Martin Rost, Sebastian Welke

SDM 2.0 und ITIL 4 „verschränkt“

Dieser Artikel zeigt auf, wie eine Umsetzung des Standard-Datenschutzmodells mit Elementen des IT-Service Management Best Practice „ITIL 4“ erfolgen kann.

1 Einleitung

Geschäftsführer geben die Umsetzung der Anforderungen der DSGVO gerne in die Hände ihrer CIOs oder IT-Leiter. In den IT-Abteilungen der Verantwortlichen sind vielfach bereits funktionierende Prozesse und Strukturen etabliert, in die eine Methode zur Sicherstellung des operativen Datenschutzes eingeordnet werden kann und sollte.

DatenschützerInnen legt dieser Artikel die Beschäftigung mit den wohlverstandenen „Management Practices“ von ITIL 4 nahe. Den ProzessgestalterInnen im ITIL-Kontext wird die Beschäftigung mit den Komponenten und Strategien des Standard-Datenschutzmodells („SDM“) nahegelegt. Das SDM unterstützt die vollständige und systematische Transformation von normativen Anforderungen der DSGVO in funktionale Anforderungen.

2 Was ist das SDM?

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder („DSK“) empfiehlt seit November 2019 die Anwendung des Standard-Datenschutzmodells in der Version 2.0 („SDM-V2“), um eine Verarbeitungstätigkeit konform mit der Datenschutz-Grundverordnung (DSGVO) zu gestalten, zu betreiben und prüfbar zu machen.[1]

a) Die für Praktiker wichtigste Eigenschaft des SDM-V2 besteht darin, dass die normativen Anforderungen der DSGVO auf **sieben Gewährleistungszielen** abgebildet werden: Sicherung der Verfügbarkeit, der Integrität und Vertraulichkeit, der Transparenz, Nichtverkettung/Datenminimierung und Intervenierbarkeit. Die „Grundsätze“ des Art. 5 DSGVO sind bereits begrifflich nahe an diesen Gewährleistungszielen formuliert.

Zu jedem Datenschutz-Ziel stellt das SDM einen generischen Katalog mit Standardschutzmaßnahmen bereit. Durch die Verbindung von normativen Anforderungen mit standardisierten Maßnahmen wissen Praktiker, was zu tun ist. Das heißt, dass Betriebswirte die Kosten für Schutzmaßnahmen schon zum Planungszeitpunkt anhand von Standardmaßnahmen zumindest grob kalkulieren und Datenschutzbeauftragte und Juristen, anhand der Qualität und des Umfangs der Umsetzung dieser Maßnahme, den Grad der normativen Compliance beurteilen können. Entwicklungsingenieure und Software-Architekten können der Anforderung nachkommen, tatsächlich „Datenschutz durch Design“ (Art. 25 DSGVO) umzusetzen, indem das vollständige Set der Standardmaßnahmen von Beginn an berücksichtigt wird. Und Verantwortliche können mit Rückgriff auf das SDM sehr viel genauer als bisher abschätzen, was Aufsichtsbehörden erwarten und ihre Entscheidungen zur Gestaltung der Verarbeitungstätigkeiten treffen.[2]

Als zweites Element bietet das Modell eine **Strategie zur Bestimmung der Intensität der Wirksamkeit** dieser Schutzmaßnahmen, die von der Bestimmung der Risikostufen abhängt (DSGVO: geringes/normales oder hohes Risiko).[3] Die Datenverarbeitung einer Organisation erzeugt Risiken für Betroffene, die deren Schutzbedarf entsprechen. Während der Schutzbedarf der Betroffenen konstant bleibt, können Schutzmaßnahmen das Risiko verringern, dass eine Organisation zu stark in die Rechte und Freiheiten von Personen eingreift. Erst wenn eine Verarbeitung unstrittig legitim ist, eine Rechtsgrundlage vorliegt und auch alle operativen Vorgaben der DSGVO umgesetzt sind, ist ein angemessenes Schutzniveau für die von der Verarbeitung betroffenen Personen erreicht.

Und das dritte Modellelement besteht in der **Unterscheidung von Komponenten**, die in einer personenbezogenen Verarbeitungstätigkeit eingesetzt werden. Das Modell verlangt, die zu verarbeitenden personenbezogenen Daten, die dafür verwendeten IT-Systeme und Dienste sowie die Subprozesse von Verarbei-

1 SDM-V2-Methode: https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf, SDM-Newsletter: https://www.datenschutzzentrum.de/mailinglisten/#sdm Inzwischen liegt eine Englisch-Übersetzung des SDM-V2 vor.

2 Eine wesentliche Entdeckung zu Beginn der Modellentwicklung war, dass Gewährleistungsziele in einem Widerspruch zueinander stehen (können). Das bedeutet, dass Schutzmaßnahmen einander schwächen können (Rost 2018).

3 Diese Überlegungen gehen auf die Art. 29-Gruppe im WP248 zurück, siehe: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Martin Rost

Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

E-Mail: martin.rost@datenschutzzentrum.de

Sebastian Welke

Abteilungsleiter Governance, Risk und Compliance Consulting bei der scienITec GmbH

E-Mail: sebastian.welke@scienitec.de

tungstätigkeiten, im Privatbereich würde man von „Geschäftsprozessen“ und im öffentlichen Bereich von „Verfahren“ sprechen, auszuweisen.

Damit sind die drei Dimensionen des SDM vollständig erfasst: 3 Komponentengruppen müssen anhand von 7 Gewährleistungszielen, denen Standard-Bausteine mit Referenzmaßnahmen zugeordnet sind, entsprechend einer der beiden Risikostufen einer Verarbeitungstätigkeit gestaltet werden. *Daraus folgt, dass für jede Verarbeitungstätigkeit mit Personenbezug (zur Definition vgl. Art. 4 Abs. 2 DSGVO) systematisch 21 generische Schutzmaßnahmen-Komplexe betrachtet werden müssen.*

b) Das SDM-V2 enthält ein Kapitel zu Datenschutzmanagement (DSM), dessen Phasenmodell dem Deming-Zyklus entspricht. Damit ist das Datenschutzmanagement an die gut eingeführte Begrifflichkeit des konventionellen Qualitätsmanagements herangeführt.[4]

Art. 32 Nr. 1 lit. d DSGVO fordert von Organisationen, ein Verfahren zur Evaluation der Wirksamkeit von Schutzmaßnahmen zu betreiben, was auf den Betrieb eines organisationsweiten Datenschutzmanagements hinausläuft, das wiederum dem „Stand der Technik“ (Art. 24 DSGVO) entspricht. Diese Anforderungen lässt sich zudem, bei etwas weiterer Auslegung, auch der Aufgabenbeschreibung eines oder einer Datenschutzbeauftragten entnehmen (vgl. Art. 39 Nr. 1 lit. b DSGVO).

In der Phase **Plan** ist im Datenschutz im Wesentlichen sicherzustellen, dass eine Verarbeitungstätigkeit die Datenschutzgrundsätze bzw. Gewährleistungsziele erfüllt und dies überwacht werden kann – über sämtliche Schichten der dabei heutzutage eingesetzten IT-Technik hinweg. Das Modell unterscheidet die Herstellung von Kontrollierbarkeit (Relevanzbilanzierung), Prüfbarkeit (Soll-/Ist-Bilanzierung), Beurteilbarkeit (Compliance-Bilanzierung) und Entscheidbarkeit (Verantwortlichkeitsbilanzierung). In der Plan-Phase ist ggfs. eine Datenschutz-Folgenabschätzung (vgl. Art. 35 DSGVO, „DSFA“) durchzuführen. Das Datenschutzmanagement hat organisationsübergreifend sicherzustellen, dass für jede Verarbeitungstätigkeit eine Dokumentation, eine Schwellwertanalyse sowie ggfs. anschließend ein DSFA-Bericht bzw. die Spezifikation oder ein Pflichtenheft bzgl. des Protokollierens als konkrete Produkte dieser Phase vorliegen. Dies gilt auch für die kontinuierliche Verbesserung des Betriebs des DSM selber.

Die Phase **Do** bedeutet im Wesentlichen die Implementation oder den Betrieb einer Verarbeitungstätigkeit mit den spezifizierten Schutzmaßnahmen des Datenschutzes. Diese Phase muss als Produkt für die nächste Phase funktionale, technische, messbare Prüfdaten einer Verarbeitungstätigkeit in Bezug auf Einhaltung der Grundsätze bzw. der Gewährleistungsziele des Datenschutzes liefern. Diese bestehen vielfach aus Protokolldaten, also aus Daten, die darüber Auskunft erteilen können, welche Ereignisse zu welchem Zeitpunkt in der Vergangenheit durch welche Instanzen erzeugt wurden. Die Dokumentation muss helfen, relevante Prüfergebnisse methodisch erzeugen zu können. Das DSM muss wiederum dafür sorgen, dass alle Verarbeitungstätigkeiten Prüfdaten liefern können, insbesondere solche aus IT-Infrastrukturen, auf denen die einzelnen Verarbeitungstätigkeiten aufsetzen.

In der Phase **Check** müssen die technischen Prüfergebnisse in normative Prüfergebnisse übersetzt und dann im Lichte der normativen Vorgaben der DSGVO, der Rechtsprechung, der Verträge und auch der technischen Entwicklungen, die beständig einem Wandel unterliegen, beurteilt werden. Technische Abweichungen bei Prüfergebnissen müssen normativ nicht von Bedeutung sein, was zu beurteilen der juristischen Expertise überlassen bleibt. Aber auch juristische Beurteilungen können sich mit der Zeit ändern. Das Produkt dieser Phase besteht in konkreten Empfehlungen zur Verbesserung der Compliance einer Verarbeitungstätigkeit mit der DSGVO an die Leitung einer Organisation. Das DSM muss sicherstellen, dass alle Verarbeitungstätigkeiten kontinuierlich einer juristischen Beurteilung zum Zweck der Verbesserung der Compliance unterzogen werden.

In der Phase **Act** muss der Verantwortliche Entscheidungen zu den Empfehlungen für Verarbeitungstätigkeiten treffen. Das Produkt dieser Bewertungs- und Priorisierung-Phase sind insofern Anweisungen, welche der empfohlenen Funktionen bzgl. Datenschutz mit welcher Priorität umzusetzen sind. Mit dem Erteilen von Anweisungen kann erneut in die Planungsphase eingetreten werden. Auf diese Weise kann ein zyklisch geschlossenes System des Datenschutzmanagements entstehen.

Wie man nun im Detail funktionale Maßnahmen planen und umsetzen und deren permanente Überwachung und Fortentwicklung im Detail sicherstellen kann, können Datenschützer aus dem Kontext von ITIL (Information Technology Infrastructure Library) lernen.

3 Was ist ITIL?

ITIL wurde in den 1980er-Jahren von der britischen Central Computing and Telecommunications Agency (CCTA) als lose Sammlung von Best Practices mit dem Ziel veröffentlicht, die Erbringung von IT-Services zu standardisieren und kosteneffizienter zu gestalten. Über die Jahre und einige Iterationen entstand hierdurch ein De-Facto-Standard für das Management von IT-Services, der sich in IT-Organisationen großer Beliebtheit erfreut. In der neuesten Edition (ITIL 4 Edition) erhebt ITIL den Anspruch, sich nicht mehr ausschließlich für das Managen von IT-Services, sondern für sämtliche technologiebasierten Dienstleistungen zu eignen.

Mit der 2019 veröffentlichten vierten Edition von ITIL haben einige neue Paradigmen Einzug in ITIL gehalten. Das bisher propagierte Lebenszyklusmodell tritt etwas in den Hintergrund, bleibt aber erkennbar und wird Teil eines neu strukturierten, ganzheitlichen Ansatzes zum Managen technologiebasierter Services. In den Vordergrund tritt das Prinzip der Wertorientierung.

Der deutlich modularere Aufbau von ITIL 4 macht es möglich, einzelne Elemente durch spezifischere oder bereits im Unternehmen etablierte Standards und Methoden zu ersetzen bzw. diese miteinander zu verzahnen.

ITIL 4 enthält zwei Kernelemente, das „Vier-Dimensionen-Modell“ und das „Service-Wertesystem“. Diese Elemente sind wiederum unterteilt in weitere Standard-Elemente.

Das „**Vier-Dimensionen-Modell**“ benennt Teilbereiche, auf die das Management sein Augenmerk richten soll, wenn eine Organisation technologiebasierte Services planen, erbringen und wo-

4 Hier besteht oft das Problem, dass mit einem gemeinsamen Prozessframework Risiko-Kalküle einer Domäne (bspw. des IT-Sicherheitmanagements) andere Domänen, wie bspw. dem Datenschutz-Management zur Umsetzung von DSGVO-Anforderungen, übergestülpt werden. Das darf nicht passieren. Rechtsdogmatisch betrachtet führt Datenschutz vor IT-Sicherheit.

möglich vermarkten soll. Im Einzelnen handelt es sich um die Dimensionen

- „Organisationen und Personen",
- „Informationen und Technologien",
- „Partner und Lieferanten" sowie
- „Wertströme und Prozesse".

Zur Schaffung von Werten appelliert ITIL 4, alle Dimensionen mehr oder weniger gleichwertig zu betrachten. Das „**Service-Wertesystem**" umfasst fünf Kernelemente:

1. die Grundprinzipien,
2. die Governance,
3. die Service-Wertschöpfungskette,
4. das „Continual Improvement Model" und
5. die „Management-Praktiken" („Management Practices").

Die **Grundprinzipien** (1.) sind geprägt von einem ganzheitlichen Denken und Handeln sowie der inhaltlichen Konzentration auf das Schaffen von Werten. Dabei gilt die Idee, schnell zu starten, die Organisation in iterativen Zyklen weiter zu entwickeln und einen gewichtigen Wert auf Einfachheit, Optimierung und Automatisierung zu legen:[5]

- Wertorientierung!
- Dort beginnen, wo man steht!
- Iterative Weiterentwicklung mit Feedback!
- Zusammenarbeit und Transparenz fördern!
- Ganzheitlich denken und arbeiten!
- Auf Einfachheit und Praktikabilität achten!
- Optimieren und automatisieren!

Die **Governance** (2.) meint die Einbindung in das übergreifende Management-System der Organisation.

Die **Service-Wertschöpfungskette** (3.) beinhaltet die folgenden sechs Aktivitäten, von denen jede etwas zur Wertschöpfung beiträgt:[6] Der Zweck der Aktivität „*1. Planung*" ist ein gemeinsames Verständnis der Vision, des aktuellen Stands und der Verbesserungsrichtung für alle vier Dimensionen und alle Produkte und Dienstleistungen der Organisation sicherzustellen. Die Aktivität „*2. Verbesserung*" soll eine kontinuierliche Verbesserung von Produkten, Services und Practices über alle Aktivitäten der Wertschöpfungskette und die vier Dimensionen des Service Managements hinweg sicherstellen. Die Aktivität „*3. Engagement*" soll ein gutes Verständnis der Bedürfnisse der Stakeholder, Transparenz, kontinuierliches Engagement und gute Beziehungen zu allen Stakeholdern fördern. Die Aktivität „*4. Design und Transition*" soll sicherstellen, dass Produkte und Services die Erwartungen der Stakeholder an Qualität, Kosten und Zeit bis zur Markteinführung kontinuierlich erfüllen. Die Aktivität „*5. Erhalten/Erstellen*" ist sicherzustellen, dass Servicekomponenten verfügbar sind, wann und wo sie benötigt werden, und dass sie den vereinbarten Spezifikationen entsprechen. Die Aktivität „*6. Bereitstellung und Support*" der Wertschöpfungsketten ist sicherzustellen, dass Services gemäß den vereinbarten Spezifikationen und den Erwartungen der Stakeholder bereitgestellt und supportet werden.

Das „**Continual Improvement Model**" (4.) zur kontinuierlichen Verbesserung erscheint in ITIL 4 auf strategischer, taktischer und operativer Ebene. Es stellt der Organisation einen strukturierten Ansatz für die Umsetzung von Verbesserungen zur Verfügung. Es besteht aus einem siebenphasigen Prozess, der dem PDCA-Zyklus ähnelt, wie ihn auch das SDM-V2 beschreibt.

Die „**ITIL Management Practices**" (5.) gliedern sich in 14 allgemeine Management-Praktiken, 17-Service Management-Praktiken und drei technische Management-Praktiken. Die ITIL 4 Publikation widmet jeder Praktik einen eigenen Abschnitt und stellt ihren Zweck in einer Schlüsselbotschaft gleich zu Beginn eines jeden Abschnitts klar. Man findet außerdem in jeder Practice eine Vielzahl an erwiesen wirksamen Empfehlungen, wie diese Aufgaben konkret in Organisationen zu managen sind.

Die **allgemeinen Management Practices** umfassen Architecture Management, Continual Improvement, Information Security Management, Knowledge Management, Measurement and Reporting, Organizational Change Management, Portfolio Management, Project Management, Relationship Management, Risk Management, Service Financial Management, Strategy Management, Supplier Management sowie Workforce and Talent Management.

Die **Service Management Practices** beinhalten Availability Management, Business Analysis, Capacity and Performance Management, Change Enablement, Incident Management, IT Asset Management, Monitoring and Event Management, Problem Management, Release Management, Service Catalogue Management, Service Configuration Management, Service Continuity Management, Service Design, Service Desk, Service Level Management, Service Request Management und Service Validation and Testing.

Deployment Management, Infrastructure and Platform Management sowie Software Development and Management bilden die **technischen Management Practices**.[7]

4 Wie gelingt die Integration von SDM-V2 und ITIL 4?

a) Um SDM und ITIL funktional miteinander zu verbinden, bedarf es zunächst einer begrifflichen Klärung bzgl. Verarbeitungstätigkeit und Services. Die DSGVO definiert „Verarbeitungstätigkeiten" in Art. 4 Nr. 2 mit Bezug zu 14 Aktivitäten – von „Erheben" bis „Löschen/Vernichten". ITIL stellt dagegen Services in den Mittelpunkt der Betrachtung. Diese sind definiert als „Möglichkeit, gemeinsamen Wert zu schaffen, indem das Erreichen der von Kunden gewünschten Ergebnisse erleichtert wird, ohne dass der Kunde bestimmte Kosten und Risiken managen muss."[8] Die Verarbeitungsarten gem. Art. 4 Nr. 2 DSGVO finden sich regelmäßig als wesentliche Bestandteile von IT Services wieder. Daher kann stark vereinfacht festgehalten werden, dass IT Service Management letztlich all diese Verarbeitungstätigkeiten managt.

b) Um Service-Management und Datenschutz-Management miteinander zu verzahnen, bietet sich das Vier-Dimensionen-Modell von ITIL 4 zu nutzen als Basis an.

In der Dimension „**Organisationen und Menschen**" wäre beispielsweise das Problem zu lösen, die Organisation und die ihr angehörenden Menschen auf das Thema Datenschutz vorzubereiten. Konkrete Fragestellungen können sein, ob die Organisation durch Definition von Rollen, Verantwortlichkeiten, Kompetenz-

5 Die ITIL 4 Publikation widmet jedem Grundprinzip einen eigenen Abschnitt, mangels Platzes können wir diese leicht verständlichen Prinzipien hier nicht wiedergeben, siehe dazu: ITIL® Foundation, ITIL 4 Edition, Kapitel 4.3: Die ITIL-Grundprinzipien

6 ITIL® Foundation, ITIL 4 Edition, Kapitel 4.5: Service-Wertschöpfungskette

7 ITIL® Foundation, ITIL 4 Edition, Kapitel 5: ITIL Management Practices

8 ITIL® Foundation, ITIL 4 Edition, Kapitel 2.3.1: Konfigurieren von Ressourcen für die Wertschöpfung

und Kommunikationssysteme gut definiert ist[9], um Datenschutz-Anforderungen in gebotener Zeit umsetzen zu können oder ob alle Mitarbeiter im Datenschutz unterwiesen wurden.

Die Dimension „**Informationen und Technologien**" betrachtet die Informationen und Kenntnisse, die für das Management von Services, Technologien sowie der Beziehungen zwischen verschiedenen Komponenten des Service-Wertesystems erforderlich sind.[10] Der Bezug zum Datenschutz wird hier schon in der Namensgebung offensichtlich. Wesentliche Elemente des Datenschutzes, wie beispielsweise der Eintrag im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) einschließlich Identifikation und Dokumentation der verarbeiteten personenbezogenen Daten, die Datenschutzfolgenabschätzung sowie die technischen und organisatorischen Maßnahmen sind in dieser Dimension zu verorten.

Die Dimension „**Partner und Lieferanten**" reflektiert, dass technologiebasierte Services im Zuge fortschreitender Spezialisierung ganz oder teilweise durch Dritte erbracht werden können. Sie umfasst die Beziehungen einer Organisation zu anderen Organisationen, die an Design, Entwicklung, Deployment, Bereitstellung, Support und/oder kontinuierlicher Verbesserung von Services beteiligt sind. Sie umfasst auch Verträge und andere Vereinbarungen zwischen der Organisation und ihren Partnern oder Lieferanten.[11] Folglich können und sollten hier auch die mit der Einbindung Dritter verbundenen Fragestellungen des Datenschutzes, also Auftragsverarbeitungsvereinbarungen, Offenlegung, Drittlandsübermittlungen an externe Dienstleister etc., angesiedelt werden.

Die Dimension „**Wertströme und Prozesse**" betrachtet, wie die verschiedenen Teile der Organisation auf integrierte und koordinierte Weise zusammenarbeiten, um durch Produkte und Services Wertschöpfung zu ermöglichen. Die Dimension konzentriert sich darauf, welche Aktivitäten die Organisation unternimmt und wie diese organisiert sind, und auch darauf, wie die Organisation sicherstellt, dass sie effizient und effektiv Wertschöpfung für alle Stakeholder ermöglicht.[12] Im Kontext des Datenschutzes entfaltet diese Dimension gleich in zweierlei Hinsicht ihre Wirkung. Zum einen können hier systematisch alle Prozesse betrachtet werden, die auf ein funktionierendes Datenschutz Management System abzielen und auf diese Weise einen Wertbeitrag leisten. Zum anderen empfiehlt es sich, in dieser Dimension auch die Nicht-Datenschutzprozesse daraufhin zu untersuchen, dass bei allem Zusammenwirken mit dem Ziel der Wertschöpfung, der Wert des Datenschutzes ausreichende Beachtung findet. Ein Beispiel hierfür ist der Grundsatz der Zweckbindung. Nur allzu leicht werden personenbezogene Daten Gegenstand eines Wertstroms und finden sich in einer Verarbeitung wieder, deren Zweck nicht mit dem der ursprünglichen Verarbeitung zu vereinbaren ist. Dies verstößt gegen den Grundsatz der Zweckbindung. Das SDM bietet da Hilfestellung, wie Prozesse getrennt und dann, unter rechtlich kontrollierten Einschränkungen, aufeinander bezogen werden können.

c) Außerdem kann die Umsetzung der Maßnahmen des SDM durch die Aktivitäten und Management-Praktiken von ITIL unterstützt erfolgen. Die Umsetzung einer Maßnahme wird zunächst als Anforderungen in die Aktivität „*Planung*" eingesteuert. Die Planungsaktivität analysiert, wo die Organisation im Hinblick auf diese Maßnahme steht. Sie gibt eine Zielrichtung vor und ermittelt grob die Lücken und Mängel. Ergebnis der Planungsaktivität sind sogenannte „Outputs", die als „Inputs" von den Folgeaktivitäten aufgegriffen und weiterentwickelt werden. Die im Rahmen der Aktivität „*Planung*" maßgeblich unterstützenden Aktivitäten sind: Architecture Management, Continual Improvement, Information Security Management, Measurement and Reporting, Portfolio Management, Risk Management, Strategy Management, Availability Management, Service Continuity Management und Service Level Management.

Die Aktivität „*Design und Transition*" greift die Vorgaben der Planungsaktivität auf, um die Umsetzung der SDM Maßnahme in einem Service bzw. einer Servicekomponente zu konzipieren. Möglicherweise interagiert sie dazu auch mit der Aktivität „*Engagement*" und lässt hierdurch Produkt- und Serviceanforderungen spezifischer Stakeholder in das Design einfließen. Gleichsam können Erkenntnisse und Komponenten zu bereits bestehenden Services mit Datenschutzbezug, welche aus den Aktivitäten „*Verbesserung*" sowie „*Bereitstellung und Support*" zur Verfügung gestellt werden, in das Design einfließen. Im Rahmen dieser Aktivität können die folgenden Praktiken unterstützen: Architecture Management, Continual Improvement, Information Security Management, Measurement and Reporting, Project Management, Relationship Management, Risk Management, Service Financial Management, Supplier Management, Change Enablement, IT Asset Management, Release Management, Service Configuration Management, Service Design, Service Validation and Testing, Deployment Management und Infrastructure and Platform Management.

Die Aktivität „*Erhalten/Erstellen*" übernimmt die Anforderungen und Spezifikationen von der Aktivität „*Design und Transition*". Basierend auf bestehenden Produkten und Services und möglicherweise erforderlichen neuen Produkten und Services, die in Zusammenarbeit mit der Aktivität „*Engagement*" beschafft werden müssen, wird der Service nun „gebaut". Folgende Praktiken flankieren die Aktivität Erhalten/Erstellen: Continual Improvement, Information Security Management, Measurement and Reporting, Project Management, Risk Management, Supplier Management, Business Analysis, Change Enablement, IT Asset Management, Service Configuration Management, Service Design, Service Validation and Testing, Deployment Management, Infrastructure and Platform Management sowie Software Development and Management.

Die Aktivität „*Design und Transition*" nimmt die Umsetzung ab und überführt sie dann in den Regelbetrieb. Dieser erfolgt im Rahmen der Aktivität „*Bereitstellung und Support*". Wesentliche Practices, die mit der Aktivität interagieren, sind: Continual Improvement, Information Security Management, Knowledge Management, Risk Management, Supplier Management, Change Enablement, Incident Management, Monitoring and Event Management, Problem Management, Service Desk und Service Request Management.

Die Aktivität „*Verbesserung*" überwacht die Servicequalität und initiiert Anpassungen des Services zur kontinuierlichen Verbesserung. Practices, die hier einen Wertbeitrag leisten, sind: Architecture Management, Continual Improvement, Knowledge Management, Measurement and Reporting, Organizational Change Management, Relationship Management, Risk Management,

9 ITIL® Foundation, ITIL 4 Edition, Kapitel 3.1: Organisationen und Menschen

10 ITIL® Foundation, ITIL 4 Edition, Kapitel 3.2: Informationen und Technologie

11 ITIL® Foundation, ITIL 4 Edition, Kapitel 3.3: Partner und Lieferanten

12 ITIL® Foundation, ITIL 4 Edition, Kapitel 3.4: Wertströme und Prozesse

Workforce and Talent Management, Capacity and Performance Management, Change Enablement, Problem Management sowie Infrastructure and Platform Management.

d) Es gibt eine Reihe weiterer Elemente des SDM-V2, die mithilfe der Aktivitäten und Praktiken von ITIL 4 ohne Schwierigkeiten generiert werden können. So kann beispielsweise der gesamte Themenkomplex der Nachprüfbarkeit technischer und organisatorischer Maßnahmen mit ITIL Mechanismen abgebildet werden. Das SDM empfiehlt hierzu **Spezifikationen** für zukünftige, geplante Maßnahmen, **Dokumentationen** für den aktuellen Stand und **Protokolle** für Ereignisse der Vergangenheit. Spezifikationen werden in den Aktivitäten „*Planung*" sowie „*Design und Transition*" erarbeitet. Dokumentationen entstehen regelmäßig in der Aktivität „*Erhalten/Erstellen*". Protokolle (Events, Incidents, Problems, etc.) entstehen im Tagesgeschäft der Aktivität „*Bereitstellung und Support*". **Verträge** (wie z.B. Auftragsverarbeitungsvereinbarungen) sind regelmäßig Gegenstand der Aktivität „*Engagement*" und dort speziell in der Praktik „*Provider Management*" zu verorten.

Auch die **Umsetzung von Betroffenenrechten** treibt die Aktivität Engagement, da dort die Aufgabe liegt, die Beziehungen zu allen Stakeholdern, und somit auch mit betroffenen Personen, zu managen. Wesentliche Practice hierfür ist das „*Service Request Management*". Denkbar ist auch, dass Betroffenenrechte über die Practice „Service Catalogue Management" Eingang in den (elektronischen) Service-Katalog der Organisation finden, um dem Gedanken der vereinfachten Ausübung der Betroffenenrechte im Sinne des Erwg. 59 DSGVO Rechnung zu tragen.

e) Abschließend sei noch genannt, dass die Practice *Service Configuration Management* einen erheblichen Beitrag zur Dokumentation technischer und organisatorischer Maßnahmen leisten kann. Voraussetzung ist, dass Maßnahmen konsequent als Sub-Services modelliert und im Rahmen des Service-Modells übergeordneten Services zugeordnet werden. So „vererbt" beispielsweise der Sub-Service ‚Backup' seine Eigenschaft, auf das Gewährleistungsziel *Verfügbarkeit* einzuzahlen, auf den Service ‚Datenbankserver', der ihn nutzt. Oder der Service ‚E-Mail' „erbt" im Hinblick auf das Gewährleistungsziel Vertraulichkeit die Eigenschaft des von ihm verwendeten Sub-Service „PKI".

5 Fazit

Das Phasenmodell des SDM-V2a für ein Datenschutz-Managementsystem kann in die Standard-Services-Practices von ITIL 4 ohne Schwierigkeiten integriert werden, um Verarbeitungstätigkeiten zweckbestimmt zu planen, umzusetzen, zu kontrollieren und permanent zu verbessern. ITIL 4 als organisationsweites Management-Framework eignet sich insofern zur Umsetzung von Datenschutz-Anforderungen sehr viel besser als bspw. ein isoliertes IT-Security-Managementsystem, das selber nur einen Teilausschnitt des ITIL 4-Frameworks bildet und dabei auch nur zu einem kleinen Teil und nicht konfliktfrei die Umsetzung der vielfältigen Datenschutz-Anforderungen in den Blick stellen kann.

Literatur

Axelos 2020: ITIL® Foundation, *ITIL 4 Edition* (German Edition), https://www.axelos.com/.

DSK 2019: *Das Standard-Datenschutzmodell V2a* – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, https://www.datenschutzkonferenz-online.de/media/ah/20191209_sdm-methode_v2.0a.pdf.

Rost, Martin, 2018: *Die Ordnung der Schutzziele*, in: DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 13-18.