Baustein 42 „Dokumentieren“

Version: V1.0a
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Dokumentieren_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_Dokumentieren_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit. a DS-GVO)	Transparenz
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2 DS-GVO)	Transparenz
Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO)	Transparenz

2. Beschreibung

Das Dokumentieren ist neben dem Spezifizieren und dem Protokollieren der Verarbeitung Teil des Datenschutzmanagements und trägt maßgeblich dazu bei, den ordnungsgemäßen Betrieb einer Verarbeitungstätigkeit und die Einhaltung spezifischer datenschutzrechtlicher Vorschriften kontrollieren und prüfen zu können. Dabei umfasst das Dokumentieren die Beschreibung der Verarbeitung, insbesondere unter Ausweis des Zwecks der Verarbeitungstätigkeit und der Zweckbindung der verarbeiteten Daten. Es dient dazu, die rechtmäßige Verarbeitung dauerhaft sicherstellen und nachweisen zu können, sowohl für die Organisation selbst als auch anderen Organisationen und Aufsichtsbehörden gegenüber. Das Dokumentieren unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten und der Gewährleistung der Auskunftsrechte gegenüber den betroffenen Personen.

Eine Dokumentation dient der Sicherung der Transparenz insbesondere

- von Datenbeständen,
- von Transformationen zwischen Daten,
- der benutzten Systemkomponenten, deren Funktionen und Schnittstellen,
- der Prozesse innerhalb von IT-Systemen und Organisationen und über IT-Systemgrenzen und Organisationsgrenzen hinweg und
- der Nachvollziehbarkeit von Entscheidungen und Verarbeitungshandeln.

Transparenz ist keine gegebene Eigenschaft einer Verarbeitungstätigkeit, sondern muss als eine Anforderung, insbesondere durch Dokumentieren, hergestellt werden. Zur Umsetzung des Gewährleistungsziels Transparenz ist es sowohl erforderlich, die Verarbeitungstätigkeit selbst umfassend zu dokumentieren (inhaltliche Anforderungen), als auch zu dokumentieren, *wie* das Dokumentieren und deren Strukturierung erfolgt (formale Anforderungen). Die formalen Anforderungen an eine Dokumentation können klar festgelegt werden, die inhaltlichen Anforderungen hingegen können nur musterhaften Charakter haben, da sie immer von der Struktur der Organisation und der Verarbeitung anhängig sind.

Formale Anforderungen an die Dokumentation sind daher insbesondere:

- die **Strukturierung der Gesamtdokumentation** (M42.P01) einer Organisation. Die Dokumentation einer Organisation sollte in Module gegliedert werden. Ein Modul ist die datenschutzrechtlich und sicherheitstechnisch erforderliche Dokumentation. Andere Module können aus Dokumentationsanforderungen anderer Regulierungs- und Kontrollinstanzen (Wirtschafts- und Steuerprüfungen, Rechnungshöfe, Umweltauflagen etc.) resultieren. Wenn in einem Dokument auf ein anderes Dokument auch Modul-übergreifend verwiesen wird, so muss das referenzierte Dokument auch verfügbar sein.
- Eine Dokumentation darüber, welcher Teil der Dokumentation der Verarbeitung als **Papierausdruck** und welcher Teil **elektronisch** (M42.P02) vorliegt. Wenn eine (Teil-)Dokumentation elektronisch vorliegt, so ist für diesen Teil ein aktuelles Backup-Medium (M42.P03) vorzusehen, das von einem Systemausfall nicht betroffen wäre. Liegt eine Dokumentation im Produktivbetrieb primär elektronisch vor, sind Vorkehrungen auf Papier zu dokumentieren, wie bei einem Ausfall der IT zu verfahren ist, z. B. ein Verweis auf den Standort eines gesicherten Backupmediums inklusive Anleitung zur Verfügbarkeit der Dokumentation (Notfall-Management).
- Die **Angemessenheit** der Dokumentation: Dies erfordert, dass die Dokumentation tatsächlich bestehende datenschutzrechtliche Anforderungen erfüllt. Ein Übermaß an Dokumentierung gilt es dabei zu vermeiden. Es ist z. B. nicht angemessen, unbesehen vollständige Ausdrucke von Herstellerhandbüchern, Sicherheitsstandards oder Aktivitätsprotokolle zu einem Teil der Datenschutz-Dokumentation zu erklären. Insbesondere, wenn in solchen Herstellerhandbüchern unterschiedliche mögliche Maßnahmen aufgezeigt werden, muss aus der Dokumentation hervorgehen, welche konkreten Maßnahmen für die Verarbeitung, auf die sich die Dokumentation bezieht, realisiert wurden. Das Aufzeigen verschiedener Möglichkeiten ist somit für eine Dokumentation von Datenbeständen, IT-Systemen und Prozessen nicht ausreichend.
- Die **Vollständigkeit** einer Dokumentation: Diese ist dann gegeben, wenn alle Verarbeitungsprozesse mit allen rechtlichen Forderungen und allen Daten, Systemen und Diensten sowie Teilprozessen so erfasst sind, dass der Produktivbetrieb einer Organisation hinreichend genau und aktuell beschrieben und prüfbar ist. Die SDM-Methodik ist mit der Orientierung an Gewährleistungszielen und den damit verbundenen rechtlichen Anforderungen zum Erreichen von Vollständigkeit hilfreich.

Daneben können standardisierte Check-Listen oder ähnliche Hilfsmittel herangezogen werden.

- Die **Revisionsfestigkeit** einer Dokumentation: Dies bedeutet einerseits, dass der Stand der Dokumentation nachweisbar ist. Typischerweise lässt sich dies sicherstellen durch Versionierungs- und Fortschreibungsregeln (M42.P04). Zum anderen ist sicherzustellen, dass nur berechtige Personen auf die Dokumentation zugreifen und ggf. wiederum dokumentierte Änderungen vornehmen dürfen (M42.P05). Die zu ergreifenden Maßnahmen sind dabei abhängig:
    - vom Schutzbedarf,
    - der **Aktualität** der Dokumentation: Die Dokumentation muss regelmäßig aktualisiert werden, damit sie sich auf einem aktuellen Stand befindet,
    - der **Fortschreibung** der Dokumentation: Es sind Vorgaben darüber erforderlich, wie die Dokumentation fortgeschrieben wird (M42.P04). Bei maßgeblichen Änderungen an Verfahren muss das Nachführen der Dokumentation bereits im Planungsprozess berücksichtigt werden.

Die inhaltlichen Anforderungen an die Dokumentation können wie folgt musterhaft beschrieben werden:

Eine Dokumentation sollte aus Gründen der besseren Strukturierung modular aufgebaut sein (M42.P01). Sie kann sich an folgender Struktur orientieren und je nach Anforderungen an die konkrete Verarbeitung folgende Einzeldokumente enthalten:

- Eine übergreifenden Übersicht und Gliederung sowie Beschreibung des Aufbaus der Dokumentation inklusive der Aufbewahrungsorte und –medien sowie Namenskonventionen (M42.P06),
- Einbeziehung organistionsweit vorhandener, nicht-verarbeitungsspezifischer Dokumente (Rahmendokumentation):
    - Organigramm bzw. Geschäftsverteilungsplan (M42.P07),
    - übergreifende Geschäftsprozesse (Datenflüsse) (M42.P08),
    - Dokumentation der Bestellung des/der Datenschutzbeauftragten (M42.P09),
    - Netzpläne und Schnittstellendokumentationen (M42.P10),
    - Dienst-/Betriebsanweisungen und –vereinbarungen (M42.P11),
    - Rahmen-Datenschutzkonzept (Handbücher, übergreifende Schutzmaßnahmen, Verantwortliche und Ansprechpartner) (M42.P12),
    - Dokumentation der Datenschutzorganisation gemäß Art. 24 Abs. 1 DS-GVO (M42.P13),
    - ggf. Nachweise von Zertifizierungen für Datenschutz und Informationssicherheit (M42.P14),
    - ggf. IT-Konzept (M42.P15),
    - ggf. Risikohandbuch (M42.P16),
    - ggf. Sicherheitsrichtlinie (M42.P17),
    - ggf. Sicherheitskonzept (M42.P18),

    - ggf. Notfallkonzept (M42.P19),
- Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (M42.P20),
- Dokumentation der Umsetzung der Betroffenenrechte gemäß Erwägungsgrund 39 DS-GVO (M42.P21),
- Löschkonzept (M42.P22)
- ggf. Verträge zur Auftragsverarbeitung (M42.P23),
- für den Fall einer gemeinsamen Verantwortung die Vereinbarung zwischen den gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 DS-GVO (M42.P24)
- Konzept der Verarbeitung aus der Planungsphase (sowie bspw. Lastenheft und Pflichtenheft) (M42.P25),
- Dokumentation der eingeholten Einwilligungen gemäß Art. 7 Abs. 1 DS-GVO (M42.P26)
- Dokumentation der Schwellwert-Analyse einer Datenschutz-Folgenabschätzung (M42.P27),
- für den Fall einer erforderlichen Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO:
    - Bericht zur Datenschutz-Folgenabschätzung (M42.P28),
    - Nachweis der Wirksamkeit der ergriffenen Schutzmaßnahmen (M42.P29)
- Dokumentation für Ausnahmen für bestimmte Fälle von Übermittlungen gemäß Art. 49 Abs. 6 DS-GVO (M42.P30),
- Dokumentation von Sicherheitsvorfällen gemäß Art. 33 Abs. 2 DS-GVO (M42.P31),
- Protokollierungskonzept bzw. Dokumentation der genutzten Protokolle inklusive deren Aufbewahrungsorte, Aufbewahrungsfristen und Zugriffsregelungen (M42.P32),

Daten

Ein wesentlicher Bestandteil des Dokumentierens einer Verarbeitung besteht in der Dokumentation der Daten. Diese dient als Ausgangspunkt für die Beschreibung von Schnittstellen und für die gesetzeskonforme Umsetzung der Datenübertragbarkeit. Hier liefert das Datenmodell (M42.D01), mit dem die Struktur und die Syntax der verarbeiteten Daten detailliert beschrieben wird, die notwendigen Inhalte.

Darüber sollte die Dokumentation der Daten für die Einhaltung der Rechte der betroffenen Person genutzt werden. So ist klar zu dokumentieren, welche Daten für

- die Informationspflichten (Art. 12 bis 14 DS-GVO),
- das Auskunftsrecht (Art. 15 DS-GVO),
- das Recht auf Berichtigung (Art. 16 DS-GVO),
- das Recht auf Löschung (Art. 17 DS-GVO),
- das Recht auf Einschränkung (Art. 18 DS-GVO),
- der Mitteilungspflicht (Art. 19 DS-GVO),
- das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO),
- das Widerspruchrecht (Art. 21 DS-GVO),

- automatisierte Entscheidungen im Einzelfall (Art. 22 DS-GVO) sowie
- Beschränkungen (Art. 23 DS-GVO),

notwendig sind und wo diese verarbeitet werden und ggf. gelöscht bzw. berichtigt werden können.

Systeme und Dienste

Die Dokumentation der Systeme und Dienste (M42.S01) umfasst im Wesentlichen die Darstellung aller in die Verarbeitung personenbezogener Daten involvierten Systeme und Dienste.

Prozesse

Die Dokumentation der Prozesse (M42.P33) umfasst die Darstellung aller in die Verarbeitung personenbezogener Daten involvierten Prozesse und Arbeitsabläufe sowie eine funktionale Beschreibung, die Prozesse, welche unmittelbar die Dokumentation selbst betreffen, also Aktualität, Vollständigkeit, Eindeutigkeit, Verständlichkeit und Verfügbarkeit gewährleisten.

Dabei ist zu unterscheiden zwischen der Dokumentation der Sachbearbeitung (M42.P34), welcher als unmittelbar operatives Geschäft einer Organisation eine besondere Bedeutung aus Betroffenensicht zukommt, und der Dokumentation der Administration (M42.P35). Dies umfasst die technische Administration der Systeme als auch innerorganisatorische administrative Hilfsprozesse wie Personalverwaltung und Führungsaufgaben.

3. Differenzierung bei hohem Schutzbedarf

Aus Datenschutzsicht bedeutet ein hoher Schutzbedarf bzgl. der Transparenz einer Verarbeitung, dass erhöhte Anforderungen an die Qualität insbesondere der Revisionsfestigkeit, der Vollständigkeit in der Breite und Tiefe, der gesicherten Aktualität durch Fortschreibung durch Befugte und der Unterstützung, wie methodisch Prüfergebnisse hergestellt werden können, der Dokumentation bestehen. Es müssen die Prüfinteressen nicht nur der Organisation selber, sondern auch der Betroffenen sowie der Aufsichtsbehörden sowie ggfs. von anderen Organisationen, mit denen zusammengearbeitet wird, beachtet werden.

Ein hoher Schutzbedarf wirkt sich auf das Dokumentieren aus, insbesondere auf die Auswahl und Ausgestaltung von Maßnahmen, mit denen die Inhalte einer Dokumentation generiert werden. Somit sind zur Absicherung der Gewährleistungsziele Verfügbarkeit, Integrität und Transparenz Maßnahmen zu einem geregelten Dokumentationsmanagement zu treffen, die insbesondere sicherstellen, dass eine aktuelle, vollständige, zutreffende und revisionsfeste Dokumentation einer Verarbeitung jederzeit ohne Verzug prüffähig zur Verfügung gestellt werden kann.

Weiterhin ist ein geeigneter und angemessener Manipulationsschutz der Dokumentation erforderlich (M42.P36). Dies verlangt typischerweise entweder eine Signatur der

Dokumentation oder den Betrieb eines dezidierten Dokumentationssystems, dessen Zugriff mit einem dokumentationsspezifischen Berechtigungs- und Rollenkonzept geregelt ist.

Dass Teile der Dokumentation als vertraulich zu behandeln sind, ergibt sich bereits für normalen Schutzbedarf. Genügen dort einfache Regelungen und Prinzipien (Erforderlichkeitsprinzip), erfordert der Schutz der Vertraulichkeit der Dokumentation von Verarbeitungstätigkeiten, aus denen ein hohes Risiko resultiert, ein Konzept, mit welchem die Vertraulichkeit wirksam erreicht und dauerhaft aufrechterhalten werden kann.

4. Referenzen

DSK: *Muster Verarbeitungsverzeichnis Verantwortlicher*
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/VVT/MusterVerarbeitungsverzeichnisVerantwortlicher.pdf

Muster Verarbeitungsverzeichnis Auftragsverarbeiter
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/VVT/MusterVerarbeitungsverzeichnisAuftragsverarbeiter.pdf

Hinweise zum Verzeichnis von Verarbeitungstätigkeiten
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/VVT/HinweisezumVerzeichnisvonVerarbeitungstaetigkeiten.pdf

Kurzpapier Nr. 1 (Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO)
https://www.datenschutz-mv.de/static/DS/Dateien/Publikationen/Kurzpapiere/Kurzpapier_Nr_1.pdf

BSI: *OPS.1.1.2 Ordnungsgemäße IT-Administration*
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_2_Ordnungsgem%C3%A4%C3%9Fe_IT-Administration.html

5. Zusammenfassung der Maßnahmen

Die einzelnen Maßnahmen können hinsichtlich des Anwendungsbereichs unterschieden werden nach Maßnahmen, welche primär auf einzelne Verarbeitungen angewandt werden sollten (*kursive Darstellung*) und solche, welche primär die gesamte Organisation betreffen und damit im Rahmen des Datenschutzmanagements gebündelt und verwaltet werden sollten. Weiterhin sind alle Maßnahmen grob den Phasen des Datenschutzmanagement-Prozesses (siehe SDM-Methode) zugordnet. Maßnahmen, die in früheren Versionen des Bausteins enthalten waren, aber in einer nachfolgenden Version ungültig wurden, werden weiterhin aufgeführt (~~durchgestrichene Darstellung~~). Damit bleibt die Nummer einer

Maßnahme bei einer neuen Version erhalten. Die Spalte „Gültigkeit“ gibt an, seit welcher Version die Maßnahme in der enthaltenen Form gültig ist. Bei ungültigen Maßnahmen enthält diese Spalte die Versionsnummer des Bausteins, in der die Maßnahme letztmalig gefordert bzw. empfohlen wurde.

Ebene Daten

Nr.	Maßnahme	PDCA	Gültigkeit
M42.D01	Prüfung auf hinreichende Darstellung des Datenmodells in M42.P20	P, C	V1.0

Ebene Systeme

M42.S01	Dokumentation der Systeme und Dienste, ggf. Querverweise in M42.P20 (P, C)	P, C	V1.0

Ebene Prozesse

M42.P01	Strukturierung der Gesamtdokumentation	P	V1.0
M42.P02	Festlegung zur Form der Dokumentation (Papier/Datei/Datenbank)	P	V1.0
M42.P03	Festlegungen für ein in Notfällen verfügbares und aktuelles Backup der Dokumentation	P	V1.0
M42.P04	Festlegungen von Aktualisierungs- und Fortschreibungsregeln für die Dokumentation	P	V1.0
M42.P05	Zugriffssicherung der Dokumentation	P	V1.0
M42.P06	Rahmendokumentation mit Übersicht und Beschreibung des Aufbaus der Dokumentation sowie der Aufbewahrungsorte und –medien		V1.0
M42.P07	Organigramm bzw. Geschäftsverteilungsplan	P, C	V1.0
M42.P08	übergreifende Geschäftsprozesse	P	V1.0
M42.P09	Dokumentation der Bestellung des/der Datenschutzbeauftragten	P, C	V1.0
M42.P10	Netzpläne	P, C	V1.0
M42.P11	Dienst-/Betriebsanweisungen und –vereinbarungen (P, C)		V1.0
M42.P12	Rahmen-Datenschutzkonzept (Handbücher, übergreifende Schutzmaßnahmen, Verantwortliche und Ansprechpartner)	P, C	V1.0
M42.P13	Dokumentation der Datenschutzorganisation gemäß Art. 24 Abs. 1 DS GVO	P	V1.0
M42.P14	Nachweise von Zertifizierungen für Datenschutz und Informationssicherheit	P, C	V1.0

M42.P15	IT-Konzept	P	V1.0
M42.P16	Risikohandbuch	P	V1.0
M42.P17	Sicherheitsrichtlinie	P	V1.0
M42.P18	Sicherheitskonzept	P	V1.0
M42.P19	Notfallkonzept	P	V1.0
M42.P20	Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO	P, C	V1.0
M42.P21	*Dokumentation der Umsetzung der Betroffenenrechte gemäß Erwägungsgrund 39 DS-GVO*	P	V1.0
M42.P22	*Löschkonzept*	P	V1.0
M42.P23	*Verträge zur Auftragsverarbeitung*	P, C	V1.0
M42.P24	*Vereinbarung zwischen den gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 DS-GVO*	P, C	V1.0
M42.P25	*Konzept der Verarbeitung aus der Planungsphase (sowie bspw. Lastenheft und Pflichtenheft)*	P, C	V1.0
M42.P26	Dokumentation der eingeholten Einwilligungen gemäß Art. 7 Abs. 1 DS-GVO	P, C	V1.0
M42.P27	*Dokumentation der Schwellwert-Analyse einer Datenschutz-Folgenabschätzung*	P, C	V1.0
M42.P28	*Bericht zur Datenschutz-Folgenabschätzung*	P	V1.0
M42.P29	*Nachweis der Wirksamkeit der ergriffenen Schutzmaßnahmen*	P	V1.0
M42.P30	Dokumentation für Ausnahmen für bestimmte Fälle von Übermittlungen gemäß Art. 49 Abs. 6 DS-GVO	P	V1.0
M42.P31	Dokumentation von Sicherheitsvorfällen gemäß Art. 33 Abs. 2 DS-GVO	P, C	V1.0
M42.P32	Protokollierungskonzept bzw. Dokumentation der genutzten Protokolle inklusive deren Aufbewahrungsorte, Aufbewahrungsfristen und Zugriffsregelungen	P, C	V1.0
M42.P33	*Dokumentation der Prozesse und ggf. Querverweise in M42.P20*	P, C	V1.0
M42.P34	*Dokumentation der Sachbearbeitung und ggf. Querverweise in M42.P20*	P, C	V1.0
M42.P35	*Dokumentation der Administration und ggf. Querverweise in M42.P20*	P, C	V1.0
M42.P36	*Manipulationsschutz der Dokumentation*	P	V1.0

6. Bezug zum Datenschutzmanagement

Dieser Baustein bezieht sich in weiten Teilen auf Anforderungen an eine Gesamtdokumentation einer Organisation und bildet Dokumentationspflichten des

Verantwortlichen ab, welche auf eine einzelne Verarbeitungstätigkeit aber auch die gesamte Organisation angewendet werden können. Wird der Baustein auf die die gesamte Organisation angewendet, sind die getroffenen Maßnahmen im Datenschutzmanagement der Organisation zu betrachten.

7. Anmerkung zur Nutzung dieses Bausteins

Dieser Baustein darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird:

„Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz). Veränderungen, Bearbeitungen, neue Gestaltungen oder sonstige Abwandlungen der bereitgestellten Daten sind mit einem Veränderungshinweis im Quellenvermerk zu versehen. Datenlizenz Deutschland – Namensnennung – Baustein Dokumentieren (www.govdata.de/dl-de/by-2-0).“