Christian Ricardo Kühne, Martin Rost, Stefan Zwierlein

Risiken in 3D

Risiken im Datenschutz methodisch verorten

Wie lassen sich aus Sicht eines operativ wirksamen Datenschutzes die Datenschutzrisiken eines Geschäftsprozesses bzw. eines Verwaltungsverfahrens – die DSGVO spricht von „Verarbeitung" (Art. 4 Nr. 2 DSGVO) und „Verarbeitungstätigkeit" (Art. 32 DSGVO) – methodisch bestimmen bzw. systematisch analysieren?

1 Einleitung

Die Modellierung von Risiken, die die Verarbeitungstätigkeiten von Organisationen für Personen erzeugen, ist eine wesentliche Voraussetzung zur Bestimmung risikomindernder Schutzmaßnahmen für das Erreichen des von der DSGVO geforderten Schutzniveaus. Nachfolgend wird ein dreidimensionales Modell („Datenschutzwürfel") vorgestellt, das bei der Verortung der Risiken und der Bestimmung von Schutzmaßnahmen hilft.

In der ersten Dimension des Modells werden die typischen Phasen einer Verarbeitungstätigkeit – vom Erheben über das Nutzen bis zum Löschen von Daten – aufgeführt. Das Modell unterscheidet mit Rückgriff auf Art. 4 Nr. 2 DSGVO acht Phasen, die phasenspezifische Risiken erzeugen.

Die zweite Dimension des Modells listet die Komponenten auf, die bei einer Verarbeitungstätigkeit heutzutage typischerweise genutzt werden. Konkret umfasst diese Dimension die personenbezogenen Daten sowie die genutzten Betriebsmittel, also typischerweise IT-Systeme (Hardware, Software) sowie Dienste. Die verschiedenen Komponenten erzeugen komponentenspezifische Risiken.

In der dritten Dimension werden die Gewährleistungsziele des Datenschutzes aufgeführt. Diese sieben Ziele dienen der Operationalisierung der Grundsätze des Art. 5 DSGVO und sind ihrerseits ein heuristisches Mittel, mit dem sich die spezifischen Risiken des Datenschutzes in einer Art Rundblick bestimmen lassen. Für jede Phase einer Verarbeitungstätigkeit und für jede genutzte IT-Komponente müssen alle Ziele herangezogen und in Bezug auf Risiken analysiert und beurteilt werden.

Das Modell berücksichtigt nicht alle für eine Analyse von Datenschutzrisiken wichtigen Aspekte. Über das Modell hinausgehend müssen die folgenden Punkte beachtet werden:

- der Anwendungskontext und die Rechtsbeziehungen der Beteiligten,
- die Modellierung der Angreifer sowie
- die Bestimmung der Höhe des Risikos einer Verarbeitungstätigkeit.

1.1 Anwendungskontext

Der Anwendungskontext und die Beziehungen der Beteiligten zueinander müssen explizit rechtlich geklärt sein. Das bedeutet u. a., dass die Legitimität der Verarbeitungstätigkeit durch den Verantwortlichen gegenüber den betroffenen Personen nicht in Zweifel stehen darf und die Rechtsgrundlagen, die das Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO) zweckbestimmt durchbrechen, vorliegen.

Christian Ricardo Kühne

studierte Philosophie, Informatik und Soziologie. Er ist Referent bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit und forscht im Bereich der Commons-Theorie und Kritischen Informatik zu emanzipatorischen Informations- und Kommunikationstechnologien.
E-Mail: christian.kuehne@datenschutz-berlin.de

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

Stefan Zwierlein

studierte Informatik an der FU Berlin und arbeitete als Berater in der Softwareindustrie mit den Schwerpunkten IT-Security und Compliance für ERP-Systeme. Seit 2019 ist er Referent mit dem Schwerpunktthema Datenschutz-Folgenabschätzung bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI).
E-Mail: stefan.zwierlein@datenschutz-berlin.de

Die Ausführungen der Autoren geben ausschließlich deren persönliche Auffassung wieder.

1.2 Angreifer

Die Hauptangreifer und deren Ressourcen sind im Datenschutz, im Unterschied zu Analysen der Informationssicherheit, bekannt. Als Hauptangreifer gilt vornehmlich die Organisation selber, die die personenbezogenen Daten verarbeitet und für deren Rechtskonformität der Verantwortliche einstehen muss. Der Verantwortliche bzw. die Organisation ist, aus Datenschutzsicht, insofern als allmächtiger Angreifer zu modellieren, weil er die Zwecke und wesentlichen Details einer Verarbeitung bestimmt.

1.3 Risiko

Bezüglich der Höhe des Risikos unterscheidet die DSGVO zwei Risikostufen, nämlich normales (geringes Risiko wird wie „normal" beurteilt) und hohes Risiko. Bei einer Verarbeitungstätigkeit durch eine Organisation kann es „kein Risiko" nicht geben. Die Bestimmung der Risikohöhe ist als Schwellenwertanalyse durchzuführen und ergibt sich weitgehend aus der Logik der Verarbeitung in Bezug auf die Intensität des damit verbundenen Grundrechteeingriffs (Art. 25 DSGVO, [5]).

Auch wenn eine (ausreichende) Rechtsgrundlage vorliegt, muss eine Risikoanalyse durchgeführt werden; bei einem hohen Risiko in Form einer Datenschutz-Folgenabschätzung („DSFA", vgl. Art. 35 DSGVO).

2 Die drei Dimensionen des Modells

Das Modell soll einem Verantwortlichen, einer oder einem Datenschutzbeauftragten, einer Datenschutzmanagementabteilung sowie einer Datenschutz-Aufsichtsbehörde, die Interesse an einer objektiven Darstellung der materiellen Risiken von betroffenen Personen haben, helfen, die datenschutzspezifischen Risiken für eine geplante oder zu prüfende Verarbeitung personenbezogener Daten zu bestimmen. Angestrebt wird dabei eine Orientierung auf dem Niveau eines Streckenplans einer U-Bahn, der wie alle Kartenwerke ausschließlich dem Zweck der Orientierung und dem Erreichen eines Ziels dient, nicht jedoch der perfekten Abbildung sämtlicher Verhältnisse.

2.1 Verarbeitungsphasen

Die DSGVO untergliedert eine „Verarbeitung" beispielhaft als eine Reihe von 18 einzelnen „Vorgängen", mit denen personenbezogene Daten verarbeitet werden. Aufgelistet werden das Erheben, das Erfassen, das Organisieren, das Ordnen, das Speichern, das Anpassen, das Verändern, das Auslesen, das Abfragen, das Verwenden, das Offenlegen durch Übermittlung, das Verbreiten, das Bereitstellen, das Abgleichen, das Verknüpfen, das Einschränken, das Löschen und das Vernichten (vgl. Art. 4 Nr. 2 DSGVO).

Die DSGVO impliziert durch die Reihenfolge der Benennungen ein Lebenszyklusmodell für personenbezogene Daten. Bei einer Verarbeitung sollten, so das Anliegen des Modells, die Verarbeitungsformen (struktureller Aspekt) von den Phasen (zeitlicher Aspekt), bei denen unterschiedliche Formen der Verarbeitung aufeinander folgen, unterschieden werden. In einer Verarbeitung können sich demnach verschiedene Formen von Verarbeitungen aneinanderreihen oder parallel verlaufen und wiederholen.

Wir schlagen vor, diese 18 Aktivitäten aufgrund der semantischen Überlappungen in acht typische Phasen zusammenzufassen, die grundsätzlich bei jeder Verarbeitungstätigkeit funktional analysiert, modelliert sowie rechtlich beurteilt werden können und sollten:

1. *Erheben* (Erhalten, Erfassen, Erzeugen)
2. *Aufbewahren* (Organisieren, Ordnen, Speichern, Archivieren)
3. *Nutzen* (Auslesen, Abfragen, Verwenden, Filtern)
4. *Verändern* (Anpassen, Bearbeiten)
5. *Bereitstellen für Dritte* (Offenlegung, Verbreitung, Übermitteln)
6. *Verknüpfen* (Abgleichen, Verknüpfen mit Daten von Dritten)
7. *Einschränken* (Sperren, Sichern)
8. *Löschen* (Vernichten)

Es stellt sich die Frage, ob die Menge der Verarbeitungsvorgänge aus Art. 4 Nr. 2 oder diese Auflistung vollständig sind. Die DSGVO erwähnt nämlich weitere Verarbeitungsformen wie das Profiling und die Pseudonymisierung (Art. 4 Nr. 4 und 5 DSGVO) sowie die Anonymisierung (Erw. 26 S. 5 DSGVO). Informationstheoretisch liegt es nahe, das Anonymisieren dem Löschen und das Pseudonymisieren dem Sperren zur Seite zu stellen, da deren hemmende Wirkung auf Zugriffe der Organisation paarweise ähnlich sind (vgl. [1], S. 20 f.). Wir beanspruchen hier keine abschließende Auflistung aller Verarbeitungsformen. Diese Einteilung in Phasen einer Verarbeitungstätigkeit soll drei Eigenschaften erfüllen: Die Phasen sollen voneinander unterscheidbar sein und Brüche markieren, weil sich die Informationsverarbeitung ändert oder andere Betriebsmittel (typischerweise andere Hardware und Software) eingesetzt werden. Und sie sollen auf unterschiedliche Grundrechte und Freiheiten Betroffener sowie rechtlich zu regelnde Eigenschaften beziehbar sein (vgl. [1], S. 20).

In Bezug auf konkrete Planungsaktivitäten helfen die typisierten Phasen dabei, die Struktur der Verarbeitung besser zu überblicken und bieten gleich mehrere Anknüpfungspunkte für die mit der Gestaltung und Prüfung befassten Professionen. Für organisations- und prozessentwickelnde Personen gehört das Arbeiten mit Prozessdiagrammen zum methodischen Handwerkszeug, sodass diesen die Liste der Phasentypen vertraut vorkommen sollte, um die jeweiligen Schritte in einem Business Process Model (BPM) mit korrespondierenden Phasentags zu markieren. Aus informatischer Sicht haben einige der Phasentypen sogar eine unmittelbar technische Bedeutung; und für Jurist*innen sind unterschiedliche normative Aspekte leitend, bspw. Verantwortungsübergänge bei einer Übermittlung von Daten.

Erwähnenswert ist, dass die doppelte Natur der Anonymisierung als phasenspezifische Schutzmaßnahme einerseits und als riskante Teilverarbeitung andererseits (vgl. [10]) die Durchführung einer DSFA erfordert, was ebenso auf das Löschen, das Protokollieren und die Vergabe von Zugriffsrechten zutreffen kann.

Differenziert man nach der beratenden und der prüfenden Perspektive auf eine Verarbeitungstätigkeit, so verfügt die erste der beiden nun über ein Mittel, Datenschutz durch Technikgestaltung besser umzusetzen und die zweite über eine höhere Auflösung bei der nachträglich-rekonstruierenden Risikomodellierung.

2.2 Gewährleistungsziele

Um die für die Praxisumsetzung unmittelbar relevanten normativen Anforderungen der DSGVO aufzunehmen, nutzt das Modell die im operativen Datenschutz inzwischen als etabliert gelten-

den Gewährleistungsziele des Datenschutzes (vgl.[4]), die zur Entwicklung des Standard-Datenschutzmodells („SDM“ [2]) führten.

Die Grundsätze aus Art. 5 DSGVO fokussiert das SDM auf sieben operationalisierungsfähige „Gewährleistungsziele“. Diese fungieren als Bindeglied zwischen den insgesamt 23 vom Verantwortlichen praktisch umzusetzenden Anforderungen der DSGVO und einer Liste von Schutzmaßnahmen zu deren Umsetzung. Zudem formuliert das SDM eine Strategie, mit der bei hohen Risiken die Maßnahmen zum Schutz betroffener Personen vor einer Verarbeitungstätigkeit besonders wirksam ausgeformt, betrieben und überwacht werden können. Diese die Schutzmaßnahmen (M.) gruppierenden Gewährleistungsziele lauten:

- *Verfügbarkeit* (typische Maßnahme: Backup sicherstellen)
- *Integrität* (M.: Hashwerte managen, Schwellenwerte festlegen, Korrekturaktivitäten etablieren)
- *Vertraulichkeit* (M.: Datenbestände und Kommunikationsbeziehungen verschlüsseln)
- *Transparenz* (M.: Umsetzung der anderen Grundsätze mit Hilfe von Spezifikation, Dokumentation, Protokollierung prüfbar machen)
- *Nichtverkettung* (M.: Trennungen, Anonymisieren, Pseudonymisieren, Rollen- und Berechtigungen implementieren)
- *Intervenierbarkeit* (M.: Löschen, Beschwerden managen)
- *Datenminimierung* (M.: Datenschutzfreundliche Voreinstellungen setzen*)*

Die Gewährleistungsziele erlauben, die normativen Anforderungen der DSGVO in einer konzentrierten, fokussierten Form sowohl an die logisch-funktionale Gestaltung der einzelnen Verarbeitungstätigkeiten als auch an die funktionale Gestaltung der Betriebsmittel (Hardware, Software und Dienste) heranzutragen. Als anzustrebende Ziele „mahnen“ sie eine Organisation und deren Mitglieder im Sinne von „Design-Strategien“ daran, bestimmte funktionale Eigenschaften durchgängig in allen personenbeziehbaren Verarbeitungsvorgängen zu beachten.

Bei der Analyse der Risiken anhand der Gewährleistungsziele ist zu beachten, dass sich die Ziele – und damit auch die Maßnahmen – untereinander beeinflussen können. Gewährleistungsziele stehen nicht als unabhängige Dimensionen zueinander, die unabhängig voneinander zu betrachten sind. Ziele bzw. Maßnahmen können einander sowohl verstärken als auch schwächen; letzteres insbesondere dann, wenn ein Gewährleistungsziel einseitig überbetont wird. Für eine geplante oder zu prüfende Verarbeitungstätigkeit bedarf es deshalb der rechtlichen und funktionalen Abwägung [10]. Wenn zum Beispiel zur Bearbeitung des Risikos einer mangelhaften Prüffähigkeit (Transparenz) eine durchgängig hochauflösende Vollprotokollierung sämtlicher Ereignisse und Aktivitäten von Beschäftigten implementiert wird, dann kann das zu einer rechtlich nicht mehr vertretbaren Steigerung des Risikos für die strenge Zweckbindung (Nichtverkettung) führen. In diesem Beispiel können vorliegende Protokolldaten den Verantwortlichen unwiderstehlich motivieren, diese auch zu anderen als den festgelegten Zwecken zu nutzen, etwa zur Strafverfolgung oder zur Leistungskontrolle von Beschäftigten.

2.3 Komponenten der Verarbeitung

Jede Verarbeitungstätigkeit nutzt Betriebsmittel wie bspw. menschliche Arbeitsleistungen und „Werkstoffe“ sowie Gebäude und Maschinen. Zu den „Werkstoffen“ einer Verarbeitungstätigkeit einer Organisation zählen die „*personenbeziehbaren Daten*“ (Art. 4 Nr. 1 DSGVO) der von der Verarbeitungstätigkeit betroffenen Personen. Und zu den Maschinen zählen die *IT-Komponenten*, also die große Zahl an unterschiedlicher Hardware und Programmen. Diese Hardware und Software wird dabei nicht mehr nur innerhalb von organisationseigenen Gebäuden zusammengebunden, sondern sie setzen auf weltweit betriebene IT-Ressourcen (Programm-Bibliotheken, Protokollen, Diensten) auf.

Während eine Verarbeitung allein durch ihren Zweck schon Risiken für Betroffene erzeugt – man denke wieder an das staatliche Meldewesen, in dem gesetzlich geregelt 56 Eigenschaften der Einwohner eines Landes erfasst werden und auf das unterschiedliche Behörden (z. B. Personenstandswesen Sicherheitsbehörden, Finanzamt, Rentenversicherungen) zugreifen –, erzeugen die von der Verarbeitung verwendeten Betriebsmittel zusätzlich betriebsmittelspezifische Risiken, wonach Daten bspw. durch mangelhaft durchgesetzte Trennung von Datenbeständen oder IT-Prozessen zweckdehnend genutzt werden können und diese Nutzung zudem nicht prüfbar ist. Daher muss bspw. sichergestellt sein, dass der Zugriff auf die Datenbestände durch geeignete Authentisierungs- und Autorisierungsmechanismen für Mensch und Maschine gesichert und befugt erfolgt. Wie IT-Systeme gesichert – auch vor dem Zugriff der berechtigt datenverarbeitenden Organisation selber – zu betreiben und zu prüfen sind, ist Gegenstand der Maßnahmenkataloge des SDM sowie in Bezug zur Informationssicherheit des IT-Grundschutz des BSI oder der ISO.

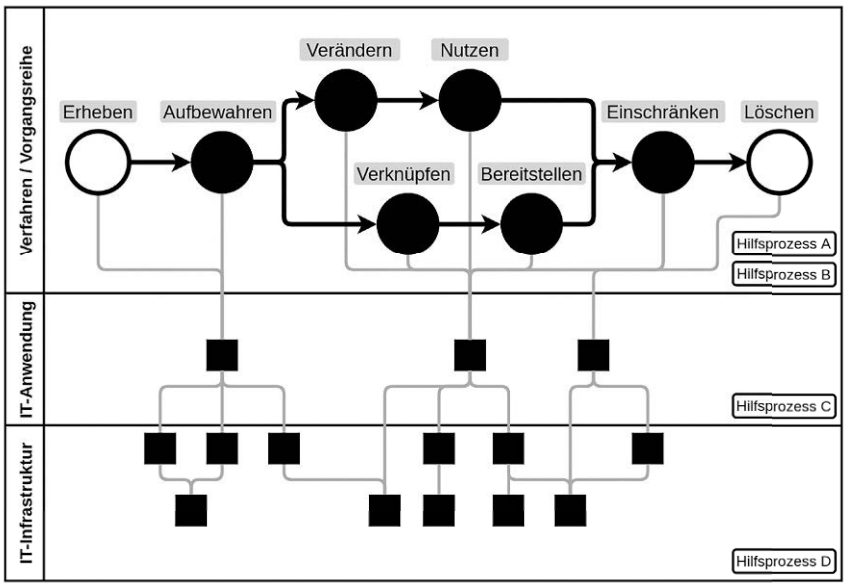
3 Die drei Teilkonstellationen des Modells

3.1 Verarbeitungsphasen und Komponenten

Eine angemessene Risikomodellierung muss die Möglichkeit berücksichtigen, dass Risiken auf der Verfahrensebene mit Risiken auf der Ebene der Komponenten punktuell und strukturell verstärkend zusammenwirken können. Daher muss nach der Modellierung des Verfahrens bzw. der Vorgangsreihe anhand standardisierter Phasen die funktionale Zuordnung der geplanten oder eingesetzten Betriebsmittel zu jedem Prozessschritt folgen. Auf diese Weise werden Pfade sichtbar, auf denen sich vererbbare oder emergierende Risiken „fortpflanzen“ (propagieren), Risiken geblockt oder geteilt werden. Das aktuelle Beispiel der Corona-Kontaktnachverfolgung zeigt, dass sich mit Papier und Stift oder mit einem Smartphone Daten erheben lassen. Entsprechend unterschiedlich muss die Phase des Löschens durch einen Schredder oder eine automatisierte Löschroutine eines Datenbanksystems erfolgen, mit weiteren Analysen bzgl. des Datenbank- und Betriebssystems sowie der Hardware.

Um die Übersichtlichkeit insbesondere für mittlere und große Organisationen zu verbessern und eine arbeitsteilige Bearbeitung zu ermöglichen, bietet es sich an, drei Verarbeitungsebenen zu unterscheiden. Auf der obersten Ebene („Fachverfahrensebene“) befindet sich das in Prozessschritten gegliederte Verfahren und die darin jeweils verarbeiteten personenbezogenen Daten. Auf der darunterliegenden Anwendungsebene befindet sich die IT, in der die unmittelbar von sachbearbeitenden Personen und betroffenen Personen verwendeten Betriebsmittel aufgehoben sind. Die Infrastrukturebene bildet die dritte Ebene, in der IT-Server, IT-Dienste, Schnittstellen, Netzwerke usw. als Basisdienste bereitstehen. Zusätzliche für die Verarbeitung relevante Hilfs- oder Betriebsprozesse, die wiederum eigene Risiken erzeugen, können auf der jeweiligen Ebene dann se-

Abbildung 1 | Verarbeitungsformen und Phasen



parat aufgeführt und referenziert werden. Das Ergebnis der Modellierung sollte ein vollständiges Verarbeitungsmodell sein, das nun als Input für die verfeinerte Maßnahmenmodellierung (bspw. nach SDM, IT-Grundschutz oder ISO) bereitsteht.

3.2 Verarbeitungsphasen und Gewährleistungsziele

Grundsätzlich gilt zunächst, dass in jedem Verarbeitungsprozess alle Gewährleistungsziele anzuwenden sind.[1] Wir betrachten im Folgenden beispielhaft nur die Phasen der „Erhebung" und der „Aufbewahrung" und beschränken uns dabei auf die beiden Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung, um die Systematik deutlich zu machen.

Bei der Erhebung gelangen Informationen über eine Person in den Herrschaftsbereich einer Organisation. Im Falle der Intervenierbarkeit besteht häufig das Risiko, dass sowohl Verantwortliche als auch die betroffenen Personen nicht in der Lage sind, die Verarbeitung rechtmäßig einzuschränken oder gar zu löschen. Die Anforderung der Nichtverkettung, also die technisch-operative Sicherstellung der Zweckbindung über sämtliche Betriebsmittel einer Verarbeitungstätigkeit hinweg, muss in der Erhebungsphase durch eine ganz enge „Filterstellung der Sensorik" umgesetzt werden – man denke beispielsweise an die zweckgemäße Gestaltung der Fragen eines Fragebogens (Prinzip: „need to know", nicht „nice-to-have") oder an die Beschränkung des Sichtfelds von Videokameras.

Wesentlich für die Phase der Aufbewahrung ist die Fähigkeit einer Organisation, über das Abbild einer Person auch in der Zukunft zu verfügen. Im Kontext der Aufbewahrung besteht folglich bezogen auf die Intervenierbarkeit das typische Risiko zukünftiger Fremdbestimmung oder, spezifischer, dass eine Änderung oder Löschung dieses Abbilds nicht in angemessener Weise möglich ist. Hinsichtlich der Nichtverkettung besteht das Risiko, dass Datenbestände unterschiedlicher Verarbeitungszwecke „zu nah" beieinander liegen und eine Aufhebung der Zweckbindung wahrscheinlicher wird. Ein bekanntes Szenario ist die Nutzung eines populären Cloud-Dienstes, wenn der Auftragsverarbeiter zu eigenen Zwecken die Daten verknüpft.

Zusätzlich zur Analyse der einzelnen Phasen ist zuletzt die Verarbeitung als Ganze zu analysieren, da sich besondere Risiken aus der Wechselwirkung einzelner Phasen oder dem Zusammenwirken aller Phasen ergeben können. Nimmt die Komplexität der Verarbeitung zu, steigt auch dessen Risikoniveau. Bisweilen kann die Zwecksetzung oder das verwendete Datenmodell als Teil dieser übergeordneten Analyse zu unterschiedlichen Vorgangsreihen mit je unterschiedlichen Ensemblen von Risiken führen.

Des Weiteren ist zu beachten, dass ein „hohes Risiko", das für die Verarbeitungstätigkeit insgesamt festgestellt wird, dann auch für jede Phase durchgesetzt werden muss. Die Risiken für betroffene Personen können sich in einzelnen Phasen verdichten. Es kommt hinzu, dass sich in unterschiedlichen Phasen unterschiedlich führende Gewährleistungsziele identifizieren lassen [1, 3]. So ist es bspw. von überragender Bedeutung für die gesamte Verarbeitungstätigkeit, dass im Erhebungszusammenhang Maßnahmen zur Sicherung der Integrität der erhobenen Daten getroffen werden. Auch wenn Auskunftspflichten alle Phasen betreffen können, so stellt die DSGVO in diesem Sinne gut begründbar insbesondere auf die Prüfbarkeit der Erhebungsphase ab (Art. 13, 14 DSGVO).

3.3 Komponenten und Gewährleistungsziele

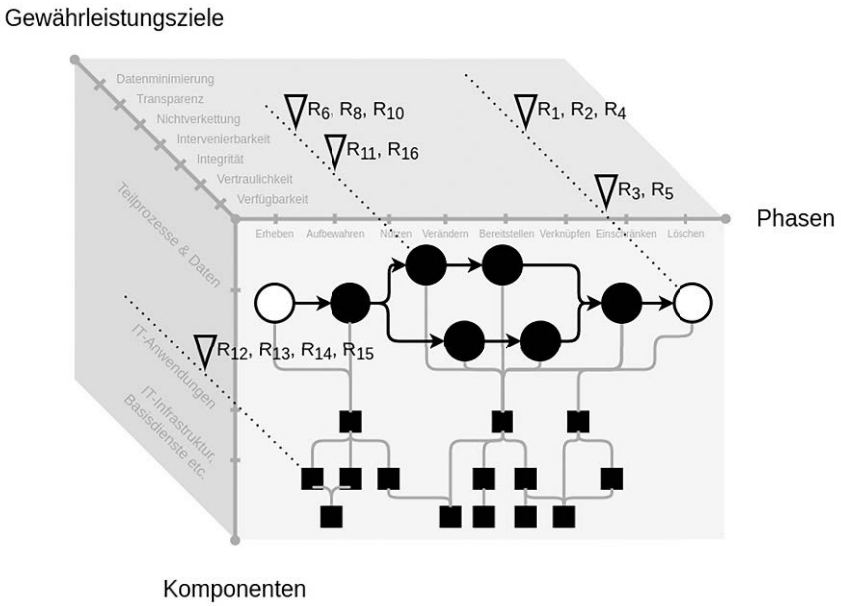
Verschiedene Komponenten, die im Kontext der Verarbeitungstätigkeit genutzt werden, erzeugen im Durchgang durch die sieben Gewährleistungsziele komponentenspezifische Risiken, für die Komponenten spezifische Schutzmaßnahmen zu treffen sind.

Diese Form der Risikoanalyse ist eine typische Aktivität im Kontext der IT-Sicherheit. Im Unterschied zur IT-Sicherheit nutzt der operative Datenschutz zur Modellierung von Risiken nicht nur drei (Verfügbarkeit, Integrität, Vertraulichkeit) sondern sieben Ziele, wobei die sieben Gewährleistungsziele untereinander auch noch abzuwägen sind. Und das Schutzobjekt sind natürliche Personen mit ihren Rechten und Freiheiten, nicht die Geschäftsprozesse oder Verfahren oder die Betriebsmittel bzw. Komponenten, die darin zum Einsatz kommen.

Zu beachten sind insbesondere Risiken für die Transparenz und Intervenierbarkeit auf der Ebene der Betriebsmittel, wenn diese von einem Auftragsverarbeiter in Form externalisierter Dienste bereitgestellt werden. Längere und weitverzweigte Auftragsverarbeitungsketten können zu längeren Bearbeitungszeiten bei Sicherheitsvorfällen oder der Beantwortung von Informationsanfragen führen und gewissermaßen als ein emporsteigendes Risiko in einer Phase hervortreten.

1 Selbst wenn eine Verarbeitungstätigkeit nicht vollständig abgeschlossen wird und die Datenverarbeitung in einer Phase „steckenbleibt", weil bspw. papierene Patientenakten durch Insolvenzwirren vergessen, nicht vernichtet oder kontrolliert und an Bedingungen geknüpft vom Nachfolger eingelagert werden, und man Zweifel daran hegt, ob es sich um eine Verarbeitung handelt, wenn Papierakten ohne weitere „Transformationsabsicht" nur eingelagert werden (vgl. OVG Hamburg, Beschl. v. 15.10.2020, Az.: 5 Bs 152/20), so enthebt das den Rechtsnachfolger unseres Erachtens nicht, sämtlichen Anforderungen der DSGVO zumindest für eine solche Phase zu genügen.

Abbildung 2 | Der Datenschutzwürfel



4 Der Datenschutzwürfel

Beide Analysebereiche, die Phasen und die Komponenten der Verarbeitung, laufen entlang der Kante der Gewährleistungsziele zusammen und bilden einen leicht zu merkenden Datenschutzwürfel mit einem imaginären Innenraum für die strukturellen Risiken einer so aufgezogenen Verarbeitung.[2] Die umzusetzenden Ziele sind immer die gleichen, die zu analysierenden Risiken sind dagegen phasen- und komponentenabhängig, mit entsprechenden zu treffenden risikenmindernden Maßnahmen.

Die Dimension der Gewährleistungsziele kann bei Bedarf höherauflösend auf spezifische Normen und Regelungen der DSGVO zurückgeführt werden; bei den wechselseitigen Transformationen zwischen normativen und funktionalen Anforderungen leistet das SDM große Hilfe. Die Verarbeitungsphasen können separiert betrachtet werden und die phasenabhängig getroffenen Maßnahmen entlang des PDCA-Zyklus der kontinuierlichen Verbesserung höher auflösend behandelt werden. Und die Risiken der Komponenten lassen sich ebenfalls höherauflösend, entsprechend den jeweiligen Ebenen bestimmen. Insofern lässt sich behaupten: Der Datenschutzwürfel (V2) verbindet die Anforderungen der DSGVO mit einer phasenspezifischen Managementstrategie des PDCA-Zyklus mit der Ebene der konkreten Datenschutzmaßnahmen.

Sowohl eine DSFA [9] als auch ein Datenschutzmanagementsystem (vgl. Art. 32 Nr. 1 lit. d DSGVO [2], S. 50f) oder eine datenschutzrechtliche Zertifizierung (vgl. Art. 42 [7]) müssen systematisch und auf Vollständigkeit bedacht durchgeführt werden. Vielfach sind diese Aktivitäten selber als Verarbeitungen aufzufassen, die ihrerseits den Grundsätzen bzw. Qualitätsanforderungen der DSGVO nach Zweckbestimmtheit, Integrität, Transparenz, Interventionsfestigkeit, kompetenter (befugter) Durchführung genügen müssen, weil sie im Kontext von Verarbeitungen mit Personenbezug stehen.

2 Bereits 2011 wurde eine erste Version eines Datenschutz-Würfels vorgestellt, in dem „personenbezogene Daten" zum Ausgangspunkt zur Bestimmung von Schutzmaßnahmen genommen wurden (vgl. [6]). Aufgrund der Fokussierung auf „Verarbeitung" durch die DSGVO sowie zunehmende Erfahrungen bei der Modellierung von Verarbeitungstätigkeiten des „Dataprotection-By-Design" (Art. 25 DSGVO) war eine gründliche Überarbeitung des Modells geboten.

5 Fazit

Das Modell des „Datenschutzwürfels" gibt systematischen Halt bei der Umsetzung der Anforderung nach einer „systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung"; es hilft auf einem hohen Niveau bei der methodischen Erfüllung der Voraussetzungen für „Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen" und der Ermittlung der „zur Bewältigung der Risiken geplanten Abhilfemaßnahmen" (Art. 35 Nr. 7 DSGVO). Diese Anforderungen sind grundsätzlich für jede personenbezogene Verarbeitung zu erfüllen. Das Modell unterstützt bei der Auflösung und Bestimmung von Risiken sowie der Festlegung von deren Bearbeitung. Es setzt die Dimensionen der Verarbeitungsschritte sowie die zur Durchführung eingesetzten Komponenten in Bezug auf die Gewährleistungsziele in eine Beziehung, die dabei hilft, die Mittel für den Datenschutz durch Technikgestaltung angemessen zu bestimmen.

6 Literatur

[1] Pohle, Jörg, 2018: Zur Zeitdimension der Schutzziele, DuD – Datenschutz und Datensicherheit, 42. Jahrgang, Heft 1: 19-22.

[2] DSK 2020: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele; https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode_V20b.pdf .

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

[4] Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358.

[5] DSK 2018: Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf .

[6] Rost, Martin, 2011: Datenschutz in 3D – Daten, Prozesse und Schutzziele in einem Modell; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 5: 351-355.

[7] Prietz, Christian / Rost, Martin / Stoll, Julia, 2020: Prüfverfahren zur datenschutzrechtlichen Zertifizierung, in: DuD – Datenschutz und Datensicherheit, 44. Jahrgang, Heft 10.

[8] Rost, Martin / Welke, Sebastian, 2020: SDM 2.0 und ITIL 4 „verschränkt", in: DuD – Datenschutz und Datensicherheit, 44. Jahrgang, Heft 4: 258-262.

[9] DSK 2018: Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf .

[10] Ohm, Paul, 2010: Broken Promises of Privacy: Responding to the surprising failure of anonymization, in: UCLA Law Review, Heft 57: 1701-1777.