D4 Datenschutzmanagement mit dem Standard- Datenschutzmodell

Das Datenschutzmanagement ist eine umfassende Methode, um systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umzusetzen. Im Folgenden wird ein Datenschutzmanagement im Zusammenspiel mit dem SDM näher beschrieben.

D4.1 Rechtliche Grundlagen des Datenschutzmanagements

Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss den Nachweis darüber erbringen können. Konkret muss der Verantwortliche gemäß Art. 30 DS-GVO ein Verzeichnis führen, in dem die personenbezogenen Verarbeitungstätigkeiten der Organisationen aufgelistet sind. Zudem muss er bereits zum Zeitpunkt der Festlegung der Mittel geeignete technische und organisatorische Maßnahmen treffen (Art. 25 Abs. 1 DS-GVO - Datenschutz durch Technikgestaltung). Für Verarbeitungstätigkeiten, die ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, muss er gemäß Art. 35 DS-GVO darüber hinaus eine Datenschutz-Folgenabschätzung (DSFA) durchführen. Um zu beurteilen, ob von einer Verarbeitungstätigkeit ein voraussichtlich hohes Risiko ausgeht und demnach die Durchführung einer DSFA erforderlich ist, muss für jede Verarbeitung eine Schwellwertanalyse durchgeführt werden. Auch ohne DSFA müssen geeignete technische und organisatorische Maßnahmen bestimmt und dauerhaft umgesetzt werden, um ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung personenbezogener Daten zu gewährleisten. Schließlich muss der Verantwortliche die Umsetzung und die Wirksamkeit der Maßnahmen nachweisen, evaluieren und ggf. verbessern können und auf diese Weise aktuell halten.

Damit der Verantwortliche den detaillierten Anforderungen in Bezug auf die operative Umsetzung der Betroffenenrechte und seinen Rechenschafts- und Nachweispflichten (vgl. Abschnitt B1.8) nachkommen kann, ist eine systematische Vorgehensweise bei der Prüfung und Beurteilung erforderlich, die sich sowohl auf jede einzelne Verarbeitungstätigkeit als auch auf sämtliche Verarbeitungstätigkeiten mit Personenbezug der gesamten Organisation und die dazu gehörigen technischen und organisatorischen Maßnahmen bezieht. Diese Rechenschafts- und Nachweispflichten sind eine dauerhafte Aufgabe für den Verantwortlichen und sollte daher als dauerhafter, zyklischer Prozess etabliert werden. Mit dem aus dem Qualitätsmanagement bekannten und bewährten PDCA-Zyklus (Plan, Do, Check, Act) steht ein kontinuierlicher Verbesserungsprozess in vier Phasen zur Verfügung, der die Grundlage für den hier beschriebenen Datenschutzmanagement-Prozess (DSM-Prozess) bildet. Der DSM-Prozess dient somit einerseits dem Verantwortlichen bei der systematischen Planung, dem dauerhaften Betrieb, der regelmäßigen Überprüfung der Datenschutzkonformität und der Verbesserung von Verarbeitungstätigkeiten. Er schafft somit Transparenz für den Verantwortlichen. Andererseits hilft der DSM-Prozess auch den Datenschutzaufsichtsbehörden bei der Beratung von Verantwortlichen und bei der datenschutzrechtlichen Prüfung dieser Verarbeitungstätigkeiten, da die Datenschutzprüfungen der Aufsichtsbehörden in der Regel diesem Prozess-Ablauf entsprechen.

D4.2 Vorbereitungen

Vor dem Start des DSM-Zyklus sind ebenso wie vor der Anwendung des SDM [1)] die folgenden drei Voraussetzungen zu klären:

1. Klarheit über die sachlichen Verhältnisse, im Rahmen derer die zu betrachtende Datenverarbeitung stattfindet oder stattfinden soll.
2. Prüfung der Zulässigkeit der Verarbeitung. [2)]
3. Weitere materiellrechtliche Beurteilungen der Rechtmäßigkeit dieser Verarbeitung.

Zur Feststellung der sachlichen Verhältnisse beim Verantwortlichen der Verarbeitungstätigkeit sind beispielsweise folgende Fragen zu klären:

- Welche Stellen sind an der Verarbeitung beteiligt?
- Wer trägt für welche Teile der Verarbeitung die Verantwortung?
- Welche Geschäftsprozesse des Verantwortlichen werden durch die Verarbeitung unterstützt?
- Welche Daten werden in welchen Schritten und unter Nutzung welcher Systeme und Netze verarbeitet?
- Welche Personen nehmen die Datenverarbeitung vor und durch welche Personen erfolgt eine Kontrolle?
- Welche Hilfsprozesse werden zur Unterstützung der Verarbeitungstätigkeit betrieben?

Im Rahmen der Prüfung der Zulässigkeit der Verarbeitung ist die Rechtsgrundlage für die Verarbeitung zu bestimmen. Dazu können bei der Verarbeitung personenbezogenen Daten [3)] insbesondere die folgenden aus Art. 6 Abs. 1 DS-GVO abgeleiteten Fragen herangezogen:

- Bilden Einwilligungen der Betroffenen die Rechtsgrundlage der Verarbeitungstätigkeit?
- Ist die Verarbeitung für die Erfüllung eines Vertrags erforderlich, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen?
- Ist die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt?
- Ist die Verarbeitung erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen?
- Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde?
- Ist die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich? Überwiegen dabei die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt?

Die materiellrechtliche Bewertung beurteilt, inwieweit die vom Verantwortlichen geplante und gegebenenfalls von der Aufsichtsbehörde zu prüfende Verarbeitungstätigkeit grundsätzlich zulässig ist. Darüber hinaus gibt sie Antworten insbesondere auf die folgenden Fragen, die die Anwendung des SDM vorbereiten:

- Welches nationale Datenschutzrecht ist auf die Verarbeitung anzuwenden?
- Welche legitimen Zwecke können mit der Verarbeitung verfolgt werden und welche

Zweckänderungen sind im Zuge der Verarbeitung zulässig?

- Welche Daten sind für die Erfüllung der zulässigen Zwecke erheblich und erforderlich?
- Welche Rechtsgrundlagen bestehen zur Übermittlung von Daten an Personen innerhalb und außerhalb der beteiligten Stellen sowie von diesen an Dritte?
- Sind die erforderlichen Vereinbarungen getroffen, wenn mehrere Verantwortliche in die Verarbeitungstätigkeit involviert sind und gemeinsam verantwortlich sind (Art. 26 DS-GVO)?

- Sind Auftragsverarbeiter in die Verarbeitung involviert und sind die

Rechtsverhältnisse zwischen ihnen geregelt (Art. 28 DS-GVO)?

- Welchen, auf den Einzelfall bezogenen, besonderen Anforderungen müssen die technischen und organisatorischen Maßnahmen genügen?

Ausführlichkeit und Detaillierungsgrad insbesondere der Feststellungen zu den sachlichen Verhältnissen werden von Verarbeitung zu Verarbeitung variieren, ebenso wie der Grad der Formalisierung des Vorgehens von informeller Befragung bis hin zum Einsatz von standardisierten Fragebögen. Eine strukturierte Zusammenfassung der Ergebnisse ist unabhängig davon ebenso üblich wie für die weiteren Schritte unentbehrlich. Die Feststellungen zu den sachlichen Verhältnissen gehen in die Phase 1 „Planen/Spezifizieren“ des DSM-Zyklus ein.

D4.3 Spezifizieren und Prüfen

Grundlegende Voraussetzung für ein Spezifizieren (siehe Abschnitt D4.5.1) und ein späteres Prüfen (siehe Abschnitt D4.5.3) ist die Festlegung, wie die Gewährleistungsziele für die betrachtete Datenverarbeitung operationalisiert werden.

- In Abhängigkeit vom festgestellten Risiko (siehe dazu auch Abschnitt D3) und unter Bezug auf die konkreten rechtlichen Anforderungen sind die aus den jeweiligen Gewährleistungszielen resultierenden Eigenschaften der Verarbeitungstätigkeit qualitativ näher zu bestimmen: **Verfügbarkeit** *Innerhalb von welchen Prozessen ist für wen die Verfügbarkeit von welchen Daten zu gewährleisten? Innerhalb welcher Zeiten müssen Daten für wen verfügbar und ggf. wiederherstellbar sein?* Der Einfluss der ordnungsgemäßen Verwendung der Daten auf die Interessen der Betroffenen ist der Maßstab für die Konkretisierung des Gewährleistungsziels der Verfügbarkeit.
- **Integrität** *Welche Daten sind auf eine identifizierte oder identifizierbare Person bezogen und müssen daher unversehrt und aktuell gehalten werden?* Wie wird sichergestellt, dass die Prozesse, Systeme und Dienste dem gesetzten Zweck entsprechend korrekt geplant, betrieben und kontrolliert werden? Auch hier ist das Interesse der Betroffenen der Maßstab.
- **Vertraulichkeit** *Wem ist die Kenntnisnahme welcher Daten zu verwehren? Welche Prozesse, Systeme und Dienste sind potentiell für unbefugte Zugriffe anfällig?* Das Ausmaß des befugten Zugriffs ist zunächst technikunabhängig aus den jeweiligen Geschäftsprozessen abzuleiten. Hiermit ist der Rahmen bestimmt, innerhalb dessen sich die Maßnahmen zum Vertraulichkeitsschutz gegenüber unbefugten Beschäftigten des Verantwortlichen zu bewegen haben. Der Rahmen für die Kenntnisnahme Dritter ist durch die in der materiell-rechtlichen Analyse festgestellten Übermittlungsbefugnisse gegeben.
- **Transparenz** *Wie und in welcher Form ist die Datenverarbeitung gegenüber betroffenen Personen und Aufsichtsbehörden transparent zu halten?* Es sind Anforderungen an die Informations- und Auskunftspflichten gemäß Art. 12 ff DS- GVO, die Benachrichtigungspflicht nach Art. 34 DS-GVO, an die Dokumentation der Verarbeitung nach Art. 30 DS-GVO, an die interne Dokumentation der Verarbeitungsvorgänge und deren Auswertbarkeit sowie an die Revisionsfähigkeit der Verarbeitung festzuhalten.
- **Intervenierbarkeit** *In welcher Ausprägung sind Betoffenenrechte zu gewähren?* Es muss festgelegt werden, wie betroffene Personen ihre Rechte wahrnehmen können, wie sichergestellt wird, dass Anfragen berechtigt stattfinden, wie in die Verarbeitung personenbezogener Daten eingegriffen werden kann (z. B. durch Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten) und in welche Form Daten von oder zu anderen

Verantwortlichen übertragen werden können.

- **Nichtverkettung** *Welche Zweckänderungen sind zulässig? Welche Zwecke von Hilfsprozessen leiten sich aus den Kernprozessen legitim ab?* Benötigt werden lediglich Aussagen zu solchen Zwecken, welche die Verantwortlichen tatsächlich verfolgen bzw. zu verfolgen beabsichtigen. Maßnahmen zur Gewährleistung der Nichtverkettung sollen mit dem Ziel ergriffen werden, die Verarbeitung oder Nutzung der Daten für alle außer den festgelegten legitimen Zwecken auszuschließen.
- **Datenminimierung** *Auf welche Weise wird das Gebot der Datenminimierung umgesetzt?* Es ist zu klären, wie die Kenntnisnahme von und die Ausübung welcher Verfügungsgewalt über welche Daten der Betroffenen durch welche Personen und Stellen zu minimieren sind. Dazu gehört es auch Speicherfristen für personenbezogene Daten sowie Prozesse zur Sicherstellung ihrer Einhaltung festzulegen. Ausgangspunkt sind dabei erneut die Interessen der Betroffenen, auch innerhalb einer Verarbeitung zu legitimen Zwecken die Belastung auf das erforderliche Maß zu begrenzen.
- **Belastbarkeit** *Sind Systeme und Prozesse auf Ereignisse, welche Störungen der regulären Abläufe verursachen, hinreichend vorbereitet?* Es ist zu klären, welche Schadensereignisse, Störungen oder Angriffe negative Auswirkungen für Betroffene haben können und ob hierfür Gegenmaßnahmen zur Verfügung stehen und diese zielgerichtet und zeitnah angewandt werden können. Aufgrund des Querschnittscharakters des Ziels der Belastbarkeit kann davon ausgegangen werden, dass bei einem hohen Reifegrad der Umsetzung der übrigen Gewährleistungsziele ein hinreichender Grad an Belastbarkeit erreicht ist.

Nachdem die Gewährleistungsziele bzgl. der Verarbeitungstätigkeit qualitativ konkretisiert wurden, können technische und organisatorische Maßnahmen bestimmt werden. Zu diesem Zweck werden die Ergebnisse der Datenschutzfolgen-Abschätzung herangezogen, sofern eine durchgeführt wurde. Das im Rahmen der Risikobeurteilung festgestellte Risiko für die Rechte und Freiheiten der von der Verarbeitung Betroffenen ist maßgeblich für das weitere Vorgehen. Ihr Ergebnis fließt in dreierlei Form in die weiteren Betrachtungen ein.

Zum Ersten können die Gewährleistungsziele quantitativ näher bestimmt werden. Beispiele für Präzisierungen sind Antworten auf folgende Fragen: Für welchen Zeitraum ist der Verlust der Verfügbarkeit der Daten für die Betroffenen in welchem Grad tolerabel? Mit welcher Verzögerung soll die Aktualität der Daten garantiert werden? Mit welcher zeitlichen Präzision muss die Verarbeitung im Nachhinein nachvollzogen werden können? In welchem zeitlichen Rahmen muss der Verantwortliche in der Lage sein, die jeweiligen Betroffenenrechte zu gewähren? Wie lange dürfen Daten zu welchen Zwecken verarbeitet werden, bevor diese von der Verarbeitung ausgeschlossen oder gelöscht werden?

Zum Zweiten bildet das Ergebnis der Risikoprüfung bzw. der Datenschutz-Folgenabschätzung die Grundlage für die Abwägung zwischen der Wahrung der Interessen der Betroffenen und dem hierfür erforderlichen Aufwand des Verantwortlichen. Für übliche Verarbeitungskontexte ist das Ergebnis einer solchen Abwägung durch die Darstellung typischer Referenzmaßnahmen in Kapitel D1 vorgezeichnet.

Zum Dritten fließt das Ergebnis der Datenschutz-Folgenabschätzung in die Bewertung der Restrisiken ein, die nach Umsetzung der Maßnahmen verbleiben, die mit einem Aufwand ergriffen werden können, der in angemessenem Verhältnis zum Zweck der Verarbeitung besteht. Diese Risiken können von dem Interesse Dritter oder Beteiligter abhängen, die Gewährleistungsziele zu verletzen, sei es um Daten der Betroffenen unbefugt zur Kenntnis zu nehmen, um sie für illegitime Zwecke, über das erforderliche Maß hinaus oder in intransparenter Weise zu verarbeiten.

D4.4 Datenschutzmanagement-Prozess

Ausgehend von den Vorbereitungen (siehe Abschnitt D4.2) kann bestimmt werden, in welcher Ausprägung die Gewährleistungsziele (siehe Abschnitt D4.3) anzuwenden und zu betrachten sind.

Der DSM-Prozess (siehe Abbildung 1) wird in Anlehnung an den bewährten PDCA-Zyklus ausgestaltet. Der Datenschutz-PDCA-Zyklus (DSM-Zyklus) umfasst die folgenden vier Phasen:

- Plan: Planen und Spezifizieren / DSFA / Dokumentieren
- Do: Implementieren / Protokollieren
- Check: Kontrollieren / Prüfen / Beurteilen
- Act: Verbessern

Das SDM unterstützt den Verantwortlichen bei der Durchführung von Schwellwertanalyse und Datenschutz-Folgenabschätzung und der daraus resultierenden Auswahl eines Satzes von technischen und organisatorischen Maßnahmen (Soll-Werte), indem individuell gewählte Maßnahmen mit den generischen Maßnahmen (vgl. Abschnitt D1) und den im Referenzmaßnahmen-Katalog vorgeschlagenen Maßnahmen abgeglichen werden (in **Phase 1** des DSM-Zyklus). Die ausgewählten Maßnahmen werden in **Phase 2** für den laufenden Betrieb umgesetzt. Die aus der Planungsphase resultierenden funktionalen Soll-Werte werden mit den aus dem laufenden Betrieb resultierenden funktionalen Ist-Werten verglichen (**Phase 3a**). Anschließend erfolgt eine Beurteilung der Erfüllung der rechtlichen Vorgaben und der ggf. verbleibenden Restrisiken für die Rechte und Freiheiten der Betroffenen (**Phase 3b**). Ein zu geringes Schutzniveau bzw. als zu hoch beurteilte Restrisiken müssen dann durch entsprechende Verbesserungen etwa durch zusätzliche Maßnahmen auf ein akzeptables Maß gemindert werden (**Phase 4**).

Die zum Ende von Phase 3 getroffene Beurteilung kann in der Folge sowohl Grundlage für die Empfehlung bzw. die Aufforderung der Aufsichtsbehörde als auch der Anweisungen des Verantwortlichen bilden, entweder durch zusätzliche technische oder organisatorische Maßnahmen die Defizite zu beheben oder von der Verarbeitungstätigkeit Abstand zu nehmen, soweit sich die Rechtskonformität nicht herstellen oder eine ausreichende Risikominderung mit verhältnismäßigen Mitteln nicht erreichen lässt (Phase 4 des DSM- Zyklus).

Die nachfolgende Grafik zeigt den gesamten DSM-Zyklus, in den das SDM eingebunden ist.

Abbildung 1: Der PDCA-Zyklus des Datenschutzmanagements (DSM-Zyklus) als Rahmen für die Anwendung des Standard- Datenschutzmodells bei Planungs-, Beratungs- und Prüfvorgänge

Für jede Verarbeitungstätigkeit wird es in der Regel erforderlich sein, den DSM-Zyklus mehrfach zu durchlaufen. Das betrifft insbesondere den Verantwortlichen bei der Planung von Verarbeitungstätigkeiten. So könnte bei der Inbetriebnahme eines Fachverfahrens ein erster Zyklus dessen Testbetrieb betreffen, der zweite Zyklus den Pilotbetrieb und der dritte Zyklus den Wirkbetrieb. Die Häufigkeit der Durchläufe hängt davon ab, wie weit der Verarbeitungskontext an die Erfordernisse des Datenschutzes in der Planungsphase oder im Rahmen eines Prüfprozesses der Aufsichtsbehörde angepasst werden musste.

D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren

In Phase 1 zur Planung einer Verarbeitungstätigkeit mit Personenbezug werden angemessene Maßnahmen bestimmt, durch die die Risiken des Grundrechtseingriffs gemildert, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. Um den Nachweis der Wirksamkeit der Maßnahmen erbringen zu können, müssen funktionale Anforderungen (Soll-Werte) festgelegt und dokumentiert werden. Diese werden aus den gesetzlichen Anforderungen (Soll) hergeleitet (siehe Teil B Anforderungen der DS-GVO). Erst dann wird festgelegt, welche Aktivitäten der Programme und Systeme und welche Ereignisse von Prozessen zu protokollieren sind.

Eine wesentliche Komponente der Phase 1 ist die Durchführung einer Schwellwert-Analyse und eine daraus ggfs. resultierende Datenschutz-Folgenabschätzung (DSFA).

Eine DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Ob ein voraussichtlich hohes Risiko durch eine Verarbeitungstätigkeit mit Personenbezug besteht, ist vorher im Rahmen einer obligatorischen Schwellwert-Analyse festzustellen (siehe Teil D3.2.1). Ein Ergebnis der DSFA ist der DSFA-Bericht, in dem die Risiken aufgezeigt und die Funktionen und technischen und organisatorischen Maßnahmen zur Verringerung von Risiken bestimmt werden. Häufig werden in diesem Bericht zusätzlich Empfehlungen zur weiteren Vorgehensweise bei der Implementierung der zu ergreifenden Maßnahmen angegeben, weil Art. 35 DS-GVO die Implementierung von solchen Abhilfemaßnahmen fordert.

Der Verantwortliche muss während der Phase 1 über die DSFA entscheiden. Am Ende der Phase 1 entscheidet er über die geplante Implementierung der Funktionen und der technischen und organisatorischen Maßnahmen.

Die Durchführung einer DSFA ist dabei kein einmaliger Vorgang. Sollten sich wesentliche Änderungen im Verfahren oder bei den Umständen der Verarbeitung , die die Bewertung bereits erkannter Risiken ändern, oder neue Risiken bekannt werden, so ist die DSFA zu überprüfen und anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung von Funktionen empfohlen. Dieser iterative Prozess der DSFA ist in den DSM-Prozess eingebunden.

Die Implementierung der empfohlenen Funktionen und der technischen und organisatorischen Maßnahmen geschieht in Phase 2 des DSM.

Weitere Details zur systematischen Durchführung einer Datenschutz-Folgenabschätzung können dem Kurzpapier Nr. 5 der Datenschutzkonferenz entnommen werden. [4)]

D4.4.2 Do: Implementieren / Protokollieren

In Phase 2 werden die aus den Ergebnissen der Phase 1 empfohlenen Maßnahmen entsprechend den Anweisungen des Verantwortlichen umgesetzt. Auf der Basis der Dokumentation der funktionalen Soll-Werte werden Aktivitäten von IT-Systemen und Administratoren und welche Ereignisse prüffähig dokumentiert und protokolliert. Beim Vorliegen eines DSFA-Berichts muss der Verantwortliche dessen Ergebnisse bei der Implementierung von Verarbeitungstätigkeiten berücksichtigen.

Bei der Implementierung von Systemen und Programmen ist darauf zu achten, dass anhand von System-Dokumenten und Protokollen die Funktionen der Fachapplikationen und der Schutzvorkehrungen von IT-Systemen und Diensten auf den verschiedenen Ebenen (Client, Server) überprüft werden können. Das Vorliegen dieser Dokumente und Protokolle (Ist- Werte) ist die

Voraussetzung zur Durchführung der Phase 3 des DSM.

D4.4.3 Check: Kontrollieren, Prüfen Beurteilen

Der Kern der Anwendung des SDM im DSM-Zyklus besteht darin, die in der Planungsphase bestimmten funktionalen Soll-Werte mit den festgestellten Ist-Werten in Beziehung zu setzen (Phase 3a). Zudem werden die relevanten Referenzmaßnahmen mit den tatsächlich umgesetzten technischen und organisatorischen Maßnahmen verglichen. Abweichungen vom Soll sind danach zu beurteilen, inwieweit sie die Umsetzung der Grundsätze aus Artikel 5 DS-GVO bzw. das Erreichen der Gewährleistungsziele gefährden. In einem Prüfvorgang der Aufsichtsbehörde erlaubt die bis zu diesem Punkt geführte Analyse aus einem Verfehlen der Gewährleistungsziele auf (ggf. sanktionierbare) datenschutzrechtliche Mängel zu schließen.

In der Prüf- und Beurteilungspraxis lässt sich häufig mit nur geringem Aufwand feststellen, ob Anforderungen nicht erfüllt werden, weil die entsprechend zugeordneten Maßnahmen fehlen, Maßnahmen falsch oder unzureichend umgesetzt sind oder die Referenzmaßnahmen nicht korrekt angewendet wurden. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Maßnahmen des Referenzmaßnahmen-Katalogs gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, muss separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Risiko entsprechen. An dieser Stelle hilft das SDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene technische oder organisatorische Maßnahme funktional äquivalent bzw. wirkungsgleich zur Referenzmaßnahme ist.

Ausgangspunkt für die datenschutzrechtliche Beurteilung einer Verarbeitungstätigkeit ist die Feststellung der funktionalen Soll-Ist-Differenzen. Diese Differenzen werden in der Beurteilungsphase (Phase 3b) wieder ins Rechtliche übersetzt und mit den datenschutzrechtlichen Anforderungen (Soll) verglichen. Im Rahmen einer datenschutzrechtlichen Beurteilung werden aus den festgestellten Abweichungen ggfs. „normative Mängel“. Je gravierender ein Mangel ist, umso wirksamer muss er durch entsprechende Änderungsanweisungen in Phase 4 des DSM-Prozesses für ein erneutes Durchlaufen aller Phasen des DSM-Zyklus abgestellt werden. Das Ergebnis der Phase 3b besteht in Beurteilungen, die geeignet sind, um rechtliche und funktionale Verbesserungen herbeizuführen.

D4.4.4 Act: Verbessern und Entscheiden

Die in Phase 3b festgestellten Mängel müssen so formuliert sein, dass anschließend konkrete funktionale Maßnahmen getroffen werden können. Diese Beurteilungen als Ergebnisse aus Phase 3 sind vom Verantwortlichen in Phase 4 zu sichten, zu beraten und zu priorisieren. In dieser Phase 4 müssen festgestellte Mängel zu Entscheidungen des Verantwortlichen und daraus resultierenden Anweisungen zu Änderungen von Maßnahmen oder zu neuen Maßnahmen führen, die dann im einen neuen Zyklus zu planen, zu implementieren und zu prüfen sind. Wurden Maßnahmen getroffen, die alle Mängel beseitigen, kann davon ausgegangen werden, dass alle Defizite beseitigt wurden und die Verarbeitungstätigkeit rechtskonform ist.

---

1) S. hierzu bereits Fn. 5.

2) Zur Differenzierung zwischen Zulässigkeit und Rechtmäßigkeit s. Kapitel A1.

3)

Werden besondere Kategorien personenbezogener Daten verarbeitet, ist zudem Art. 9 DS-GVO zu beachten.

4) https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf, Stand: 26.04.2018, letzter Aufruf: 01.04.2019.