Anna Cardillo, Martin Rost

Der SDM-Würfel für Jurist*innen

Regelungsbedarfe für die Verarbeitungspraxis systematisch analysieren und bearbeiten

Spätestens seit einer aktuellen Entscheidung des LG Mannheim wird es für Jurist*innen Zeit, sich mit dem Standard-Datenschutzmodell zu beschäftigen. Wie auch immer man zu dem Modell stehen mag – es ist bei den deutschen Gerichten angekommen. Dieser Artikel möchte insbesondere Jurist*innen aufzeigen, wie sie zur datenschutzrechtlichen Analyse und Bearbeitung der von der DSGVO vorgegebenen Risiken insbesondere den SDM-Würfel des Standard-Datenschutzmodells heranziehen und juristische Regelungsbedarfe identifizieren können.

1 Einleitung

Das LG Mannheim hat sich in einem Rechtsstreit (Az: 1 O 93/23) mit der Frage beschäftigt, ob der Wegfall der „Unbeschwertheit" der Nutzung von Social Media bei Scraping von personenbezogenen Daten aus sozialem Netzwerk einen immateriellen Schadensersatzanspruch nach Art. 82 DSGVO begründet. Das Gericht verneinte einen solchen Anspruch. Allein der objektive Kontrollverlust reiche nicht aus, um einen solchen zu bejahen (LG Mannheim, Urt. v. 15.03.2024 – Az.: 1 O 93/23). So spannend, wie die Frage, was ein Schaden im Sinne von Art. 82 DSGVO ist, sein mag, so beachtenswert sind die weiteren Ausführungen des Gerichts:

Martin Rost

ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und u.a. Leiter der Arbeitsgruppe zur Entwicklung des „Standard-Datenschutzmodells" (SDM).

E-Mail: martin.rost@datenschutzzentrum.de

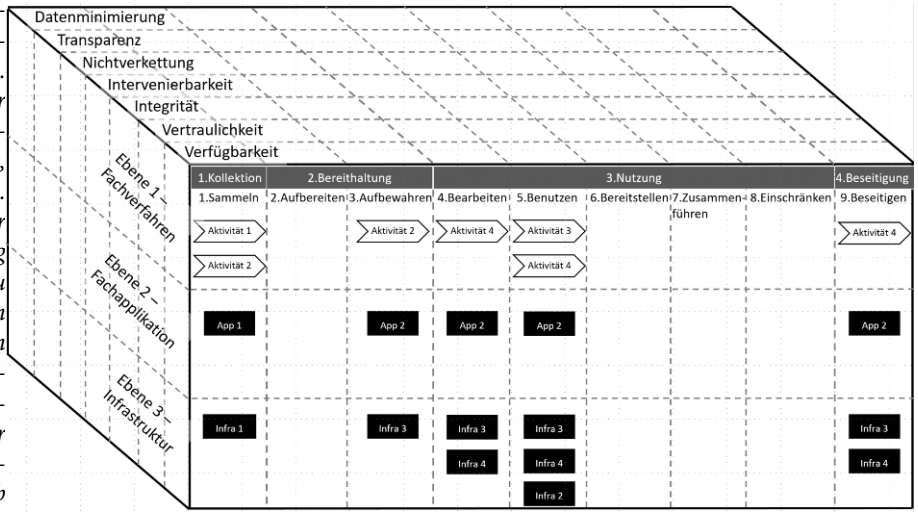
Anna Cardillo

ist Rechtsanwältin und Partnerin bei MYLE, einer auf IT-, Daten- und Datenschutzrecht spezialisierten Boutique-Kanzlei.

E-Mai: anna.cardillo@myle-law.com

„Es oblag der Beklagten aufgrund ihrer Rechenschaftspflicht in Art. 5 Abs. 2, 24 Abs. 1 DSGVO darzulegen und zu beweisen, dass die von ihr getroffenen Sicherheitsmaßnahmen i.S.v. Art. 32 DSGVO in diesem Sinne geeignet waren (vgl. EuGH, Urteil vom 14.12.2023 – C-340/21). Dies hat die Beklagte nicht schlüssig getan. Die Beklagte hat sich in ihrem Vortrag darauf beschränkt, Maßnahmen wie Übertragungsgrenzen oder Bot-Erkennung schlagwortartig zu benennen. Die Anforderungen des Art. 32 DSGVO liegen jedoch weit höher. Richtig weist die Beklagte darauf hin, dass ihr ein Entscheidungs- bzw. Ermessensspielraum bei der Wahl der geeigneten technischen und organisatorischen Maßnahmen zugestanden habe. Gleichwohl muss ein nationales Gericht die komplexe Beurteilung, die der Verantwortliche vorgenommen hat, bewerten können und sich dabei vergewissern können, dass die vom Verantwortlichen gewählten Maßnahmen geeignet sind, ein solches Sicherheitsniveau zu gewährleisten. Es muss eine materielle Prüfung dieser Maßnahmen anhand aller in diesem Artikel genannten Kriterien sowie der Umstände des Einzelfalls und der dem Gericht dafür zur Verfügung stehenden Beweismittel vornehmen. Eine solche Prüfung erfordert eine konkrete Untersuchung sowohl der Art als auch des Inhalts der vom Verantwortlichen getroffenen Maßnahmen, der Art und Weise, in der diese Maßnahmen angewandt wurden, und ihrer praktischen Auswirkungen auf das Sicherheitsniveau, das der Verantwortliche in Anbetracht der mit dieser Verarbeitung verbundenen Risiken zu gewährleisten hatte (vgl. EuGH, Urteil vom 14.12.2023 – C-340/21, Rn. 43). Gemessen hieran hat die Beklagte nicht schlüssig vorgetragen, dass sie ihr Ermessen pflichtgemäß ausgeübt hat. So hätte es zunächst einer Bewertung des Schutzniveaus der Daten (nach BSI-Grundschutz 200-2: „Schutzbedarfsfeststellung"; ebenso das Standard-Datenschutzmodell der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) bedurft. Jedoch fehlt jeglicher Vortrag der Beklagten zu dem Schutzniveau nicht nur der stets öffentlichen Daten, sondern vor allem der Telefonnummer. Weiter bedarf es einer Betrachtung der Daten in den verschiedenen Verarbeitungsvorgängen, hier also speziell der Kontakt-Import-Funktion (nach

Abbildung 1 | Der SDM-Würfel (vgl. DSK 2024, S. 47)



*BSI-Grundschutz 200-2: „Erfassung der Geschäftsprozesse"; nach Standard-Datenschutzmodell: „Verarbeitungstätigkeit (Geschäftsprozesse)". Ob die Beklagte die Verarbeitung der Telefonnummer bei diesem Verarbeitungsvorgang überhaupt beachtet hat, ist weder vorgetragen noch ersichtlich. Ausgehend von dem Schutzniveau der Daten und dem Verarbeitungsvorgang war es erforderlich etwaige Risiken zu identifizieren und zu bewerten (nach BSI-Grundschutz: Risikoanalyse; nach Standard-Datenschutzmodell: Risikobetrachtung). Auch hierzu fehlt konkreter Vortrag. Die Beklagte gibt zwar pauschal an, dass das Risiko von Scraping schon immer bestanden habe. Ob und zu welchem Ausmaß die Beklagte sich jedoch gerade für die Kontakt-Import-Funktion der Möglichkeit eines Missbrauchs durch das gegenwärtige Angriffsszenario der sequentiellen Telefonnummernerstellung und -abfrage bewusst war, bleibt offen. Erst jetzt, also wenn das Schutzniveau der personenbezogenen Daten bestimmt, die beteiligten Verarbeitungsvorgänge (Geschäftsprozesse) analysiert und die einzelnen Risiken diesbezüglich festgestellt und bew*ertet *worden sind, kommt es auf die konkreten technischen und organisatorischen Maßnahmen an, um den jeweiligen Risiken in geeigneter und angemessener Weise zu begegnen (nach BSI-Grundschutz 200-2: „Modellierung). Entsprechend unterscheidet auch der Europäische Gerichtshof zwischen zwei Schritten: Zum einen sind die von der betreffenden Verarbeitung ausgehenden Risiken einer Verletzung des Schutzes personenbezogener Daten und ihre möglichen Folgen für die Rechte und Freiheiten natürlicher Personen zu ermitteln. Diese Beurteilung muss konkret unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der ermittelten Risiken erfolgen. Zum anderen ist zu prüfen, ob die vom Verantwortlichen getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke dieser Verarbeitung diesen Risiken angemessen sind (EuGH, Urteil vom 14.12.2023 – C-340/21, Rn. 42). Den Ausführungen der Beklagten ist nach alledem schon nicht zu entnehmen, dass sie in dieser strukturierten Weise vorgegangen wäre. Dabei ist organisatorischer Datenschutz ein wesentlicher Bestandteil, um die Sicherheit der Verarbeitung zu gewährleisten (ausführlich zur Methodik: BSI-Grundschutz 200-2 oder auch das Standard-Datenschutzmodell). Die schlagwortartig bezeichneten technisch-organisatorischen Maßnahmen bleiben vor diesem Hintergrund ohne erhebliche Aussagekraft. Irgendwelche Maßnahmen in den Raum zu stellen, ohne auf die weiteren Schritte der notwendigen Gesamtbetrachtung einzugehen, ermöglicht dem Gericht nicht, die ergriffenen Maßnahmen – wie es von ihm verlangt wird (vgl. EuGH, Urteil vom 14.12.2023 – C-340/21, Rn. 45) – im Rahmen von Art. 32 DSGVO beurteilen zu können.* Wie also können Jurist*innen das Standard-Datenschutzmodell anwenden?

Der SDM-Würfel ist Bestandteil des von der DSK zuletzt im Mai 2024 bestätigten Standard-Datenschutzmodells Version 3.1 (SDM-V3.1). Der Würfel weist mit seinen drei Dimensionen analytisch wesentliche Erkenntnispfade aus, die ein systematisches „Abklappern" datenschutzrechtlich relevanter Fragestellungen unterstützen (vgl. DSK 2024, S. 47).

Auf der X-Achse des Würfels sind Phasen aufgelistet, die die Einzelvorgänge einer „Verarbeitung" in Art. 4. Nr. 2 DSGVO gruppieren. Auf der Y-Achse wird eine Verarbeitung in drei Ebenen aufgefächert, die nach dem „Stand der Technik" (Art. 25 DSGVO) zu beachten sind. Auf der Z-Achse befinden sich die Gewährleistungsziele des SDM, die die „Grundsätze" des Art. 5 DSGVO wiedergeben. Jedes Gewährleistungsziel steht für einen spezifischen Typ von zu bearbeitendem Risiko, für das das SDM mindestens eine Standardmaßnahme zur Verringerung des Risikos ausweist.

Dieser Artikel soll zeigen, wie anhand des Würfels systematisch die wesentlichen juristischen Regelungsbedarfe einer Verarbeitung personenbezogener Daten identifizierbar werden, die verbindlich zu regeln dem Verantwortlichen auferlegt sind. Leser*innen sollten dabei jedoch nicht verkennen, dass stets auch technische und organisatorische Maßnahmen berücksichtigt werden müssen.

2 Die Anwendung des SDM-Würfels

Die nachfolgenden Ausführungen betreffen ausschließlich die Verarbeitung personenbezogener Daten. Weil es für die Darstellung der Nützlichkeit des SDM-Würfels zum Erkennen von Regelungsbedarfen nicht darauf ankommt, wo genau eine Norm oder Regel am Ende dann niedergelegt ist, ist nachfolgend abstrakt nur von einem „Regelwerk" die Rede. Im öffentlichen Bereich besteht das Regelwerk aus Gesetzen oder Verordnungen bzw. Ausführungsbestimmungen; es kommen auch Ausführungsbestimmungen, Verfahrensvorschriften oder Dienstvereinbarungen infrage. Im privaten Bereich spielen neben Gesetzen auch vertragliche Regelungen und Betriebsvereinbarungen eine Rolle. Im Hinblick auf Regelungen zwischen Organisationen und Betroffenen – Bürger*innen, Kund*innen, Patient*innen – sind Regelungen typischerweise Bestandteile von Verträgen, Datenschutzerklärungen und Einwilligungen.

Die Erarbeitung der angesprochenen Regelungen wird in diesem Artikel gemäß SDM-Würfel in der Planungsphase und auf

der Modellierungsebene (Ebene 1) einer Verarbeitung verortet. Das ist allerdings eine unrealistische Annahme. Zumeist läuft eine Verarbeitung bereits seit vielen Jahren. Bei der nachträglichen Ermittlung eines vollständigen Solls für die Vergangenheit ist zu beachten, dass dieses Soll sachlich und rechtlich gedeckt ist und es nicht so ermittelt wird, dass es bequemerweise bereits dem aktuellen Ist-Zustand entspricht.

Zuletzt: Der Würfel kann nicht alle rechtlichen Anforderungen des DSGVO generieren, sondern ausschließlich solche, die sich im Kontext der Bearbeitung der operativen Risiken einer Verarbeitung durch den Verantwortlichen und Dienstleister für Betroffene ergeben.

2.1 Die Phasen einer Verarbeitung („X-Achse")

Auf der X-Achse des SDM-Würfels sind die funktional verketteten Vorgänge aufgetragen, aus denen jede Verarbeitung besteht und die für eine datenschutzrechtlich motivierte Risikoanalyse unterschieden werden müssen. In einer abstrakter ansetzenden, etablierten Modellierungsbegrifflichkeit würde man von Teilprozessen, Phasen oder Verarbeitungsvorgängen eines „Geschäftsprozesses" (bei Unternehmen), „Verfahrens" (bei Behörden) oder „Forschungsprojekts" (bei Hochschulinstituten) sprechen. *Die Dimension der Verarbeitungsvorgänge bzw. Phasen ermöglicht die Identifikation materiellrechtlicher Regelungsbedarfe.*

Die DSGVO gibt in Art. 4 Nr. 2 14 unterschiedliche Vorgänge von Verarbeitungen vor, die grundsätzlich einzeln zu betrachten sind. Es kann jedoch ausreichen, neun Vorgänge zu unterscheiden. Bei einem normalen Risiko der Verarbeitung kann in der einfachsten Variante der Modellierung die Unterscheidung von vier Phasen ausreichen: 1. die Erhebungsphase, 2. die Speicherungsphase, 3. die Nutzungsphase und 4. die Löschphase. Der Begriff „Phase" soll dabei nicht auf die Dauer von Aktivitäten abstellen, sondern auf eine kausal notwendige Reihenfolge der Verarbeitung von Daten als einem Lebenszyklus.

Jede der vier Phasen einer Verarbeitung steht für eine andere Form der Bearbeitung von Daten, die entsprechend von der Rechtsgrundlage aufgegriffen werden bzw. gedeckt sein muss. Für die Phase 1 muss geregelt sein, auf welcher Rechtsgrundlage die (Roh-)Daten erhoben werden, etwa mit einem entsprechenden Verweis auf die Regelungen der DSGVO, ob es sich bspw. um eine Direkterhebung bei Betroffenen, eine Erhebung bei Dritten oder um eine Übernahme von Daten aus einer anderen Verarbeitung handelt. Gemäß Phase 2 ist die Organisation und Speicherung der Daten regelungsbedürftig, insbesondere wenn Daten mit einem hohen Risiko für Betroffene bei einem externen Dienstleister gespeichert werden sollen. Für die Phase 3 muss die zweckgemäße Nutzung und ggfs. die Übermittlung von Daten an bzw. der Abruf von Daten durch Dritte rechtlich geregelt werden. Und die Phase 4 verlangt, die Umstände des Löschens von Daten zu regeln und die Informations- und Aufbewahrungspflichten zu sondieren. So müssen typischerweise Löschfristen gesetzt werden und es muss geregelt sein, welche Daten bspw. stattdessen zu archivieren oder an eine Statistikstelle bspw. anonymisiert weiterzuleiten zu sind.

2.2 Die Ebenen einer Verarbeitung („Y-Achse")

Die Y-Achse des SDM-Würfels repräsentiert drei unterscheidbare Ebenen einer Verarbeitung: Die Ebene 1 steht für die abstrakte „Modellierung" der Verarbeitung, an der die Dokumentation des Zwecks der Verarbeitung, der Kategorien der Daten und Empfänger usw. und die Beschaffung bzw. Beachtung der Rechtsgrundlagen ansetzen. Die Ebene 2 des Würfels steht für die Sachverhalte der konkreten Implementation einer Verarbeitung als „Sachbearbeitung". Und die Ebene 3 steht für all die Sachverhalte von ggfs. in Anspruch genommenen Dienstleistungen bzw. Auftragsverarbeitungen. *Die Dimension der Ebenen ermöglicht die Identifikation der regelungsbedürftigen Rechte und Pflichten in den Beziehungen des Verantwortlichen zu den Mitarbeiter*innen, zu den Kund*innen und Bürger*innen sowie zu den in der Regel beteiligten Akteuren wie Herstellern von Fachapplikationen, Dienstleistern/Auftragsverarbeitern und Aufsichtsbehörden.*

Auf der Ebene 1 liegt die Modellierung der Verarbeitung dokumentiert vor, bei der es sich in einer einfachen Variante um einen Prosatext handeln kann. In einer professionellen Variante sind zusätzlich die Datenflüsse bspw. in der Form von swimlanes und/oder in einer Prozess-Modellierungsnotation, bspw. als Sequenz der Unified Modelling Language (UML) oder mit der Business Process Modeling Language (BPML) dargestellt. Diese sorgen dafür, dass die Phasen und die (rechtlich) relevanten Akteure mit ihren zu definierenden Zuständigkeiten, Rechten und Pflichten, Teil-Verantwortlichkeiten und Zuständigkeiten bzgl. der Verarbeitung der Daten aufgeführt sind. Typische Akteure sind IT-Architekt*innen, die die funktionalen Aspekte einer Verarbeitung entsprechend der funktionalen Zweckbeschreibung planen. Hinzu kommen mindestens Jurist*innen, Betriebswirt*innen, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, QM- oder QS-Beauftragte, die aus ihren Aufgabenstellungen heraus, z.B. weil gemäß Art. 25 dataprotection-by-design umzusetzen ist, spezifischen Einfluss auf das Design der Abläufe und die Inhalte nehmen (müssen) und zumeist spezifisch festzulegende Regelungsbedarfe anmelden.

Datenschutzrechtlich relevant ist bei der Beschreibung der Verarbeitung eine möglichst enge Festlegung des Zwecks und die Minimierung der Daten und Mittel der Verarbeitung, die allesamt einen limitierenden Einfluss auf die Erforderlichkeiten bei der Erhebung der Daten, der Funktionen (und damit der IT-Komponenten) der Verarbeitungen und den Übermittlungen/Abrufen von Daten der Verarbeitung nach dem Prinzip „need-to-know" haben. Eine enge Zweckdefinition erleichtert die rechtliche Feststellung der Legitimität bzw. die Erstellung der Rechtsgrundlagen für die Verarbeitung sowie das Festlegen von Regelungen, um faktische Zweckdehnungen oder Zwecküberschreitungen zu vermeiden.

Die Ebene 2 repräsentiert die konkrete Implementation der Verarbeitung mittels Hardware- und Software-Komponenten („Fachapplikation") und der Sachbearbeitung durch Personen. Diese Ebene muss die rechtlichen Anforderungen an die Verarbeitung der einzelnen Akteure, die auf Ebene 1 rechtlich expliziert wurden, mittels konkreter Regeln und Sollwerte erfüllen. Hier entscheidet sich, welche Formen von Regelwerk (Gesetze, Vereinbarungen) mit Blick auf die Praxis angemessen sind. Wenn bspw. ein Landesministerium eine landesweite Verarbeitung, die von Kommunen durchgeführt werden soll, aufsetzt, dann muss das Ministerium einerseits die Erstellung der gesetzlichen Grundlagen durch das Parlament in Gang setzen und andererseits für die ausführende Seite der Kommunen möglichst konkrete Vorgaben und Regeln in Verordnungen und Ausführungsbestimmungen oder auch Standardverträgen für das Betrei-

ben der IT-Komponenten durch IT-Dienstleister erarbeiten. Die Anforderungen an die Mitarbeiter*innen, bspw. deren Verpflichtung auf Verschwiegenheit, die oftmals auch über das Arbeitsverhältnis hinaus gelten soll, sollten arbeitsvertraglich geregelt werden; ebenso das Ausmaß der erforderlichen Verhaltenskontrolle anhand von Protokolldaten.

Die Ebene 3 steht für all diejenigen Vorgänge einer implementierten Verarbeitung, die als Infrastruktur organisationsübergreifend genutzt wird („Betriebsmittel") und die in Form von „Diensten" vielfach zumindest teilweise von Auftragsverarbeitern, also zumeist IT-Dienstleistern, übernommen wird (vgl. Art. 28 DSGVO, vgl. DSK2018a). Ein Clouddienstleister stellt bspw. Speicherplatz (für Phase 2 einer Verarbeitung, siehe oben) bereit, während die Berechnungen der Fachlichkeit (Phase 3) auf den Servern und Clients in den Räumen des Verantwortlichen durchgeführt werden. Andere IT-Dienstleister stellen gleich die gesamten Funktionalitäten einer Verarbeitung mit den Verarbeitungsphasen 1 bis 4 bereit, so dass die Sachbearbeitung nur einen Client-PC mit Webbrowser nutzt. Im Falle der Auftragsverarbeitung wäre wesentlich zu regeln, welche Zugriffsrechte der Verantwortliche beim Dienstleister – vom Betreten der Örtlichkeiten über Eigenschaften der Hardware und Software bis zur Definition der Inhalte von Protokoll- bzw. Logdaten – beanspruchen muss, um seiner Verantwortlichkeit mit den Rechenschaftspflichten nach Art. 5 DSGVO für die Verarbeitung auch beim Dienstleister faktisch / sachlich nachkommen zu können. Zu regeln ist auch, welche Aktivitäten aufgrund von Mängelfeststellungen erfolgen müssen.

Bei einer „gemeinsamen Verarbeitung" (vgl. Art. 26 DSGVO, vgl. DSK2018b) wären die speziellen Rechte und Pflichten beider Verantwortlicher gegenüber den Betroffenen zu regeln. Im öffentlichen Bereich ist eine typische Regelung, dass das Land verantwortlich die Infrastruktur (Ebene 3) betreibt, während die Kommunen für die Inhalte auf der Sachbearbeitung (Ebene 2) verantwortlich sind. Die beiden Verantwortlichen können in den verschiedenen Verarbeitungsphasen in unterschiedlichem Maße aktiv sein, so dass die unterschiedlichen Grade der Verantwortlichkeiten rechtlich festgelegt werden sollten. Besonderen Wert sollte bei einer derart komplizierten Konstellation auf verständliche Ausführungen zu den Betroffenenrechten (vgl. Art. 12 DSGVO) gelegt werden.

2.3 Die Risiken einer Verarbeitung („Z-Achse")

Die Z-Achse des SDM-Würfels enthält die Gewährleistungsziele des SDM. Die Ziele lassen sich durch Negation begrifflich als Risiken umformulieren, wonach bspw. das Datenschutzrisiko darin besteht, dass eine Verarbeitung nicht ausreichend vertraulich, zu weitgehend zweckdehnend oder gar zweckungebunden oder intransparent usw. geschieht. Diese Ziele bzw. Risiken gehen auf die in Art. 5 DSGVO aufgelisteten Grundsätze zurück. Die Negationen der Grundsätze entsprechen den spezifischen Datenschutzrisiken, die die verantwortliche Organisation, und womöglich weitere an der Verarbeitung beteiligte Dienstleister, im alltäglichen Normalbetrieb erzeugen. Die Nicht-Verfügbarkeit als Risikokriterium stellt bspw. auf eine mangelhafte Sicherung der zugesagten Leistung einer Verarbeitung ab. Die Integrität von Daten, IT-Systemen und organisierten Verarbeitungsvorgängen verlangt, dass diese aktuell gehalten werden und insgesamt korrekt sind. Eine gesicherte Vertraulichkeit verlangt den Schutz von Daten, IT-Systemen und Verarbeitungsvorgängen vor unbefugtem Zugriffft. Die Nichtverkettung und Datenminimierung verlangen den Schutz vor einem zweckungebundenen Gebrauch von Daten, IT-Systemen und Verarbeitungsvorgängen. Intervenierbarkeit verlangt wiederum eine im Prinzip jederzeit mögliche Änderbarkeit von Daten, IT-Systemen und Verarbeitungsvorgängen. Und die Transparenz verlangt die Prüfbarkeit von all dem als Voraussetzung für die rechtliche Beurteilbarkeit der Verarbeitungspraxis einer Organisation insgesamt, zumal die Umsetzung dieser Ziele teilweise einander entgegenlaufen und deshalb die zu treffenden Schutzmaßnahmen gegeneinander abzuwägen sind. Insofern lässt sich zusammenfassend sagen: *Diese Dimension der Risiken ermöglicht die Identifikation der datenschutzrechtlich regelungsbedürftigen Inhalte einer Verarbeitung, in den verschiedenen Phasen und auf den verschiedenen Ebenen bei den beteiligten Akteuren*.

Dadurch, dass das SDM jedem der genannten Grundsätze bzw. Ziele Standardmaßnahmen zur Risikobearbeitung zuweist, können in den datenschutzrechtlichen Regelwerken wünschenswert konkret Maßnahmen ausgewiesen werden.

Zur Umsetzung des Schutzziels Transparenz sollten im Regelwerk Details zu den Inhalten der Protokolle enthalten sein, mit denen die Wirksamkeit der Maßnahmen zur Umsetzung der Anforderungen für die Vergangenheit technisch prüfbar bzw. rechtlich nachweisbar wird. Zu regeln ist in diesem Zusammenhang auch die Protokollierung der Aktivitäten von Sachbearbeiter*innen und Administrator*innen, zu welchen Zwecken (also: im Rahmen welcher Verarbeitungsphasen) der Zugriff auf diese personenbezogenen Protokolldaten erfolgen muss oder darf und durch wen, bspw. im Rahmen der Fachaufsicht, des Datenschutz-Managements oder bei Datenschutzvorfällen. Weil anhand von Protokolldatenauswertungen etwaige Mängel und Verfehlungen des Dienstleisters feststellbar sein können, müssen mit dem Dienstleister besondere Maßnahmen zur Sicherung des Zugriffs, der Vertraulichkeit, der Integrität und der Zweckbindung der durch ihn erstellten Protokollierungsdaten vereinbart werden. Die Kontrollierbarkeit qua Protokollierung ist insbesondere dann zu intensivieren, wenn die getroffenen technischen Maßnahmen zur Verhinderung von grundsätzlich unbefugten Zugriffen auf Inhalts-, Konfigurations- oder Protokolldaten nicht in jedem Aspekt ausreichen.

Das Gewährleistungsziel der Verfügbarkeit nimmt insbesondere die Anforderungen von Art. 5, 13, 15, 20 DSGVO auf. Auch wenn die Sicherung der Verfügbarkeit in der Regel im Interesse des Verantwortlichen liegt, sollte darauf geachtet werden, dass die Zusicherung der Verfügbarkeit einer Verarbeitung geregelt ist, insbesondere wenn nützliche Serviceleistungen oder Beschwerdemöglichkeiten für Betroffene zugesichert sind. Deshalb müssen Regelungen für Backups und Vertretung (Arbeitsvertrag, Geschäftsverteilungsplan) getroffen werden.

Die Sicherung der Integrität einer Verarbeitung, die insbesondere in den Artikeln 5, 25 und 32 DSGVO gefordert wird, stellt zum einen darauf ab, dass durch eine Authentisierung/Autorisierung nur gesichert befugte, adressable Entitäten – das können Menschen, Computer oder auch andere Verarbeitungen und Organisationen sein – Zugriff auf die Verarbeitung mit ihren Komponenten haben. Im zugehörigen Regelwerk sollte entsprechend eine abschließende Liste dieser Entitäten aufgeführt sein. Ein anderer Aspekt betrifft die Qualität von Daten und IT-Systemen, wonach diese aktuell, korrekt und vollständig zu halten sind, mit entsprechenden Regeln für Prozesse, die das sicherstellen. Eine

typische programmtechnisch-risikenmindernde Maßnahme zur Sicherstellung von korrekten Absendern und Adressaten sowie von Dateiinhalten sind die auf Hashwertvergleiche basierenden Zertifikate. Hier wären Details zur Nutzung einer bestimmten Public-Key-Infrastrucure (PKI) sowie zum Umgang mit Schlüsseln und Authentizitätsnachweisen durch Mitarbeiter*innen festzulegen.

Die Sicherung der Vertraulichkeit ist eine Anforderung aus den Artikeln 5, 25, 28, 29 und 32 DSGVO, die bei einer Verarbeitung typischerweise durch Verschlüsselung, sei es von Datenbeständen oder Kommunikationsverbindungen, umsetzbar ist. Bei einer Ende-zu-Ende-Verschlüsselung wäre zu regeln, welche Entitäten als Enden fungieren sollen, ob bspw. die Organisation insgesamt, die Fachabteilung oder die Mitarbeiterin der Fachabteilung das Ende bildet. Vielfach muss darüber hinaus geregelt werden, dass bestimmte Inhalte nicht per Mail oder Fax oder über einen Kurznachrichtendienst kommuniziert werden dürfen. Typischerweise müssen besondere Vertraulichkeitsvereinbarungen für die Sachbearbeitung oder beim Auftragsverarbeiter geschlossen werden, die auch das Ausscheiden aus der Organisation überdauern können. So sind, insbesondere bei einem hohen Risiko, Administrator*innen grundsätzlich nicht befugt, auf Inhalte von Dateien, Mails oder Datenbankinhalten Zugriff zu nehmen. Der Zugang der Administratoren zu Fachapplikationen und Servern sollte immer explizit geregelt werden, unabdingbar insbesondere dann, wenn keine technischen Maßnahmen zur lückenlosen Vertraulichkeits- und Zweckbindungssicherung installiert werden können. Wie bei der Sicherung der Integrität sind Details zu PKI und Umgang mit Schlüsseln und Passworten festzulegen; inkl. einer Liste der zu nutzenden Technologien im Regelwerk.

Die Sicherung der Nichtverkettung nimmt Anforderungen der Art. 5, 17, 22 und 25 DSGVO auf. Die wesentliche Maßnahme zur Durchsetzung ist eine architektonisch vorgenommene Trennung von Datenbeständen, IT-Komponenten, Prozessen bzw. generell die Trennung unterschiedlicher Verarbeitungen („Dataprotection-By-Design", Art. 25 DSGVO). Hier sind die rechtlichen Voraussetzungen und konkreten Bedingungen festzulegen, unter denen Daten zu anderen Zwecken genutzt bzw. Daten zwischen unterschiedlichen Verarbeitungen abgerufen werden dürfen. Im Rollen- und Berechtigungskonzept sind die Zuständigkeiten und Regeln festzulegen, mit denen befugt auf Daten, IT-Systeme und Verarbeitungen zugegriffen werden darf; diese Regelungen strahlen bis in die Arbeits- und Dienstleistungsverträge sowie Geschäftsverteilungspläne hinein. Auch Regeln für das Pseudonymisieren und Anonymisieren sind festzulegen.

Die Sicherung der Datenminimierung, die in den Artikeln 5 und 25 DSGVO angesprochen wird, ist in einem besonderen Maße auf normative Festlegungen und Regeln angewiesen, um Schutz für Betroffene zu erzeugen. Sie verlangt ein verständiges Durchgehen aller in der Verarbeitung bezogenen oder erzeugten Daten sowie von geplanten Datensätzen bzw. Datenbank-Feldern nach der „need-to-know"-Regel. Unter dieses Schutzziel fällt auch die Beurteilung, ob die Inbetriebnahme der Verarbeitung ganz generell gerechtfertigt werden kann.

Die Sicherung der Intervenierbarkeit dient insbesondere der Umsetzung der Betroffenenrechte (Art. 5, 13 bis 22, 25, 32 DSGVO). Beim Durchgang durch die Anforderungen dieser Artikel finden sich eine ganze Reihe von Anlässen für konkrete Regelungen insbesondere mit IT-Dienstleistern. Außerdem müssen Regelungen im Kontext des Changemanagements festgelegt werden, wie mit Störungen, Problemen und Änderungsbedarfen umzugehen ist. Dies können konkret Änderungen von Gesetzen, Marktsituationen, Verfahrensweisen, Techniken sein. Oder es bezieht sich auf Interventionen bspw. von Aufsichts- und Sicherheitsbehörden. So kann die Polizei vor der Tür stehen und die Herausgabe von Daten verlangen: Wer ist zu beteiligen und was ist dann zu tun?

3 Fazit

Dieser Artikel zeigte an Beispielen auf, wie anhand der vom SDM-Würfel aufgespannten Risikokonstellationen relevante Regelungsbedarfe im Kontext der betrieblichen Verarbeitungspraxis identifizierbar werden. Die Nutzung des SDM hilft allerdings nur bei der Identifikation der Regelungsbedarfe, die Formulierung passender rechtlichen Regelungen bleibt weiterhin dem juristischen Sachverstand vorbehalten. Allerdings darf man vermuten, dass im Zuge der Standardisierung von Datenschutzprüfungen durch das SDM analog zu den technischen Standardmaßnahmen auch die rechtlichen Regelungen standardisiert werden.

4 Literatur

DSK 2018a: Kurzpapier Nr. 13 – Auftragsverarbeitung; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf .

DSK 2018b: Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf .

DSK 2024: Das Standard-Datenschutzmodell V3.1 – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele; https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ .

Windrich, Melanie, 2023: Kategorisierung und Visualisierung von Datenschutzaspekten in Geschäftsprozessmodellen (Dissertation an der CAU Kiel), https://macau.uni-kiel.de/servlets/MCRFileNodeServlet/macau_derivate_00004921/Dissertation_Melanie_Windrich_public.pdf .