Gegenüberstellung der rechtlichen Anforderungen und Empfehlungen zum Verzeichnis von Verarbeitungstätigkeiten (VVT)*

(Stand: 21.01.2023)

Rechtliche Anforderungen laut DSGVO / DSK - Empfehlungen

Rechtliche Anforderungen laut DSGVO		DSK - Empfehlungen
Pflichtangaben DSGVO - Artikel 30 Abs. 1: Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:		*Mustervorlage (PDF):* *https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf* *Hinweise:* *https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf*
lit. a	**Den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten**	Anzugeben sind die postalische, elektronische und telefonische Erreichbarkeit, um zu gewährleisten, dass die Aufsichtsbehörde den Verantwortlichen auf einfachem Wege (und in Eilfällen auch über verschiedene Kanäle) erreichen kann (s.a. WP 243, Ziff. 2.6). Bei Behörden und juristischen Personen sind nicht zwingend Daten zu Leitungspersonen gefordert, aus aufsichtsbehördlicher Sicht ist die Angabe des operativ verantwortlichen Ansprechpartners wünschenswert. Dementsprechend sollte ein Eintrag unter „Ansprechpartner“ erfolgen. Zzgl. evtl. Vertreters für in Drittstaaten ansässige Verantwortliche (Art. 4 Nr. 17, Art. 27 DS-GVO).
lit. b	**Die Zwecke der Verarbeitung**	Je Beschreibung einer Verarbeitungstätigkeit ist der Verarbeitungszweck zu dokumentieren. Für jede Verarbeitung sind vorher die Zwecke festzulegen. Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann. Es ist zu empfehlen, den Namen der jeweiligen Verarbeitungstätigkeit von dem Verarbeitungszweck ausgehend festzulegen (z. B. „Personalaktenführung“/“Stammdaten“, „Lohn-, Gehalts- und Bezügeabrechnung“ usw.).
lit. c	**Eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten**	Zu beschreiben sind die Kategorien betroffener Personen und die Kategorien personenbezogener Daten. Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO sollte gesondert beschrieben werden (Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person). Dabei empfiehlt es sich hinsichtlich der einzelnen Kategorien personenbezogener Daten laufende Nummern zu vergeben, die so eine Zuordnung zu den weiteren konkreten Angaben gem. Art. 30 Abs. 1 S. 2 lit. d bis g DS-GVO ermöglichen, z. B. zu konkreten Löschregeln. Aufgegliedert z. B. in der Darstellung der „Kategorie Beschäftigte“ und „Kategorie Kundendaten“ in die unterschiedliche Daten-Kategorien.
lit. d	**Die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen**	Zu beschreiben sind die Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Empfänger können auch Teile eines Unternehmens oder einer Behörde sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist (z. B. 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 Angaben zu den zugriffsberechtigten Personen sind nach der DS-GVO zwar nicht vorgesehen. Es wird jedoch empfohlen, Angaben zu diesen zu machen. 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 werden, 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 Mailversand 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.
lit. e	**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**	Angaben zu Übermittlungen von personenbezogenen Daten in 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 DS-GVO 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 DSGVO im Verzeichnis der Verarbeitungstätigkeiten aufnimmt.
lit. f	**Wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien**	Angabe der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, z. B. o die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten, Kundendaten etc. o geltende Aufbewahrungs- und Löschfristen für Schülerdaten, Prüfungsunterlagen etc. o gesetzlich vorgesehene Löschungsfristen (z. B. § 14 Bundesmeldegesetz) o vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, vielmehr sind präzise Angaben erforderlich.
lit. g	**Wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1**	Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar. Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DS-GVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept). Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DSGVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen. Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.

Sind die Anforderungen/Empfehlungen in den Mustern der Aufsichtsbehörden übernommen worden

	BW	Bayern	Schleswig-Holstein	Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrheinwestfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Thüringen
	Mustervorlage (MS Excel) *https://www.baden-wuerttemberg.datenschutz.de/praxishilfen/#verarbeitungsverzeichnis_und_loeschkonzeption*	*Muster-VVTs (MS Word)* *https://www.lda.bayern.de/de/suche.html?q=vvt&submit=Suchen#/?h=kYBNv4IBUDDqi9dfbZVE(- Suche nach "Verzeichnis der Verarbeitungstätigkeiten"*	Muster-VVT (MS Word) https://www.datenschutzzentrum.de/dokumentation/	
lit. a	✗	✓	✓	
lit. b	✓	✓	✓	
lit. c	✓	✓	Vergeben Sie für die unterschiedlichen Betroffenenkategorien laufende Nummern, so können Sie später bei den verarbeiteten Daten (Datenkategorien) auf die entsprechenden Betroffenenkategorien verweisen.Vergeben Sie für die unterschiedlichen Datenkategorien laufende Nummern, so können Sie später bei den Daten-übermittlungen und den Speicherfristen auf die entsprechenden Datenkategorien verweisen. ✓	
lit. d	✓	✓	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. ✓	
lit. e	✓	✓	✓	Verweis auf die Mustervorlagen (MS Word) der DSK (siehe Spalte "DSK-Empfehlungen") ✓
lit. f	Löschkonzept mit detaillierten Angaben direkt im VVT enthalten ✓	Löschfristen *(z.B. 10 Jahre (Gesetzliche Aufbewahrungsfrist)* ✓	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. ✓	
lit. g	✗	Im Muster steht meist: siehe IT-Sicherheitskonzept *(unter dem VVT als Extra-Zeile dann auch: "Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen)" mit ein paar Beispielen)* ✓	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. ✓	

Sind die Anforderungen/Empfehlungen von diesen Quellen übernommen worden

	Bitkom	GDD
	Leitfaden und Muster (MS Word) *https://www.bitkom.org/sites/main/files/file/import/180529-LF-Verarbeitungsverzeichnis-online.pdf*	**Praxishilfe und Muster (MS Word)** *https://www.gdd.de/aktuelles/startseite/ueberarbeitete-gdd-praxishilfe-zum-verzeichnis-von-verarbeitungstaetigkeiten-verantwortlicher-online/resolveuid/e165bbd908e84f939c40df38077027b9*
lit. a	✓	Im Vorblatt 1 werden Angaben zum Verantwortlichen erfasst, im Vorblatt 2 (optional) Angaben zu übergreifenden Regelungen und Sachverhalten. Hierdurch sollen sich ansonsten wiederholende Angaben nur einmal dokumentiert werden, um den Pflegeaufwand zu erleichtern. Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind im VVT Name und Kontaktdaten (ladungsfähige Anschrift) des oder der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift). ✓
lit. b	Aus der Zweckbestimmung muss sich die Rechtsgrundlage für die Datenverwendung ableiten lassen. In der Praxis werden die Aufgaben und Ziele der einzelnen Prozesse genannt, beispielsweise »Personalmanagement«. ✓	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. ✓
lit. c	✓	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. ✓
lit. d	Es empfiehlt sich in der Regeln eine Benennung der natürlichen oder juristischen Personen, Behörden, Einrichtungen oder anderen Stellen, die Daten planmäßig erhalten sollen. Unabhängig davon, ob es sich um eine aktive Übertragung oder einen Direktzugriff des Empfängers auf die Verarbeitung handelt. ✓	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten, z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw. Laut Gesetz sind nur die Kategorien von Empfängern anzugeben. Bei genauerer Darstellung sind spätere Änderungen zu berücksichtigen und die regelmäßige Pflege der Angaben ist zu gewährleisten. ✓
lit. e	Bei Datenübermittlungen nach Art. 49 Absatz 1 Untersatz 2 handelt es sich um Übermittlungen, die ausnahmsweise zulässig sind, obwohl weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt, noch geeignete Garantien nach Art. 46 bestehen. ✓	Drittländer sind solche außerhalb der EU/des EWR. Beispiele für internationale Organisationen: Institutionen der UNO/EU. Lediglich in Ausnahmefällen wird es erforderlich sein, Angaben zu geeigneten Garantien anzugeben, nämlich dann, wenn keine der genannten Garantien vorliegt, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DS-GVO). D.h. falls es sich bspw. um ein Drittland mit Angemessenheitsbeschluss der EU-Kommission handelt, EU-Standarddatenschutzklauseln abgeschlossen wurden, die Datenübermittlung unter dem Schirm des EU-US Privacy Shield erfolgt, oder verbindliche interne Datenschutzvorträge vorliegen, sind nähere Angaben zu den Garantien nicht erforderlich. ✓
lit. f	Das »wenn möglich« ist nicht optional zu verstehen, sondern so, dass eine Löschregel in dem jeweils möglichen Konkretisierungsgrad angegeben werden soll. *HINWEIS EMODEON: in den Mustern steht oftmals nur "nach Ablauf von handels- und steuerrechtlichen Aufbewahrungsfristen".* ✓	Vorsicht vor der Formulierung „wenn möglich“ in Art. 30 Abs. 1 lit. f und g DS-GVO: Es wird erwartet, dass diese Informationen vorliegen. Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus. ✓
lit. g	Hier kann auf das allgemeine Sicherheitskonzept / übergreifende TOMs verwiesen werden, so dass nur Abweichungen davon für das jeweilige Verfahren extra aufgeführt werden müssen. ✓	Vorsicht vor der Formulierung „wenn möglich“ in Art. 30 Abs. 1 lit. f und g DSGVO: Es wird erwartet, dass diese Informationen vorliegen. 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. ✓

Was wurde in die EMODEON-Vorlage übernommen

	EMODEON *Mustervorlage (MS Excel)*
lit. a	Extra Tab "Angaben zum Verantwortlichen" mit Kontaktmöglichkeiten (Name, Adresse, Telefon, E-Mail) für: o Verantwortlichen (oder operativ Verantwortlichen) / o Vertreter des Verantwortlichen o Bei Verantwortlicher Stelle in Drittstaaten: Im Inland ansäßiger Vertreter o Datenschutzbeauftragter / o Optional: operativ verantwortlicher Ansprechpartner für die Aufsichtsbehörden Plus zuständige Fachabteilung bei jeder der Verarbeitungstätigkeiten im Tab "Verarbeitungsverzeichnis". Hier pro Fachabteilung eine Spalte, damit gefiltert (z.B.: "Welche Fachabteilung verantwortet welche Verarbeitungstätigkeit") und der Name des Fachverantwortlichen auch leicht geändert werden kann. ✓
lit. b	Pro Verarbeitungstätigkeit gibt es im VVT eine Spalte für die <u>Bezeichnung der Verarbeitungstätigkeit</u> sowie eine weitere Spalte für die <u>genauere Beschreibung des Zwecks der Verarbeitungstätigkeit</u>. ✓
lit. c	Pro Kategorie der betroffenen Person gibt es eine Spalte. Dies ermöglicht auch ein Filtern (z.B.:"Welche Betroffenen sind in welcher Verarbeitungstätigkeit involviert"). Somit ist auch eine Nummerierung nicht notwendig. ✓ Die Kategorien personenbezogener Daten (z.B. "Mitarbeiter Stammdaten") sind detailliert nach Datenfeldern (Vorname, Nachname usw.) aufgeführt, da somit auch auf einen Blick gesehen werden kann, welche Daten GENAU in welcher Verarbeitungstätigkeit verarbeitet werden. Besondere Kategorien personenbezogener Daten sind farblich hervorgehoben. Ist das Unternehmen größer oder werden sehr viele unterschiedliche pbD verarbeitet, empfiehlt es sich, die detaillierten Datenfelder in einem separaten Dokument der Datenarten und Löschregeln aufzuführen.
lit. d	Empfängerkategorien (Datenempfänger oder Zugriffsberechtigte) werden in Spalten dargestellt mit der Unterteilung nach: o Intern (z.B. Name der Fachabteilung) o Extern (auch Zusammenfassung von Gruppen von externen Dienstleistern, z.B. "Finanzdienstleister". Hier dann als Kommentar noch näher erläutern, um welche einzelnen Finanzdienstleister es sich handelt) o Drittland (Name des Landes oder der internationalen Organisation) sowie im Kommentarfeld auch Name der eingesetzten Software) Die DSK-Empfehlung bezüglich der Nennung der Zugriffsberechtigten wurde umgesetzt, indem in der jeweiligen Zelle der Empfänger-Spalte pro Verarbeitungstätigkeit entweder ein "x" für Empfänger oder ein "z" für Zugriff der Daten (=Zugriffsberechtigter) steht. So kann auf einfachem Wege auch gefiltert werden. Dass es für die Verarbeitungstätigkeit <u>keine Empfänger in einem Drittland</u> gibt, kann dadurch ermittelt werden, dass diese Zelle leer ist. Die <u>Übermittlung</u> von personenbezogenen Daten <u>in ein Drittland</u> wird in der untenstehenden Zeile beschrieben. ✓
lit. e	Pro Drittland gibt es eine Spalte (z.B. "USA"). Ein "x" in dieser Spalte besagt, dass eine Übermittlung der Daten in z.B. die USA erfolgt. So kann sehr gut gefiltert werden, bei welcher Verarbeitungstätigkeit eine Übermittlung in das jeweilige Drittland erfolgt. Daneben gibt es noch eine Spalte "Dokumentation der Garantien" , um bei einer Übermittlung der personenbezogenen Daten in ein Drittland hinterlegen zu können, welche Garantien dokumentiert wurden und auf welcher Grundlage. Hier wird auch der genaue Empfänger der pbD eingetragen. Falls keine Übermittlung in ein Drittland stattfindet, sollte in dieser Spalte ein Vermerk "Keine Übermittlung der Daten in ein Drittland" eingetragen werden. ✓
lit. f	Es gibt einen Unterschied zwischen Löschfristen und Aufbewahrungsfristen. Im VVT selbst sind die Aufbewahrungs- und Löschfristen in einer Spalte hinterlegt. Separate Spalten mit den Aufbewahrungs- und Löschfristen pro Verarbeitungstätigkeit bzw. den enthaltenen Datenarten mit allen weiteren relevanten Daten zur Löschung sind dann in einem separten Dokument aufgelistet. *Grund: zum einen, um das VVT nicht aufzublähen und zum anderen, da die Inhalte unterschiedliche Zielgruppen haben (VVT = DSB / Löschregeln = DSB sowie jeweilige Fachbereiche).* *Denn: kein Dokument ohne Mehrwert für den jeweiligen Fachbereich bzw. das Unternehmen!* ✓
lit. g	Es ist eine Spalte für die Beschreibung der technischen und Organisatorischen Maßnahmen (TOMs) vorhanden. Hier kann dann ein Link z.B. auf ein übergreifendes Sicherheitskonzept hinterlegt oder auch eventuelle Abweichungen erläutert werden. *Siehe Beispiele in den Vorlagen.* ✓

Empfehlungen für weitere Informationen im VVT, die nicht in der DSGVO gefordert sind

Empfehlung	DSK
Rechtsgrundlage bzw. Nachweis der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a und Art. 6 DSGVO	Es bietet sich an, das Verzeichnis sinnvollerweise auch folgendermaßen einzusetzen bzw. zu verwenden: o als Nachweis der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 lit. a DS-GVO
Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DS-GVO	o Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren o Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren o Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen o Dokumentation von Einwilligungen und Widersprüchen o Protokollierung von Zugriffen und Änderungen o Nachweis der Quellen von Daten (Authentizität) / o Versionierung o Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts o Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept
Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DS-GVO	o Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten o programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten o regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung o Trennung nach Organisations-/Abteilungsgrenzen o Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens o Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle o Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten / o geregelte Zweckänderungsverfahren
Maßnahmen zur Gewährleistung der Betroffenenrechte (Intervenierbarkeit) – Art. 13 ff. DS-GVO	o differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten o Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen o dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes o Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem o Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen o Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte o Einrichtung eines Single Point of Contact (SPoC) für Betroffene o operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
Änderungshistorie	Um Änderungen der Eintragungen im Verzeichnis nachvollziehen zu können (z. B. wer war wann Verantwortlicher, Datenschutzbeauftragter etc.), sollte eine Dokumentation der Änderungen mit einer Speicherfrist von einem Jahr erfolgen. Dies lässt sich auch aus dem Grundsatz der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO herleiten
Referenzdokumente	Es wird empfohlen, weitere Bausteine einer umfassenden Dokumentation der Datenschutzstrategie, wie z. B. o die Dokumentation interner Verhaltensregeln, o die Dokumentation einer Risikoanalyse oder allgemeinen Datensicherheitsbeschreibung, o ein umfassendes Datensicherheits- oder Wiederanlaufkonzept, / o ein Zertifikat oder o Ergebnisse einer Datenschutz-Folgenabschätzung am Ende der Dokumentation der Verarbeitungstätigkeit unter „Sonstiges“ als Referenz anzugeben. Auf Nachfrage können diese Referenzdokumente zusätzlich zum Verzeichnis der Aufsichtsbehörde vorgelegt werden; es ist sinnvoll, zumindest die für das Verständnis und die Bewertung des Verarbeitungsverzeichnisses essentiellen zusätzlichen Dokumente bereits im ersten Schritt freiwillig mitzuliefern. Insofern stellen die zusätzlich aufgeführten Dokumentationen keine Anlagen zum Verzeichnis dar, sondern weitere, darüber hinausgehende Bausteine einer umfassenden Dokumentation der organisationsinternen Datenschutzstrategie, auf welche verwiesen werden und die neben dem Verzeichnis vorgehalten werden können. Sie dienen zusammen mit dem Verzeichnis der Umsetzung der aus Art. 5 Abs. 2 DS-GVO resultierenden Rechenschaftspflicht. Wird innerhalb des Verzeichnisses auf andere Dokumente, wie z. B. ein anderes Verarbeitungsverzeichnis Bezug genommen, so ist dies an dieser Stelle als Referenzdokument aufzuführen.

Wurden die weiteren Empfehlungen der DSK von den Aufsichtsbehörden der Ländern übernommen

Empfehlung	BW	Bayern	Schleswig-Holstein	Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrheinwestfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Thüringen
Rechtsgrundlage	✓	✗	Einzelne Fragen zu Art. 6 Abs. 1 lit. a-f DSGVO: 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). ✓	
Transparenz	Spalten (Relevante Systeme) für: o kommende Datenflüsse o verarbeitendes System o gehende Datenflüsse ✓	✗	<u>Einzelne Seiten im Dokument zum Ausfüllen:</u> o verwendete Programme (Software) o Speicherort o IT-Geräte, auf denen die Programme installiert sind o Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen o Maßnahmen zur Protokollierung der Verarbeitungstätigkeit o Prüfung der Datenverarbeitung o Test und Freigabeverfahren o Dokumentation von Test- und Freigabeverfahren *Hilfestellungen und Beispiele sind in den Ausfüllhinweisen enthalten.* ✓	
Zweckbindung	✗	✗	Einzelne Seiten im Dokument zum Ausfüllen: o Dokumentation der Berechtigungen der aufgeführten Programme (Benutzer und Administration) *Hilfestellungen und Beispiele sind in den Ausfüllhinweisen enthalten.* ✓	
Betroffenenrechte	✗	✗	<u>Einzelne Seiten im Dokument zum Ausfüllen:</u> o Maßnahmen zur Sicherstellung der Informationspflicht des Verantwortlichen o Maßnahmen zu Auskunftsansprüchen von betroffenen Personen o Maßnahmen zur Berichtigung von personenbezogenen Daten o Maßnahmen zur Löschung von personenbezogenen Daten o Maßnahmen zur Einschränkung der Verarbeitung o Maßnahmen zur Gewährleistung der Datenübertragbarkeit *Hilfestellungen und Beispiele sind in den Ausfüllhinweisen enthalten.* ✓	Verweis auf die Mustervorlagen der DSK (siehe Spalte "DSK-Empfehlungen") ✓
Änderungshistorie	✓	✗	✓	
Referenzdokumente	✗	✗	<u>Zur DSFA:</u> 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. ✓	

Sind die weiteren Empfehlungen der DSK von anderen Quellen übernommen worden

Empfehlung	Bitkom	GDD
Rechtsgrundlage	Neben der verpflichtenden Erfassung des Verarbeitungszwecks sollte zur Erfüllung der Rechenschaftpflichten gem. Art. 5 auch die Rechtsgrundlage mitsamt ggfs. erforderlicher Abwägungen, Einwilligungsklauseln und Prüfvermerken, ob bspw. die Anforderungen an Widerspruchsmöglichkeiten oder die automatisierte Einzelentscheidung berücksichtigt wurden. ✓	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. ✓
Transparenz	✓	<u>Wesentliche Prozessschritte</u> Hiermit ist eine Übersicht über die einzelnen Verarbeitungsschritte gemeint, z.B. in chronologischer Form. Es kann auch auf Datenflussdiagramme o.ä. verwiesen werden. <u>Beteiligte IT-Systeme</u> 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. Falls personenbezogene Daten auch in Nicht-Produktivsystemen verarbeitet werden, sollten hier entsprechende Angaben zur Rechtmäßigkeit sowie zu Schutzmaßnahmen gemacht werden. ✓
Zweckbindung	Bezieht sich auf Art. 5 Abs.1 c-e: Datenminimierung/Privacy by design/Privacy by default: Dies kann bspw. durch einen Prüfvermerk des Datenschutzbeauftragten, ob diese Grundsätze nach seiner Einschätzung ausreichend berücksichtigt wurde, dokumentiert werden. Richtigkeit der Daten/Speicherbegrenzung / Löschung oder Einschränkung der Verarbeitung: Dokumentation bspw. durch Referenz auf Maßnahme. ✓	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. ✓
Betroffenenrechte	<u>Art. 12-14: Informations- und Benachrichtigungspflichten</u> a) Vollständigkeit der Informationen, b) Einhaltung der Fristen, c) Formvorgaben Es sollte je Verfahren dokumentiert werden, wo und wie den Informationspflichten jeweils nachgekommen wird. Dies kann bspw. durch Verweis auf Datenschutzhinweise, Vertragsbestandteile, Disclaimer in Formularen, bei Mitarbeiterdaten z.B. auch durch Verweise bei Erhebung auf intern bekanntgemachte Betriebsvereinbarung etc. erfolgen. <u>Art. 20 Datenportabilität</u> Es sollte erfasst werden, ob für dieses Verfahren ein Anspruch seitens des Betroffenen besteht, wenn ja für welche Datenkategorien (ggfs. einschließlich Begründung). Es sollte der Stand der Umsetzung bzw. geplante Maßnahmen erfasst werden. ✓	<u>Wie und zu welchem Zeitpunkt werden die Informationspflichten erfüllt?</u> Hier ist zu dokumentieren, wie die Informationspflichten nach Art. 12-14 DS-GVO erfüllt werden. <u>Wahrung der (weiteren) Betroffenenrechte</u> 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 ✓
Änderungshistorie	✓	✓
Referenzdokumente	<u>Zur DSFA:</u> Es sollte das Ergebnis der Prüfung, ob eine DSFA erforderlich ist oder nicht einschl. Begründung dokumentiert werden. Sofern eine DSFA durchgeführt werden muss, sollte die DSFA ausführlich dokumentiert werden. ✓	<u>Ergänzende Dokumente und Unterlagen</u> Hier sollten ggfs. relevante Datenflusspläne, Handbücher, Lasten-, Pflichtenhefte, Produktbeschreibungen, Internet-Adressen zu Produkten, Angaben zu Datenquellen und Schnittstellen etc. beigefügt oder verlinkt werden. <u>Zur DSFA:</u> 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. ✓

Was von den weiteren Empfehlungen wurde in die EMODEON-Vorlage übernommen

Empfehlung	EMODEON
Rechtsgrundlage	Für Art. 6 Abs. 1 a-f ist je eine Spalte zum Ankreuzen vorhanden. Dies ermöglicht auch ein Filtern (z.B.:"Welche Verarbeitungstätigkeit beruht auf Art. 6 Abs. 1 lit. a" - für lit. a gibt es auch eine zusätzliche Spalte für den Nachweis der Einwilligung). Für Art. 6 Abs. 1 a-f ist darüber hinaus der genaue Gesetzestext sowie ggf. weitere Erläuterungen des jeweiligen Artikels als Kommentar hinterlegt. Darüber hinaus gibt es noch eine Spalte für weitere Rechtsgrundlagen. Für jede Rechtsgrundlage ist eine kurze Erklärung vorhanden (z.B. bei Bewerbungen: *§ 15 Abs. 4 i.V.m. Abs. 1 AGG - (Anspruch muss innerhalb von 2 Monaten geltend gemacht werden*) ✓
Transparenz	o Je eine Spalte pro verwendete Software für die Verarbeitungstätigkeit o Je eine Spalte für den Speicherort der personenbezogenen Daten (digital/analog) o Eine Spalte für das Datenflußdiagramms. Hier sollte nur angegeben werden, ob es vorhanden ist oder nicht (ja/nein) inkl. den Link auf den Ablageort o Eine Spalte für das Test- und Freigabekonzept sowie Protokollierung von Zugriffen und Änderungen. Hier sollte nur angegeben werden, ob vorhanden oder nicht (ja/nein) inkl. den Link auf den Ablageort *<u>Hinweise:</u>* *o bei einer komplexeren IT-Architektur sollten die IT-Systeme in einem separaten (Excel)Dokument aufgeführt werden* *o die IT-Systeme, Datenbestände und Datenflüsse erstelle ich im Zuge des Löschkonzepts zur Erzeugung von Transparenz anhand einer IT-Architekturübersicht* ✓
Zweckbindung	Eine Spalte für (Zugriffs)Berechtigungen und Rollen. Hier sollte nur angegeben werden, ob ein solches Konzept vorhanden ist oder nicht (ja/nein) inkl. den Link auf den Ablageort der Dokumentationen. Es würde zu weit führen, diese Informationen gesammelt in das VVT zu übertragen. ✓
Betroffenenrechte	Für Art. 15 ff. je eine Spalte zum Ankreuzen mit der Erläuterung des jeweiligen Artikels als Kommentar. Hierdurch kann gewährleistet werden, dass an alle Betroffenenrechte gedacht wurde. Daneben gibt es noch Spalten für den Link auf die Maßnahmen/Prozesse sowie auf Datenschutzerklärungen / Maßnahmen zur Sicherstellung der Informationspflicht ("Recht auf transparente Information") nach Art 12,13,14 DSGVO. *Hinweis:* *Zur besseren Veranschaulichung würde ich eine grafische Darstellung der Prozesse empfehlen. Am besten BPMN, es reicht aber auch jede andere anschauliche Darstellung.* ✓
Änderungshistorie	Dokumentationsmöglichkeit für Änderungen im Deckblatt (extra Tab) vorhanden. ✓
Referenzdokumente	Extra Tab für "Übergreifende Regelungen und Dokumente". Inklusive Zeilen für die Schwellwertanalyse und die Datenschutzfolgenabschätzung (vorhanden ja/nein und Link auf Dokumentationen) ✓

* Kein Anspruch auf 100% Korrektheit, da jede Stelle die Empfehlungen anders auslegt bzw. aufgliedert. Anregungen/Änderungswünsche jederzeit gern an nfolchert@emodeon.de.