Baustein 80 „Datenschutzmanagement“

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

Dieser Baustein ist von grundlegender Bedeutung für das gesamte SDM und betrifft daher alle im Kapitel 5 des SDM beschriebenen Gewährleistungsziele.

2. Beschreibung

2.1 Zweck des Datenschutzmanagements

Die Herstellung von Transparenz ist immer erforderlich um beurteilen zu können, ob eine Verarbeitung dauerhaft datenschutzkonform betrieben wird. Das Datenschutzmanagement (DSM) ist eine wesentliche Voraussetzung zur Herstellung der Transparenz bei zunehmend komplizierter werdenden Verarbeitungen in komplexen IT-Dienstlandschaften.

Datenschutzmanagement bezeichnet einen kontrollierten und gesteuerten Prozess über den gesamten Lebenszyklus einer oder mehrerer Verarbeitungstätigkeiten mit dem Ziel, die gesetzlichen und betrieblichen Anforderungen des Datenschutzes umzusetzen. Mit Hilfe eines klassischen PDCA-Zyklus (Plan, Do, Check, Act) unterstützt das DSM den Verantwortlichen bei der Umsetzung der Anforderungen der DS-GVO und dabei insbesondere bei der Beachtung der der Grundsätze aus Art. 5 DS-GVO. Der Verantwortliche muss

- geeignete technische und organisatorische Maßnahmen ergreifen und dauerhaft vorhalten, um ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung personenbezogener Daten zu gewährleisten und
- die Umsetzung und Wirksamkeit dieser Maßnahmen nachweisen, evaluieren, ggf. verbessern und sie auf diese Weise aktuell halten.

Ziel des Datenschutzmanagements ist auch die dauerhafte Sicherstellung der Wirkung der technischen und organisatorischen Maßnahmen bei einer fortwährenden Beurteilbarkeit der datenschutzrechtlichen Konformität einer Verarbeitung personenbezogener Daten. Um die datenschutzrechtliche Konformität beurteilen zu können, müssen alle relevanten Komponenten der Verarbeitung spezifiziert, dokumentiert und anhand funktionaler Soll-

Werte prüfbar sein. Die im Handbuch in Kapitel 7 beschriebenen generischen Maßnahmen können herangezogen werden um zunächst kursorisch zu prüfen, ob die vorhandenen Maßnahmen bereits ausreichen oder noch ergänzt werden müssen. Die in den Bausteinen aufgelisteten Referenzmaßnahmen dienen dann der detaillierten Prüfung der Vollständigkeit der für eine datenschutzkonforme Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen.

Ein funktionierendes Datenschutzmanagement kann die rechtliche Prüfung einer Verarbeitung erheblich unterstützen. Dazu muss das Datenschutzmanagement an den Grundsätzen gem. Art. 5 DS-GVO insbesondere in Bezug auf Integrität (auch im Sinne einer sachgerechten Verarbeitung), Vollständigkeit und Transparenz von Datenschutzprüfungen ausgerichtet sein.

Der Verantwortliche wird durch das Datenschutzmanagement in die Lage versetzt, Datenschutzverstöße seiner Organisation zu erkennen und darauf angemessen zu reagieren (M80.23). Ein Datenschutzverstoß innerhalb einer Organisation kann bspw. vorliegen, wenn

- für eine Verarbeitung oder Verarbeitungstätigkeit keine Rechtsgrundlage vorliegt,
- die Erforderlichkeit einer Verarbeitung oder Verarbeitungstätigkeit weder rechtlich nachgewiesen noch durch Einwilligung erklärt werden kann oder
- eine Verarbeitung oder Verarbeitungstätigkeit organisatorisch und technisch unzulänglich realisiert ist, weil z. B.
    - das Personal einer Organisation, das mit der Verarbeitung befasst ist, nicht zuständig oder nicht ausgebildet ist oder
    - Funktionen und Prozesse falsch spezifiziert, implementiert, konfiguriert, betrieben, nicht überwacht sind oder unbefugt außer Betrieb gesetzt werden.

Solche Datenschutzverstöße können durch die Anwendung des SDM-basierten PDCA-Prozesses im Rahmen einer Kontrolle oder einer Prüfung festgestellt werden.

Ein Datenschutzmanagementsystem wird nicht für einzelne Verarbeitungen personenbezogener Daten eingerichtet und betrieben, sondern übergreift die gesamte Organisation in ihrer Struktur, in ihren Geschäftsprozessen oder ihren Abläufen, den resultierenden Management-Prozessen und damit alle Verarbeitungen, in denen personenbezogene Daten verarbeitet werden. Jede Verarbeitung muss deshalb von dem organisationsweiten Datenschutzmanagement erfasst sein. Bei der Spezifikation einer Verarbeitung und dem Führen des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DS-GVO) ist darauf zu achten und darauf hinzuwirken, dass eine Verarbeitung die Voraussetzungen erfüllen kann, um in das organisationsweite Datenschutzmanagementsystem integriert werden zu können. Das gilt besonders dann, wenn die Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) erforderlich ist.

2.2 Der PDCA-Zyklus des Datenschutzmanagements

Der SDM-basierte PDCA-Zyklus beschreibt einen kontinuierlichen Verbesserungsprozess und ist eine geeignete Methode für die ständige Beobachtung des laufenden Betriebs und dessen permanenter Optimierung. Der Prozess der kontinuierlichen Verbesserung und der PDCA-Zyklus sind grundlegende Bestandteile der Familien technischer Normen DIN EN ISO 9000, ISO 14000, ISO/IEC 20000 und ISO/IEC 27001. Die klassischen PDCA-Phasen sind beim Datenschutzmanagement wie folgt zu verstehen:

- Plan: Planen / Spezifizieren
- Do: Kontrollieren / Prüfen
- Check: Beurteilen
- Act: Verbessern

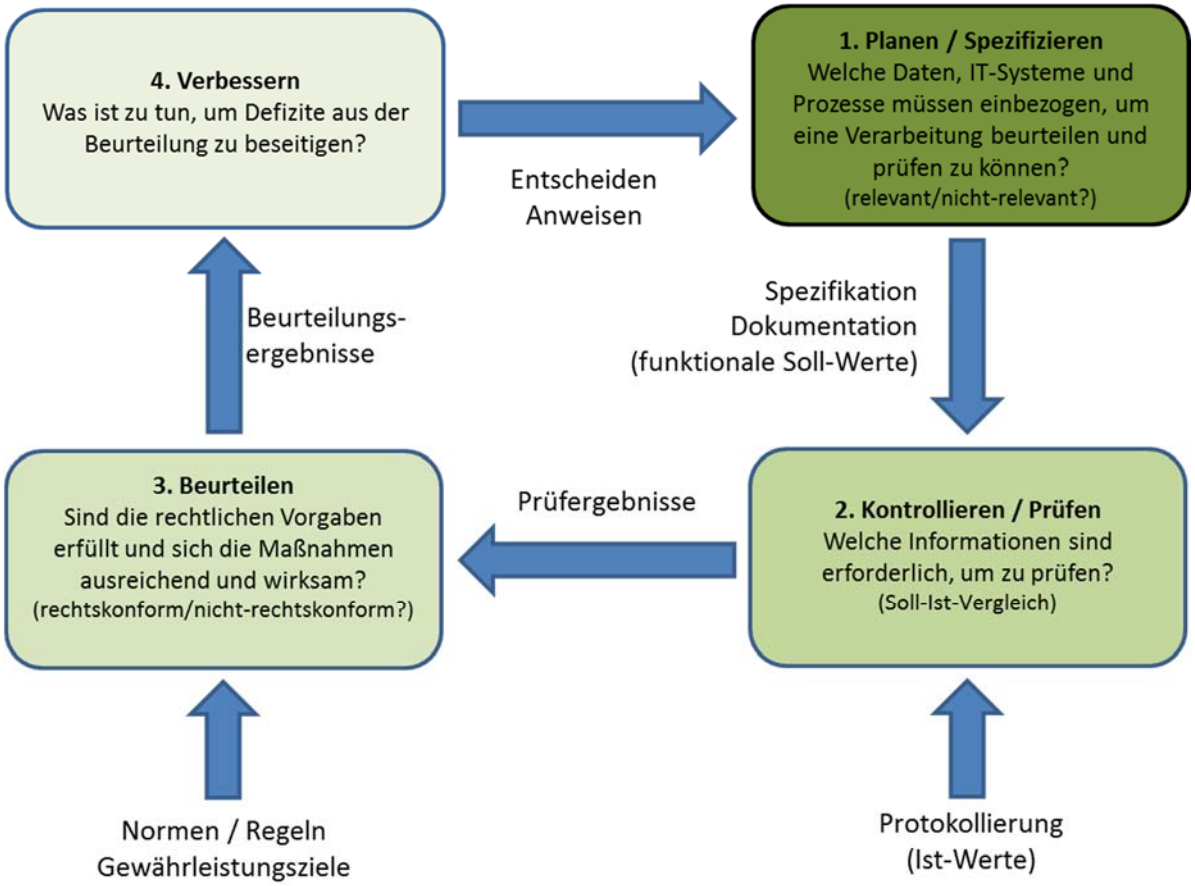

Abbildung 1: Der PDCA-Zyklus des Datenschutzmanagements

Phase 1 „Planen / Spezifizieren“: Bei der Planung / Spezifikation einer Verarbeitung ist darauf zu achten, dass eine Verarbeitung personenbezogener Daten im Betrieb datenschutzrechtlich den Anforderungen folgt und dies vollständig prüffähig ist. Zu diesem Zweck müssen alle funktionalen und rechtlich relevanten Komponenten der beabsichtigten Verarbeitung zusammengestellt werden und anhand von Dokumentation und auch Log- bzw. Protokolldaten geprüft werden können. In der Planungsphase müssen die normativen Soll-Werte, also die rechtlichen Vorgaben insbesondere der DS-GVO (wie z. B.

Zweckbindungsgebot oder Sicherstellung der Integrität und der Vertraulichkeit auch unter Belastung der Systeme und IT-Dienste auf Dauer), in funktionale Soll-Werte der Technik und Organisation (wie z. B. Trennungsmaßnahmen, Verschlüsselungsmaßnahmen oder das Zertifikatsmanagement in einem Router) umgesetzt werden. Das schließt die Prüfdaten ein, mit denen der Nachweis der Wirksamkeit der getroffenen Maßnahmen möglich wird.

Der SDM-Baustein „Planung und Spezifikation“ listet hierfür erforderliche technische und organisatorische Maßnahmen auf.

Phase 2 „Kontrollieren / Prüfen“: Diese Phase erzeugt Prüfergebnisse aus dem Kontext technischer und organisatorischer Prozesse einer Verarbeitung personenbezogener Daten. Zu jedem normativen Soll-Wert ist ein funktionaler Ist-Wert zu bestimmen, der während des Kontrollierens oder des Prüfens zu ermitteln ist. Der Zweck einer Kontrolle besteht darin sicherzustellen, dass alle relevanten Komponenten einer Verarbeitung und entsprechende Verarbeitungstätigkeiten erfasst sind. Der Zweck einer Prüfung ist es, die Ist-Werte im laufenden Betrieb der Systeme oder IT-Dienste mit Hilfe der Dokumentation und der Protokolldaten zu ermitteln mit den Soll-Werten zu vergleichen. Bereits die Ermittlung von Ist-Werten und die anschließende Zusammenstellung von Soll- und Ist-Werten liefert ein erstes Prüfergebnis.

Der Zweck einer Dokumentation besteht darin, die für eine Verarbeitung relevanten Daten, Systeme und Prozesse sowie die funktionalen Soll-Werte, die aus den normativen Soll-Werten (insbesondere der DS-GVO) abzuleiten sind, auszuweisen. Die Dokumentation soll darüber hinaus sowohl der Organisation selbst als auch externen Prüfern (z. B. Auditoren und Datenschutzaufsichtsbehörden) und den von der Verarbeitung betroffenen Personen sowohl einen Überblick über die Zusammenhänge der verschiedenen Komponenten (Datenbestände, IT-Systeme und technische und organisatorische Prozesse) als auch Einblicke in spezifische Details während des Betriebs der Systeme und IT-Dienste geben.

Der Zweck der Protokollierung ist die Aufklärung technischer, organisatorischer oder administrativer Aktivitäten, die in der Vergangenheit stattfanden. Das Vorliegen von Protokolldaten (Ist-Werten) ist Voraussetzung, um eine Verarbeitung prüfen zu können. Der Vergleich der in der Dokumentation ausgewiesenen funktionalen Soll-Werte mit den aktuellen Ist-Werten (Kontrollieren / Prüfen) ist eine wesentliche Voraussetzung dafür, dass die Ordnungsmäßigkeit einer Verarbeitung nachgewiesen werden kann.

Die SDM-Bausteine „Dokumentation“ und „Protokollierung“ listen technische und organisatorische Maßnahmen auf, mit denen Prüfungsergebnisse des laufenden Betriebs gewonnen werden können.

Phase 3 „Beurteilen“: Diese Phase dient der rechtlichen Beurteilung von Prüfergebnissen im funktionalen Kontext einer Verarbeitung personenbezogener Daten und entspricht damit einer datenschutzrechtlichen Prüfung. In dieser Phase werden Prüfergebnisse in Bezug auf den praktischen Betrieb einer Verarbeitung bzw. Verarbeitungstätigkeit beurteilt. Die

Beurteilung dieser Prüfergebnisse ist eine eigene Phase, weil Prüfergebnisse in einem erweiterten funktionalen und gleichzeitig rechtlichen Kontext zu beurteilen sind. Eine solche Prüfung geht insofern über die Detailprüfungen der einzelnen Systeme hinaus. Ein wesentlicher Zweck des SDM besteht also darin, die rechtliche Prüfung einer Datenverarbeitung zu unterstützen. Deshalb muss das Datenschutzmanagement selbst den Grundsätzen für die Verarbeitung personenbezogener Daten gem. Art. 5 DS-GVO genügen. Die Ergebnisse der Phase 3 bilden die Grundlage zur Behebung von Defiziten (Verbessern).

Phase 4 „Verbessern“: Diese Phase dient dazu, Konsequenzen aus den in Phase 3 gewonnen Ergebnissen der Beurteilung einer Verarbeitung zu ziehen. Die Konsequenz kann darin bestehen darauf hinzuwirken, dass eine Datenverarbeitung funktional verändert wird, um etwa deren Eingriffsintensität zu mindern. Mit Hilfe weiterer oder verbesserter Maßnahmen sind bspw. in der Beurteilungsphase erkannte Risiken für Rechte und Freiheiten betroffener Personen zu verringern. Gegenstand der Verbesserungen sind nicht nur die verschiedenen Verarbeitungstätigkeiten in Bezug auf personenbezogene Daten. Sie betreffen auch die Management-Prozesse der Organisation sowie technische Anpassungen. Der vollständige Katalog mit SDM-Referenzmaßnahmen kann dazu herangezogen werden, um die bereits umgesetzten technischen und organisatorischen Maßnahmen zu verbessern und zu ergänzen.

Schließlich muss auch sichergestellt werden, dass das DSM mit anderen Management-Systemen, bspw. mit der internen Revision, dem Betriebs- oder Personalrat, dem Projektmanagement sowie insbesondere natürlich mit dem IT-Sicherheitsmanagement, zusammenarbeiten kann. Folglich muss auch das DSM fortwährend evaluiert und ggf. verbessert werden. Zu diesen Verbesserungen des DSM kann bspw. die Nutzung von Leistungskennzahlen („Key Performance Indicator“, siehe Abschnitt 3.1) zählen.

Ein Datenschutzverstoß innerhalb einer Organisation kann bspw. vorliegen, wenn

- eine Verarbeitung nicht nachweislich hinreichend geplant und spezifiziert wurde,
- keine hinreichende Dokumentation und keine Protokolldaten zur Kontrolle, keine methodischen Prüfung oder Beurteilung einer Verarbeitung vorliegen,
- der laufende Betrieb einer Verarbeitung keiner fortwährenden Kontrolle und Prüfung unterliegt oder
- bei vom Datenschutz-Management bzw. dem/der Datenschutzbeauftragten festgestellten Mängeln keine wirksamen Aktivitäten der Verbesserung entfaltet werden.

Grundsätzlich ist damit zu rechnen und auch wünschenswert, dass künftig Technik (etwa Prüfautomaten) zur Kontrolle, Prüfung und zur regelgeleiteten Beurteilung der von der Verarbeitung verwendeten Technik eingesetzt wird. Vertrauenswürdige Prüfergebnisse kann die für die Kontrolle und Prüfung genutzte Technik jedoch nur dann liefern, wenn sie ihrerseits den Anforderungen der Gewährleistungsziele genügt. Deshalb sollte eine Organisation künftig anstreben, geprüfte, rechtskonforme Verarbeitungstätigkeiten mit geprüften und ggf. zertifizierten Datenschutz-Prüfautomaten überwachen.

2.3 Die Einrichtung des Datenschutzmanagement-Systems

Zur Einrichtung und zum laufenden Betrieb eines Datenschutz-Managementsystems (DSMS) sind die nachfolgend aufgeführten Schritte erforderlich.

2.3.1 Die Initialisierung eines Datenschutzmanagement-Systems (DSMS)

Die Einrichtung eines DSMS zur Umsetzung eines DSM zur Unterstützung aller Verarbeitungen und Verarbeitungstätigkeiten, in denen personenbezogene Daten verarbeitet werden, ist aus folgenden Gründen erforderlich:

Insbesondere bei großen Organisationen mit zahlreichen Verarbeitungen genügt es in der Regel nicht, dass eine Organisation eine/n Datenschutzbeauftragte/n beschäftigt, der oder die sich um die Umsetzung datenschutzrechtlicher Anforderungen fallweise kümmert.

Aus datenschutzrechtlicher Sicht reicht es nicht aus, nur Maßnahmen zur Gewährleistung der Informationssicherheit auszuwählen und umzusetzen, also nur ein IT-Sicherheitsmanagement zu betreiben. Obwohl es in Teilen Überschneidungen in technischen Anforderungen in Bezug auf Umsetzung einer zu gewährleistenden Datensicherheit gibt, stimmen die Schutzobjekte des Datenschutzes mit denen der IT-Sicherheit nicht überein. Das zeigt sich in vielfach auftretenden Konflikten, die entstehen, wenn Anforderungen aus den IT-gestützten Geschäftsprozessen und die Wahrung der Rechte der betroffenen Personen aufeinandertreffen.

Um Datenschutz- und IT-Sicherheitsfragen „auf gleicher Augenhöhe“ behandeln zu können, ist ein/e Projektmanager/-in zu ernennen, der/die die Einrichtung eines Datenschutzmanagement-Systems verantwortlich betreut (M80.07). Dabei ist auch die Rolle und die Funktion des/der Datenschutzbeauftragten zu klären. Vielfach wird er/sie, insbesondere in kleineren Organisationen, die Rolle des Projektmanagers/der Projektmanagerin einnehmen müssen. Andernfalls muss das Verhältnis zum/zur Projektmanager/-in beim Aufbau des DSMS geklärt werden, so wie auch die Abgrenzung zur Leitung der IT-Revision, zum/zur IT-Sicherheitsbeauftragten sowie insbesondere zur Projektleitung für die Datenschutz-Folgenabschätzungen (M80.08).

Es sind die Prozesse, die das Datenschutz-Management durchzuführen hat, zu erarbeiten und damit zu planen (M80.09).

Es sind die Prozesse zu spezifizieren und zu dokumentieren, die durch das Datenschutzmanagement-System zu unterstützen sind (M80.35).

In Kooperation mit dem/der Datenschutzbeauftragten ist sicherzustellen, dass die Verzeichnisse der Verarbeitungstätigkeiten (Art. 30 DS-GVO) vollständig vorliegen (M80.36). Bestehende Verzeichnisse sind zu evaluieren und ggf. zu aktualisieren. Diese Verzeichnisse sind wesentliche Grundlage für ein effektives Datenschutzmanagement.

Das Verzeichnis der Verarbeitungstätigkeiten ist um die Verarbeitungen zu ergänzen, die dem Betrieb des DSMS dienen (M80.37).

Die Ressourcen für den Betrieb des DSM und des DSMS (Personalkapazitäten, Instrumente, Zeit, Budget) sind sicherzustellen (M80.10).

2.3.2 Die Erstellung eines Datenschutzkonzepts

Der Verantwortliche legt fest und dokumentiert, wie die Anforderungen des Datenschutzrechts an personenbezogene Verarbeitungstätigkeiten mit Hilfe des Datenschutz-Managementsystems wirksam umgesetzt werden sollen (M80.11). Der/Die Datenschutzbeauftragte unterstützt den Verantwortlichen und den/die Projektmanager/-in.

2.3.3 Die Etablierung des SDM-basierten PDCA-Prozesses

Die speziellen rechtlichen Rahmenbedingungen der datenschutzrechtlichen Zulässigkeit der Verarbeitungen, die im DMS und dazugehörigen DSMS zu verwalten sind, sind zu prüfen und die Ergebnisse zu dokumentieren (M80.43).

Für die bereits laufenden Verarbeitungstätigkeiten sind die erforderlichen, vorhandenen und fehlenden Schutzmaßnahmen zu erheben (M80.01).

Diese Erhebung von Verarbeitungen und ihren Verarbeitungstätigkeiten mit allen Datenbeständen, IT-Systemen, Prozessen und Beteiligten muss geplant werden (M80.02). Drei spezifisch auf die Sicherung von Datenschutzanforderungen abzielende Leitfragen geben dabei Orientierung:

- Ist alles Relevante der Verarbeitung erfasst (Herstellung Kontrollierbarkeit und damit Vorbereitung von möglichen Kontrollen)?
- Können Prüfergebnisse im Rahmen von Soll-Ist-Bilanzen der relevanten Bestandteile der Verarbeitung erstellt werden (Herstellung von Prüfbarkeit und Prüfergebnissen und Vorbereitung von möglichen Prüfungen)?
- Können die erzielbaren Prüfergebnisse rechtlich beurteilt werden (Herstellung der Beurteilbarkeit im Hinblick auf Feststellung des Änderungsbedarfs, um zu verbessern)?

Im Ergebnis der juristischen Beurteilung der Prüfergebnisse können Anforderungen an die Verbesserung (PDCA-Phase 4) formuliert werden, die im Idealfall auch einen Projektplan zur Umsetzung beinhalten (M80.12).

Die Verantwortlichkeiten und Zuständigkeiten für einzelne Aspekte der Verarbeitung (Auftragsverarbeitung, zentrale Stellen, Wartungsarbeiten usw. inkl. Verträge, etc.) sind zu kontrollieren, ggf. festzulegen und zu dokumentieren (M80.13).

Es muss geprüft werden, ob die Verantwortlichkeiten und Zuständigkeiten für Verarbeitungstätigkeiten in einer Verarbeitung bei der Erbringung von IT-Diensten definiert sind. Ggf. sind sie festzulegen und zu dokumentieren (M80.38).

Im Rahmen der Erstellung oder der Aktualisierung von Verzeichnissen der Verarbeitungstätigkeiten ist zu entscheiden und zu dokumentieren, ob eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist. Dazu ist das Risiko für betroffene Personen durch eine geplante Verarbeitung abzuschätzen und der Schutzbedarf entsprechend

festzustellen (M80.14). Wenn ein hohes Risiko besteht, muss eine vollständige Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchgeführt werden. Wenn die DSFA erforderlich ist, ist sie in dieser Phase durchzuführen (M80.15).

Ein DSFA-Bericht nach erfolgter DSFA sollte eine juristische Beurteilung der Empfehlungen enthalten (M80.39) und mit einer formellen Freigabe der Verarbeitung durch den Verantwortlichen abschließen (M80.40).

Zu klären ist, welche Rolle das DSM in Bezug auf die Durchführung einer DSFA einnehmen soll.

Für jede Verarbeitung personenbezogener Daten sind die Regelungen zur operativen Sicherstellung der Rechte der betroffenen Personen zu kontrollieren, ggf. festzulegen und zu dokumentieren. Idealerweise gibt es zu jeder Verarbeitungstätigkeit eine spezifische Anweisung mit Bezug zur Umsetzung der datenschutzrechtlichen Anforderungen durch die Mitarbeiter/-innen (M80.41).

2.3.4 Die Etablierung eines DSM

Teil der Etablierung des DSM ist eine Unterrichtung und Verpflichtung der Mitarbeiter/-innen bei der Verarbeitung der personenbezogenen Daten auf die Erfüllung von Datenschutz-Anforderungen (M80.16). Es ist zu klären, auf welche Weise der/die Datenschutzbeauftragte in die betriebliche Datenschutz-Weiterbildung einzubeziehen ist (M80.17).

Für jede Verarbeitung personenbezogener Daten sind die Regelungen zur operativen Sicherstellung der Rechte der betroffenen Personen zu erstellen bzw. zu prüfen. (M80.18).

Die Datenschutzkonformität der Verträge bspw. mit Auftragsverarbeitern oder Kooperationspartnern ist zu prüfen (M80.04).

Es ist zu prüfen, ob die Verarbeitungstätigkeiten (bzw. Änderungen an der Verarbeitung) auch explizit datenschutzrechtlich freigegeben wurden (M80.19).

2.3.5 Überwachung des laufenden Betriebs

Ein DSM muss den laufenden Betrieb aller Systeme und IT-Dienste in einer ggf. komplexen IT-Dienstlandschaft für eine Organisation unterstützen. Das ist aus datenschutzrechtlicher Sicht erforderlich, um z. B. die Einhaltung von Trennungsgeboten zwischen Organisationsteilen (z. B. Abteilungen oder auch Filialen) kontrollieren, prüfen und beurteilen zu können. Des Weiteren ist z. B. bei den übergreifenden Infrastrukturen einer Organisation ein unbefugter Zugriff auf Prozesse, Systeme und Daten zu verhindern.

An diesen Beispielen wird deutlich, dass im DSM auch die Verbindung zwischen Verarbeitungstätigkeiten und deren tatsächlicher Realisierung darzustellen ist. Zu diesem Zweck enthält das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) einen Verweis auf die Sicherheit der Verarbeitung (Art. 32 DS-GVO).

a) Der datenschutzrechtliche Ausgangspunkt zur Beurteilung einer Verarbeitung ist die Sachbearbeitung.

Ausgehend von der Ebene der Sachbearbeitung ist die Erforderlichkeit der Zugriffe auf personenbezogene Daten durch die Leitung der Sachbearbeitung sowie der Organisation insgesamt zu beurteilen. Als Voraussetzung für die Umsetzung der Zugriffsrechte ist ein Berechtigungs- und Rollenkonzepts einzurichten (M80.20). Gleiches gilt für die Ausführung der IT-Funktionen sowohl der Sachbearbeitungs-Programme als auch der Infrastruktur (z.B. Netze, Speicherungsmanagement, Schnittstellen) sowie die Administration der Systeme. Alle Aktivitäten auf der Ebene der Infrastruktur und der Schnittstellen müssen in einer Verbindung zur Zweckbestimmung der Verarbeitung auf der Ebene der Sachbearbeitung stehen. Sie müssen in diesem Sinne zweckbestimmt und zweckgebunden sein und den Schutzbedarf der Verarbeitung erben.

b) Das DSM muss auf Änderungsbedarfe, Probleme, Störungen oder sogar Ausfälle im laufenden Betrieb der Verarbeitung reagieren können (M80.21). Das DSMS muss über eigene Strategien der Beurteilung von Ausnahmen verfügen und jegliche Formen von Änderungserfordernissen oder -wünschen ausbilden. Das DSMS kann einen Teilprozess des organisationsweiten Changemanagements bilden.

Das DSMS muss auf folgende Änderungsbedarfe, Störungen und Probleme, reagieren (M80.22):

- Änderungen im Datenschutzrecht,
- Änderungen in Abläufen,
- Änderungen in der Prüf- und Beratungsmethodik,
- Störungen in den operativen Betriebsabläufen, die als Datenschutz- oder IT-Sicherheitsvorfall zu klassifizieren sind,
- technischer Fortschritt und reduzierter Aufwand für bisher nicht realisierte Maßnahmen.

c) Das DSMS muss Datenschutzverstöße der Organisation erkennen und darauf reagieren können (M80.23). Ein Datenschutzverstoß liegt vor, wenn

- für eine Verarbeitung oder Verarbeitungstätigkeit keine Rechtsgrundlage zur Ermächtigung einer Datenverarbeitung vorliegt,
- für eine Verarbeitung oder Verarbeitungstätigkeit die Ermächtigungsgrundlage nicht ausreicht,
- eine Verarbeitung oder Verarbeitungstätigkeit organisatorisch und technisch falsch eingerichtet ist, weil z. B. die Einteilung von Abteilungen nicht sachgerecht ist, das Personal einer Organisation, das mit der Verarbeitung befasst ist, nicht zuständig ist, nicht ausgebildet ist oder Funktionen und Abläufe falsch spezifiziert, implementiert, konfiguriert, betrieben oder außerbetrieb gesetzt werden,
- die technischen oder organisatorischen Maßnahmen einer Verarbeitung nicht hinreichend spezifiziert, nicht hinreichend dokumentiert, nicht hinreichend protokolliert, falsch implementiert oder konfiguriert, nicht hinreichend wirkungsvoll betrieben, administriert oder außerbetrieb gesetzt werden.

d) Das DSMS muss Datenschutzvorfälle managen können. Ein Datenschutz-Vorfall gilt als ein singuläres Ereignis, das unmittelbar Auswirkungen auf einen Betroffenen oder eine Gruppe von Betroffenen hat (z. B. unbefugter Zugriff über das Internet auf ein Adressverzeichnis oder die zweckentfremdende Nutzung von Daten über Zuständigkeitsgrenzen hinweg). Es ist dabei zu prüfen, ob ein Datenschutzvorfall gemeldet werden muss (gem. Art. 33 DS-GVO) (M80.25).

Das DSMS muss dafür Sorge tragen, dass auch diese singulären Vorfälle datenschutzrechtlich beurteilt und in Zusammenarbeit mit dem Leitungspersonal des Verantwortlichen und weiterer interner Stellen (IT-Sicherheitsbeauftragter, Personal-/Betriebsrat) sowie ggfs. mit der zuständigen Datenschutzaufsichtsbehörde behandelt werden. Das Ziel aus grundrechtlicher Datenschutzsicht besteht darin, auch jeden Einzelfall rechtlich korrekt, im Sinne der Betroffenen, zu behandeln. Darüber hinaus ist eine Priorisierung von technischen und organisatorischen Maßnahmen zur Problemanalyse und Problemlösung auch in struktureller Hinsicht vorzunehmen, damit sich ein singulärer Vorfall nicht wiederholt (M80.24).

e) Ergänzende Grundlage zur Festlegung der Aktivitäten im Bereich des DSM zur Überwachung insbesondere des laufenden Betriebs der IT-Dienstlandschaft (Netzwerke, Systeme, IT-Prozesse und Daten) kann ein IT-Betriebskonzept sein.

Ein solches IT-Betriebskonzept umfasst üblicherweise eine Beschreibung für die im laufenden Betrieb befindlichen Systeme, IT-Dienste oder ggf. einer komplexen IT-Dienstlandschaft. Es beschreibt, was zu tun ist, um die Sicherheit der Verarbeitung nach Stand der Technik gemäß Art. 32 DS-GVO zu gewährleisten. Ein IT-Betriebskonzept muss für die gesamte Laufzeit der Systeme, IT-Dienste oder ggf. komplexen IT-Landschaften Gültigkeit besitzen. Ein solches Betriebskonzept sollte daher mittels eines eigenen Lebenszyklus (im Sinn des PCDA-Zyklus) verwaltet und aktuell gehalten sein.

Daraus ergeben sich für das DSM zu implementierende Prozesse, die mit dem Betriebskonzept verbunden sind. Im Rahmen des DSM ist zu klären, wie solche Betriebskonzepte mit der Reflektion der tatsächlichen Realisierung von Schutzmaßnahmen und nach Stand der Technik einzubinden sind (M80.03).

f) Ein Notfallplan beschreibt Maßnahmen, die zu ergreifen sind, wenn es zu einem solchen außergewöhnlichen – aber denkbaren – Notfall kommt. Ein speziell auf den IT-Betrieb ausgerichteter Notfallplan soll es ermöglichen, zeitnah gestörte oder ausgefallene Systeme wieder bereitzustellen (M80.05). Aus der Sicht des DSM können bei einer Störung oder sogar einem Ausfall ein oder mehrere Verarbeitungstätigkeiten bzw. Realisierungen einzelner oder mehrerer IT-Dienste betroffen sein.

Es ist zu klären, wie datenschutzrechtliche Anforderungen aus dem Notfallmanagement in das DSM zu überführen sind (M80.06).

g) Das DSM muss bei der Umsetzung erforderlicher Schutzmaßnahmen im Rahmen der Spezifikation von Verarbeitungen beteiligt sein. Das DSM unterstütz Verantwortliche dabei,

Spezifikationen auf Datenschutzrelevanz zu kontrollieren, zu prüfen und zu beurteilen. Dadurch kann initiativ auf Änderungsbedarfe, auf Störungen und Probleme in Abläufen, auf Datenschutzverstöße und auf Datenschutzvorfälle mit Bezug zu einzelnen Betroffenen reagiert werden (M80.26).

h) Das DSMS muss die kontrollierte Beendigung einer Verarbeitung regeln. Dazu muss der Verantwortliche ein Konzept zur Außerbetriebnahme erstellen, das insbesondere das Löschen von Datenbeständen und Zugriffsberechtigungen auf IT-Systeme sowie das Beenden von Prozessen beinhaltet (M80.27). Die Außerbetriebnahme einer Verarbeitung ist Teil des Regelbetriebs.

Der Lebenszyklus einer Verarbeitung überdauert in der Regel den Lebenszyklus vieler von der Verarbeitung genutzten Techniken und Organisationsprozesse. Während des Lebenszyklusses der Verarbeitung werden mitunter alte IT-Systeme (Personalcomputer, Netzkomponenten, Firewalls usw.) außer Betrieb genommen und gegen neue ausgetauscht. Programme werden fortwährend auf den neuesten Stand gebracht, oftmals mit erweiterten Funktionalitäten. Die Zuständigkeiten auf der Sachbearbeitungs- oder Administrationsebene werden geändert. In all diesen Fällen ist das Datenschutz-Management zu beteiligen (M80.28). Da der Datenschutzbeauftragte an der Spezifikation beteiligt ist muss er ggfs. prüfen, welche Änderungen in der Dokumentation, der Protokollierung, der Datenbestände, der Datentransfers, de Systeme und Prozesse einschließlich der Änderungen von Eskalationsprozessen zu erwarten sind und ggf. die Spezifikation für den laufenden Betrieb anpassen.

3. Differenzierung bei hohem Schutzbedarf

Bei hohem Schutzbedarf für Verarbeitungstätigkeiten mit Personenbezug sind auch erhöhte Anforderungen an das Datenschutz-Management-System einer Organisation umzusetzen.

Werden vom DSMS verwaltete Verarbeitungen mit hohem Schutzbedarf geprüft, müssen diese Datenschutzkontrollen und -prüfungen selbst ebenfalls den Grundsätzen des Art. 5 DS-GVO bzw. den Gewährleistungszielen genügen.

Ausgangspunkt ist die Beschreibung des Zwecks der Kontroll- und Prüftätigkeiten des DSMS und die Abgrenzung von anderen, benachbarten Zwecken (M80.31).

Ein DSMS ist seinerseits zu spezifizieren, zu dokumentieren und die Aktivitäten von (automatisierten) Prüfungen sind zu protokollieren (M80.30). Zudem ist zu klären, inwieweit bspw. anhand von Kennzahlen sichergestellt werden kann, dass das DSMS selbst einer permanenten Verbesserung unterliegt (M80.33).

Das DSMS muss für die zuständigen Personen verfügbar sein (M80.29), nämlich für

- den Verantwortlichen einer Organisation,
- die Projektleitung bei der Initiierung eines DSMS,

- die Projektleitung bei neuen Projekten, die entsprechende Verzeichnisse der Verarbeitungstätigkeiten zu erstellen haben,
- den Projektleitungen, die mit Projekten betraut sind, die zu Änderungen in bestehenden Systemen, IT-Diensten oder IT-Dienstlandschaften führen,
- Zuständige im Änderungs- bzw. Change-Management, so dass Änderungen in den verwalteten Verarbeitungen und ihren Verarbeitungstätigkeiten sachgerecht und zeitnah angestoßen werden können, und
- Zuständige in der Revision, die ebenfalls Änderungen initiieren könnten.

Diese zuständigen Personen benötigen einen Zugang und Zugriff auf bestimmte Daten unter Regelung ihrer Befugnisse und mit Abbildung der entsprechenden Rollen. Zur Sicherstellung der Verfügbarkeit zählt auch, dass für diese Rollen und möglichst auch für den/die Datenschutzbeauftragte/n, Stellvertreter/-innen benannt werden sollten (M80.42).

Für das DSMS muss spätestens bei hohem Schutzbedarf geklärt werden,

- ob und inwieweit die Verzeichnisse der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO gemeinsam mit den zu erstellenden Dokumenten einer DSFA gem. Artikel 35 DS-GVO verwaltet werden,
- ob und ggf. welche Verhaltenskontrollen mit Hilfe des DSMS gestuft durchgeführt werden können,
- welche (Rest-)Risiken verbleiben und welche Maßnahmen zur Verringerungen dieses Risikos getroffen wurden,
- ob und inwieweit und in welcher technischen Form Datenbestände zur Prüfung der Wirksamkeit des Datenschutzes einer Organisation an übergeordnete Stellen (in Konzern- und Behördenstrukturen) und insbesondere an externe Organisationen (Staatsanwaltschaft, externe Auditoren) übermittelt werden dürfen (M80.32).

Ein Datenschutz-Management-System, mit dem Verarbeitungen und Verarbeitungstätigkeiten für hohen Schutzbedarf unter permanente Prüfung und Beurteilung gestellt werden, muss einen bestimmten *Prozessreifegrad* aufweisen. Reife Prozesse zeichnen sich dadurch aus, dass sie zumindest definiert sind und dass sie in einem weiteren Schritt der Verbesserung zunehmend standardisiert sind. Ein Datenschutz-Managementsystem mit standardisierten Prüfprozessen, das die im obigen Abschnitt genannten Eigenschaften aufweist, ist die Voraussetzung zur Prüfung von Verarbeitungen mit hohem Schutzbedarf. Die Standardisierung eines DSMS kann bis hin zu weitgehend technisch gestützten, automatisierten Prüfabläufen reichen.

Reifere Prozesse des Datenschutzmanagements führen dazu, dass alle erforderlichen Prüfungen integer, vollumfänglich und nachvollziehbar durchgeführt und notwendige Korrekturen der Praxis auch umgesetzt werden.

3.1 Die Nutzung von Key-Performance-Indicators für DSMS

Ein seit Jahrzehnten erprobtes Instrument zur Beurteilung der Reife und der Effizienz von Managementsystemen von Organisationen mittlerer Größe bilden „Key-Performance-Indicators“ (KPI). Wenn eine Organisation bereits über Erfahrungen mit KPIs verfügt, sollte auch das Datenschutz-Managementsystem Indikatoren für die Prüfung und Umsetzen von Korrekturmaßnahmen im Bereich des Datenschutzes aufweisen können (M80.34).

KPIs für das DSMS müssen bereits bei der Spezifikation von technischen und organisatorischen Maßnahmen gebildet werden. KPIs müssen so entwickelt werden, dass sie die (Tendenz der) Verbesserung der Wirksamkeit von Schutzmaßnahmen anzeigen. Ob eine tendenzielle Verbesserung von Maßnahmen stattgefunden hat, kann dadurch festgestellt werden, indem bspw. ein aktuell ermittelter Messwert mit dem Messwert des Vorjahres verglichen wird. Der Zweck des Datenschutz-Managements im engeren Sinne bestünde dann darin, die Umsetzung von Korrekturmaßnahmen in Gang zu setzen und anhand von KPI die allmähliche Verbesserung der Wirksamkeit von Schutzmaßnahmen zu verfolgen.

In Bezug auf die Gewährleistungsziele können zum Beispiel folgende *Kennzahlen für die kontinuierliche Verbesserung von technischen und organisatorischen Maßnahmen* gebildet werden:

- Ausfallzeiten als Kennzahl für die Verfügbarkeit
- Anzahl der Widersprüche zu einer Verarbeitung als Kennzahl für die Integrität
- Anzahl der eingespielten und durch Zertifikate oder Hash-Werte gesicherten Softwareupdates als Kennzahl für die Integrität
- Anzahl der bewältigten Sicherheitsvorfälle in einem bestimmten Zeitraum als Kennzahl für die Vertraulichkeit
- Anzahl der Nutzung von Verschlüsselungsmechanismen als Kennzahl für die Vertraulichkeit
- Anzahl der ordnungsgemäß dokumentierten Verarbeitungen als Kennzahl für die Transparenz,
- Anzahl der geprüften Protokollierungen als Kennzahl für die Transparenz,
- Anzahl der Verarbeitungen, für die eine Prüfung der Rechtsgrundlagen erfolgreich abgeschlossen wurde als Kennzahl für die Nichtverkettung
- Antwortzeiten auf Anfragen Betroffener als Kennzahl für die Intervenierbarkeit

Hier kann die Praxis zeigen, welche Indikatoren für ein DSMS zu bilden wirklich sinnvoll sind und wie sie zur Verbesserung der Wirkung von Schutzmaßnahmen insbesondere bei hohem Schutzbedarf tatsächlich beitragen.

4. Referenzen

BSI: *ISMS (Informations-Sicherheitsmanagementsystem) https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ISMS/ISMS_1_Sicherheitsmanagement.html*

DIN: *https://www.din.de*

Reifegradmodell für Prozesse: Übersicht zu CMMI (Capability Maturity Model Integration) https://de.wikipedia.org/wiki/Capability_Maturity_Model_Integration#cite_note-Go08-2

5. Zusammenfassung der Maßnahmen

Ebene Daten

M80.01 Inventarisierung von Schutzmaßnahmen
M80.02 Planung der Inventarisierung der Bestandteil einer Verarbeitung

Ebene Systeme

M80.03 Erarbeitung eines Betriebskonzepts für IT-Infrastruktur
M80.04 Prüfung der Verträge mit Auftragsverarbeitern und Kooperationspartnern
M80.05 Erarbeitung eines Notfallplans
M80.06 Sicherung der Erfahrungen aus einem Notfall

Ebene Prozesse

M80.07 Ernennung eines Projektmanagers/einer Projektmanagerin, der/die das DSMS aufbaut
M80.08 Abgrenzung der Zuständigkeiten und Rolle des DSB
M80.09 Erarbeitung der Prüfprozesse des DSMS
M80.10 Sicherstellung von Ressourcen für das DSMS
M80.11 Erstellung eines Datenschutz-Konzepts
M80.12 Formulieren der Anforderungen an Verbesserungen
M80.13 Klärung von Teilverantwortlichkeiten
M80.14 Durchführung einer DSFA-Vorabprüfung in Bezug auf Risikofeststellung
M80.15 Durchführung einer DSFA (vollständig gem. Art. 35 DS-GVO)
M80.16 Unterrichtung und Verpflichtung der Mitarbeiter/-innen auf Datenschutz
M80.17 Planung innerbetrieblicher Datenschutz-Schulungen
M80.18 Erarbeitung von Anweisungen an Mitarbeiter/-innen in Bezug auf Einhaltung von Datenschutz-Anforderungen
M80.19 Prüfung der Freigabe von Verarbeitungen in Bezug auch auf Berücksichtigung datenschutzrechtlicher Anforderungen
M80.20 Einrichtung der beschränkten Zugriffe auf Daten der Verarbeitung

M80.21 Einrichtung des Incident-, Problem- und Changemanagement speziell für die Belange des Datenschutzes
M80.22 Klärung, welche Änderungen, Störungen und Probleme als datenschutzrelevant gelten
M80.23 Festlegen, welche Ereignisse als ein Datenschutz-Verstoß gelten
M80.24 Analyse von Datenschutzvorfällen, damit sich diese nicht wiederholen
M80.25 Prüfen, ob ein Datenschutzvorfall gemeldet werden muss
M80.26 Prüfen der Spezifikation von Abläufen und Schutzmaßnahmen im Hinblick auf deren Datenschutzkonformität
M80.27 Erstellung eines Konzepts zur Außerbetriebnahme einer Verarbeitung
M80.28 Erstellung eines Konzepts zum Austausch von Gerätschafen unter Beibehaltung des laufenden Betriebs
M80.29 Sicherstellung des Betriebs eines DSMS
M80.30 Sicherstellung, dass Veränderungen des DSMS nur durch Befugte erfolgt
M80.31 Sicherstellung, dass die Aktivitäten im Kontext des DSMS spezifiziert und dokumentiert sind und protokolliert werden
M80.32 Klärung, ob, inwieweit und in welcher Form Daten, die für Datenschutzprüfungen genutzt werden, an Externe übermittelt werden dürfen
M80.33 Sicherstellung der permanenten Verbesserung des DSMS selber
M80.34 Bildung von KPIs zur Messung der Effizienz eines DSMS
M80.35 Spezifikation und Dokumentation der Prozesse, die vom DSMS zu unterstützen sind
M80.36 Erstellung des Verzeichnisses von Verarbeitungstätigkeiten
M80.37 Ergänzung des Verzeichnisses für Verarbeitungstätigkeiten um Verarbeitungstätigkeiten, die das DSMS betreffen
M80.38 Dokumentation von Verantwortlichkeiten für Teilprozesse.
M80.39 Juristische Beurteilung eines DSFA-Berichts
M80.40 Formelle Freigabe der Verarbeitung durch den Verantwortlichen
M80.41 Anweisungen an Mitarbeiter zum Umgang mit datenschutzrechtlichen Anforderungen
M80.42 Sicherstellung der Stellvertretung von Rollen im DSM
M80.43 Dokumentation der datenschutzrechtlichen Zulässigkeit einer Verarbeitung

6. Anmerkung zur Nutzung dieses Bausteins

„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).“