

Verzeichnis von Verarbeitungstätigkeiten

- Ausfüllhinweise –

Die rechtliche Grundlage für das Verzeichnis von Verarbeitungstätigkeiten (VVT) findet sich in Art. 30 Datenschutz-Grundverordnung (DSGVO). Gemäß Erwägungsgrund 82 der DSGVO dient es dem „Nachweis der Einhaltung dieser Verordnung“.

Jeder Verantwortliche führt **ein** Verzeichnis aller Verarbeitungstätigkeiten. Das entsprechende Formular besteht aus einem allgemeinen und einem besonderen Teil. Da bei allen Verarbeitungstätigkeiten Angaben zum Verantwortlichen und Datenschutzbeauftragten gemacht werden müssen, werden diese Angaben in einem **allgemeinen Teil** vorgezogen. Sofern bspw. die Person des Datenschutzbeauftragten wechselt, kann dieser Teil ausgetauscht werden, ohne dass jedes individuelle Verfahren, das in einem **besonderen Teil** hinter den allgemeinen Angaben aufgelistet ist, bearbeitet werden muss.

Bei diesen Angaben gibt es Angaben, die das Gesetz fordert, sowie Angaben, die für die Arbeit des Verantwortlichen bzw. des Datenschutzbeauftragten bei der Sicherstellung der datenschutzrechtlichen Anforderungen erforderlich sind. So kann beispielsweise nur dann beurteilt werden, ob die technischen und organisatorischen Maßnahmen ausreichend sind, wenn bekannt ist, welche Hard- und Software eingesetzt wird, wie die Vernetzung realisiert ist und welcher Personenkreis Zugriff auf die Daten benötigt.

Das Muster-VVT ist insoweit als Instrument zu sehen, das auch im Rahmen der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO genutzt wird.

Aus der Kennzeichnung im Verzeichnis selbst (dort mit ¹ oder ²) und den nachstehenden Hinweisen ergibt sich, ob die Angabe zwingend Bestandteil des VVT ist oder ob die Angabe aus Gründen der Rechenschaftspflicht notwendig ist. Natürlich kann der Rechenschaftspflicht auch anderweitig Rechnung getragen werden, indem die entsprechende Dokumentation außerhalb des VVT geführt wird. Aus Sicht eines wirksamen Datenschutzmanagements sollte das VVT, das ohnehin zu erstellen ist, jedoch auch dafür genutzt werden.

Das VVT ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen (Art. 30 Abs. 4 DSGVO). In diesem Falle werden dann auch die optionalen Angaben der Aufsichtsbehörde bekannt, was zunächst nicht erforderlich wäre. Allerdings würden sich ohne diese Angaben nach unserem Dafürhalten für die Aufsichtsbehörde Rückfragen nach genau diesen Angaben ergeben.

I. Allgemeiner Teil des VVT

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. a DSGVO.

Im Gegensatz zu vielen anderen Mustern wurde vorliegend auf die Angabe, ob es sich um die Hauptniederlassung handelt und auf Angaben zum Vertreter von nicht in der Union niedergelassenen Verantwortlichen verzichtet. Diese Fallgestaltungen dürften in der Hochschullandschaft grundsätzlich nicht vorkommen.

Bitte tragen Sie Name und Kontaktdaten der Hochschule ein sowie die Angaben zum Datenschutzbeauftragten. Sofern es sich um einen externen handelt, ist dessen Anschrift erforderlich.

II. Besonderer Teil (Individuelles Verfahren)

1. „Bezeichnung der Verarbeitungstätigkeit“

Die Notwendigkeit der Angaben des Zwecks ergibt sich aus Art. 30 Abs. 1 lit. b DSGVO.

Verwenden Sie beim Zweck eine möglichst eindeutige und aussagekräftige Festlegung, zu welchen Zwecken die Daten im Rahmen des gesamten Verfahrens verarbeitet werden (vollständige Aufzählung).

Beispiel: „Abwicklung von Fortbildungsveranstaltungen (Anmeldung von Teilnehmern, Verwaltung von Teilnehmerdaten, Ausstellung von Teilnahmebescheinigungen)“

Als Bezeichnung für die Verarbeitungstätigkeit wählen Sie möglichst einen beschreibenden Sammelbegriff, der die Verarbeitungstätigkeit möglichst konkret und eindeutig kennzeichnet. Es ist darauf zu achten, dass er nicht missinterpretiert werden kann (er sollte daher alle Datenverarbeitungsformen des Verfahrens erfassen). Gegebenenfalls ist ein beschreibender Zusatz voranzustellen: Beispiele: „Lernplattform Moodle“, „Raumvergabesystem ROMA“

2. „Innerorganisatorische Ansprechpartner“

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Zur Sicherstellung der Einhaltung der Grundsätze für die Verarbeitung ist es unerlässlich, die verantwortlichen Ansprechpartner schnell identifizieren und erreichen zu können. Daher werden hier Angaben zu den Ansprechpartnern benötigt. Es kann natürlich auch vorkommen, dass beide Ansprechpartner identisch sind.

3. „Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen“

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. a DSGVO.

Die DSGVO kennt die Konstruktion der gemeinsamen Verantwortlichkeit: „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche.“ (Art. 26 Abs. 1 Satz 1 DSGVO)

Liegt eine solche Konstellation vor, ist hier der weitere Verantwortliche mit Name und Kontaktdaten anzugeben.

Hinweis: Bei einer gemeinsamen Verantwortlichkeit ist es **nicht** erforderlich, dass jeder Verantwortliche für die entsprechende Verarbeitungstätigkeit ein Verzeichnis führt. Vielmehr können die Verantwortlichen in der nach Art. 26 DSGVO erforderlichen Vereinbarung festlegen, wer von ihnen das Verzeichnis erstellt und führt.

4. „Beschreibung der Verarbeitungstätigkeit“

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Unsere Erfahrung zeigt, dass alleine aus den zwingend gesetzlichen Angaben zum früheren Verfahrensverzeichnis heraus die Verfahrensabläufe nicht immer zu verstehen waren. Entsprechendes wird auch für die Verarbeitungstätigkeit und das VVT gelten. Daher gibt es hier Raum, um als Freitext die Prozesse und die dabei erfolgenden Verarbeitungstätigkeiten zu beschreiben.

Bitte nehmen Sie in die Beschreibung auf, wann die Verarbeitungstätigkeit beginnt bzw. begonnen hat.

Sofern die Datenverarbeitung (auch) auf eine Einwilligung gestützt wird, muss dies aus der Beschreibung hervorgehen. Legen Sie bitte den Prozess der Einwilligung dar. Dies bedeutet, dass insbesondere beschrieben wird, wie die Einwilligung eingeholt wurde, wie mögliche Drucksituationen vermieden wurden, wie viel Zeit die Betroffenen zur Abgabe der Einwilligung hatten, wie der Nachweis geführt wird, dass der Betroffene eingewilligt hat (vgl. Art. 7 Abs. 1 DSGVO) oder ggf. welche Anstrengungen bei einer Einwilligung von Kindern gemäß Art. 8 DSGVO unternommen wurden, um sich zu vergewissern, dass auch tatsächlich der gesetzliche Vertreter eingewilligt hat.

Soweit im Rahmen des Verfahrens personenbezogene Daten erhoben werden, müssen Informationspflichten erfüllt werden (Artt. 13,14 DSGVO). Legen Sie bitte dar, auf welchem Weg den Betroffenen die Pflichtinformationen zugänglich gemacht werden und fügen Sie zum Nachweis die entsprechenden Dokumente bei (z.B. Screenshot bei der Datenerhebung mittels eines Onlineformulars).

Werden die entsprechenden Daten mittels eines Fragebogens erhoben, fügen Sie diesen bitte zum Nachweis als Anlage bei.

Zudem sind Grundsätze für die Verarbeitung personenbezogener Daten die Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und die Speicherbegrenzung (Art. 5 Abs. 1 lit. e). Die Beschreibung der Prozesse hier dient insoweit im Rahmen der Rechenschaftspflicht dem Nachweis, wie diesen Grundsätzen durch die Gestaltung der Abläufe Rechnung getragen wird.

5. „Kategorien personenbezogener Daten“

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. c DSGVO.

Aufzuführen sind alle personenbezogenen Daten, die bei der Verarbeitungstätigkeit verarbeitet werden. Soweit sinnvoll können einzelne Daten zu Kategorien zusammengefasst werden, wenn die Kategoriebezeichnung aus sich heraus erkennen lässt, welche Datenarten erfasst sind.

Beispiel: „Anschrift“ als Kategorie für die Daten „Straße, Hausnummer, PLZ, Wohnort, Land“; nicht ausreichend wäre dagegen die unspezifische Bezeichnung „Daten zur Person“ oder „Erreichbarkeitsdaten“.

In der Spalte „Bes.“ ist ein „x“ zu setzen, wenn das jeweilige Datum zuzuordnen ist entweder

- einer besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO. Das sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
Oder
- Art. 10 DSGVO. Das sind Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängenden Sicherungsmaßnahmen.

Bitte beachten Sie: Wenn bei irgendeinem Datum in der Spalte „Bes.“ ein Kreuz gesetzt werden muss, ist zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist (siehe Ziffer 13 im VVT).

6. Kategorien betroffener Personen

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. c DSGVO.

Es ist möglichst konkret anzugeben, wessen Daten verarbeitet werden. Hierfür ist die jeweilige Personengruppe möglichst konkret zu bezeichnen.

Beispiel: Sind alle Studierenden betroffen, genügt die Angabe „Studierende“. Sind nur Studierende ab dem 5. Semester betroffen oder bspw. Hochschulmitarbeiter bestimmter Entgeltgruppen, so muss das aus dem Eintrag hervorgehen.

7. Rechtsgrundlage der Verarbeitungstätigkeit

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Einer der Grundsätze für die Verarbeitung personenbezogener Daten ist die Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DSGVO). Damit die Datenverarbeitung rechtmäßig ist, müssen personenbezogene Daten mit Einwilligung der betroffenen Person oder auf einer sonstigen Rechtsgrundlage verarbeitet werden (vgl. Erwägungsgrund 40 der DSGVO).

Wenn die Datenverarbeitung auf eine oder mehrere Rechtsvorschrift(en) gestützt wird, ist die Vorschrift mit Paragraph, Absatz, Satz und Gesetzesbezeichnung zu benennen.

Wird die Datenverarbeitung auf eine Einwilligung gestützt,

- geben Sie hier „Einwilligung“ an,
- fügen Sie den Text der Einwilligungserklärung dem VVT als Anhang bei,
- erwähnen Sie die Einwilligungserklärung in der Beschreibung der Verarbeitungstätigkeit unter 4 und legen dort den Einwilligungsmechanismus dar (z.B. Angaben dazu, wie die Einwilligung eingeholt wurde, wie Drucksituationen vermieden wurden, wie viel Zeit die Betroffenen zur Abgabe der Einwilligung hatten, wie der Nachweis geführt wird, dass der Betroffene eingewilligt hat (vgl. Art. 7 Abs. 1 DSGVO) oder welche Anstrengungen bei einer Einwilligung von Kindern gemäß Art. 8 DSGVO unternommen werden, um sich zu vergewissern, dass auch tatsächlich der gesetzliche Vertreter eingewilligt hat).

Die Angaben hier dienen im Rahmen der Rechenschaftspflicht dem Nachweis, dass der Grundsatz der Rechtmäßigkeit eingehalten wird.

8. Empfänger personenbezogener Daten

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. d und e DSGVO.

Unter Empfänger versteht Art. 4 Nr. 9 DSGVO nicht mehr nur - wie früher das Landesdatenschutzgesetz - Dritte, sondern auch interne Stellen/Personen. Daher unterscheidet das VVT zunächst interne und externe Empfänger.

8.1. Interne Empfänger

Interne Empfänger sind Personen oder Stellen innerhalb des Verantwortlichen, also innerhalb der Hochschule. Diese erhalten die Daten entweder für denselben Zweck, den das konkrete VVT beschreibt oder sie verarbeiten die Daten zweckändernd weiter.

8.2. Externe Empfänger

Externe Empfänger sind alle Personen und Stellen, die nicht Teil der Rechtsperson Hochschule sind. Dazu gehören insbesondere auch Auftragsverarbeiter im Sinne von Art. 28 DSGVO.

Da der Fall der Auftragsverarbeitung (ADV) besondere datenschutzrechtliche Anforderungen nach sich zieht und das VVT auch der Rechenschaftspflicht dient, bitte in der Spalte „ADV“ durch Setzen eines X kenntlich machen, wenn ein Empfänger als Auftragsverarbeiter tätig ist.

Sofern Empfänger ihren Sitz in einem **Drittland** haben (das sind Länder außerhalb der EU bzw. des EWR) oder es sich um eine **internationale Organisation** handelt, ist eine Weitergabe nur unter besonderen Bedingungen zulässig. Die Angabe, worauf die Weitergabe gestützt wird, dient entsprechend der Eigenkontrolle und der Erfüllung der Rechenschaftspflicht, dass die gesetzlichen Anforderungen eingehalten werden. Bitte kreuzen Sie die entsprechende Option an und machen - wo erforderlich (das wird aus dem Wortlaut im VVT ersichtlich) - weitere Angaben.

Bitte dokumentieren im Fall einer Datenweitergabe nach Artikel 49 Absatz 1 Unterabsatz 2 DSGVO geeignete Garantien gegebenenfalls in einem Anhang zum VVT.

9. Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Es ist anzugeben, welche Personen(gruppen) Zugriff auf die Daten haben. Nicht erforderlich ist die namentliche Nennung von Personen; vielmehr sind funktionsbezogene Angaben zu verwenden. Es kann sinnvoll sein, in der Spalte „Umfang“ anzugeben, ob der Zugriff lesender, schreibender oder beider Art ist.

Diese Angabe ist zum einen erforderlich, da sich daraus Rückschlüsse auf die Einhaltung der Grundsätze des Art. 5 DSGVO ergeben und erfolgt insoweit auch zur Erfüllung der Rechenschaftspflicht.

Zum anderen spielt die Angabe auch eine Rolle, um Anforderungen an die TOM abzuleiten.

10. Fristen für die Löschung

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. f DSGVO.

Es muss festgelegt werden, innerhalb welcher Fristen die personenbezogenen Daten gelöscht werden. Wenn nicht alle Daten innerhalb derselben Frist gelöscht werden, muss nach den einzelnen Daten(-arten) unterschieden werden. Es kann sinnvoll sein auch kenntlich zu machen, ob die Löschung manuell durchgeführt wird oder automatisiert erfolgt.

Die Löschfristen richten sich vorrangig nach bereichsspezifischen Regelungen. Wenn solche nicht bestehen, gilt Art. 17 Abs. 1 lit a DSGVO, d. h. eine Löschung muss erfolgen, wenn die Daten für die Aufgabenerfüllung nicht mehr benötigt werden.

Beispiel: „6 Monate ab Erhebung“, „Unverzüglich nach Exmatrikulation“ Nicht: „6 Monate ab erfolgreicher Auswertung“, wenn offen bleibt, wann die Daten ausgewertet werden.

11. Allgemeine Beschreibung der eingesetzten Hardware, Software und der Vernetzung

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Um beurteilen zu können, ob die getroffenen TOM ausreichend sind und den in Art. 32 DSGVO erwähnten Stand der Technik berücksichtigen, ist die Kenntnis der eingesetzten Hard- und Software sowie der Vernetzung unerlässlich.

11.1. Eingesetzte Software auf Klienten und Servern

Alle verwendete Software, die an der Verarbeitung der Daten beteiligt ist, muss hier aufgeführt werden. Ausgenommen ist/sind das/die verwendeten Betriebssystem(e). Mit „Art der Software“ ist die allgemeine Kategorie gemeint - wie zum Beispiel: Webserver, Datenbank, Textverarbeitung, Tabellenkalkulation o.ä. In der nächsten Spalte ist dann das konkrete Softwareprodukt zu nennen, wie zum Beispiel: Apache Webserver, MS Word o.ä. Danach die Version der Software, die zum Zeitpunkt der Einführung des Verfahrens installiert ist. Dieser Versionsstand muss nicht fortlaufend gepflegt werden, sondern jeweils dann, wenn eine Änderung des Verfahrens zu dokumentieren ist.

In der letzten Spalte ist anzugeben, ob die Software auf dem Server oder einem Klienten zum Einsatz kommt oder auf beidem.

Sollten virtualisierte Server bei dem Verfahren zum Einsatz kommen, so ist die Software, mit der die Virtualisierung realisiert wird, hier zu nennen. Siehe auch Hinweise zu Punkt 11.3.

11.2. Beteiligte Klienten

Sofern es sich bei dem eingesetzten Verfahren nicht um eine Webanwendung handelt, bedarf es der Angabe zu den eingesetzten Klienten. Die Beschreibung der Klienten können über die Angabe der Anzahl zusammengefasst werden, sofern diese sich in der Konfiguration und Funktion gleichen. Der Typ des Klienten kann sehr unterschiedlich sein und vom Laptop oder der Workstation bis zur Videokamera reichen. Als nächstes müssen die Bezeichnung des Betriebssystems und die Bezeichnung der Version zum Zeitpunkt der Einführung des Verfahrens angegeben werden sowie die auf dem Klienten installierte Software aus 11.1. Sollte der Klient über eine Netzwerkanbindung verfügen, ist in dieser Spalte ein Haken bei einer oder bei beiden der IP-Versionen zu setzen. Ferner muss noch angegeben werden, ob der Klient über SSD-Medien verfügt. Sollen auf diesen personenbezogene Daten gespeichert werden, hat dies gegebenenfalls Auswirkung auf die Maßnahmen, wie Daten auf diesen Medien gespeichert und gelöscht werden müssen. Siehe hierzu die Erläuterungen unter Punkt 12.3 unter der Überschrift „Maßnahmen beim Einsatz von SSD-Medien“. Gleiches gilt für externe Medien. Die zu treffenden Maßnahmen sind im Einzelfall in Bezug auf die Verhältnismäßigkeit abzuwägen. Zuletzt müssen noch die auf diesem Klienten verarbeiteten oder gespeicherten Daten aus 5 referenziert werden.

11.3. Beteiligte Server

Analog zu den Angaben zu den Klienten, müssen hier alle Server, die am Verfahren beteiligt sind, aufgeführt werden. Dabei ist die Funktion des Servers anzugeben, zum Beispiel „Anwendungsserver“, „Datenbankserver“, o.ä. Auch hier erfolgen als nächstes die Bezeichnung des Betriebssystems, die Bezeichnung der Version zum Zeitpunkt der Einführung des Verfahrens und die Angabe, ob der Server eine virtuelle Instanz ist. Bei virtuellen Instanzen sind sowohl bei den Angaben der verwendeten Software (Punkt 11.1) der verwendete Hypervisor zu ergänzen, als auch die beteiligten Server, auf denen die Infrastruktur des Hypervisors läuft. Sollte diese Infrastruktur aus mehr als einem Server oder aus einem Servercluster bestehen, so reicht es aus, stellvertretend einen repräsentativen Server zu beschreiben. Danach folgt die auf dem Server installierte Software aus 11.1. Bei der Hardware ist anzugeben, ob SSD-Medien zum Einsatz kommen. Dies hat, analog zu den Klienten, gegebenenfalls Auswirkung auf die Maßnahmen, wie Daten auf diesen Medien gelöscht werden müssen. Siehe hierzu die Erläuterungen unter Punkt 12.3 unter der Überschrift „Maßnahmen beim Einsatz von SSD-Medien“.

Sofern der Server nicht in den Räumlichkeiten des Verantwortlichen steht, ist hier bei extern ein Haken zu setzen, sonst bei intern. In jedem Fall ist die Lokation des Servers als Adresse anzugeben. Als letztes erfolgt die Angabe der gespeicherten Daten aus 5.

11.4. Datensicherung

Für die Sicherung der Daten ist das Speichermedium anzugeben, zum Beispiel „Festplatte“, „Bänder“ o.ä. Aus 11.3 sind als nächstes die Server zu benennen, auf denen die Datensicherung erfolgt sowie die Software aus 11.1, mit der die Datensicherung erstellt wird. Bei dem Aufbewahrungsort sind das Behältnis zu nennen und der Brandabschnitt, in dem die Sicherungsmedien aufbewahrt werden. Dieser Brandabschnitt hat ein anderer zu sein als der, in dem die Server stehen, auf denen die personenbezogenen Daten gespeichert werden. Als letztes erfolgt die Angabe der gesicherten Daten aus 5.

11.5. Darstellung der Netzstruktur

Bei Verarbeitungstätigkeiten, die eine komplexere Struktur haben und eine Kommunikation zwischen Server und Klienten erfordern, ist es für das Verständnis der Netzstruktur meist unabdingbar, eine grafische, schematische Darstellung zu haben. Dabei sollte die Darstellung nur die relevanten infrastrukturellen Komponenten beinhalten. Klar ersichtlich sollten aber die Kommunikationswege sein und welche aktiven Komponenten (Switch, Firewall, Router o.ä.) bei der Übertragung beteiligt sind, sofern diese im Besitz oder Einfluss des Verantwortlichen oder ggf. des Auftragsverarbeiters sind.

11.6. Verwendete Protokolle, Dienste und Verschlüsselung

Die hier aufgeführten Übertragungsabschnitte sollten sich in der Darstellung der Netzstruktur eindeutig wiederfinden. Sofern eine Software aus 11.1 mit anderen Systemen kommuniziert, sind die entsprechenden Übertragungsabschnitte hier einzutragen. Für jeden Übertragungsabschnitt, der eine unverschlüsselte Kommunikation hat, muss eine Erläuterung der Erforderlichkeit und/oder Risikoabwägung im Abschnitt 12.3 unter „Gewährleistung der Vertraulichkeit“ oder in einem erläuternden Dokument, auf welches dort referenziert wird, erfolgen. Im Weiteren sind das betreffende Protokoll und der verwendete Port zu nennen, sowie die technischen Parameter der Verschlüsselung (Algorithmus (RSA, AES usw.), Schlüssellänge, Verschlüsselungsprotokoll mit Version (TLS o.ä.) oder weiteren Maßnahmen wie zum Beispiel „HSTS-Header“, „PFS“, usw. Die Angaben hier sind nicht auf das allgemein verwendete Internetprotokoll (IP) beschränkt, sondern umfassen auch Techniken, wie zum Beispiel Bluetooth, Zigbee, Z-Wave o.ä.

12. Technische und organisatorische Maßnahmen (TOM)

Die Notwendigkeit der Angaben ergibt sich aus Art. 30 Abs. 1 lit. g DSGVO.

Gibt es ein Datenschutz- und Datensicherheitskonzept oder ein anderes Dokument, das die TOM enthält, müssen die Angaben nicht hier im VVT erfolgen, sondern es kann stattdessen (oder zusätzlich) auf dieses Dokument verwiesen und als Anhang zum VVT genommen werden. In diesem Fall bitte das entsprechende Dokument mit genauer Bezeichnung und unter Angabe von Version und/oder Stand bezeichnen.

Es ist dabei zu bedenken, dass dieses Dokument samt Anlagen im Einzelfall der Aufsichtsbehörde zur Verfügung gestellt werden muss. Insoweit sollte nicht auf ein Dokument verwiesen werden, das auch schutzbedürftige interne IT-Sicherheitsinformationen enthält, die nicht relevant sind für die beschriebene Verarbeitungstätigkeit, oder die entsprechenden Angaben sollten in der Anlage zumindest unkenntlich gemacht werden.

12.1. Pseudonymisierung

In der ersten Maßnahme ist darzustellen, wie die personenbezogenen Daten unter dem Aspekt einer getrennten Verwaltung im System gespeichert sind.

Hierzu zählen beispielweise:

- Trennung von Stammdaten und weiteren zu den Stammdaten zuordenbaren Daten wie zum Beispiel Umsatzdaten, Protokolldaten, Ausleihe, Gehaltsabrechnungen usw. Es ist darzulegen, ob und wie eine Trennung dieser Daten erfolgt.
- Verwendung von Kennziffern oder anderen eindeutig identifizierenden Merkmalen statt Namen oder anderen direkt personenbeziehbaren Merkmalen.

12.2. Verschlüsselung

Diese Maßnahme ist nicht zu verwechseln mit der Angaben zu 11.6. („Verwendete Protokolle, Dienste und Verschlüsselung“). Die Angaben dort beziehen sich ausschließlich auf die Netzwerkkommunikation. Alle weiteren Verschlüsselungen die für die Verarbeitungstätigkeit erforderlich sind, sind hier zu beschreiben. Dabei ist auf eine möglichst genaue Angabe der technischen Umsetzung zu achten. Insbesondere sind immer die verwendeten Algorithmen und die Mindestlänge der verwendeten Schlüssel anzugeben.

Zu den weiteren erforderlichen Verschlüsselungen zählen beispielsweise:

- Verschlüsselung von Festplatten in Arbeitsplatzrechner oder Laptops sowie Medien, die zum Transport oder bei der Verarbeitung oder zur Speicherung von personenbezogenen Daten eingesetzt werden.

- Verschlüsselung bei Chipkarten - und zwar sowohl die Speicherung auf der Karte als auch bei der Kommunikation mit der Karte.

12.3. Gewährleistung der Vertraulichkeit

Bei dieser Maßnahme soll hauptsächlich beschrieben werden, wie verhindert wird, dass ein unautorisierte Zugang oder Zugriff auf personenbezogene Daten erfolgt. Dies gilt zum einen innerhalb der Organisation des Verantwortlichen selbst als auch beim Transport bzw. Weitergabe zu einem Auftragsverarbeiter oder bei der Übermittlung zu einem Dritten. Ferner ist hier zu beschreiben, wie eine Trennung von Mandanten erfolgt.

Zu den Maßnahmen zählen beispielweise:

- Zugangskontrolle
 - Gesicherter Gebäudezutritt durch Sicherheitsschleuse, Ausweiskontrolle, elektronisches oder mechanisches Schließsystem, unterschiedliche Sicherheitszonen, usw.
 - Gesicherter Raumzutritt durch Sicherheitstür, Zwei-Faktor-Authentifizierung, usw.
 - Sonstige Gebäude- und Raumsicherung durch Sicherheitsglas gemäß DIN V 18054 (einbruchshemmend), Gitter, Sichtschutz, Alarmanlage mit direkter Benachrichtigung von Polizei, Feuerwehr oder Bewachungsunternehmen, usw.
 - Schlüsselregelung durch Schlüsseltresor, Richtlinie zur Schlüsselvergabe an Dritte (Reinigungspersonal, Wartungsarbeiter, Besucher, Gäste, Feuerwehr usw.), Protokollierung der Schlüsselvergabe, usw.
 - Zutrittsregelung durch Festlegung der befugten Personen, des Umfangs des Zutritts, der Dauer des Zutritts und der Zutrittszeit, usw.
- Zugriffskontrolle
 - Festlegung und Kontrolle der Zugriffsbefugnisse, differenziert nach Daten und Programmen.
 - Protokollierung misslungener sowie ggfs. erfolgreicher Zugriffsversuche.
 - Authentisierung durch Chipkarte, Passwort, Token, Zwei-Faktor, usw.
 - Durchsetzung von Passwortrichtlinien, wie zum Beispiel weiter unten beschrieben.
 - Dokumentiertes und technisch umgesetztes Rollen- und Rechtekonzept.
 - Netzwerksegmentierung oder Benutzerzuordnung einzelner Computer, zur Zugriffssteuerung auf Netzwerkkomponenten oder Funktion.
 - Benutzer- oder gruppenspezifische, abgestufte Rechteverwaltung auf Laufwerke, Freigabe, Unterverzeichnis- und Dateiebene.
 - Aufbewahrung von Daten, z.B. auf Speichermedien, in einem Panzerschrank, o.ä.
 - Einsatz von Firewalls.

- Vermeidung gleichzeitiger identischer Netzwerkanmeldungen eines Benutzers.
- Administrativer Zugriff auf Netzkomponenten ist nur aus bestimmten IP-Bereichen möglich.
- Automatische passwortgeschützte Sperrung des Bildschirms nach spätestens 5-10 Minuten Inaktivität des Benutzers.
- Plausibilitätskontrollen bei Formularen.
- Weitergabekontrolle
 - Erstellung einer Übersicht, die erkennen lässt, an welchen Stellen während welcher Zeitspanne welche personenbezogenen Daten übermittelt werden konnten bzw. können.
 - Dokumentation der Abruf- und Übermittlungsprogramme.
 - Dokumentation der Abruf-, Übermittlungs- und Kommunikationswege und deren verwendete Hardware.
 - Protokollierung der Abruf- und Übermittlungsaktivitäten.
 - Remote-Zugriff auf Arbeitsplatzrechner nur nach anlassbezogener Einwilligung des Benutzers.
 - Regelung zum Remote-Zugriff auf Server.
- Mindestanforderungen an eine Passwortrichtlinie
 - Das Passwort besteht aus mindestens 10 Zeichen; bei administrativen Benutzerkonten oder Passwörter für verschlüsselte Datenträger, Container oder Dateien aus mindesten 12 Zeichen.
 - Das Passwort besteht mindestens aus drei der vier Zeichenklassen Groß-, Kleinbuchstaben, Ziffern oder Sonderzeichen (z. B. Satzzeichen).
 - Das Passwort ist nicht im Klartext und auch nicht reversibel verschlüsselt gespeichert. Entweder wird hierfür die Methode wie im folgenden Punkt beschrieben oder eine qualitativ äquivalente verwendet.
 - Zur irreversiblen Speicherung des Passwortes wird derzeit mindestens SHA2 oder besser verwendet. Dabei wird auf die Erhöhung der Entropie entweder durch ein kryptografisches „Salt“ oder einem „rehashen“ oder durch eine qualitativ äquivalente Methode bei der Speicherung geachtet.
 - Das Passwort wird durch den jeweiligen Benutzer eigenständig gewählt und eingegeben.
 - Das Passwort darf nicht leicht zu erraten sein. Insbesondere dürfen nicht verwendet werden
 - triviale Zeichenfolgen wie „1234“, „qwertz“, „asdf“, usw.,
 - Wörter, Begriffe oder Namen aus dem privaten oder beruflichen Umfeld oder auch Teile hiervon,
 - Daten, die man sich als Außenstehender leicht erschließen kann, wie Geburtsdatum, Ort, Straße, usw. zu denen die Person einen Bezug hat.
 - Sofern möglich oder erforderlich kann eine Zwei-Faktor-Authentifizierung mittels OTP- bzw. Token-Generatoren oder Chipkarte oder biometrischen

Verfahren in Kombination mit einem Passwort, das den obigen Richtlinien genügt, verwendet werden. Dies bietet eine erhöhte Sicherheit. Biometrische Identifizierungsverfahren sowie die OTP- bzw. Token- Generatoren oder Chipkarte alleine sind **keine** ausreichende Authentifizierung, da diese nur über Besitz funktionieren.

Maßnahmen beim Einsatz von SSD-Medien:

Da bei SSD-Medien - hierzu zählen auch USB-Sticks, SD-Karten o.ä. - durch mehrfaches Überschreiben (anders als bei magnetischen Festplatten) eine Löschung der Daten nicht gewährleistet ist, ist es in der Regel erforderlich, weitere Maßnahmen zu treffen. Hierzu zählen:

- Kryptografische Container
- Grundverschlüsselung des Mediums
- Vernichtung des Mediums nach DIN 66399

Die konkreten Maßnahmen sind je nach Art der gespeicherten personenbezogenen Daten im Einzelfall abzuwägen. Weitere Informationen zur Löschung von Daten auf SSD finden sie z.B. unter: <http://www.zendas.de/themen/vernichtung/ssd/loeschen.html>

12.4. Gewährleistung der Integrität

Diese Maßnahme dient dazu zu beschreiben, dass personenbezogene Daten nicht unbemerkt oder ungewollt geändert werden können.

Zu den Maßnahmen zählen beispielweise:

- Ausfüllanweisungen
- Plausibilitätskontrollen in den Eingabemasken oder durch nachgelagerte automatisierte oder manuelle Prozesse.
- Automatisierte Protokollierung der Dateneingabe, -änderung oder -löschung.
- Automatisierte Protokollierung der Benutzer- und Administrator-Aktivitäten.
- Sicherung der Protokolldaten gegen Verlust oder Veränderung.
- Zentrale Protokollierung über einen Protokollierungsserver.
- Personalisierte Benutzerkonten
- Dokumentation der Eingabeprogramme und Schulung der Mitarbeiter, die die Programme bedienen.
- Dokumentation der Personen, die zur Dateneingabe, Änderung oder Löschung berechtigt sind.
- Protokollierung der Aktivitäten auf dem Server.
- Durchsetzen des Vier-Augen-Prinzips, wo erforderlich.
- Organisatorische Regelung für die regelmäßige manuelle oder automatische Auswertung der Protokolle nach vorher definierten Auffälligkeitsmustern.

Darüber hinaus fordert der § 15 DSGVO die Angabe zu „Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen“. In der Regel bedeutet dies, dass ein verstärkter Fokus auf die benutzerspezifische Protokollierung der Dateneingabe, -änderung und -löschung oder ähnlicher geeigneter Maßnahmen gelegt werden muss.

12.5. Gewährleistung der Verfügbarkeit

Diese Maßnahme soll sicherstellen, dass die personenbezogenen Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn diese gebraucht werden.

Zu den Maßnahmen zählen beispielweise:

- Verfügbarkeitskontrolle
 - Installation einer unterbrechungsfreien Stromversorgung (USV).
 - Verwendung von geeigneten Behältern (z.B. Tresoren, Schränken) zur Aufbewahrung von Sicherungsmedien.
Einsatz eines Anti-Virenprogramms.
 - Supportverträge für Hardware oder Software mit einer festgelegten Reaktionszeit.
 - Für Testzwecke werden keine Originaldateien oder Originaldaten verwendet, sondern Kopien oder Testdaten.
 - Brandschutzmaßnahmen wie zum Beispiel Rauchmelder, Brandfrühsterkennung, Brandabschnitte, CO₂-Löscher, Reduzierung oder Vermeidung von Brandlasten usw.
- Auftragskontrolle
 - Dokumentiertes und umgesetztes Datenschutzkonzept des Auftragsverarbeiters zu den getroffenen technischen und organisatorischen Maßnahmen.
 - Dokumentiertes und technisch umgesetztes IT-Sicherheitskonzept des Auftragsverarbeiters.
 - Schutzmaßnahmen auf Seiten des Verantwortlichen, um die wechselseitige Beeinflussung von Daten verschiedener Aufträge zu verhindern (logisch/physikalisch/funktional getrennte Verarbeitung der Daten)
 - Datenschutzgerechte Löschung der Daten nach Beendigung des Vertrags (ggf. Rückgabe an Verantwortlichen oder Löschung)
 - Regelmäßige Kontrolle des Auftragsverarbeiters durch den Verantwortlichen.
 - Regelungen im Falle von datenschutzrechtlicher Verstöße des Auftragsverarbeiters.

12.6. Gewährleistung der Belastbarkeit der Systeme

Diese Maßnahme soll sicherstellen, dass die Systeme, die die personenbezogenen Daten verarbeiten sowohl den Belastungen des regulären Betriebs als auch punktuell hohen Belastungen standhalten. Insbesondere bei den punktuell hohen Belastungen darf das System nicht in dem Sinn kippen, dass es Übertragungs-, Lese- oder Schreibfehler produziert und damit die personenbezogenen Daten korrumpiert oder zerstört. Idealerweise ist das System so konzipiert, dass es transaktionsorientiert nach dem ACID-Prinzip (siehe: [https://de.wikipedia.org/wiki/Transaktion_\(Informatik\)#ACID-Prinzip](https://de.wikipedia.org/wiki/Transaktion_(Informatik)#ACID-Prinzip)) arbeitet.

Aspekte, die diese Maßnahmen betreffen sind beispielsweise:

- Hohe Netzwerklast durch punktuelle Massenverarbeitung oder durch einen Angriffsversuch wie zum Beispiel ein Denial of Service (DoS).
- Hohe Last auf Platten Ein- und Ausgabe bei zum Beispiel Datenbanken oder Dateisystemen.
- Hohe Prozessorlast, die das System derart beeinflussen, dass es zum Beispiel nicht mehr reagieren kann oder abstürzt und damit die Daten möglicherweise unbemerkt in einem inkonsistenten Zustand hinterlässt.
- Fehlerhafte Daten dürfen nicht zu einer fehlerhaften Speicherung führen. Eingabedaten sind auf Plausibilität zu prüfen. Diese Plausibilitätsprüfung hat robust gegenüber Fehleingaben zu sein und darf das System nicht in einen inkonsistenten Zustand bringen.

12.7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Zu den Maßnahmen zählen beispielweise:

- Datensicherungskonzept und Notfallpläne (Was wird gesichert, wie wird gesichert, wann wird gesichert und wo werden die Backupmedien gelagert); Erstellung einer Dokumentation zum Ablauf und Wiederherstellung für Teile der Sicherung und einer vollständigen Wiederherstellung nach einem Totalausfall.
- Redundante Datenspeicherung
- Doppelte IT-Infrastruktur
- Schatten-Rechenzentrum
- Vermeidung von Single Point of Failure. Dies heißt, dass kritische Komponenten derart redundant ausgelegt sind, dass der Ausfall einer dieser Komponenten nicht den Ausfall des gesamten Systems bewirkt.

12.8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Zu den Maßnahmen zählen beispielweise:

- Entwicklung eines Sicherheitskonzepts.

- Prüfungen des DSB, der IT-Revision.
- Externe Prüfungen, Audits, Zertifizierungen.
- Regelmäßige Abstimmung zwischen den IT- und Datenschutz-Verantwortlichen.
- Festlegung von Regeln, Standards und Normen für die Entwicklung, Freigabe und Tests von DV-Verfahren (z. B. Projektrichtlinien, Programmierhandbuch).
- Einhaltung von (Qualitäts-)Standards und Normen beim Einsatz von DV-Verfahren (z.B. DIN-Normen, ISO-Normen, BSI-Grundschutz, BSI Best Practices).
- Beschreibung der Verfahren, wie und wann Aktualisierungen evaluiert und eingespielt werden, damit die eingesetzte Software auf einem aktuellen Stand ist.

12.9. Weitere Maßnahmen

Teilweise nehmen Landesgesetzgeber Konkretisierungen der in Art. 32 DSGVO genannten Maßnahmen vor bzw. regeln TOM, um dem Erfordernis nach „angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ im Falle der Verarbeitung von Daten im Sinne von Art. 9 DSGVO nachzukommen (z.B. § 15 DSG NRW).

Einige davon sind hier aufgeführt und können angekreuzt bzw. weiter beschrieben werden.

Spezifische Verfahrensregelungen zur Sicherstellung der gesetzlichen Anforderungen im Falle einer Übermittlung können beispielsweise Nutzungsbedingungen sein, wie mit den Daten nach der Übermittlung im Weiteren zu verfahren ist (z.B. Begrenzung der Speicherdauer beim Empfänger, Nutzung durch den Empfänger nur zu festgelegten (Forschungs-)Zwecken).

Außerdem können zusätzliche TOM beschrieben werden, die nicht zu einem der vorstehenden Punkte passen.

12.10. Weitere Dokumente

Sofern eines dieser aufgelisteten Dokumente vorhanden ist und Bestandteil des Verfahrens sein soll, kann dies hier kenntlich gemacht werden. Diese können entweder einzelnen oder mehrere technische und organisatorische Maßnahmen in der Beschreibung ergänzen oder ersetzen. Im Übrigen gilt dasselbe, wie bei 2.2.12. eingangs gesagt wurde, dass zu bedenken ist, dass diese Dokumente im Einzelfall der Aufsichtsbehörde zur Verfügung gestellt werden müssen.

13. Datenschutz-Folgenabschätzung

Die Angabe erfolgt in Erfüllung der Rechenschaftspflicht.

Dieser Text basiert auf einer Vorlage der Zentrale Datenschutzstelle der baden-württembergischen Universitäten (ZENDAS)
Stand: Mai.2018

Eine Datenschutz-Folgenabschätzung ist in den Fällen des Art. 35 DSGVO erforderlich. Absatz 3 enthält eine nicht abschließende Aufzählung von Fallgestaltungen. Darunter ist der Fall aufgeführt, dass eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftatgen gemäß Artikel 10 DSGVO erfolgt.

Völlig offen hat der Gesetzgeber leider gelassen, wann eine Verarbeitung „umfangreich“ ist.

In Betracht kommen dürften hier vor allem Forschungsprojekte aus dem Bereich der Medizin, Psychologie und Soziologie.

Eine etwaig erforderliche Datenschutz-Folgenabschätzung muss getrennt vom VVT erfolgen, braucht in der Regel jedoch als Grundlage die Angaben im VVT.