Martin Rost

Standardisierte Datenschutzmodellierung

Es wird ein standardisiertes Datenschutzmodell vorgestellt, das aus sechs elementaren Schutzzielen, drei Verfahrenskomponenten und drei Schutzbedarfsabstufungen besteht. Mit diesen Bestandteilen lässt sich ein Maßnahmenkatalog erzeugen, der 54 generische Referenzmaßnahmen des Datenschutzes enthält, gegen den sich jedes Verfahren mit Personenbezug systematisch und vollständig prüfen lässt.

1 Einleitung

Die Kerntätigkeit eines jeden Datenschutzbeauftragten besteht darin, geplante oder laufende Verfahren mit Personenbezug zu prüfen.[1] Bei einer Prüfung personenbezogener Verfahren wird zwischen Sollvorgaben aus Normen- und Vertragstexten bzw. Einwilligungserklärungen, aus mehr oder weniger explizierten Organisationsregelungen sowie aus Maschinenbefehlen auf verschiedenen Ebenen von IT-Systemen permanent hin- und rückübersetzt. Eine Prüfung von Soll- und Ist-Eigenschaften allein innerhalb des Rechts oder der Prozessabläufe oder der Technik ist bereits methodisch anspruchsvoll genug. Noch anspruchsvoller ist die Bewältigung des Transformationsrisikos beim Domänenübertritt, der wahlweise willkürlich, unreflektiert, trivialisierend[2] oder aus Effiziens- oder Kompetenzgründen erzwungen dilletantisch vorgenommen wird. Das Gewahrwerden dieses Risikos sollte eigentlich zur kontrollierten Zusammenarbeit zwischen den Disziplinen auffordern, wird aber zumeist nur einem der beteiligten Experten einseitig aufgebürdet.

Ein typischer Sachverhalt aus der Prüfpraxis soll dieses Transformationsrisiko veranschaulichen. Es gilt, dass die grundrechtlich gebotene Gewaltenteilung bzw. die informationelle Gewaltenteilung auch in einem Rechenzentrum der öffentlichen Verwaltung bei der Nutzung gemeinsamer IT technisch gesichert realisiert ist. Die Skala für die Durchsetzung der normativ gebotenen Anforderung der „Trennung von Verfahren“ kann dabei eine physische Trennung von Daten (sowie von IT-Systemen und Verarbeitungs-, Administrations- und Sicherungs-Prozessen) in unterschiedlichen Gebäuden oder unterschiedlichen Rechenzentren unterschiedlicher Länder bedeuten, oder ebenso die Trennung entlang von virtualisierten Systemen auf einer gemeinsamen Hardware-Basis oder eine Mandantentrennung auf der Ebene von unterschiedlichen Zugriffsrechten in einer gemeinsam genutzten Applikation. Man trifft aber auch Lösungen an, bei denen die IT-Administration oder Sachbearbeitung schlicht zusichern, nicht auf ein System und deren Daten zuzugreifen obwohl sie es könnten. Sowohl juristischer, organisatorischer als auch technischer Sachverstand sollten für die Lösung eines solchen Problems wie dem Finden eines angemessenen Arbeitspunkts für „Trennung“ in einem gemeinsam akzeptierten Transfer-Modell formulieren können, um zu einer gemeinsam tragfähigen Gesamtentscheidung bzgl. der Datenschutzgerechtigkeit eines Verfahrens zu gelangen.

Eine rechtskonforme und sachgerechte Gesamtentscheidung kann hier nur zustande kommen, wenn keine der beteiligten Rationalitätsdomänen die andere dominiert. Und das eingedenk dessen, dass die beiden großen Rationalitätsdomänen im Datenschutz, Recht und Technik, jeweils aus ihrer Logik mit vollem Recht sehr wohl die Vorherrschaft beanspruchen. Das Recht fordert gegenüber der Technik, dass Technik dem sich im Recht ausdrückenden kollektiven Willen schlicht zu folgen hat. Die Technik wiederum fordert ein, dass das Recht nicht an der technischen Praxis vorbei etwas regeln sollte, was technisch betrachtet überholt oder disfunktional ist. Praxisfremdheit untergräbt Legitimation. Ob die Legitimation qua Gesetz oder qua normativer Kraft des Faktischen erzwungen werden kann, lässt sich in einer modernen Gesellschaft sachgerecht nicht einseitig entscheiden. Beide Logiken müssen bei einer Datenschutzprüfung zusammenkommen und am jeweils konkreten Punkt von personenbezogenen Verfahren transparent ausweisen können, wie eine Verfahrenseigenschaft zu beurteilen und ein festgestellter Mangel zu be-

1 Dieser Artikel ist in engem Kontakt zu den Artikeln von Bock/Meissner sowie Probst (beide in diesem Heft) entstanden. Bock/Meissner weisen nach, dass die Schutzziele sowohl mit dem BDSG als auch mit dem gegenwärtigen Entwurf der EU-Datenschutzverordnung (Stand: 2012/01) und der EU-Richtlinie 95/46/EG sowie beispielhaft mit dem LDSG-Schleswig-Holstein vereinbar sind. Sie führen außerdem vor, wie der genuin juristische Prozess des Abwägens von Normen im Medium der Schutzziele durchführbar ist. Probst beschäftigt sich mit der Auflistung von technisch-organisatorischen Referenzmaßnahmen.

2 Die schlichte Behauptung “code is law” (Lawrence Lessig) behebt das Transformationsproblem einseitig, also: gar nicht.

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz“ beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein,

E-Mail: martin.rost@datenschutzzentrum.de

heben ist. Das zu leisten ist eine wesentliche Funktion des hier vorzustellenden Standard-Datenschutzmodells (SDM).

Darüber hinaus verbessert das Modell die Integrität von Datenschutzprüfungen, weil Prüfungen sowohl für Betroffene als auch für andere Datenschutzkollegen und nicht zuletzt Gerichte oder dem Gesetzgeber überprüfbar werden und damit ihrerseits dem rechtstaatlichen Mechanismus der Checks & Balances unterworfen sind. Wenn eine Datenschutzprüfung oder ein Privacy Impact Assessment (PIA) fortan anders als am SDM orientiert modelliert und durchgeführt wird, muss das eigentlich einen erhöhten Begründungsaufwand bedeuten.

2 Komponenten des SDM

Die durch Datensicherheit und Datenschutz initiierten Aktivitäten operationalisieren gemeinsam Vertrauenswürdigkeit für die Tätigkeiten und Kommunikationen zwischen Organisationen und Personen. Beide Aktivitäten und Perspektiven drängen Organisationen darauf nachweisen zu können, dass sie ihre Prozesse sicher beherrschen und fair betreiben[3]. Aber Datenschutz und Datensicherheit agieren mit unterschiedlichen Perspektiven: Das Angreifermodell der Datensicherheit zielt auf die Sicherung des Betriebs einer Organisation vornehmlich gegenüber Personen ab, die als (ehemalige) Mitarbeiter, unlautere Bürger oder betrügerische Kunden oder als Hacker Schaden anrichten könnten. Dagegen modelliert Datenschutz die andere Richtung, nämlich Organisationen mit ihren Verfahren systematisch als latente Angreifer auf die Integrität von Personen zu modellieren. Organisationen bedrohen latent das Souveränitätsversprechen, das im Rechtsstaat den generischen Rollen des Bürgers, Kunden, Klienten, Patienten, Menschen, Subjekts, Individuums innewohnt. Aus Datenschutzsicht besteht somit die Aufgabe sicherzustellen, dass Organisationen vertrauenswürdig gegenüber Personen agieren. Um das zu leisten, müssen Organisationen sich selbst, den Betroffenen und den Aufsichtsbehörden, die das gesamtgesellschaftliche Interesse vertreten, gegenüber transparent darstellen, dass sie ihre Prozesse beherrschen und rechtskonform betreiben.[4]

Der kurz angedeutete Unterschied in der Aufgabenstellung von Datensicherheit und Datenschutz drückt sich u.a. darin aus, dass den drei bekannten Schutzzielen der Datensicherheit – nämlich die Sicherung der *Verfügbarkeit*, *Integrität*, *Vertraulichkeit* – spezifische Schutzziele des Datenschutzes zur Seite gestellt sind, nämlich die Sicherung der *Transparenz*, der *Intervenierbarkeit* und der *Nicht-Verkettbarkeit* von Organisationsaktivitäten. Die Sicherstellung dieser sechs Schutzziele durch Schutzmaßnahmen ist von Organisationen prüffähig nachzuweisen. Trotz dieser teilweise gegenläufigen Sicherheits- bzw. Schutzinteressen von Datenschutz und Datensicherheit können Mechanismen und Methodik etwa des BSI-Grundschutzes für standardisierte Datenschutzprüfungen übernommen werden.[5]

Die sechs elementaren Schutzziele bilden einen abgestimmten Kanon an Kriterien, in denen sowohl die juristische Abwägung eines Verfahrens mit Personenbezug sowie das Bestimmen der dafür zu treffenden technischen und organisatorischen Schutzmaßnahmen erfolgen können. Die Organisationsstruktur der Schutzziele macht um Recht und Technik kontrolliert aufeinander beziehbar um Verfahren prüfen zu können. Ein Verfahren besteht aus drei Komponenten, nämlich *Daten*, einem *System* zur Datenverarbeitung, das heutzutage auf der Basis eines IT-Systems geschieht, sowie *Prozessen*, die gesteuert-regulierten Abläufen entsprechen. Jeder dieser drei Verfahrenskomponenten lassen sich wiederum drei Schutzbedarfe zuordnen, nämlich normal, hoch und sehr hoch.

Aus den sechs Schutzzielen, den drei Verfahrenskomponenten und den drei Schutzbedarfen lässt sich somit ein Gesamtkatalog von 54 systematisch gewonnenen Referenzschutzmaßnahmen formulieren, die als generische Soll-Vorgaben dienen, um einen Vergleich mit den Ist-Eigenschaften eines zu prüfenden Verfahrens und dessen Datenschutzmaßnahmen zu ermöglichen.

2.1 Schutzziele

Das Konzept der Schutzziele verspricht, dass es die wesentlichen materiell-rechtlichen Anforderungen – nämlich Sicherstellung der Zweckbindung, Erforderlichkeit, Berücksichtigung der Betroffenenrechte und revisionsfeste Prüffähigkeit durch Transparenz – an datenschutzgerecht betriebene Verfahren in operationalisierbarer Form enthält.[6] „Ziele“ sind dabei sowohl dem normativen Sollen inhärent als auch ein Aspekt jeder Prozessregelung sowie als Verwendungszweck in einem technischen System materialisiert. Es kann dann eine gleichsinnige Ausrichtung durch übereinstimmende Ziele verschiedener Rationalitätsdomänen solange von maßgeblichen Akteuren unterstellt werden, solange kein Konflikt offenbar wird.[7]

3 Beherrschbarkeit wird explizit im §7 Abs. 3 Niedersächsisches Datenschutzgesetz (NDSG) gefordert.

4 Deshalb ist beim Neuen Personalausweis der Zwang zur Nutzung eines Berechtigungszertifkats, das genau diese gegenseitige Authentifizierung von Organisation und Person fordert, nachdem zuvor vom Bundesverwaltungsamt der Zweck der Erhebung personenbezogener Daten geprüft wurde, eine aus konzeptioneller Datenschutzsicht geradezu vorbildliche Lösung.

5 Die zu treffenden Datenschutz-Schutzmaßnahmen lassen sich für einen zu modellierenden IT-Verbund bzw. ein Verfahren transparent prüfen, sie lassen sich einbinden in das IT-Sicherheitsmanagement nach ISO27001, in das Risikomanagement nach ISO27005 oder in das ITIL- oder CoBIT-Framework und sind nicht zuletzt betriebswirtschaftlich kalkulierbar.

6 Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6: 353-358. Inzwischen wurde die Nützlichkeit dieses Ansatzes mit mehreren Studien belegt (bis auf (5) sind die Studien aktuell per Internet zugänglich): (1) ULD, 2011: Juristische Fragen im Bereich altersgerechter Assistenzsysteme, Vorstudie im Auftrag des VDI/VDE-IT im Rahmen des BMBF-Förderungsschwerpunkte „Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben – AAL“; (2) VDE, 2012: Die deutsche Normungs-Roadmap AAL, N.N., 2012: (3) Usecases „Smart-Metering“, Papier der Datenschutzbeauftragten (im Erscheinen); (4) Geisberger, Eva / Broy, Manfred (Hrsg.), 2012: > agendaCPS, Integrierte Forschungsagenda Cyber-Physical Systems, acatech Studie, Deutsche Akademie der Technikwissenschaften; (5) Zwingelberg, Harald / Hansen, Marit, 2012: „Privacy Protection Goals and Their Implications for eID Systems“, in Jan Camenisch, Bruno Crispo, Simone Fischer- Hübner Ronald Leenes, Giovanni Russello (Eds). “Privacy and Identity Management for Life – 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 International Summer School Trento, Italy, September 2011 Revised Selected Papers“, Springer Boston, to appear 2012.

7 Es gibt keine Instanz, die eine semantische Identität von senderseitig Gesagtem und empfängerseitig Verstandenem feststellen könnte. Diejenige Instanz, die Identität behauptete, ist auch nur eine Instanz, die dem gleichen Problem unterliegt. Die Funktion von „Zielen“ besteht in der Fokussierung. Auch „Prinzipien“ können von verschiedenen Ausgangspunkten bzw. Rationalitätsdomänen zur Koordinierung anvisiert werden, man kann sich auf diese einigen, ohne dass bei einem Konflikt für Akteure daraus irgend etwas anderes folgen muss, außer dem anderen vielleicht „Unvernunft“ zu attestieren. In diesem Sinne sind „Prinzipien“, die in den Bemühungen um eine stärkere Kohärenzbildung von Datenschutz nach wie vor eine Rolle spielen, eher Indikatoren konzeptioneller Unreife.

Die aufgeführten sechs Schutzziele lassen sich entweder direkt den Abschnitten zu den technisch-organisatorischen Sicherheitsmaßnahmen der Ländergesetze entnehmen – als vollständiger Satz der sechs „elementaren Schutzziele" dem LDSG-SH oder zu einem Anteil den LDSGen der Neuen Bundesländer sowie Berlin, Hamburg, Nordrhein-Westfalen – oder sie lassen sich aus dem Bundesdatenschutzgesetz, insbesondere Anhang zu § 9 oder dem derzeit aktuellsten Versuch einer modernen Datenschutzgesetzgebung, nämlich dem Entwurf zur EU-Datenschutzverordnung, ableiten.[8] Die Schutzziele passen außerdem in das strategisch ausgerichtete Konzept des „Privacy by Design" und der „General Privacy Standards".[9] Und sie lassen sich als Systematisierung und Konkretisierung der „Privacy-Principles" des Privacy-Frameworks der ISO29100/ ISO29101 heranziehen und, unmittelbar als Schutzziele formuliert, auch für ein Privacy Impact Assessment nutzen.[10] Neben der rechtlichen Einbettung der Schutzziele dirigieren diese die technisch-organisatorischen Schutzmaßnahmen, zu denen insbesondere die Privacy-Enhancing-Technologies (PET) zählen.

Für jedes Schutzziel gibt es jeweils einen Katalog an paradigmatisch dominierenden Schutzmaßnahmen, die an dieser Stelle nur kurz erwähnt werden sollen:[11] Verfügbarkeit von Verfahren wird durch Redundanz gesichert, Integrität durch Steuerung und Regulation von Prozessen sowie Hashwert-Vergleichen bei Daten, Vertraulichkeit durch Berechtigungskonzepte und Verschlüsselung. Die Sicherung der Transparenz eines Verfahrens dient der Herstellung primär der Prüfbarkeit und wird insbesondere durch Dokumentation sowie Protokollierung von Prozessabläufen auf IT-Systemen umgesetzt. Die Sicherung der Intervenierbarkeit in ein Verfahren führt dazu, dass eine Organisation nachgewiesenermaßen über ein gesteuert-reguliertes Changemanagement verfügen muss, um strukturell rechtskonform zu sein sowie jederzeitig vollumfänglich die Betroffenrechte (auf Auskunft, Korrektur, Löschung) bedienen zu können. Und die Sicherung der Nicht-Verkettbarkeit wird auf Seiten einer Organisation vor allem durch die Trennung von Verfahren bzw. durch Setzen von Systemgrenzen realisiert sowie in Bezug auf personenbezogene Daten durch die Nutzung von Pseudonymisierung und Anonymisierung oder besonders wirkungsvoll durch Bereitstellung und Nutzung anonymer Credentials. Diese Maßnahmen lassen sich skalierbar, entsprechend des Schutzbedarfs, konzipieren, implementieren und kontrolliert betreiben.

Es ist methodisch wichtig zu betonen, dass die Systematik der elementaren Schutzziele das datenschutzrechtlich-normative Abwägen unmittelbar im Medium der Schutzziele erlaubt, weil die Schutzziele entlang von drei Dual-Achsen entwickelt wurden: Verfügbarkeit-Vertraulichkeit, Integrität-Intervenierbarkeit, Transparenz-Nicht-Verkettbarkeit. Auf diesen drei Achsen kann man die Schutzziele auf beiden Polen nicht gleichzeitig maximieren wollen, ohne sich in einen Widerspruch zu verwickeln. Formal eine gesicherte Verfügbarkeit und eine gesicherte Nichtverfügbarkeit zugleich zu fordern, ist ein Konflikt, der zugleich Abwägbarkeit ermöglicht. Ein Dual soll dabei einen Typ von Beziehung bezeichnen, der sowohl unverzichtbar komplementär als zugleich auch widersprüchlich ist. Diese spezifische Dualität-Eigenschaft insbesondere bei drei Achsen ist zwar eine problematische Eigenschaft, wenn man bestrebt ist, Datenschutz ähnlich formal wie Datensicherheit abzuhandeln. Sie ist aber zugleich eine wesentliche Eigenschaft, um eine juristische Abwägung zwischen verschiedenen berechtigten Anforderungen an ein System treffen zu können.[12]

Die Schutzziele bilden nicht nur das Medium bzw. einen Kanon zur Bestimmung von Gründen und zur juristischen Abwägung sowie zum Dirigieren und Festsetzen der (Intensität der) zu treffenden technischen Schutzmaßnahmen. Schutzziele sind auch geeignet, um das Datenschutzmanagement einer Organisation zu steuern bzw. standardisiert überprüfbar zu machen. Letzteres kann etwa im Hinblick darauf geschehen, ob eine Organisation Prozesse ausgebildet hat, die ein Controlling und daran gekoppelt, eine Steuerung von Verfahren entlang der Schutzziele erlauben, um Transparenz herzustellen, die Separierung von Datenbeständen, IT-Systemen und Prozessen sowie die Umsetzung der Betroffenenrechte kontrolliert durchzusetzen. Von einem Datenschutzmanagementsystem, das bspw. einen sehr hohen Schutzbedarf unterstützte, muss insbesondere eine Schnittstelle zum Identitätenmanagement für Betroffene sowie standardisierte Prüfanker insbesondere für Auditoren und externe Aufsichtsinstanzen enthalten sein.

Aus den sechs elementaren Schutzzielen lassen sich weitere Schutzziele ableiten, so dass auch innerhalb des hier vorgestellten Modellierungsrahmens für besondere Verfahren bzw. Verfahrensbestandteile spezifischer zugeschnittene Schutzziele hinzugenommen werden können.[13]

2.2 Verfahrenskomponenten: Daten, Systeme, Prozesse

Um eine hinreichende Auflösung für eine datenschutzgerechte Gestaltung bzw. Prüffähigkeit von personenbezogenen Verfahren zu bieten, sollten die folgenden Komponenten eines Verfahrens jeweils für sich betrachtet werden, um jeweils angemessene Schutzmaßnahmen für die entsprechende Verfahrenskomponente nutzen zu können:

- *Daten* und Datenstrukturen (Formate)
- *IT-System* und Schnittstellen
- *Prozesse* und Rollen / Adressen.

Die Daten bieten einen Import eines Sachverhalts der Welt in das Modell. Über die Rollen, die von den Prozessen einer Organisation angefordert werden, wird der Aspekt der rechtlichen Verantwortlichkeit im Modell angedockt. Und das IT-System bie-

8 Vgl. dazu ausführlich: Bock / Meissner, in diesem Heft.

9 Zugleich beheben sie sie deren Schwächen, indem sie konkretisieren, was bspw. „Privacy by Default" konzeptionell heißt, vgl. Rost, Martin / Bock, Kirsten, 2011 Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD – Datenschutz und Datensicherheit, 35. Jahrgang, Heft 1: 30-34.

10 Wichtig ist, dass bei einem PIA tatsächlich die Risikoperspektive des Betroffenen eingenommen und von der Risikoperspektive einer Organisation geschieden bearbeitet wird. Besonders deutlich zeigt sich die aus Datenschutzsicht falsche Entschiedenheit für die Organisationsperspektive am ICO 2009: Privacy Impact Assessment Handbook, version 2.0 – http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/html/1-Chap2-2.html sowie im „Privacy Impact Assessment Guideline", der 2011 vom BSI, in Zusammenarbeit mit WU-Wien/ Spiekermann herausgegeben wurde. Beide leisten vornehmlich ein Security-Impact-Assessment.

11 Vgl. dazu ausführlicher: Probst, in diesem Heft.

12 Weitere Details zur vollständigen Abbildbarkeit datenschutzrechtlicher Anforderungen in den Schutzzielen bei Bock/ Meissner in diesem heft.

13 Das Gesamtkonzept der Neuen Schutzziele weist acht weitere Schutzziele aus, die aus den sechs genannten Elementarschutzzielen ableitbar sind: Verbindlichkeit, Anonymität, Kontingenz (bzw. Abstreitbarkeit), Zurechenbarkeit, Findbarkeit, Ermittelbarkeit, Verdecktheit, Unbeobachtbarkeit.

tet wiederum das Medium universeller Abbildbarkeit und spezifischer Automation.

Derart aufbereitet kann man nun bspw. angeben, wie das Schutzziel Transparenz in einem Referenzmodell generisch umsetzbar ist. Bezogen auf Daten kann Transparenz zu sichern konkret bedeuten, dass funktionaler Zweck und semantische Erforderlichkeit einzelner Datenfelder etwa in einer Datenbank fachlich und rechtlich zu begründen sind und die Datenstrukturen im Hinblick auf deren Semantik zu dokumentieren sind.[14] Bei IT-Systemen sind die Komponenten mit ihren funktionalen Eigenschaften zu inventarisieren sowie der IT-Verbund und deren Schnittstellen untereinander und zu anderen Verbünden zu dokumentieren. Und bei Prozessen sind deren Initiierung und Terminierung bzw. Abgrenzung sowie das Changemanagement und die Dokumentation von Rollen mit ihren Zugriffsberechtigungen und Organisationsschnittstellen zu betrachten. Für Prozesse sind insbesondere Soll-Werte im Vorhinein festzulegen, die normativ verankert, technisch konfiguriert und organisatorisch geregelt sind. Systemzustände sind zu protokollieren, so dass diese Ist-Werte eine Basis für die Kontrollierbarkeit und kontrollierte Intervenierbarkeit für das „integre Schwingen" von Prozessen bilden. Über alle drei Komponenten hinweg ist dann eine Protokollierung von Datenströmen auf der Basis von Aktivitäten von IT-Systemen und Rollen möglich. Der Zweck von Dokumentation und Protokollierung besteht insofern darin, Soll- und Ist-Werte für den Prüfprozess, der im Rahmen eines Datenschutzmanagementsystems implementiert ist, bereit zu stellen.

2.3 Schutzbedarfsfeststellungen: normal, hoch, sehr hoch

Der Schutzbedarf für personenbezogene Verfahren und deren Komponenten lässt sich mit einer dreiteiligen Bewertungsskala normal, hoch sowie sehr hoch feststellen. Diese Skala hat ebenfalls ihren Ursprung in der Datensicherheit nach BSI-Grundschutz.[15] Die Definition der Schutzbedarfe bzw. deren Differenzierung untereinander kann, wegen der unterschiedlichen Angreifermodelle von Datensicherheit und Datenschutz, allerdings nicht vom Grundschutz-Vorbild übernommen werden. Entsprechend muss die Definition der Datenschutz-Schutzbedarfskategorien aus der Perspektive des Betroffenen erfolgen:

Die Schutzbedarfskategorie *normal* bedeutet, dass die Schadensauswirkungen begrenzt und überschaubar sind und etwaig eingetretene Schäden für den Betroffenen relativ leicht zu heilen sind.

Die Schutzbedarfskategorie *hoch* ist dann angemessen gewählt, wenn die Schadensauswirkungen von einer Person als beträchtlich eingeschätzt werden, z.B. weil bei Wegfall einer von einer Organisation zugesagten Leistung – wie das Zurverfügungstellen von Strom oder Kommunikationsdiensten, die eine materielle Voraussetzung sind, um in einer modernen Gesellschaft informationelle Selbstbestimmung ausüben zu könne, – die Gestaltung des Alltags nachhaltig veränderte und der Betroffene auf zusätzliche Hilfe angewiesen wäre.

Die Schutzbedarfskategorie *sehr hoch* bleibt solchen Fällen vorbehalten, in denen Schadensauswirkungen ein existentiell bedrohliches, katastrophales Ausmaß erreichen können.

Die Auswirkungen auf eine Person oder einen Haushalt mit mehreren Personen lassen sich typischen Szenarien zuordnen, etwa: Verstoß gegen Normen (Gesetz/ Vertrag), Beeinträchtigung der bezogenen Funktionalität auf den Lebensalltag, Beeinträchtigung des Vertrauensverhältnisses zur Organisation, finanzielle Auswirkungen sowie unmittelbare Auswirkungen auf eine Person im Hinblick auf Folgen für ihre Selbstbestimmtheit im Sinne von Bürger- und Kundenrechten sowie für die körperliche Unversehrtheit.

Am Beispiel der Schutzziele Integrität und Transparenz erläutert, würde die Feststellung eines normalen Schutzbedarfs bspw. bedeuten, dass die Protokolldaten der im Verfahren verwendeten Anwendungsprogramme und Betriebssysteme regelmäßig automatisiert geprüft werden. Stellte man dagegen einen sehr hohen Schutzbedarf für diese beiden Ziele fest, so bedeutete dies u.a., dass die Protokollierung auch von lesenden Aktivitäten von Mitarbeitern einer Organisation auf einem dedizierten Protollierungsserver erfolgen sollte, der dem Zugriff der Administration auf dem Produktiv-IT-System eines Fachverfahrens entzogen ist. Das wäre dann als eine Referenzlösung ausweisbar. Wenn bei einem sehr hohen Schutzbedarf eine andere als diese Referenzlösung zur Sicherung insbesondere der Transparenz gewählt wird, so muss die funktionale Äquivalenz durch die verantwortliche Stelle nachgewiesen werden.

Der Schutzbedarf wird typischerweise in einer Risikoanalyse ermittelt bzw. festgesetzt, wobei die zu betrachtenden Risikokriterien den Schutzzielen des Datenschutzes entsprechen. Zu beantworten ist bspw. die Frage, wie riskant für einen Betroffenen ein intransparentes, nicht prüffähiges Verfahren einzuschätzen ist. Entsprechend des festgestellten Schutzbedarfs ist das Verfahren dann einzurichten und mit den dafür angemessenen Kontroll- und Schutzmechanismen auszustatten und der Umgang mit dem verbliebenen Restrisiko zu regeln.

Dass Religionszugehörigkeit oder medizinische Daten einer Person pauschal einen zumindest hohen Schutzbedarf haben, lässt sich relativ einfach und direkt aus Datenschutzgesetzen herleiten und erübrigt somit jede Diskussion, auf welchem Niveau entsprechende Schutzmaßnahmen, bspw. bei einem Krankenhausinformationssystem, einzurichten sind. Es wäre wünschenswert, wenn der Gesetzgeber zukünftig den Schutzbedarf von Verfahren normativ festlegte.

3 Arbeiten mit dem Modell

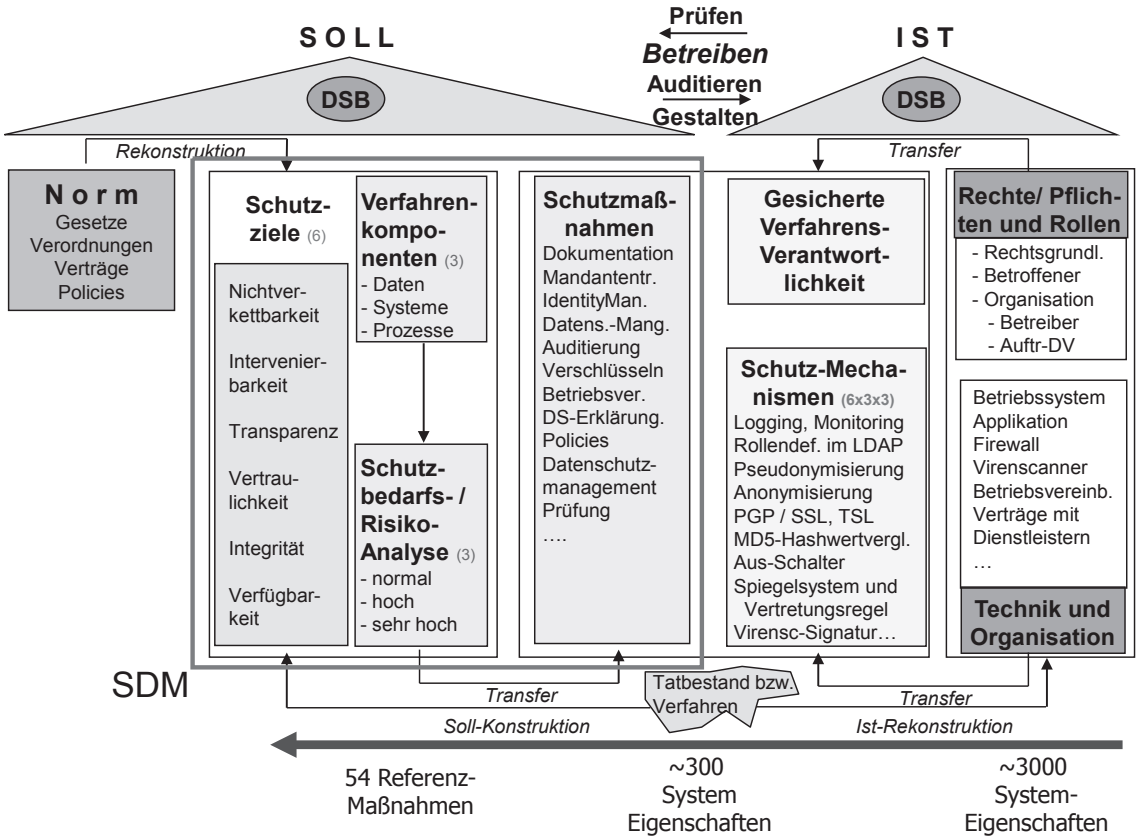
Welchen Nutzen bringt das SDM bei der täglichen Arbeit eines professionellen Datenschützers?

Schutzziele dienen der Vermittlung von Rechtsnormen für Verfahren mit Personenbezug auf der einen Seite mit den technischen und organisatorischen Eigenschaften und Schutzmaßnahmen auf der anderen Seite. Das standardisierte Datenschutzmodell erlaubt, diese beiden Seiten in einem Modell zusammen zu bringen, ohne dass eine Logik die andere dominiert. Beide Seiten werden im Modell kontrollierbar aufeinander bezogen und tref-

14 In der öffentlichen Verwaltung in Deutschland geschieht das auf einem systematisch zunehmend besser reflektierten Niveau einer Qualitätssicherung im Rahmen der vom IT-Planungsrat gesteuerten und von der KOSIT implementierten XÖV-Standardisierungen.

15 Siehe: BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, ab S. 49 https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf

Abbildung 1 | Standardisiertes Datenschutzprüfmodell (SDP)



fen bei den Maßnahmen und der Beurteilung von deren Wirksamkeit zusammen.

Die juristische Expertise erfasst die rechtlich relevanten Eigenschaften eines Verfahrens und der Verfahrensbeteiligten. Es sind die gesetzlich gültigen bzw. die vertraglichen Regelungen, in Form von Codes of Conduct oder Dienst- und Betriebsvereinbarungen oder von Vertragswerken zur Auftragdatenverarbeitung festzustellen. Außerdem sind die Organisationsstruktur mit Rollen und Verantwortlichkeiten sowie die Schnittstelle zur Fachlichkeit eines Verfahrens mit der Abklärung der einzelnen Daten bzw. Datenfelder einer zur Verarbeitung genutzten Applikation zu erheben. Die Abschätzung des Verfahrenszwecks und der Erforderlichkeit, sowie Thesen bzgl. der Möglichkeiten, Datensparsamkeit walten zu lassen und das frühest mögliche Löschdatum ausfindig zu machen oder die Notwendigkeit einer Vollidentifikation einer Person, all das muss auch fachlich beurteilt werden und ergibt sich nicht zwingend allein aus juristischer oder technischer Perspektive. Nach der Klärung der rechtlich relevanten Eigenschaften lassen sich die normativen Abwägungen und Entscheidungen dann in das Medium der Schutzziele übersetzen, sofern diese Abwägungen nicht bereits innerhalb der Schutzziele vorgenommen und Entscheidungen getroffen werden.[16] Mit dieser Schutzziele-Darstellung entsteht dann eine Modellierung des Verfahrens, aus dem modellgestützt der Betrieb eines Verfahrens sowie die theoretisch erwartbaren Schutzmaßnahmen resultieren.

Die technische und organisatorische Expertise erfasst die Eigenschaften der drei Verfahrenskomponenten. Diese Eigenschaften werden zusammengestellt und typisiert und zu Maßnahmenbündeln aggregiert, die der Sicherstellung der Datensicherheit und des Datenschutzes dienen. Dabei wird auch die durch die vorgefundenen Maßnahmen erzielte Intensität der Schutzwirkungen festgestellt.

Die Erfassung des Ist-Zustands des Betriebs eines Verfahrens sowie der festgestellten Datenschutz-Schutzmaß-nahmen und deren Ausprägung im Hinblick auf den Schutzbedarf lassen sich dann mit den aus der Schutzziele-Modellierung abgeleiteten Soll-Schutzmaßnahmen in Beziehung setzen. Durch dieses Verfahren wird eine Bilanzierung von Soll und Haben ermöglicht, die eine transparente Begründung des Urteils erlaubt, ob ein Verfahren mit seinen Verfahrenskomponenten datenschutzgerecht eingerichtet und mit den angemessenen Schutzmaßnahmen betrieben wird oder nicht. Darüber hinaus können aufgrund der Modellierung der Sollmaßnahmen bei festgestellten Mängeln vielfach konkrete Vorschläge gemacht werden, wie sich diese Mängel beheben lassen (siehe Abbildung 1).

Sowohl zur Feststellung rechtlicher als auch technischer und organisatorischer Eigenschaften eines Verfahrens bedarf es der Transparenz, die in der Prüfungspraxis vielfach jedoch nicht hinreichend gegeben ist. Wenn sich weder die Rechtsgrundlagen und Verantwortlichkeiten noch die technischen Eigenschaften der Komponenten eines Verfahrens ermitteln lassen, reicht allein die-

16 Die These ist, dass die Übersetzung der Normen in Schutzziele nicht nur weitgehend verlustfrei möglich ist, sondern dass die Normen, mit der Zuspitzung durch die Schutzziele, an Diskriminierungskraft bzw. Normenklarheit gewinnen.

se Feststellung, um ein Verfahren als intransparent und deshalb als nicht mit dem Datenschutzrecht vereinbar zu beanstanden.

4 Risikomodellierung?

Zum Abschluss sollen fünf Datenschutz-Risiken aufgelistet werden, die sich aus diesem Modell systematisch ableiten lassen und die bspw. in einem umfassend ansetzenden PIA aus unserer Sicht anzusprechen wären.[17]

Das *Verfahrensrisiko* bezeichnet das Risiko, das für eine Person durch ein Verfahren erzeugt wird. Aus Datenschutzsicht ist das Vorliegen einer Rechtsgrundlage und ein gesicherter IT-Betrieb allein noch nicht hinreichend, um einem Verfahren Datenschutzgerechtigkeit zu attestieren.[18]

Das *Modellierungsrisiko* bezeichnet ein unzureichend angelegtes Konzept von „Datenschutzprüfung", wenn etwas als „Datenschutzprüfung" oder als „Privacy Impact Assessment" für ein Verfahren deklariert ist, obwohl a) nur ein Teil der Schutzziele, zumeist die der Datensicherheit bei unveränderter Übernahme der Definitionen des BSI, betrachtet wird oder b) nicht alle drei Verfahrenskomponenten geprüft werden oder c) die Schutzbedarfsfestsetzungen zu niedrig ausfallen.

Das *Schutzmaßnahmen-Risiko* betrifft solche Problemstellungen, für die keine Schutzmaßnahmen getroffen wurden oder bei denen getroffene Schutzmaßnahmen unwirksam sind.

Auch muss das *Kompetenzrisiko* benannt werden, wenn die Personalausstattung sowie die Fähigkeiten und Motivationslagen von PrüferInnen und Prüfern nicht hinreichen, um Sachverhalte der Welt eingedacht und sachgemäß in eine transparente und integre Prüfsystematik zu überführen.

Und zuletzt sei das *Gesetz- und Kontrollrisiko* genannt, das darin besteht, dass Bürger/Innen, KundInnen, PatientInnen und MitarbeiterInnen aufgrund der bloßen Existenz von Datenschutzgesetzen und Datenschutzbeauftragten davon ausgehen, dass Datenschutz gewahrt ist und ggfs. vertrauenswürdige, weil transparente und integre, Datenschutzprüfungen tatsächlich, insbesondere bei den rechtsstaatlich besonders heiklen Organisationen wie Geheimdiensten, Sozialversicherungen und Social Networks stattfinden. Auch vertrauen Betroffene darauf, dass Datenschutzgesetze, auf deren Grundlage Prüfungen erfolgen, geeignet sind, für einen materiell wirkungsvollen Datenschutz zu sorgen.

Datenschützer sind dafür zuständig, diese Risiken zu thematisieren und diese nicht nur juristisch, sondern auch politisch, konzeptionell sowie forschend zu bearbeiten und konkret zu verringern.

5 Fazit

Die Schutzziele bilden einen Kanon an Kriterien zur Abwägung rechtlicher Anforderungen an personenbezogene Verfahren in einer operationalisierbaren Form. Im Zusammenspiel von Schutzzielen mit Schutzbedarfsfeststellungen für Daten, IT-Systeme und Prozesse ist es möglich, die Intensität von Maßnahmen – bzw. das Ausmaß von Risiken – in einem Gesamtmodell festzulegen. Das aus diesen Komponenten zusammengesetzte Grundmodell legt einen Referenz-Prüfrahmen für die Betrachtung von theoretisch 54 Standardschutzmaßnahmen nahe.

Die Nutzung allein eines solchen generischen Prüfmodells erzwingt noch keine Kohärenz für jeden Fall einer datenschutzrechtlichen Beurteilung. Aber es hilft, Dissens bei Mängelfeststellungen zu markieren und ggfs. diese einem Gericht zur Entscheidung vorzulegen und/oder eine Änderung von Rechtsgrundlagen zu erwirken.

17 Die konventionelle Definition von Risiko stellt darauf ab, ein Risiko als das Produkt von Eintrittshäufigkeit bzw. Eintrittswahrscheinlichkeit und Ereignisschwere bzw. Schadensausmaß zu definieren. Hier soll von Risiko abstrakter die Rede sein, wonach anhand von Kriterien Differenzen festgestellt und Informationen gewonnen werden können, die einen Transfer von unbestimmbaren Gefahren in bestimmbare Risiken leisten. Die Schutzziele erzeugen eine Bestimmtheit, die Ereignissen in einer Organisation eine mögliche negative Auswirkung bei Personen beizumessen gestatten.

18 Dass vielfach Skepsis gegenüber der Sensibilität des Gesetzgebers für die Belange des Datenschutzes gut begründet ist, zeigen insbesondere die vielen Aktivitäten des Bundesverfassungsgerichts, mit denen Gesetze, die keinen angemessenen Datenschutz gewähren, kassiert wurden.