Ausfüllhinweise zum Dokument: Angaben für den Eintrag in das Verzeichnis der Verarbeitungstätigkeiten (Teil A)

(02_Verarbeitungsverzeichnis.docx)

Dieses Dokument gibt Ihnen Hinweise und teilweise Beispiele dazu, welche Informationen in die Formularfelder der im Titel genannten Vorlage gehören. In diesem Dokument werden keine Verweise auf die gesetzlichen Grundlagen gegeben und keine Gesetzestexte kommentiert oder ausgelegt. Diese Ausfüllhinweise stellen einzig eine **Arbeitshilfe** dar.

Bitte beachten Sie:

- Bei dieser Vorlage handelt es sich um ein Word- bzw. ein OpenOffice-Formular. Wenn Sie es in einem anderen Format speichern, können Sie die Formularfunktionalität ggf. nicht mehr verwenden.
- Die Felder, die ausgefüllt werden müssen, sind grau hinterlegt.
- Insbesondere in Tabellen ist nur die erste Zeile mit Formularfeldern versehen. Benötigen Sie mehrere Zeilen, dann arbeiten Sie in der „normalen“ Tabelle weiter. Standardmäßig sind zwei Zeilen pro Tabelle vorgesehen. Ergänzen Sie fehlende Zeilen, wenn Sie mehrere benötigen. Zur besseren Lesbarkeit des Dokuments sollten Sie nicht benötigte Zeilen in Tabellen löschen.

zu (1) Bezeichnung der Verarbeitungstätigkeit

Der Begriff „Verarbeitung“ bezeichnet gemäß Art. 4 DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Die reine Nennung programmname …

Die DSK definiert eine Verarbeitungstätigkeit folgendermaßen: „Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt.“ [1]

Benennen (Name, Bezeichnung) Sie daher die Verfahrenstätigkeit so, dass anhand der Bezeichnung auf den Zweck geschlossen werden kann, beispielsweise

- *„Personalaktenführung/Stammdaten*
- *Lohn-, Gehalts- und Bezügeabrechnung*
- *Arbeitszeiterfassung*
- *Urlaubsdatei*
- *Nutzungsprotokollierungen IT/Internet/E-Mail*
- *Bewerbungsverfahren*
- *Telefondatenerfassung*
- *Firmenparkplatzverwaltung*
- *Videoüberwachung an Arbeitsplätzen, in Schulen etc.*
- *Schülerverwaltung, Unterrichtsplanung , Zeugniserstellung*
- *Beschaffung/Einkauf sowie Finanzbuchhaltung*

- *Antragsbearbeitung (Bauanträge, Wohngeldanträge etc.)*
- *Rats- und Bürgerinformationssysteme*
- *Meldewesen (Melderegister)*
- *Fahrerlaubnisregister und Fahrzeugregister*
- *Wahlen (Wählerverzeichnis)*
- *amtsärztliche Untersuchungen“* [1]

Als Verarbeitungstätigkeit wird im Allgemeinen ein Geschäftsprozess auf geeignetem Abstraktionsniveau verstanden. Es ist ein strenger Maßstab anzulegen, so dass jeder neue Zweck der Verarbeitung eine eigene Verarbeitungstätigkeit darstellt.

Beschreiben Sie die Verarbeitungstätigkeit in

zu (2) Zweck der Verarbeitung

„Für jede Verarbeitung sind vorher die Zwecke festzulegen.

Die Zwecke müssen eindeutig und transparent sein, damit die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung prüfen kann.“ [1]

Beschreiben Sie die Zwecke der Verfahrenstätigkeit detailliert. Das ist besonders wichtig, wenn mit dem Fachverfahren mehrere Aufgaben im Zusammenhang mit einer Verarbeitungstätigkeit durchgeführt werden können.

Beispiele:

Für die Verarbeitungstätigkeit „*Meldewesen*“ könnten z. B. die Zwecke

- *Bürgerservice (Auskunfts- und Änderungsdienst, Bearbeitung von Vorgängen zum Steuerkennzeichen, Bearbeitung des Pass- und Personalausweis-Registers usw.)*
- *Einarbeitung von XMeld-, XPersonenstand und XAusländer-Nachrichten*
- *Datenauswertungen (Listen, Statistiken)*
- *Datenübermittlungen, Führungszeugnisanträge*
- *Massendatenverarbeitung bei Wahlen und Abstimmungen*
- *Archivierung*
- *Controlling*

definiert werden.

Für die Verarbeitungstätigkeit „*Finanz- und Haushaltswesen*“ könnten z. B. die Zwecke

- *Haushaltsplanung*
- *Haushaltsbewirtschaftung*
- *Auftragsverwaltung*
- *Buchführung*
- *Zahlungsabwicklung*
- *Jahresabschluss*

definiert werden.

Wenn für Ihre Verarbeitungstätigkeit die Konstellation „***gemeinsam Verantwortliche“*** (bitte im Art. 26 DSGVO nachlesen) zutrifft, dann wählen Sie das Ja-Optionsfeld und beschreiben im darunter liegenden Textfeld detailliert, welche Verantwortlichen für welche Verpflichtungen zuständig sind.

Hier können Sie auch auf externe Dokumente verweisen, z. B. auf eine schriftliche Vereinbarung zwischen den *Gemeinsam Verantwortlichen*.

zu (3) Rechtmäßigkeit der Verarbeitung

Wählen Sie eine der aufgeführten Bedingungen auf und konkretisieren Sie diese im Textfeld unterhalb der Optionen, um die Rechtmäßigkeit der Verarbeitung zu dokumentieren. Bei Nennung von gesetzlichen Grundlagen reicht hier eine reine Nennung des Gesetzes nicht aus, sondern präzisieren Sie Ihre Angabe (eine betroffene Person sollte sich anhand Ihrer Angabe über die Rechtmäßigkeit informieren können).

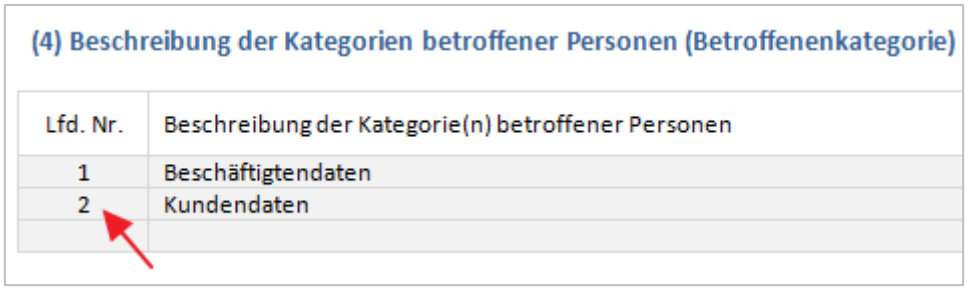
Im Textfeld können auch ergänzende Angaben oder weitere Erläuterungen zur Rechtmäßigkeit (beispielsweise zur Einwilligung oder zu einem Vertrag) vermerkt werden.

zu (4) Beschreibung der Kategorien betroffener Personen (Betroffenenkategorien)

Benennen Sie die Kategorien der betroffenen Personen, von denen Sie personenbezogene Daten verarbeiten, z. B.

- *„Kategorie Beschäftigte*
- *Kategorie Kundendaten*
- *Kategorie Abgeordnetendaten*
- *usw.“* [1]

Vergeben Sie für die unterschiedlichen Betroffenenkategorien laufende Nummern, so können Sie später bei den verarbeiteten Daten (Datenkategorien) auf die entsprechenden Betroffenenkategorien verweisen.



(4) Beschreibung der Kategorien betroffener Personen (Betroffenenkategorie)

Lfd. Nr.	Beschreibung der Kategorie(n) betroffener Personen
1	Beschäftigtendaten
2	Kundendaten

zu (5) Beschreibung der Kategorien der zu verarbeitenden Daten (Datenkategorien)

Benennen Sie die Kategorien der Daten, die Sie verarbeiten.

„Aufgegliedert z. B. in der Darstellung der „Kategorie Beschäftigte“ in die Daten-Kategorien:

- *Mitarbeiter-Stammdaten*
  (mit Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen etc.)
- *Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten etc.*
- *Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc.*
- *Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten etc.*
- *Betriebsarztuntersuchungen mit Adressdaten, Gesundheitsdaten etc.*
- *Stundenplan als Einsatzplan für Lehrkräfte*
- *Videoüberwachung an Arbeitsplätzen etc.*

Aufgegliedert z. B. in der Darstellung der „Kategorie Kundendaten“ in die Kategorien:

- *Kunden-Kontaktdaten mit Adressdaten, Ansprechpartnern etc.*
- *Kundengruppe/-interesse*
- *Umsatzdaten bisher*
- *Bonitätsdaten*
- *Zahlungsdaten usw.*
- *für Schulen: Fehlzeiten, Schulleistungsnachweise*

Aufgegliedert z. B. in der Darstellung „Kategorie Abgeordnetendaten“ in die Kategorien:

- *Namen und Kontaktdaten (Adresse, Telefon, E-Mail) von Abgeordneten*
- *Fraktionszugehörigkeit*“ [1]

Vergeben Sie für die unterschiedlichen Datenkategorien laufende Nummern, so können Sie später bei den Datenübermittlungen und den Speicherfristen auf die entsprechenden Datenkategorien verweisen.

(5) Beschreibung der Kategorien der zu verarbeitenden Daten (Datenkategorie)

Lfd. Nr.	Betroffenen-kategorie (aus (4))	Beschreibung der Kategorie(n) der zu verarbeitenden Daten	Daten nach Art. 9 DSGVO	
			ja (x)	nein (x)
1	1	Name		x
2	1	Anschrift		x
3	1	Geburtsdaten		x
4	1	Kontoverbindung		x
5	2	Name, Anschrift		x
6	2	Ansprechpartner		x
7	2	Umsatzdaten		x

Verweis auf die Kategorien betroffener Personen (aus (4))

Laufende Nummer vergeben

Am Ende der Zeile können Sie die Sensibilität der Daten kennzeichnen: Daten nach Art. 9 DSGVO (personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind) – markieren Sie die Spalte „ja“ oder „nein“.

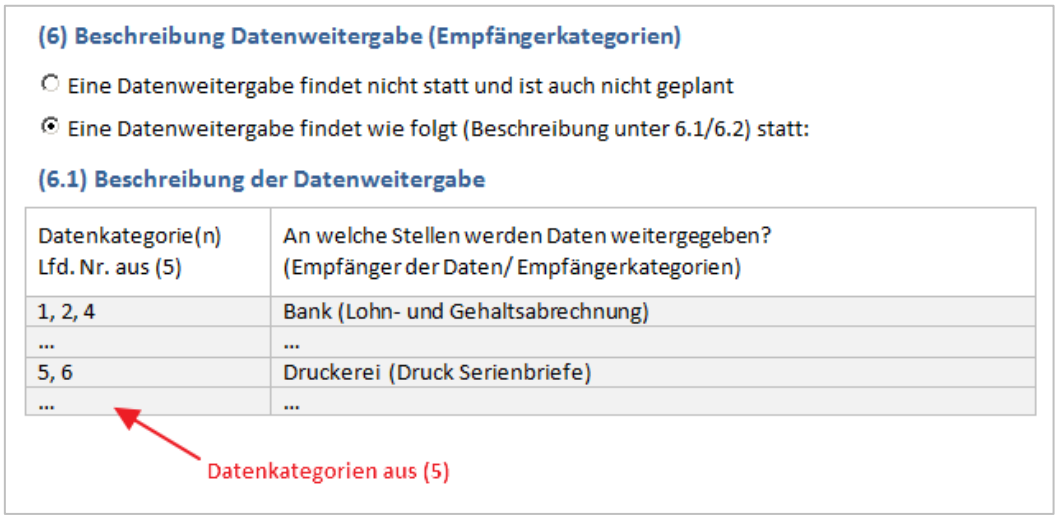
zu (6) – Datenweitergabe

Bei den Datenübermittlungen werden die Kategorien der Empfänger genannt, denen Daten offengelegt werden. Als Empfänger wird eine Person oder eine Organisation bezeichnet, kann aber auch ein anderes Fachverfahren oder einen anderen Prozess betreffen, sofern Daten dorthin weitergegeben werden. Weiterhin können Daten auch in Drittländer übermittelt werden.

Wenn Sie Daten übermitteln, dann beschreiben Sie in diesen Feldern die übertragenen Daten und die Empfänger der Daten. Konkretisieren Sie die übertragenen Daten, indem Sie auf die laufende Nummer der Datenkategorie verweisen.

„Aufgegliedert z. B.: für die Lohn- und Gehaltsabrechnung:

- *Banken*
- *Sozialversicherungsträger*
- *Finanzämter*
- *unternehmensinterne andere Datenempfänger (z.B. Betriebsrat, Fachvorgesetzte)*
- *ggf. Gläubiger bei Lohn-/Gehaltspfändungen*
- *ggf. Träger der Betriebsrente*
- *ggf. Auftragsverarbeiter*
- *ggf. Muttergesellschaft“* [1]



(6) Beschreibung Datenweitergabe (Empfängerkategorien)

○ Eine Datenweitergabe findet nicht statt und ist auch nicht geplant

◉ Eine Datenweitergabe findet wie folgt (Beschreibung unter 6.1/6.2) statt:

(6.1) Beschreibung der Datenweitergabe

Datenkategorie(n) Lfd. Nr. aus (5)	An welche Stellen werden Daten weitergegeben? (Empfänger der Daten/ Empfängerkategorien)
1, 2, 4	Bank (Lohn- und Gehaltsabrechnung)
...	...
5, 6	Druckerei (Druck Serienbriefe)
...	...

Datenkategorien aus (5)

„Angabe der Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern.

Empfänger können auch Teile eines Unternehmens oder einer Behörde sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist (z. B. ein Zugriff auf Unternehmens- oder Kundendaten bei bundesweit tätigen Banken oder abgebende und aufnehmende Schule bei gleichem Schulträger).

Der Begriff „Datenempfänger“ ist daher zu ergänzen durch „Zugriffsberechtigte“. Die Zugriffsberechtigten sollten, wie bisher, ohne namentliche Angabe angegeben werden. Sie müssen jedoch z. B. über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein. Es kann aber, z. B. beim o. g. filialseitigen Zugriff auf die Daten, sinnvoll sein, die Angabe einer Zahl der Zugriffsstellen bzw. Zugriffsberechtigten mit Bezug zum aktuellen Stand (Tagesdatum) anzugeben.

Zu „Drittländern“ sollte in jedem Fall eine Aussage getroffen werden, also auch angegeben wer-den, wenn eine Übermittlung in Drittländer nicht stattfindet und auch nicht geplant ist.

Eine Übermittlung in Drittländer erfolgt auch, wenn sich dort der Server befindet oder der Mail-versand hierüber abgewickelt wird. Ebenso kann eine Übermittlung in Drittländer vorliegen, wenn Supportdienstleistungen aus diesem erbracht werden.

„Offenlegung“ bedeutet, dass sowohl die Empfänger in der Vergangenheit, als auch jene in der Zukunft zu benennen sind.

Angaben zu gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien Empfänger in Drittländern und internationale Organisationen sind keine Kategorien und daher konkret zu benennen.

Art. 49 Abs. 6 DS-GVO ist zu beachten, wonach der Verantwortliche die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Art. 49 Abs. 1 Unterabsatz 2 im Verzeichnis der Verarbeitungstätigkeiten aufnimmt." [1]

zu (7) – Löschfristen

Tragen Sie in diesen Feldern die Löschfristen für die entsprechenden Datenkategorien ein. Entweder haben Sie gesetzlich festgelegte Löschfristen oder Sie legen die Aufbewahrungszeit der gespeicherten Daten selbst fest (Kontrollkästchen). Mit Hilfe der laufenden Nummer der Datenkategorie können Sie eine präzise Zuordnung der konkreten Löschfristen zu den entsprechenden Datenkategorien vornehmen.

„Angabe der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, z. B.

- *die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten, Kundendaten etc.*
- *geltende Aufbewahrungs- und Löschfristen für Schülerdaten, Prüfungsunterlagen etc.*
- *gesetzlich vorgesehene Löschungsfristen (z.B. § 14 Bundesmeldegesetz)*
- *vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen*

Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, vielmehr sind präzise Angaben erforderlich." [1]

zu (8) – Beschreibung der technischen und organisatorischen Maßnahmen

Es ist nicht das Ziel, an dieser Stelle die technischen und organisatorischen Maßnahmen der gesamten Organisation zu beschreiben (und damit Redundanzen in der Dokumentation zu erzeugen). Vielmehr sollten die technischen und organisatorischen Maßnahmen in einer zentralen Dokumentationsstruktur beschrieben werden, auf die an dieser Stelle referenziert werden kann.

Tragen Sie in diesem Feld nur technische und organisatorische Maßnahmen (TOMs) ein, die von Ihrer Gesamtkonzeption der TOMs abweichen und/oder speziell für diese Verarbeitungstätigkeit gelten.

Bei der Planung und Beschreibung der TOMs können Sie sich u. a. orientieren an

- den Grundsätzen für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO)
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit

- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

- den Gewährleistungszielen des Datenschutzes im Standard-Datenschutzmodell:
  - Verfügbarkeit (es ist sichergestellt, dass Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können)
  - Integrität (es ist sichergestellt, dass Daten unversehrt, vollständig, zurechenbar und aktuell bleiben)
  - Vertraulichkeit (es ist sichergestellt, dass nur befugt auf Verfahren und Daten zugegriffen werden kann)
  - Nicht-Verkettung (es ist sichergestellt, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können)
  - Transparenz (es ist sichergestellt, dass die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann)
  - Intervenierbarkeit (es ist sichergestellt, dass das Verfahren so gestaltet ist, dass es den Betroffenen die Ausübung der ihnen zustehenden Rechte wirksam ermöglichen)
- nationalen und internationalen Standards zur Informationssicherheit (z. B. IT-Grundschutz des BSI oder ISO 2700x).

Mit Hilfe z. B. der IT-Grundschutz-Standards können Sie auch überprüfen, ob die Maßnahmen, die Sie einsetzen wollen, auch dem Stand der Technik entsprechen. Möchten Sie beispielsweise ein Verschlüsselungsverfahren bei Ihrer Verarbeitungstätigkeit einsetzen, so gibt beispielsweise

- der Baustein M2.164 (Auswahl eines geeigneten kryptographischen Verfahrens) einen Überblick über Verschlüsselungsverfahren nach dem Stand der Technik,
- der Baustein M 2.46 (Geeignetes Schlüsselmanagement) einen Überblick über eine Verwendung kryptographischer Sicherheitsmechanismen (z. B. Verschlüsselung, digitale Signatur) nach dem Stand der Technik
- usw.

Verweise

[1] Auszug aus dem Dokument „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten“ der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK)

[2] AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele V.1.0 – Erprobungsfassung, 2016