Muster für eine Verarbeitungsmeldung

Die Verarbeitungsmeldung dient den Unternehmen dazu, die Verarbeitungen personenbezogener Daten mit den erforderlichen Angaben zur Erfüllung der Nachweispflichten i.S.d. Art. 5, 24 DS-GVO zu dokumentieren (s.a. 5. Anlage Muster für ein VVT). Darüber hinaus stellt sie ein wichtiges Werkzeug für die Beratung der Fachbereiche des Unternehmens im Hinblick auf ihre Datenschutzpflichten dar.

In der Praxis hat es sich bewährt, dass die Fachbereiche die Verarbeitungsmeldung - unter Nutzung der Erläuterungstexte - zunächst, soweit wie ihnen möglich ist, selbst ausfüllen und im zweiten Schritt eine Vervollständigung mit Unterstützung der Datenschutzorganisation erfolgt.

Verarbeitungsmeldung

Angaben für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO

**0. Verantwortliches Unternehmen:**

**1. Bezeichnung der Verarbeitungstätigkeit:**

**2. Verantwortlicher Fachbereich/sonstige Zuordnungskennzeichen:**

**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:**

*[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)**

Gemäß folgender Beschreibung (ggfs. unter Verweis auf ein Löschkonzept):

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

*[ggfs. hier die Maßnahmenbeschreibungen einfügen oder verlinken]*

☐ Bezug zum IT-Sicherheitskonzept, Abweichungen bzw. Ergänzungen:

☐ Gemäß folgender Zertifizierung:

☐ Gemäß Vereinbarung mit dem Dienstleister:

☐ Gemäß folgender Beschreibung:

Weitergehende Angaben zur Verarbeitung zur Erfüllung der Rechenschaftspflichten gem. Art. 5 (2) DS-GVO

**10. Datum und Art der Meldung**

Datum:

☐ Neumeldung ☐ Änderung ☐ Löschung

**11. (Geplanter) Beginn der Verarbeitung**

Datum:

**12. Wesentliche Prozessschritte**

**13. Ergänzende Dokumente und Unterlagen**

*(ggfs. Anlagen hier einbinden oder verlinken)*

**14. Verarbeitung von besonderen Kategorien personenbezogener Daten**

☐ Es werden besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) verarbeitet.

**15. Rechtsgrundlage der Verarbeitungstätigkeit**

☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1 b) DS-GVO.

☐ Berechtigtes Interesse des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 f) DS-GVO):

☐ Spezialgesetzliche Regelung außerhalb der DS-GVO:

☐ Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DS-GVO:

☐ Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses
(§ 26 BDSG-neu)

☐ Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag):

☐ Sonstiges:

**16. Weitere Angaben bei gemeinsamer Verantwortlichkeit gem. Art. 26 DS-GVO**

Auf welche Vorgänge bezieht sich die gemeinsame Verantwortlichkeit:

Liegt eine Vereinbarung der gemeinsam Verantwortlichen vor:

Liegen die diesbezüglichen wesentlichen Informationen der Betroffenen vor:

Erfüllung der Informationspflichten:

**17. Empfänger, denen die Daten offengelegt worden sind oder noch offengelegt werden**

Empfänger Empfänger-Kategorie EU/EWR/Drittland

an Empfänger innerhalb des Verantwortlichen

☐ EU/EWR

☐ Drittland:

an Empfänger (Dritte) außerhalb des Verantwortlichen

☐ EU/EWR

☐ Drittland:

**18. Eingebundene Dienstleister**

Dienstleister

Auftragsverarbeitung ☐ ja ☐nein

Orte der Datenverarbeitung

☐ EU/EWR:

☐ Drittland:

Ggfs. vertragliche Vereinbarungen

**19. Garantien im Falle von Datenübermittlungen in Drittländer oder internationale Organisationen (vgl. Pkt. 17 und 18)**

☐ Anerkannter Drittstaat

☐ EU-Standardvertrag Controller/Controller

☐ EU-Standardvertrag Controller/Processor

☐ Aufsichtsbehördlich genehmigter Vertrag

☐ BCR gem. Art. 47 DS-GVO

☐ Andere getroffene Garantien (Art. 49 Abs. 1. UAbs. 2 DS-GVO):

**20. Beteiligte IT-Systeme**

☐ DV-Anlagen:

☐ Software (und ggf. Unterprogramme):

☐ Schnittstellen:

☐ Sonstige Programme, Anwendungen und IT:

Alternativ ist auch der Verweis auf externe Dokumentation möglich (ggfs. Link hier einfügen):

Ggfs. Angaben zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten in Nicht-Produktivsystemen:

**21. Informationspflichten**

Wie werden die Informationspflichten erfüllt?

☐ Datenschutzinformation mittels (z.B. Information am (Arbeits-) Vertrag, am Formular, an der Einwilligung):

Bitte ggfs. Datenschutzinformation hier einfügen:

☐ Datenschutzerklärung der Webseite - bitte Link oder Ausdruck hier einfügen:

☐ Sonstiges:

Zu welchem Zeitpunkt erfolgt die Information?

**22. Durchführung der Verarbeitung für weitere Unternehmen als Dienstleistung**

Wird die Verarbeitung auch dienstleistend für weitere Unternehmen, z.B. als Shared Service im Konzern/in der Gruppe durchgeführt?

☐ Ja, auf Grundlage folgender vertraglicher Vereinbarungen:

☐ Nein

**23. Zugriffsberechtigungen**

Wie sind die Zugriffsberechtigungen geregelt?

Bitte beschreiben Sie die Personengruppen und Berechtigungsrollen mit Umfang und Art des Datenzugriffs, sowie den Prozess zur Erlangung und Verwaltung der Berechtigungen (alternativ Verweis auf ein eingebettetes oder verlinktes Berechtigungskonzept):

**24. Umfang der Verarbeitung**

Angaben zum Umfang der Verarbeitung:

Ungefähre Anzahl der Betroffenen/Datensätze, sowie Anzahl Datenfelder pro Betroffenen/Datensatz:

**25. Risiko der Verarbeitung und Datenschutz-Folgenabschätzung**

* Wurde eine Bewertung der Datenschutz-Risiken durchgeführt (unter Berücksichtigung der Blacklists der Datenschutz-Aufsichtsbehörden - „Schwellenwert-Analyse“)?

☐ Ja, mit folgendem Ergebnis:

☐ Nein

* Falls im Rahmen der „Schwellenwert-Analyse“ ein „Hohes Risiko“ ermittelt wurde, bitte die erforderliche Dokumentation der Risiken und der ergriffenen Schutzmaßnahmen in Form einer Datenschutz-Folgenabschätzung hier einbetten:

**26. Wahrung der (weiteren) Betroffenenrechte**

Die weiteren Betroffenenrechte (Recht auf Auskunft, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit sowie im Zusammenhang mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling) werden wie folgt sichergestellt:

**27. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

Wie wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sichergestellt?

Hier bitte Beschreibungen oder ausgefüllte Checklisten einbetten:

Erläuterungen

Angaben für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DS-GVO

0. Verantwortliches Unternehmen

Benennung des für die Datenverarbeitung verantwortlichen Unternehmens.

Diese Angabe in der Verarbeitungsmeldung ist vornehmlich im Konzern bzw. in Unternehmensgruppen relevant, um sicherzustellen, dass die Verarbeitungsmeldungen der unterschiedlichen Unternehmen dem richtigen Verzeichnis zugeordnet werden müssen.

Die Angabe kann bei Einzelunternehmen, bei denen die Zuordnung der Verantwortlichkeit eindeutig ist, entfallen.

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

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), Geburtsdatum, 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.

Die Angaben können als Kategorien aus den detaillierteren Angaben unter Pkt. 17/18 übernommen werden.

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

Es sind hier Datenübermittlungen in Drittländer oder an internationale Organisationen anzugeben.

Drittländer sind solche außerhalb der EU/des EWR.

Beispiele für internationale Organisationen: Institutionen der UNO, der EU.

Es ist die Angabe des betreffenden Drittlandes erforderlich.

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) . Falls es sich bspw. um ein Drittland mit Angemessenheitsbeschluss der EU-Kommission handelt, EU-Standarddatenschutzklauseln abgeschlossen wurden, die Datenübermittlung unter dem Schirm des EU-US Privacy Shield erfolgt oder verbindliche interne Datenschutzvorträge vorliegen, sind nähere Angaben zu den Garantien nicht erforderlich.

Detailliertere Angaben zu internen Nachweiszwecken erfolgen unter Pkt. 19.

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. Falls für einzelne Verarbeitungsschritte, unterschiedliche Fristen gelten, ist dies jeweils zu dokumentieren.

Soweit die Fristen in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf dieses 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.

Weitergehende Angaben zur Verarbeitung zur Erfüllung der Rechenschaftspflichten gem. Art. 5 (2) DS-GVO.

10. Datum und Art der Meldung

Es ist das Datum anzugeben, an dem die Verarbeitungsmeldung ausgefüllt wurde.

Es ist darüber hinaus anzugeben, ob es sich um die Meldung einer neuen Verarbeitung handelt, oder um die Änderung oder Löschung einer bestehenden Verarbeitung.

11. Geplanter Beginn der Verarbeitung von personenbezogenen Daten oder tatsächlicher Beginn

Dabei ist schon die erstmalige Übertragung oder Speicherung von personenbezogenen Daten relevant.

12. Wesentliche Prozessschritte

Hiermit ist eine Übersicht über die einzelnen Verarbeitungsschritte gemeint, z.B. in chronologischer Form. Es kann auch auf Datenflussdiagramme o.ä. verwiesen werden (siehe Pkt. 13).

Beispiele:

* Erstellung von werblichen Briefen an Kunden durch Vertrieb
* Auswahl Kunden und Anschriften
* Weiterleitung Kundenanschriften an Dienstleister (Auftragsverarbeitung)
* Druck und Versand incl. Werbematerial durch Dienstleister
* Löschen der Kundendaten beim Dienstleister

13. Ergänzende Dokumente und Unterlagen

Hier sollten ggfs. relevante Datenflusspläne, Handbücher, Lasten-, Pflichtenhefte, Produktbeschreibungen, Internet-Adressen zu Produkten, Angaben zu Datenquellen und Schnittstellen etc. beigefügt oder verlinkt werden.

14. Verarbeitung von besonderen Kategorien personenbezogener Daten

Hier sollte noch einmal gesondert dargestellt werden, ob in der Verarbeitungstätigkeit besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO) oder Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) verarbeitet werden.

15. Rechtsgrundlage der Verarbeitungstätigkeit

Bei Unklarheiten sollte dieser Punkt in Abstimmung mit dem Datenschutzbeauftragten oder anderen Mitarbeitern der Datenschutzorganisation gemeinsam ausgefüllt werden.

Insbesondere wichtig ist jedoch die Information seitens des Fachbereiches, ob es spezialgesetzliche Regelungen gibt, in denen die Verarbeitung personenbezogener Daten geregelt wird.

Die zutreffende Rechtsgrundlage sollte angekreuzt und erläutert werden. Es können innerhalb einer Verarbeitungsmeldung auch mehrere Rechtsgrundlagen für unterschiedliche Daten oder Verarbeitungsschritte zutreffen.

* Spezialgesetzliche Regelung außerhalb der DS-GVO: Benennung von Vorschrift, Paragraph, Absatz, Satz.
* Einwilligung des Betroffenen (Art. 6 Abs. 1a DS-GVO): Erläuterung der Einwilligungsklausel und des Einwilligungsmechanismus
* Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag): Benennung der Vereinbarung, Paragraph, ggfs. Absatz
* Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses
* Vertrag oder Vertragsanbahnung mit dem Betroffenen (Art. 6 Abs. 1b DS-GVO)
* Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1f DS-GVO): Benennung der berechtigten Interessen.
* Sonstiges (bspw. Art. 6 Abs. 1d und e DS-GVO)

16. Weitere Angaben bei gemeinsamer Verantwortlichkeit gem. Art. 26 DS-GVO

Falls eine gemeinsame Verantwortlichkeit vorliegt, sollten hier weitere Angaben gemacht werden.

So ist darzulegen, auf welche Vorgänge innerhalb der Verarbeitungstätigkeit sich die gemeinsame Verantwortlichkeit bezieht. Darüber hinaus sollten die Verträge zur gemeinsamen Verantwortlichkeit hier einsehbar/abrufbar sein, und es sollten Angaben zur Erfüllung der Informationspflichten, sowie weiterer relevanter Aspekte im Einzelfall (z.B. zur Erfüllung der Betroffenenrechte) gemacht werden.

17. Empfänger, denen die Daten offengelegt worden sind oder noch offengelegt werden

Es sind getrennt alle Stellen im Unternehmen und außerhalb des Unternehmens anzugeben, die regelmäßig (= organisatorisch vorgesehen) personenbezogene Daten erhalten. Ob es sich um schriftliche oder IT-technische Datenweitergabe handelt, ist nicht entscheidend.

Es werden hier folgende Empfänger unterschieden:

* Empfänger innerhalb des Verantwortlichen: z.B. Abteilungen innerhalb des Unternehmens, die Daten im Rahmen der Verarbeitung erhalten.
* Z.B. an die Tax-Abteilung, Personalabteilung etc.
* Empfänger (Dritte) außerhalb des Verantwortlichen: Empfänger, die nicht zum Verantwortlichen gehören (andere Konzerngesellschaften, Gesellschaften außerhalb des Konzerns, Kooperationspartner, Geschäftspartner) und denen regelmäßig personenbezogene Daten im Rahmen der Verarbeitung übermittelt werden.

Die hier dokumentierten Empfänger werden dabei jeweils einer Kategorie zugeordnet. Diese Kategorien sind in einer Liste unter Pkt. 6 aufzuführen und stellen darüber hinaus eine relevante Angabe für die Datenschutzinformation dar.

Mittels Auftragsverarbeitung beauftragte Dienstleister, die Daten im Rahmen der Verarbeitung erhalten (z.B. Callcenter, Druckdienstleister) sind unter Pkt. 18 aufzuführen.

18. Eingebundene Dienstleister

Werden Dienstleister beauftragt, für den Verantwortlichen Leistungen ausführen, die mit der Verarbeitung von personenbezogenen Daten einhergehen, dann sind diese hier zu benennen.

Es ist jeweils anzugeben, ob es sich um eine Auftragsverarbeitung gem. Art. 28 DS-GVO handelt, und ggfs. die entsprechenden vertraglichen Vereinbarungen beizufügen oder zu verlinken.

19. Garantien im Falle von Datenübermittlungen in Drittländer oder internationale Organisationen (vgl. Nr. 7, Nr. 17, Nr. 18)

Im Falle von Datenweitergaben außerhalb von EU/EWR sind geeignete Garantien beim Empfänger grundsätzlich erforderlich und hier anzugeben, falls für das betreffende Land kein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DS-GVO vorliegt. Solche Garantien können gem. Art. 46 DS-GVO durch verbindliche interne Datenschutzvorschriften (BCR) oder EU-Standarddatenschutzklauseln erbracht werden.

Darüber hinaus müssen hier - falls die Datenübermittlungen nicht auf anderem Wege (wie in Art. 45-47 DS-GVO beschrieben) abgesichert sind - geeignete Garantien bei Datenübermittlungen auf der Grundlage von Art. 49 Abs. 1 UAbs. 2 DS-GVO angegeben werden.

20. Beteiligte IT-Systeme

An dieser Stelle sollte eine knappe Beschreibung der technischen Infrastruktur angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen zu ermöglichen.

Darüber hinaus kann die Beschreibung zur Identifikation von Dienstleistern mit Auftragsverarbeitungs-Relevanz dienen (vgl. Pkt. 18).

Falls personenbezogene Daten auch in Nicht-Produktivsystemen verarbeitet werden, sollten hier entsprechende Angaben zur Rechtmäßigkeit sowie zu Schutzmaßnahmen gemacht werden.

21. Wie und zu welchem Zeitpunkt werden die Informationspflichten erfüllt?

Hier ist zu dokumentieren, wie die Informationspflichten nach Art. 12-14 DS-GVO erfüllt werden.

22. Wird die Verarbeitung auch dienstleistend für weitere Unternehmen durchgeführt?

Wenn diese Verarbeitung (auch) dienstleistend für andere Auftraggeber-Gesellschaften in Form einer Auftragsverarbeitung durchgeführt wird, dann ist dies mittels eines Vertrages zur Auftragsverarbeitung (in der Rolle des Dienstleisters) abzusichern und im sog. „Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters“ (VVT-AV, vgl. Praxishilfe Vb der GDD) des Unternehmens zu dokumentieren.

23. Wie sind die Zugriffsberechtigungen geregelt?

Diese Dokumentation dient als Nachweis, dass die Vertraulichkeit der Daten gewährleistet ist, indem Berechtigungen nur im erforderlichen Umfang vergeben werden, und die vergebenen Berechtigungen stets richtig und aktuell sind.

Es sind alle Personengruppen anzugeben, die eine Berechtigung haben, die Daten zu lesen oder zu verändern (Rollen-, Berechtigungskonzept), sowie der Prozess zur Erlangung und Verwaltung der Berechtigungen.

24. Angaben zum Umfang der Verarbeitung

Die DS-GVO fordert an mehreren Stellen die Berücksichtigung des Umfanges der Verarbeitung (bspw. hinsichtlich der Bewertung der Angemessenheit der Sicherheitsmaßnahmen, oder der Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung).

Rechtsverbindliche Angaben zu Schwellenwerten für einen „großen Umfang der Verarbeitung“ liegen bislang allerdings nicht vor.

25. Risiko der Verarbeitung und Datenschutz-Folgenabschätzung

Das von der DS-GVO geforderte „risikoorientierte“ Vorgehen setzt voraus, dass eine Transparenz über das Risiko der einzelnen Verarbeitungen im Unternehmen vorliegt. Daher ist es geboten, jede Verarbeitung hinsichtlich des Datenschutz-Risikos zu bewerten, und - im Falle des Vorliegens eines hohen Risikos - ggfs. eine Datenschutz-Folgenabschätzung durchzuführen.

Siehe hierzu auch: GDD-Praxishilfe DS-GVO X - Voraussetzungen der Datenschutz-Folgenabschätzung.

26. Wahrung der (weiteren) Betroffenenrechte

Hier sollten ggfs. relevante Angaben gemacht werden, wie die Wahrnehmung der unterschiedlichen weiteren Betroffenenrechte (Recht auf Auskunft, Berichtigung, Einschränkung, Widerspruch, Datenübertragbarkeit sowie im Zusammenhang mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling) ermöglicht wird.

27. Wie wird der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sichergestellt?

Hier sollten entsprechende Beschreibungen oder auch selbst erarbeitete Checklisten eingebettet werden, um den Nachweis zu erbringen, dass die Verarbeitung in Einklang mit Art. 25 DS-GVO erfolgt.