Baustein 42 „Dokumentation“

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

Hinweis: Dieser Baustein wurde von den Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein und der Evangelischen Kirche Deutschlands zur Erprobung der SDM-Methode erarbeitet und veröffentlicht. Dieser Baustein ist keine Publikation der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder.

1. Bezug zu Gewährleistungszielen

Transparenz

2. Beschreibung

Dokumentation ist Teil des Datenschutzmanagements und trägt maßgeblich dazu bei, den ordnungsgemäßen Betrieb einer Verarbeitung kontrollieren und prüfen zu können. Dabei umfasst die Dokumentation die Beschreibung der Verarbeitung, insbesondere unter Ausweis des Zwecks der Verarbeitung und der Zweckbindung der verarbeiteten Daten. Sie dient auch zur Selbstverpflichtung, die Verarbeitung dauerhaft testen zu können und informations- und auskunftsfähig gegenüber Betroffenen, der Organisation selbst sowie anderen Organisationen und Aufsichtsbehörden zu sein.

Die 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 wird insofern nicht als eine gegebene Eigenschaft einer Verarbeitung gesehen, sondern als eine Anforderung, die insbesondere durch Dokumentation hergestellt werden muss. Zur Umsetzung des Gewährleistungsziels Transparenz ist es sowohl erforderlich, die Verarbeitung selbst umfassend zu dokumentieren (inhaltliche Anforderungen), als auch zu dokumentieren, *wie* die Dokumentation 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** (M42.03) 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** (M42.04) vorliegt. Wenn eine (Teil-)Dokumentation elektronisch vorliegt, so ist für diesen Teil ein aktuelles Backup-Medium (M42.05) 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 Dokumentation 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: Dies ist dann gegeben, wenn alle Verarbeitungsprozesse mit allen rechtlichen Forderungen und allen Daten, Systemen und Prozessen so erfasst sind, dass der Produktivbetrieb einer Organisation hinreichend genau und aktuell beschrieben ist. Die SDM-Methodik ist 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 (M42.06). Zum anderen ist sicherzustellen, dass nur berechtige Personen auf die Dokumentation zugreifen und ggf. wiederum dokumentierte Änderungen vornehmen dürfen (M42.07). Die zu ergreifenden Maßnahmen sind dabei abhängig vom Schutzbedarf,
- die **Aktualität** der Dokumentation: Die Dokumentation muss regelmäßig aktualisiert werden, damit sie sich auf einem aktuellen Stand befindet,
- die **Fortschreibung** der Dokumentation: Es sind Vorgaben darüber erforderlich, wie die Dokumentation fortgeschrieben wird (M42.06).

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

Eine Dokumentation sollte aus Gründen der besseren Strukturierung modular aufgebaut sein (M42.03). Sie kann sich an folgender Struktur orientieren und je nach Anforderungen an die konkreteVerarbeitung folgende Einzeldokumente enthalten:

- Eine übergreifenden Übersicht und Gliederung sowie Beschreibung des Aufbaus der Dokumentation inklusive der Aufbewahrungsorte und –medien sowie Namenskonventionen (M42.08)
- Eine Rahmendokumentation, die alle nicht verarbeitungsspezifischen Dokumente enthält:
    - Organigramm bzw. Geschäftsverteilungsplan (M42.09),
    - Dokumentation der Bestellung des/der Datenschutzbeauftragten (M42.10)
    - Netzpläne (M42.11),
    - Dienst-/Betriebsanweisungen und -vereinbarungen (M42.12),
    - Rahmen-Datenschutzkonzept (Handbücher, übergreifende Schutzmaßnahmen, Verantwortliche und Ansprechpartner) (M42.13)
    - Dokumentation der Datenschutzorganisation gemäß Art. 24 Abs. 1 DS-GVO (M42.14),
    - ggf. Nachweise von Zertifizierungen für Datenschutz und Informationssicherheit (M42.15),
    - ggf. IT-Konzept (M42.16),
    - ggf. Risikohandbuch (M42.17),
    - ggf. Sicherheitsrichtlinie (M42.18),
    - ggf. Sicherheitskonzept (M42.19),
    - ggf. Notfallkonzept (M42.20),
    - ggf. Rechte- und Rollenkonzept (M42.21).
- Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (M42.22),
- Dokumentation der Umsetzung der Betroffenenrechte gemäß Erwägungsgrund 39 DS-GVO (M42.23),
- ggf. Verträge zur Auftragsverarbeitung (M42.24),
- für den Fall einer gemeinsamen Verantwortung die Vereinbarung zwischen den gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 DS-GVO (M42.24)
- Konzept der Verarbeitung aus der Planungsphase (sowie bspw. Lastenheft und Pflichtenheft) (M42.26),
- Dokumentation der eingeholten Einwilligungen gemäß Art. 7 Abs. 1 DS-GVO (M42.27)
- Dokumentation der Schwellwert-Analyse einer Datenschutz-Folgenabschätzung (M42.28),
- für den Fall einer erforderlichen Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO:
    - Bericht zur Datenschutz-Folgenabschätzung (M42.29),

    - Nachweis der Wirksamkeit der ergriffenen Schutzmaßnahmen (M42.30)
- Dokumentation für Ausnahmen für bestimmte Fälle von Übermittlungen gemäß Art. 49 Abs. 6 DS-GVO (M42.31),
- Dokumentation von Sicherheitsvorfällen gemäß Art. 33 Abs. 2 DS-GVO (M42.32),
- Protokollierungskonzept bzw. Dokumentation der genutzten Protokolle inklusive deren Aufbewahrungsorte, Aufbewahrungsfristen und Zugriffsregelungen (M42.33).

Daten

Ein wesentlicher Bestandteil der Dokumentation einer Verarbeitung besteht in der Dokumentation der Daten. Diese ist so wichtig, da sie als Ausgangspunkt für die Beschreibung von Schnittstellen und für die gesetzeskonforme Umsetzung der Datenübertragbarkeit dient. Hier liefert das Datenmodell (M42.01), 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,
- das Auskunftsrecht,
- das Recht auf Berichtigung,
- das Recht auf Löschung,
- das Recht auf Einschränkung,
- der Mitteilungspflicht,
- des Widerspruchrechts,
- automatisierte Entscheidungen im Einzelfall sowie
- Beschränkungen

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

Systeme

Die Dokumentation der Systeme (M42.02) umfasst im Wesentlichen die Darstellung aller in die Verarbeitung personenbezogener Daten involvierten Systeme. Den Anforderungen an eine *solche* Dokumentation ist in der Regel Genüge getan, wenn die Vorgaben des BSI erfüllt werden (u. a. IT-Grundschutzmaßnahme „M2.219 Kontinuierliche Dokumentation der Informationsverarbeitung“).

Prozesse

Die Dokumentation der Prozesse (M42.34) 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 (M42.35), welcher als unmittelbar operatives Geschäft einer Organisation eine besondere Bedeutung aus Betroffenensicht zukommt, und der Dokumentation der Administration (M42.36). 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 Dokumentation bestehen. Es müssen die Prüfinteressen nicht nur der Organisation selber, sondern auch der Betroffenen sowie der Aufsichtsbehörden beachtet werden. Bei hohem Schutzbedarf einer Verarbeitung spielen in Bezug auf die Dokumentation sind insbesondere die Gewährleistungsziele Verfügbarkeit, Integrität und Transparenz zu betrachten.

Ein hoher Schutzbedarf für eine Dokumentation wirkt sich eher nicht auf die Inhalte einer Dokumentation, sondern auf die Auswahl und Ausgestaltung von Maßnahmen aus, mit denen die Inhalte einer Dokumentation generiert, gespeichert, transformiert, übermittelt und geschützt 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 (M42.37). Dies verlangt typischerweise entweder eine Signatur der Dokumentation oder den Betrieb eines dezidierten Dokumentationssystems, dessen Zugriff mit einem dokumentationsspezifischen Rechte- 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 (Prinzip des „need-to-know“), erfordert der Schutz der Vertraulichkeit der Dokumentation von Verarbeitungen mit hohem Schutzbedarf ein Konzept, mit welchem die Geheimhaltung wirksam erreicht und dauerhaft aufrechterhalten werden kann.

4. Referenzen

DSK: *Muster Verarbeitungsverzeichnis Verantwortlicher*
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/VVT/Muster%20Verarbeitungsverzeichnis%20Verantwortlicher.pdf

Muster Verarbeitungsverzeichnis Auftragsverarbeiter
https://www.datenschutz-mv.de/static/DS/Dateien/DS-

GVO/Hilfsmittel%20zur%20Umsetzung/VVT/Muster%20Verarbeitungsverzeichnis%20Auftragsverarbeiter.pdf

Hinweise zum Verzeichnis von Verarbeitungstätigkeiten
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/VVT/Hinweise%20zum%20Verzeichnis%20von%20Verarbeitungst%C3%A4tigkeiten.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

M 2.25 Dokumentation der Systemkonfiguration
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02025.htm

M 2.34 Dokumentation der Veränderungen an einem bestehenden System
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02034.html

M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02219.html

5. Zusammenfassung der Maßnahmen

Ebene Daten

M42.01 Prüfung auf hinreichende Darstellung des Datenmodells in M42.22

Ebene Systeme

M42.02 Dokumentation der Systeme und ggf. Querverweise in M42.22

Ebene Prozesse

M42.03 Strukturierung der Gesamtdokumentation
M42.04 Festlegung zur Form der Dokumentation (Papier/Datei/Datenbank)
M42.05 Festlegungen für ein in Notfällen verfügbares und aktuelles Backup der Dokumentation

M42.06 Festlegungen von Aktualisierungs- und Fortschreibungsregeln für die Dokumentation
M42.07 Zugriffssicherung der Dokumentation
M42.08 Rahmendokumentation mit Übersicht und Beschreibung des Aufbaus der Dokumentation sowie der Aufbewahrungsorte und –medien
M42.09 Organigramm bzw. Geschäftsverteilungsplan
M42.10 Dokumentation der Bestellung des/der Datenschutzbeauftragten
M42.11 Netzpläne
M42.12 Dienst-/Betriebsanweisungen und -vereinbarungen
M42.13 Rahmen-Datenschutzkonzept (Handbücher, übergreifende Schutzmaßnahmen, Verantwortliche und Ansprechpartner)
M42.14 Dokumentation der Datenschutzorganisation gemäß Art. 24 Abs. 1 DS GVO
M42.15 Nachweise von Zertifizierungen für Datenschutz und Informationssicherheit
M42.16 IT-Konzept
M42.17 Risikohandbuch
M42.18 Sicherheitsrichtlinie
M42.19 Sicherheitskonzept
M42.20 Notfallkonzept
M42.21 Rechte- und Rollenkonzept
M42.22 Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO
M42.23 Dokumentation der Umsetzung der Betroffenenrechte gemäß Erwägungsgrund 39 DS-GVO
M42.24 Vereinbarung zwischen den gemeinsam Verantwortlichen gemäß Art. 26 Abs. 1 DS-GVO
M42.25 Verträge zur Auftragsverarbeitung
M42.26 Konzept der Verarbeitung aus der Planungsphase (sowie bspw. Lastenheft und Pflichtenheft)
M42.27 Dokumentation der eingeholten Einwilligungen gemäß Art. 7 Abs. 1 DS-GVO
M42.28 Dokumentation der Schwellwert-Analyse einer Datenschutz-Folgenabschätzung
M42.29 Bericht zur Datenschutz-Folgenabschätzung
M42.30 Nachweis der Wirksamkeit der ergriffenen Schutzmaßnahmen
M42.31 Dokumentation für Ausnahmen für bestimmte Fälle von Übermittlungen gemäß Art. 49 Abs. 6 DS-GVO
M42.32 Dokumentation von Sicherheitsvorfällen gemäß Art. 33 Abs. 2 DS-GVO
M42.33 Protokollierungskonzept bzw. Dokumentation der genutzten Protokolle inklusive deren Aufbewahrungsorte, Aufbewahrungsfristen und Zugriffsregelungen
M42.34 Dokumentation der Prozesse und ggf. Querverweise in M42.22
M42.35 Dokumentation der Sachbearbeitung und ggf. Querverweise in M42.22
M42.36 Dokumentation der Administration und ggf. Querverweise in M42.22
M42.37 Manipulationsschutz der Dokumentation

6. 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:

„Datenschutzaufsichtsaufsichtsbehörden der Bundesländer Hessen, Mecklenburg-Vorpommern, Sachsen, Schleswig-Holstein sowie der Evangelischen Kirche Deutschlands. Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).“