehörden konnten keine Hinweise oder Muster zur Führung eines VVT gefunden werden:

* Bulgarien
* Estland
* Irland
* Österreich (allerding Verweis auf Bundesministerium für Digitalisierung und Wirtschaftsstandort: https://www.usp.gv.at/Portal.Node/usp/public/content/it\_und\_geistiges\_eigentum/datenschutz\_neu/datenverarbeitungsverzeichnis/313018.html

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.htm

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-MUSTER-Verarbeitungsverzeichnis-Verantwortlicher.docx

* Niederlande
* Schweden
* Schweiz

[Stand 17.01.2020; bei weiteren Aufsichtsbehörden der EU/des EWR wurde nicht gesucht]