Ausfüllhinweise zum Dokument: Ergänzende Angaben für die Verarbeitungsdokumentation zur Rechenschaftspflicht (Teil B)

(03_Verarbeitungsdokumentation.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 Gesetzestexte kommentiert oder ausgelegt. Diese Ausfüllhinweise stellen einzig eine **Arbeitshilfe** dar.

Bitte beachten Sie:

- Bei dieser Vorlage handelt es sich um ein Word-Formular. Wenn Sie es in einem anderen Format speichern, können Sie die Formularfunktionalität nicht mehr verwenden.
- Die Optionsfelder in diesem Formular sind Active-X-Komponenten. Wenn Sie in Ihrer Wordinstallation Active-X deaktiviert haben, können Sie die Optionsfelder nicht 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.
- Die meisten Formularfelder sind mit kurzen Inhaltshinweisen versehen. Wenn Sie in das Formularfeld klicken und beginnen, Text einzugeben, wird dieser Text gelöscht. Zur besseren Lesbarkeit des Dokuments sollten Sie in Textfelder, die Sie nicht benötigen, ein Leerzeichen hineinschreiben.

zu (1) Aufgabenverteilung der zuständigen Personen (Datenschutzmanagement)

Mit der Festlegung, welche Personen bei der Verarbeitung von personenbezogenen Daten für welche Aufgaben zuständig sind (Datenschutzmanagement), können Sie im Zusammenhang mit der Rechenschaftspflicht **Transparenz** schaffen.

Beschreiben Sie in den einzelnen Aufgabenverteilungs-Tabellen die Aufgaben der Personen, die eine fachliche oder technische Zuständigkeit bei dieser Verarbeitungstätigkeit übernehmen.

Wichtig: Hier sollen nicht die Berechtigung der einzelnen Benutzer aufgeführt werden, diese werden später in diesem Dokument dokumentiert. Hier werden nur die fachlichen und technischen Managementaufgaben beschrieben,

z. B. technische Managementaufgaben

- *Systemwartung und -betrieb*
- *Überwachung der Verfügbarkeit und Integrität des verwendeten Serversystems*
- *Umsetzung und Kontrolle der technisch-organisatorischen Prozesse*
- *Verwaltung von Benutzer- und Gruppenkonten*

oder fachliche Managementaufgaben

- *Autorisierung von Benutzerberechtigung*

- *Führen der Verarbeitungsdokumentation*
- *Abnahme der Verarbeitungsdokumentation*
- *Turnusmäßige Überprüfung der Angaben nach Artikel 30 DSGVO für das Verzeichnis der Verarbeitungstätigkeiten*
- *Beantwortung von Auskunftsanfragen nach Artikel 15 DSGVO*
- *Erstellung von Datenschutzmanagementprozessen zur Gewährleistung der Betroffenenrechte*

Wenn Sie eine automatisierte Verarbeitungstätigkeit dokumentieren, sollten Sie hier zumindest Beschreibungen von drei Aufgabenbereichen aufnehmen (siehe die Beispiele weiter unten). Die Aufgaben der Personen, die

- *fachlich zuständig sind,*
- *technisch zuständig sind und*
- *die Datenschutzmanagementaufgaben übernehmen.*

Wenn Sie zusätzlich Personen berücksichtigen, die zusätzliche Aufgaben übernehmen bzw. Vertretungsregelungen übernehmen, können Sie hier auch deutlich mehr Aufgabenverteilungs-Tabellen verwenden.

Die vorhandenen acht Aufgabenverteilungs-Tabellen können Sie durch Copy&Paste beliebig erweitern bzw. zu viele vorhandene Tabellen löschen.

Beispiel:

Zuständige Person	Bereich		Aufgabenbeschreibung
FB-1_01	☒	fachlich	• Fachliche Zuständigkeit • Freigabe der Verarbeitungsdokumentation • Freigabe von Test- und Freigabeverfahren • Autorisierung von Benutzerkonten und Benutzerberechtigungen • usw.
	☐	technisch	
	☐	Vertretung	
FB-3_05	☐	fachlich	• Systemwartung und Betrieb • Sicherstellung der Verfügbarkeit und der Integrität der verwendeten Systeme • Verwaltung der Gruppen- und Benutzerkonten • usw.
	☒	technisch	
	☐	Vertretung	
DSB	☒	fachlich	• Mitarbeit bei der Erstellung der Datenschutzmanagementprozessen • Beantwortung von Auskunftsanfragen nach Artikel 15 DSGVO • Regelmäßige Überprüfung der Benutzerberechtigungen
	☒	technisch	
	☐	Vertretung	

Sie müssen in dieser Dokumentation nicht unbedingt mit Vor- und Nachnamen von Mitarbeitern arbeiten, sondern können auch z. B. Personalkennungen verwenden. So haben Sie keine Zuordnung von Personen zu Aufgaben, sondern von Stellen zu Aufgaben. Die dahinterstehenden Personen können anhand des Stellenplans identifiziert werden.

zu (2) Beurteilung zur Notwendigkeit einer Datenschutz-Folgenabschätzung

Mit der Beurteilung und ggf. dem Nachweis der Datenschutz-Folgenabschätzung können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten nach den **Vorgaben** (Art. 24 Abs. 1) **der DSGVO** verarbeitet werden.

Sie sollen sich im Zusammenhang mit der Rechenschaftspflicht ausführlich damit beschäftigen, ob für eine Verarbeitungstätigkeit eine Datenschutz-Folgenabschätzung notwendig ist oder nicht. Aus diesem Grund sollen Sie in diesem Gliederungspunkt entweder detailliert begründen, warum Sie für die vorliegende Verarbeitungstätigkeit ***keine*** *Datenschutz-Folgenabschätzung benötigen, oder – falls eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO notwendig ist – auf die entsprechende Dokumentation verweisen.*

In dieser Dokumentationsvorlage ist als Dokumentationsort der Anhang (Teil C in diesem Dokument) vorgesehen. Sie können Ihre Dokumentation aber auch anders strukturieren und verweisen dann von dieser Stelle auf den entsprechenden Dokumentationsort.

zu (3) Verwendete Programme (Software) für diese Verarbeitungstätigkeit

Mit der Beschreibung, welche Programme bei der Verarbeitung von personenbezogenen Daten verwendet werden, können Sie im Zusammenhang mit der Rechenschaftspflicht **Transparenz** schaffen.

- *Beschreiben Sie die eingesetzte Software (ein Programm oder mehrere Programme), die Sie für diese Verarbeitungstätigkeit einsetzen.*
- *Versehen Sie die Programme mit fortlaufenden Nummern. Sie können dann im Punkt (4) auf diese Nummern verweisen und erzeugen keine Redundanzen innerhalb Ihrer Dokumentation.*
- *Zu den Programmen gehören nicht nur das Fachverfahren an sich, sondern auch Programme, die direkt oder indirekt mit der Verarbeitungstätigkeit oder mit dem Fachverfahren in Verbindung stehen, z. B.*
  - *eine Datenbankanwendung, die zusätzlich zum Fachverfahren installiert werden muss, oder*
  - *Standardprogramme wie ein Textverarbeitungs- oder Tabellenkalkulationsprogramm, wenn diese zur Verarbeitung der Daten verwendet werden.*
- *Wenn es sich bei dieser Verarbeitungstätigkeit um keine automatisierte Datenverarbeitung handelt und Sie keine Programme und Hardware einsetzen, dann können Sie in diesem Formularfeld „keine automatisierte Datenverarbeitung“ vermerken.*

zu (4) Speicherort der personenbezogenen Daten

Mit der Beschreibung es Speicherorts der personenbezogenen Daten können Sie im Zusammenhang mit der Rechenschaftspflicht **Transparenz** schaffen.

- *Geben Sie für jedes der unter (3) aufgeführten Programme an, wo die mit diesem Programm verarbeiteten personenbezogenen Daten gespeichert werden. Das kann*
  - *bei einer elektronischen Datenverarbeitung z. B. ein IT-Gerät oder ein Cloudspeicher bei einem externen Dienstleister sein oder*
  - *bei einer nicht automatisierten Datenverarbeitung z. B. die Ablage einer Akte in einem Aktenschrank.*
- *Es ist auch eine gleichzeitige elektronische/nicht elektronische Speicherung möglich, wenn die elektronischen Daten auch ausgedruckt in Papierform abgelegt werden.*

zu (5) IT-Systeme, auf denen die Programme aus (3) installiert sind

Mit der Beschreibung der IT-Systeme, auf denen die Programme aus (3) installiert sind, können Sie im Zusammenhang mit der Rechenschaftspflicht **Transparenz** schaffen.

- *Geben Sie für jedes der unter (3) aufgeführten Programme die IT-Systeme an, auf denen das Programm installiert ist, und verweisen Sie auf die entsprechende Systemdokumentation.*
- *Der Verweis auf die Systemdokumentation kann entweder ein Verweis auf eine elektronische Dokumentation, z.B. eine Datei, ein Wiki, eine Dokumentations-Datenbank o.ä., oder eine Papierakte (Aktenzeichen) sein.*
- *Geben Sie zusätzlich zu den Verweisen auf die Systemdokumentation an, wo die physikalischen und logischen Verbindungen zu anderen informationstechnischen Geräten dokumentiert (Netzplan) sind. Es ist wichtig, dass Sie hier in der Regel auf ein Dokument verweisen, das in der Dokumentationsstruktur auf einer höheren Ebene angesiedelt ist. Ansonsten laufen Sie Gefahr, dass Sie die gleichen Informationen in verschiedenen Dokumenten beschreiben (Redundanz!). Wenn sich diese Informationen ändern, müssten Sie diese Änderungen in den verschiedenen Dokumentationen berücksichtigen. Nur wenn Sie für diese spezielle Verarbeitungstätigkeit eine spezielle Netzwerkfunktionalität benötigen, die Sie ansonsten in keinem anderen Bereich einsetzen, können Sie diese Funktionalität in diesem Formularfeld dokumentieren.*
- *Wenn es sich bei dieser Verarbeitungstätigkeit um keine automatisierte Datenverarbeitung handelt und Sie keine Programme und Hardware einsetzen, dann können Sie in diesem Formularfeld „keine automatisierte Datenverarbeitung“ vermerken.*

zu (6) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Mit der Beschreibung der Maßnahmen, die Sie zum Datenschutz durch Technikgestaltung und bzw. zur datenschutzfreundlichen Voreinstellungen berücksichtigen, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten nach den **Vorgaben** (Art. 24 Abs. 1) **der DSGVO** verarbeitet werden.

Verweisen Sie innerhalb dieser Verarbeitungsdokumentation an dieser Stelle auf die Dokumentationsbestandteile, in denen die internen Strategien und Maßnahmen beschrieben werden, die insbesondere den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Genüge tun.

	Zu dieser Thematik stellt das ULD eine Vorlage mit den entsprechenden Ausfüllhinweisen zur Verfügung, die im Anhang dieser Verarbeitungsdokumentation mit aufgenommen werden kann.

zu (7) Maßnahmen zur Sicherstellung der Informationspflichten des Verantwortlichen

Die DSGVO stärkt die Rechte der betroffenen Personen. Das beinhaltet

- die **Pflicht des Verantwortlichen**, betroffene Personen bei der Erhebung ihrer personenbezogenen Daten umfassend zu **informieren**,
- die betroffenen Personen darin zu **unterstützen, ihre Rechte auszuüben**, und
- die betroffenen Personen zu **benachrichtigen**, wenn es zu einer **Verletzung des Schutzes** ihrer personenbezogener Daten gekommen ist.

In diesem Dokumentationspunkt beschreiben Sie zum einen, wie Sie den betroffenen Personen die Informationen zur Verfügung stellen, und zum anderen, mit welchen internen Managementprozessen Sie die Betroffenenrechte sicherstellen.

(1) Zu den Optionsfeldern:

*Wählen Sie eines der beiden Optionsfelder, je nachdem, **wie** Sie den betroffenen Personen die **Informationen zur Verfügung stellen**. Das kann die Vorlage des ULD sein oder eine eigene Zusammenstellung, z. B. integriert in die Datenschutzerklärung der Organisation.*

*(2) Im Textfeld unterhalb der Optionsfelder können Sie beschreiben, welche Prozesse Sie definiert haben, damit die betroffenen Personen die **Informationen nach Art. 13 und Art. 14 DSGVO** erhalten, z. B.:*

- *Wie erhalten die betroffenen Personen diese Informationen (z. B. Informationsblatt, Webseite, andere Medien)?*
- *Wie informieren Sie die betroffenen Personen darüber, wo Sie die Informationen erhalten können (z. B. auf Ihrer Webseite, in der Datenschutzerklärung)?*
- *Wie stellen Sie intern sicher, dass die Informationen aktuell bleiben (z. B. regelmäßige Überarbeitung)?*

zu (8) Maßnahmen zu Auskunftsansprüchen von betroffenen Personen

Betroffene Personen können von Ihnen eine Bestätigung verlangen, dass Sie personenbezogene Daten über sie verarbeiten. Mit der Beschreibung des Datenschutz-Managementprozesses können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um den betroffenen Personen eine Auskunft nach Art. 15 DSGVO zu erteilen, z. B.:*
  - *Welche Mitarbeitende sind für die Beantwortung von Auskunftsansprüchen zuständig? (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)*
  - *Wie überprüfen Sie ggf. die Identität der anfragenden betroffenen Person, z. B.*

	durch die Zusendung eines Identitätsnachweises (z. B. geschwärzter Personalausweis, so dass nur Name und Adresse lesbar sind)? ‣ *Wie stellen Sie sicher, dass Sie die entsprechenden Informationen innerhalb Ihrer Organisation finden (z. B. gibt es Suchroutinen für Akten, Anwendungen, Systemen usw.)?* ‣ *Wie stellen Sie sicher, dass die anfragende betroffene Person zeitnah eine Antwort von Ihnen erhält? Gibt es ggf. Vertretungsregelungen?* ‣ *In welcher Form antworten Sie der anfragenden Person (z. B. per Brief oder per E-Mail)?* *Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Prozesshandbuch), dann können Sie hier auf diese Dokumentation verweisen.*

zu (9) Maßnahmen zur Berichtigung von personenbezogenen Daten

Betroffene Personen können von Ihnen verlangen, dass **unrichtige personenbezogene Daten** über sie unverzüglich zu **berichtigen** sind. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

	‣ *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um unrichtige Daten über sie zu korrigieren, z. B.:* ‣ *Welche Mitarbeitende sind für die Berichtigung zuständig (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)?* ‣ *Wie stellen Sie sicher, dass die Daten, die Sie ändern wollen, richtig sind (z. B. über einen Identitätsausweis bei Änderung von Namen oder Kontaktdaten)?* ‣ *Wie stellen Sie sicher, dass Sie unrichtige Daten an allen Stellen Ihrer Datenverarbeitung berichtigen (z. B. wenn sie in mehreren Anwendungen verarbeitet werden)?* ‣ *Wie gehen Sie mit unrichtigen Daten in Sicherungen (z. B. Datensicherung einer Fachanwendung) um?* *Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Prozesshandbuch), dann können Sie hier auf diese Dokumentation verweisen.*

zu (10) Maßnahmen zum Löschen von personenbezogenen Daten („Recht auf Vergessenwerden“)

Betroffene Personen können von Ihnen verlangen, dass **personenbezogene Daten** über sie unverzüglich zu **löschen** sind, wenn die Gründe nach Art. 17 Abs. 1 vorliegen. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

	‣ *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um ggf. die Daten der betroffenen Personen zu löschen, z. B.:* ‣ *Wie lassen sich die zu löschenden Daten innerhalb der Fachanwendung oder innerhalb einer nicht automatisierten Verarbeitung identifizieren?* ‣ *Welche Mitarbeitende sind für die Löschung zuständig (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)?* ‣ *Wie stellen Sie sicher, dass Sie die betreffenden Daten an allen Stellen Ihrer Datenverarbeitung löschen (z. B. Verarbeitung in mehreren Anwendungen)?*

- *Wie gehen Sie mit zu löschenden Daten in Sicherungen (z. B. Datensicherung einer Fachanwendung) um?*

Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Prozesshandbuch), dann können Sie hier auf diese Dokumentation verweisen.

zu (11) Maßnahmen zur Einschränkung der Verarbeitung

Betroffene Personen können von Ihnen verlangen, dass **die Verarbeitung von personenbezogenen Daten** eingeschränkt wird, wenn eine der Voraussetzungen nach Art. 18 Abs. 1 DSGVO gegeben ist. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um ggf. die Verarbeitung von personenbezogenen Daten der betroffenen Personen (in der Regel für einen definierten Zeitraum) einzuschränken, z. B.:*
  - *Wie lassen sich die einzuschränkenden Daten innerhalb der Fachanwendung oder innerhalb einer nicht automatisierten Verarbeitung identifizieren?*
  - *Welche Mitarbeitende sind für die Einschränkung der Verarbeitung zuständig (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)?*
  - *Wie stellen Sie sicher, dass Sie die betreffenden Daten an allen Stellen Ihrer Datenverarbeitung einschränken (z. B. wenn sie in mehreren Anwendungen verarbeitet werden)?*
  - *Wie stellen Sie sicher, dass keiner Ihrer Mitarbeitenden eingeschränkte Daten für den Zeitraum der Einschränkung weiterverarbeiten (z. B. durch technische Mittel oder durch unmissverständliche Kennzeichnung)?*

Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Prozesshandbuch), dann können Sie hier auf diese Dokumentation verweisen.

zu (12) Maßnahmen zur Gewährleistung der Datenübertragbarkeit

Betroffene Personen können von Ihnen verlangen, dass sie **personenbezogene Daten** über sie in einem **strukturierten, gängigen und maschinenlesbaren Format** erhalten können. Das gilt für personenbezogene Daten, die sie mit ihrer Einwilligung zur Verfügung gestellt haben oder wenn die Verarbeitung zur Erfüllung eines Vertrags notwendig ist. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um betroffenen Personen ggf. personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung zu stellen, z. B.:*
- *Wie lassen sich die betreffenden Daten aus einer beispielsweise automatisierten Fachanwendung exportieren?*
- *Welche Mitarbeitende sind für das Datenübertragbarkeitsrecht zuständig (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)?*

Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Prozesshandbuch), dann können Sie hier auf diese Dokumentation verweisen.

zu (13) Maßnahmen zur Protokollierung von Verarbeitungstätigkeiten

Mit Hilfe einer Protokollierung kann eine Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Sicherheitsmaßnahmen durchgeführt werden. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Im Textfeld können Sie beschreiben, welche Prozesse Sie definiert haben, um eine geeignete Protokollierung für die Verarbeitungstätigkeit sicherzustellen, z. B.:*
  - *Welche Datenverarbeitungen werden wann und wie protokolliert?*
  - *Welche Mitarbeitende sind für die Auswertung der Protokolle zuständig (z. B.: Wird diese Aufgabe im Datenschutzmanagement (Teil B (1)) berücksichtigt?)?*
  - *Wer hat Zugriff auf die Protokolldaten?*
  - *Wie lange werden Protokolldaten aufbewahrt und wann werden sie gelöscht?*
  - *Wo werden Protokollauswertungen dokumentiert?*

Wenn Sie z. B. in einer externen Dokumentation diese Prozesse beschrieben haben (z. B. in einem Protokollierungshandbuch), dann können Sie hier auf diese Dokumentation verweisen.

zu (14) Dokumentation der Berechtigungen

Mit der Festlegung, welche Personen welche **Berechtigungen** für die Verarbeitung von personenbezogenen Daten erhalten, können Sie im Zusammenhang mit der Rechenschaftspflicht die **Integrität** und **Vertraulichkeit** gewährleisten.

- *Sie können in jeder Zeile der Tabelle eine Angabe darüber machen, wo Sie die Berechtigungen der unter (3) aufgeführten Programme und Fachverfahren dokumentiert haben – entweder in dieser Dokumentation oder in einer „externen" Dokumentation, z. B. in einem Ticketsystem oder einer ausgelagerten Akte.*
- *Wenn die Berechtigungen „extern" dokumentiert werden, dann geben Sie hier einen Verweis auf die entsprechende Dokumentation an.*
- *Wenn die Berechtigungen in dieser Dokumentation dokumentiert werden, dann sollte die entsprechende Dokumentation (z. B. Vordruck zur Berechtigungsdokumentation des ULD) in den Anhang mit aufgenommen werden und von hier auf den Anhang verwiesen werden.*

zu (15) Managementprozesse für die Berechtigungsvergabe

Mit der Festlegung der **Managementprozesse** zur Vergabe von **Benutzerberechtigungen** können Sie im Zusammenhang mit der Rechenschaftspflicht die **Integrität** und **Vertraulichkeit** gewährleisten.

- *Kopieren Sie, wenn Sie mehr als ein Programm unter (3) aufgeführt haben, für jedes der Programme oder Fachanwendungen diese Tabelle (15) und fügen Sie sie in die Dokumentation mit ein.*

- *Dokumentieren Sie für jedes Programm, wie Mitarbeitende Zugriff auf das entsprechende Programm erhalten (Benutzername/Passwort, Single-Sign-On,*

2-Faktor-Authentisisierung usw.) und beschreiben Sie die entsprechende Methode. So dokumentieren Sie beispielsweise für die Zugriffsmethode Benutzername/Passwort,

- *ob bei dem Programm oder der Fachanwendung ein Passwort für die einzelnen Benutzenden vergeben wird,*
- *mit welcher Komplexität (Zeichenlänge, welche Zeichen (Groß/Kleinbuchstaben, Zahlen, Sonderzeichen) Passwörter gebildet werden müssen und*
- *wie häufig die Passwörter geändert werden müssen.*

- *Dokumentieren Sie für jedes Programm die dazugehörigen Managementprozesse, z. B.*
  - *wer die Berechtigungsvergabe initiiert und autorisiert,*
  - *wer die Berechtigungsvergabe technisch umsetzt,*
  - *wie die Berechtigungsvergabe protokolliert wird,*
  - *wie die korrekte Berechtigungsvergabe durch wen kontrolliert wird,*
  - *wo die Berechtigungsvergabe dokumentiert wird usw.*

Es kann sehr sinnvoll und hilfreich sein, nicht in jeder Verarbeitungsdokumentation die Managementprozesse zur Berechtigungsvergabe einzeln zu beschreiben, sondern diese Prozesse in einem eigenen Dokument, z. B. einer Passwort-Richtlinie, festzulegen. Sie können dann hier auf dieses Dokument verweisen und nur wenn es abweichende Prozesse bei dieser Verarbeitungstätigkeit gibt, sie hier dokumentieren.

Das hat den Vorteil, dass Sie generelle Änderungen nur einmal zentral ändern müssen und sie nicht in jeder einzelnen Verarbeitungsdokumentation nachdokumentieren müssen. Weiterhin halten Sie damit die Dokumentationen der einzelnen Verarbeitungsdokumentationen schlank.

zu (16) Managementprozesse für die administrative Berechtigungsvergabe

Mit der Festlegung der **Managementprozesse** zur Vergabe von **Benutzerberechtigungen für administrative Mitarbeitende** können Sie im Zusammenhang mit der Rechenschaftspflicht die **Integrität** und **Vertraulichkeit** gewährleisten.

- *Kopieren Sie, wenn Sie mehr als ein Programm unter (3) aufgeführt haben, für jedes der Programme oder Fachanwendungen die Tabelle (16) und fügen Sie sie in die Dokumentation mit ein.*

- *Dokumentieren Sie für jedes Programm, wie administrative Mitarbeitende Zugriff auf das entsprechende Programm erhalten (Benutzername/Passwort, Single-Sign-On, 2-Faktor-Authentisisierung usw.) und beschreiben Sie die entsprechende Methode. So dokumentieren Sie beispielsweise für die Zugriffsmethode Benutzername/Passwort,*
  - *ob bei dem Programm oder der Fachanwendung ein Passwort für die einzelnen administrativen Mitarbeitenden vergeben wird,*
  - *mit welcher Komplexität (Zeichenlänge, welche Zeichen (Groß/Kleinbuchstaben, Zahlen, Sonderzeichen) Passwörter gebildet werden müssen und*
  - *wie häufig die Passwörter geändert werden müssen.*

- *Dokumentieren Sie für jedes Programm den dazugehörigen Managementprozess, z. B.*

- *wer die Berechtigungsvergabe initiiert und autorisiert,*
- *wer die Berechtigungsvergabe technisch umsetzt,*
- *wie die Berechtigungsvergabe protokolliert wird,*
- *wie die korrekte Berechtigungsvergabe durch wen kontrolliert wird,*
- *wo die Berechtigungsvergabe dokumentiert wird usw.*

Es kann sehr sinnvoll und hilfreich sein, nicht in jeder Verarbeitungsdokumentation die Managementprozesse zur Berechtigungsvergabe einzeln zu beschreiben, sondern diese Prozesse in einem eigenen Dokument, z. B. einer Passwort-Richtlinie, festzulegen. Sie können dann hier auf dieses Dokument verweisen und nur wenn es abweichende Prozesse bei dieser Verarbeitungstätigkeit gibt, sie hier dokumentieren.

Das hat den Vorteil, dass Sie generelle Änderungen nur einmal zentral ändern müssen und sie nicht in jeder einzelnen Verarbeitungsdokumentation nachdokumentieren müssen. Weiterhin halten Sie damit die Dokumentationen der einzelnen Verarbeitungsdokumentationen schlank.

zu (17) Prüfung der Datenverarbeitung (Revision)

Mit Hilfe von Prüfungen kann die Wirksamkeit von technischen und organisatorischen Sicherheitsmaßnahmen durchgeführt werden. Mit der Beschreibung, wie Sie dieses gewährleisten, können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Beschreiben Sie in dem obersten Textfeld*
  - *wer festlegt, welche Prüfungen für diese Verarbeitungstätigkeit durchgeführt werden,*
  - *wie die sie durchgeführt werden (Zeitintervalle – regelmäßig oder durch „Ereignisse“, zuständige Mitarbeitende, Ablauf usw.),*
  - *welche Konsequenzen sich ergeben, wenn bei Prüfungen Auffälligkeiten festgestellt werden (was passiert dann?)*
  - *usw.*
- *Dokumentieren Sie in der Tabelle **(Prüfgegenstand)**,*
  - *welche Prüfungen für die Verarbeitungstätigkeit durchgeführt werden (z. B. Berechtigungsvergabe, administrative Zugriffe, Rechtmäßigkeit, Fortschreibung der Dokumentation usw.),*
  - *welche Person die Prüfung durchführt und*
  - *in welchen Prüfintervallen sie durchgeführt werden soll.*
- *Dokumentieren Sie im Textfeld **(Prüfberechtigungen)**, wie die durchführende Person die Berechtigungen im System erhält, damit sie eine Prüfung durchführen kann (z. B. kurzfristige Berechtigung).*
- *Dokumentieren Sie im Textfeld (**Prüfdokumentation**), wie und wo die Prüfung dokumentiert wird (z. B. innerhalb dieser Dokumentation im Anhang, in einem Prüfhandbuch o. ä.).*
- *Dokumentieren Sie im Textfeld (**Informationen der Benutzer**), wie die Mitarbeitenden über die Prüfmaßnahmen informiert werden (z. B. durch Hinweise in Dienstanweisungen, Dienstvereinbarungen o. ä.).*
- *Dokumentieren Sie im Textfeld (**Maßnahmen**), welche Maßnahmen sich aus Auffälligkeiten bei der Prüfung ergeben können (z. B. eine tiefergehende Prüfung). Hier kann auch auf ein übergreifendes Prüfkonzept verwiesen werden, sofern es vorhanden ist.*

zu (18) Test- und Freigabeverfahren

Art. 32 der DSGVO fordert ein Verfahren, mit dem eine regelmäßige „Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“ möglich ist. Das ist nur möglich, wenn zu einem definierten Zeitpunkt ein dokumentierter „Soll-Zustand“ vorliegt. Zu diesem Zeitpunkt werden

(1) alle vorhandenen Dokumentationen zu einer Verarbeitungstätigkeit (diese Verarbeitungsdokumentation und die mit dieser Dokumentation verbundenen Systemdokumentationen, Konzepte, Anweisungen, ergänzende Dokumentationen usw.) in Ihrem Bearbeitungsstrand „eingefroren“,
(2) die Wirksamkeit der technischen und organisatorischen Maßnahmen mit einem Testverfahren überprüft und
(3) der in (1) definierte und in (2) überprüfte Dokumentationsstand durch die Leitung der verantwortlichen Stelle freigegeben.

Dieser „Soll-Zustand“ kann verwendet werden, um die geforderte Überprüfung, Bewertung und Evaluierung nach Art. 32 DSGVO durchzuführen.

Mit einem dokumentierten Test- und Freigabeverfahren können Sie im Zusammenhang mit der Rechenschaftspflicht **nachweisen**, dass personenbezogene Daten **nach den Vorgaben** (Art. 24 Abs. 1) **der DSGVO verarbeitet** werden.

- *Definieren Sie in dem Textfeld, wann Sie ein neues Test- und Freigabeverfahren durchführen. Das können unterschiedliche Auslöser sein, z. B. Gesetzesänderungen, Änderungen in der Technik, wesentliche Änderungen in einem Fachverfahren, Änderungen in Dienstanweisungen oder Dienstvereinbarungen, die die Verarbeitungstätigkeit betreffen, usw.*
- *Beschreiben Sie den Prozess, wie Ihr Test- und Freigabeverfahren aussieht.*
  - *Sie können dazu beispielsweise auf eine Vorlage verweisen (z. B. die Vorlage zum Test- und Freigabeverfahren, die Sie auf der Webseite des ULD herunterladen können), die sowohl eine Checkliste beinhaltet als auch die Zuständigkeiten und Verantwortlichkeiten berücksichtigt.*
  - *Sie können aber auch ihren eigenen Prozess definieren, den Sie dann in diesem Textfeld beschreiben oder auf den Sie verweisen können.*

zu (19) Dokumentation von Test- und Freigabeverfahren

- *Geben Sie mit Hilfe der Options- und Textfelder an, wo Sie Ihre Test- und Freigabedokumente ablegen. Dazu gibt es mehrere Möglichkeiten, z. B.*
  - *als Ausdruck im Anhang (Teil C (I) und (II)),*
  - *in elektronischer Form (nur für das Testverfahren (siehe Hinweis weiter unten)*
  - *o. ä.*
- *Hinweis: Der Freigabevermerk sollte immer in Papierform vorliegen, denn hier bestätigen die Verantwortlichen den getesteten und freigegebenen „Soll-Zustand“ Ihrer Verarbeitungstätigkeit.*

zu (Teil C) Protokolle und Anhang

Im Anhang können Sie – je nachdem, wie Sie Ihre Dokumentation organisieren - verschiedene Dokumente aufnehmen:

- Testprotokolle (eine Vorlage kann auf der Webseite des ULD heruntergeladen werden)
- Freigabeprotokolle (eine Vorlage kann auf der Webseite des ULD heruntergeladen werden)
- Dokumentationen von Kontrollen (Revision)
- zusätzliche Anlagen (z. B. Dokumentation von Berechtigungen, Nachweis, wie Sie Ihren Informationspflichten nachkommen usw.)