Martin Rost

Datenschutz in 3D

Daten, Prozesse und Schutzziele in einem Modell

Es wird ein Modell vorgestellt, das allen Beteiligten einen Gesamtüberblick darüber verschafft, was aus Datenschutzsicht zu planen, zu erheben, festzulegen oder zu prüfen ist.

1 Einleitung

Ein proaktiv ausgerichteter Datenschutz sieht sich durchgängig vor die Aufgabe gestellt, für die Datenverarbeitung von und zwischen Organisationen einen angemessenen Arbeitspunkt, oder genauer formuliert: einen Arbeitsraum zu finden, der durch das Abwägen von Rechtsnormen, einzusetzenden Schutztechniken sowie von Prozessen zur Überwachung von Abläufen der Datenverarbeitung zustande kommt. Den Datenschutzexperten ist deshalb die Bereitschaft abzuverlangen, innerhalb ihres Zuständigkeitsbereichs kreativ und konstruktiv zu agieren, und darüber hinaus in der Lage zu sein, mit Experten anderer Fachlogiken, auf der Basis einer gemeinsamen Modellvorstellung, zusammen zu arbeiten. Das Ziel besteht darin, sich auf funktionierende und rechtskonforme Lösungen einigen zu können.

Dieser Artikel umreisst knapp ein Modell, in dem Daten, Prozesse und Schutzziele als *drei Kanten* eines Würfels in systematischer Weise aufeinander bezogen sind. Dadurch wird es möglich, den Lösungsraum auf einem gut austarierten Niveau zwischen Abstraktion und Konkretion allen Beteiligten vor Augen zu stellen. Jeweils eine Dimension dieses Würfels ist so angelegt, dass diese speziell von einer Fachlogik, also etwa der juristischen, primär betreut werden kann. Diese Fachlogik überblickt die Spielräume dieser Dimension fachlich am besten und weiss diese zu gestalten, während die Fachlogiken der anderen Professionen diese Ausprägungen als gegebene Fakten hinnehmen. Juristen wenden Normen nicht nur an sondern legen sie aus. Techniker überblicken technische Maßnahmen und können u.a. deren funktionale Äquivalenz zueinander feststellen oder neue Maßnahmen entwickeln. Organisationsexperten haben die Übersicht über verschiedene Prozess-Paradigmen und Regelungen und verfügen über best-practice-Expertise zu den Schnittstellen von Organisation und Technik.

Nachfolgend werden in drei Schritten die Dimensionen mit ihren Ausprägungen erläutert, dann werden drei Flächen dargestellt, dann wird der Würfel zusammengesetzt. Mit jedem Schritt soll gezeigt werden, welcher methodische und analytische Nutzen aus der Verwendung des Datenschutzwürfels gezogen werden kann. Die zur Veranschaulichung des Würfels gewählten Beispiele stammen aus einer Studie zu „Ambient Assisted Living" (AAL), für die der Datenschutz-Würfel entwickelt wurde.[1]

Martin Rost

Mitarbeiter im Referat „Systemdatenschutz" beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.
E-Mail:
martin.rost@datenschutzzentrum.de

2 Die Dimensionen

2.1 Daten

In der Dimension der Daten lassen sich bei einer Datenverarbeitung zumeist Gruppen von Daten unterscheiden: fachliche Daten, Kommunikationsdaten, Metadaten, technische Daten, Kontrolldaten. Mit einer Analyse der Daten tritt zugleich die dafür einzusetzende Technik unter zunächst rein funktionalen Gesichtspunkten in Erscheinung.

Am Beispiel von AAL-Systemen erläutert lassen sich hinreichend trennscharf die folgenden Datengruppen unterscheiden: Interventionsdaten (bspw. Fernmedikation durch Fernsetzen einer Spritze oder Verschließen von Türen bei verwirrten Menschen, von einem entfernten Leitstand aus), Vitaldaten (Blutzucker, Gewicht, Temperatur...), Verhaltensdaten (Schlaf-, Ess-, Arbeits-, Entspannungszeiten...), Technikinfrastrukturdaten, Mess- und Umgebungsdaten (Temperatur, Licht, Feuchtigkeit, Lautstärke), Triggerdaten (Alarmauslöser, An/Aus-Schaltungen). Mit diesen Daten gerät zwangsläufig auch die Technik in den Blick, mit denen diese Daten über Sensoren erzeugt, verarbeitet und an Aktoren gekoppelt, übermittelt sowie archiviert oder gelöscht werden.

2.2 Prozesse

In der Dimension der Prozesse lassen sich grundsätzlich für jeden Sachverhalt drei Prozessdomänen unterscheiden, die bei jeder Verarbeitung von Daten eine Rolle spielen können, wenn es mehrere Beteiligte gibt und folglich zwischen ihnen Rechtsbeziehungen bestehen. Diese drei Prozessdomänen bestehen zum einen aus Prozessen auf Seiten betroffener Personen – in ihren generischen Rollen als Bürger, Kunden, Patienten, Mandanten, Menschen – sowie

1 Die Protagonisten verstehen unter AAL „altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben". Derzeit gibt es eine ganze Reihe an Pilotprojekten, in denen vornehmlich Überwachungs- und Betreuungstechniken genutzt werden, um die Lebensqualität vornehmlich hilfebedürftiger Menschen technisch zu verbessern. Dies läuft absehbar auf eine Industrialisierung der Betreuung von Menschen im Kernbereich ihres Privatlebens hinaus und hat deshalb eine starke datenschutzrechtliche Relevanz (Siehe: Unabhängiges Landeszentrum für Datenschutz, 2011: Juristische Fragen im Bereich Altersgerechter Assistenzsysteme, Vorstudie im Auftrag von VDI / VDE-IT, gefördert vom Bundesministerium für Bildung und Forschung: https://www.datenschutzzentrum.de/projekte/aal/).

zum zweiten aus Prozessen auf Seiten der Organisationen und Dienstleistungen, also in Form einer öffentlichen Verwaltung, eines Unternehmens oder einer Praxis. Die dritte Prozessdomäne betrifft die Prozesse auf Seiten der Dienstleister für die oben genannten Organisationen. Zu solchen Organisationen, die Teil einer gesellschaftlichen Infrastruktur bilden, zählen typischerweise Rechenzentren, Access- und Content-Provider, aber auch Aufsichtsbehörden oder Forschungsinstitute. Diese Prozessdomäne gerät datenschutzrechtlich typischerweise als Auftragsdatenverarbeitung zwischen Organisationen in den Blick.

Diesen drei Prozessdomänen sind Prozesseigentümer zugeordnet, so dass Prozesse und die handelnden juristischen und natürlichen Personen rechtlich aufeinander bezogen sind. Diese Prozesseigentümer haben die konkrete Ausgestaltung ihrer Prozesse in Bezug zu den anderen Eigentümern der anderen Prozessdomänen zu verantworten. Im Rahmen von identifizierten Prozessen und Prozesseigentümern fallen dann typischerweise Lücken in Verantwortungszuordnungen bzw. Verantwortungsübernahmen auf. Eine diesbezüglich besonders zu betrachtende Konstellation besteht beim Cloud-Computing.[2]

Am Beispiel AAL erläutert befindet sich in der Prozessdomäne der Person typischerweise ein hilfebedürftiger Mensch, für den in seiner Lebensumgebung Assistenzsysteme eingerichtet sind, die ihn im Alltag unterstützen und dabei vor allem in lebensbedrohlichen Lagen Alarm auslösen. In dieser Prozessdomäne muss der Betroffene in der Lage sein, in Normalsituationen mit dem System umzugehen. In der Prozessdomäne Organisation agieren AAL-Betreuungs-Dienstleister, das sind typischerweise Pflegedienste (externe Betreuung oder Heimbetreuung), Wachdienste oder in selteneren Fällen auch Ärzte, die diese Assistenzsysteme bei den Betroffenen betreiben. In ihrer Rolle als Prozesseigentümer haben sie die Verantwortung für das Funktionieren von Betreuungsverfahren mit ihren Prozessen zur Kontrolle und Intervention unter Rückgriff auf Technik. Und in der Prozessdomäne der gesellschaftlichen Infrastruktur agieren typischerweise Rechenzentren, die möglicherweise in einer public cloud irgendwo auf der Welt AAL-Betreuungsszenarien rechnen lassen, sowie Internet-Accessprovider oder IT-Dienstleister. Mit den Prozessen geraten somit Organisationsstrukturen, Rechtsgrundlagen und Rechtsbeziehungen sowie Verantwortlichkeiten in den Blick.

2.3 Schutzziele

Die dritte Dimension des Würfels enthält zunächst einmal vorrangig die datenschutzrechtlich geltenden Normen, die in Form von sechs zu unterscheidenden elementaren Schutzzielen operationalisiert sind. Die Schutzziele bestehen zum einen aus den klassischen Schutzzielen der Datensicherheit auf Seiten einer Organisation, nämlich *Verfügbarkeit, Integrität und Vertraulichkeit*. Die „Neuen Schutzziele", die die klassischen Schutzziele der Datensicherheit unter Datenschutzaspekten aus Sicht von Betroffenen zum einen profilieren und zum zweiten mit eigenen Inhalten ergänzen, lauten *Transparenz, Nichtverkettbarkeit und Intervenierbarkeit*.[3]
Jedem Schutzziel steht ein Katalog mit technischen und organisatorischen Maßnahmen, mit denen ein Schutzziel in unterschiedlichem Ausmaß wirkungsvoll umgesetzt werden kann. Genau so bedeutsam wie die Kopplung der Ziele an technisch-organisatorische Schutzmaßnahmen ist zweitens die rechtliche Abwägbarkeit der Schutzziele untereinander. Die Schutzziele sind immer vollständig auf einen konkreten Sachverhalt zu beziehen, weil diese in einem systematischen Spannungsverhältnis zueinander stehen, das rechtlich zu konditionieren ist.[4] So geht eine rechtlich gebotene besonders herauszuhebende Bedeutung eines Schutzziels dann zumeist einher mit einer geringer einzuschätzenden Bedeutung eines oder auch mehrerer anderer Schutzziele. Und drittens lassen sich die Schutzziele, über automatisiert vermessbare Schutzmaßnahmen, als Stellgröße zur Regulation von Prozessen, etwa für die Prozesse des Datenschutzmanagements einer Organisation verwenden.

Am Beispiel von AAL veranschaulicht besteht die Aufgabenstellung darin, dass ein Betreuungssystem zunächst einmal grundsätzlich vollständig an den Anforderungen der Schutzziele zu überprüfen ist. So sind Aspekte der Sicherung der Verfügbarkeit und Integrität von Technik und Betreuungsprozessen zu beachten, damit bspw. Alarmmeldungen in Notfällen auch verläßlich ausgelöst werden. Zugleich darf das Leben der Betroffenen aber nicht in dem Maße ausgerichtet sein, dass es zu einem Leben für das Betreuungssystem wird. Des Weiteren muss für Betroffene, Betreiber und Aufsichtsbehörden eine jeweils auf deren unterschiedliche kognitive Kompetenzen abgestimmte Transparenz der Systeme gegeben sein. Konfigurierbarkeit als Interventionsmaßnahme muss für den Betroffenen ebenso wie für den Betreiber gegeben sein. Der Betreiber muss zudem nachweisen, dass er seine Datenverarbeitung am ausgewiesenen Zweck orientiert betreibt und keine davon abweichenden weiteren Datenverarbeitungen („Verkettungen") vorgenommen werden (können).

Erstes Zwischenfazit: Hinter jeder der drei Dimensionen des Datenschutzwürfels – den Daten, den Prozessen und den Schutzzielen – ist ein weiterer Aspekt adressierbar, der in seiner Dimension kausal, also ohne zusätzliche Freiheitsgrade, mitkontrollierbar ist. Hinter den konkreten Daten eines Verfahrens steht die konkrete IT-Technik; hinter den Prozessen stehen die Rechtsgrundlagen für die Aktivitäten der Beteiligten; hinter den Schutzzielen stehen, entsprechend der BSI-Grundschutzmethode, Kataloge mit den technisch-organisatorischen Schutzmaßnahmen zur Umsetzung der Ziele.

3 Die Flächen

Bevor man diese drei Dimensionen als Kanten eines generischen Datenschutz-Würfels zusammensetzt, macht es Sinn, die drei Ebenen „Daten und Prozesse", „Daten und Schutzziele" sowie „Prozesse und Schutzziele" gesondert zu betrachten.

3.1 Daten und Prozesse

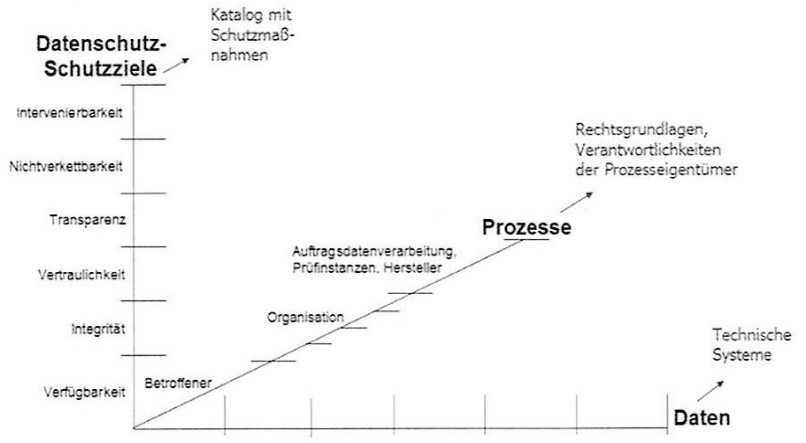
Auf der Ebene der Daten und Prozesse gilt es für Datenschützer zunächst zu verstehen, welche Aufgaben funktional zu lösen sind, für welche Prozesse welche Daten erforderlich sind, welche funktiona-

2 Vgl. Übersicht bei Hansen, Marit; Marnau, Ninja; Schlehan, Eva; Husmann, Elmar; 2011: TClouds – Auf dem Weg zur sicheren und datenschutzkonformen Cloud; in: <kes> Die Zeitschrift für Informationssicherheit, Verlagsbeilage, März 2011: 14-15.

3 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: 30-35. Siehe auch: „AAL-Studie", a.a.O., S. 96ff.

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

Abb. 1 | Der generische Datenschutzwürfel



len und welche sichernden Techniken entsprechend zum Einsatz kommen (könnten) und wer dafür dann in welchen Rollen verantwortlich ist. Anhand unterschiedlicher Prozesse lassen sich **Funktionstrennungen vornehmen und Zweckbindungen festlegen**, mit denen auch die erforderlichen Daten in den Blick geraten. Und umgekehrt gilt, dass bei Prüfungen von technischen Systemen deutlich werden muss, welche Daten erzeugt werden (können) und wer als Prozesseigentümer die Verantwortung dafür zu übernehmen hat. Die in den Prozessen zu verarbeitenden Daten müssen konkret festgelegt und typisiert werden, inhaltlich müssen diese verlässlich und gültig ausgelegt sein. Und diese Qualität an semantischer Korrektheit muss sich bei der Sicherung der Erhebungs-, Verarbeitungs- und Übermittlungstechnik fortsetzen.

Am Beispiel AAL erläutert: Betreuungsdienstleister erheben und verarbeiten Daten von Personen, die von Maschinen, weitestgehend standardisiert und automatisiert erzeugt werden. Es handelt sich um eine industrialisierte Dauerüberwachung des privaten Kernbereichs von Menschen. Dabei ist ein typischerweise anzutreffender Ausgangspunkt bei AAL-Projekten der, dass technisch gewonnene Forschungsdaten und Techniken zu deren Verarbeitung entwickelt werden, bei denen erst im Nachhinein festgelegt wird, welche Rechtsgrundlage gegeben ist und was davon nun für welche Zwecke und mit welcher rechtlichen Verantwortung verarbeitbar ist. Zugleich entstehen Begehrlichkeiten auf Seiten der Organisationen, weil mit diesen Daten und Verarbeitungstechniken eine gesteigerte Berechenbarkeit von Risiko-Entscheidungen insbesondere gegenüber betroffenen Personen in Aussicht gestellt wird.

3.2 Daten und Schutzziele

In der zweiten Ebene der Daten und Schutzziele sind vor allem die Abwägungen zur **Feststellung des Schutzbedarfs der Daten und Systeme** angesiedelt. Dazu werden die Daten und deren Produktionstechniken inventarisiert, sowie letztlich zu Datengruppen mit unterschiedlicher Sensibilität für die zu schützenden Produktionsprozesse sowie für die Umweltwirkungen und die Betroffenenrechte gruppiert. Speziell in Bezug auf Datenschutz und Datensicherheit ist dann zu klären, wie und in welchem Ausmaß der Schutzbedarf dieser Daten (und der dahinter liegenden technisch-organisatorischen Infrastruktur) durch die Maßnahmen der Schutzziel-Kataloge abgedeckt werden kann.[5] Methodisch entscheidend ist dabei, um es noch einmal zu betonen, dass der Schutzbedarf der von den technischen Systemen erzeugten bzw. erhobenen Daten an die technischen Systeme vererbt wird. Für AAL gilt bspw. zweifelsfrei, dass für die bereits erwähnten Interventions- und Vitaldaten bspw. sehr hoher Schutzbedarf zu veranschlagen ist. Entsprechend ist die gesamte technische Infrastruktur des AAL-Systems – die vom Smart-Metering des Stromversorgers über den Internet-Accessprovider bis hin selbstverständlich zu den Rechenzentren der Betreuungsdienstleister reicht – entsprechend dem sehr hohen Schutzbedarf auszulegen.[6]

3.3 Prozesse und Schutzziele

Auf der dritten Ebene, die von den Prozessen und Schutzzielen aufgespannt wird, gerät vornehmlich die **Regelung und Steuerbarkeit der Prozesse** von Organisationen in den Blick. Die Prozesse von Organisationen sind oftmals in Orientierung an Prozess-Organisationsparadigmen eingerichtet. Hinreichend bekannt sind als „ganzheitliche Ansätze" inzwischen ITIL, CoBIT oder auch das St. Gallener Modell oder Prozesse, die sich im Rahmen eines Qualitätsmanagements, das an DIN oder ISO orientiert ist, ergeben. Diese Paradigmen lassen sich mit den Schutzzielen des Datenschutzes und der Datensicherheit anreichern.[7] Typischerweise werden für zu regulierende Prozesse anhand von vorgegebenen Zielen Soll-Zustände festgelegt und Ist-Zustände (automatisiert) festgestellt. Das Datenschutzmanagement einer Organisation hat somit die Aufgabe, die derart ausgelegten Prozesse im Hinblick auf Datenschutz-Compliance kontinuierlich zu überwachen. Für organisierte Prozessen sind heutzutage Key-Performance-Indikatoren (KPI) oder Key-Risk-Indikatoren (KRI) entwickelt, wobei letztere den für Datenschutz interessanteren Aspekt des Risikoappetits einer Organisation anhand von Messgrößen kontrollierbar machen sollen. Entsprechend sind anhand der Schutzziele für die Prozesse des Datenschutzmanagements derartige Indikatoren auszubilden, an denen sich der Reifegrad der Prozesse ablesen lässt.

Am Beispiel von AAL veranschaulicht müssen angemessene technisch-organisatorische Maßnahmen entwickelt werden, die bspw. das Ausmaß einer Dauerbeobachtung eines hilfebedürftigen Menschen erkennbar machen. Der Betroffene ist zudem technisch in die Lage zu versetzen, in das Beobachtungssystem zu in-

5 Bislang liegen keine Schutzmaßnahmen-Kataloge auch für die Neuen Schutzziele des Datenschutzes, analog zu denen der Datensicherheit, vor. In den beiden zuvor referenzierten Schutzziel-Aufsätzen sowie in der erwähnten AAL-Studie sind jedoch eine ganze Reihe an Maßnahmen zur Umsetzung von Transparenz, Nichtverkettbarkeit und Intervenierbarkeit aufgeführt. Eine weitergehende Systematisierung der spezifischen Datenschutz-Schutzmaßnahmen sowie insbesondere der Profilierung der Schutzziele der Datensicherheit im Sinne des BSI-Grundschutzes steht noch aus.

6 Es wäre dann zu diskutieren, ob nicht auch bei Daten mit geringerem Schutzbedarf die für sehr hohen Schutzbedarf geeignete Infrastruktur eingesetzt werden sollte.

7 Meints, Martin, 2007: Datenschutz durch Prozesse, Musterprozesse für das Datenschutzmanagement; in: DuD – Datenschutz und Datensicherheit, 31. Jahrgang, Heft 2: 91-95.

tervenieren. Er muss die Möglichkeit haben, folgenlos diese Prozesse willkürlich ausschalten zu können. An diesem Beispiel zeigt sich, dass einerseits Anforderungen an die haftungsrechtlich relevante Systemintegrität einerseits mit den Anforderungen des grundrechtlich zu beachtenden Betroffenenrechts andererseits abzuwägen sind. Eine Lösung könnte darin bestehen, dass ein zentraler Ausschalte-Knopf für das Beobachtungssystem installiert ist, bei dem nach einigen Stunden des Ausgeschaltetseins der Betroffene eine Nachfrage zu seinem Zustand erhält, begleitet von einer Aufforderung, das System wieder zurück auf Normalbeobachtungsbetrieb anzuschalten. Das mag aus Sicht eines Systembetreibers keine wirklich schöne Lösung sein, stellt aber einen möglicherweise akzeptablen Kompromiss dar, der die Freiheitsrechte der betroffenen Person berücksichtigt.

Zweites Zwischenfazit: Die Betrachtung von Daten und Prozessen ist notwendig, um die Zweckbindung und Erforderlichkeit der Datenverarbeitung festlegen zu können. Die Betrachtung von Daten und Schutzzielen führt zur Analyse bzw. Festlegung des Schutzbedarfs der Daten und regelt entsprechend die Auswahl der technisch-organisatorischen Schutzmaßnahmen. Die Betrachtung von Prozessen und Schutzzielen führt die Prozesse und deren Regulierung im Rahmen des Datenschutzmanagements der beteiligten Organisationen vor Augen.

4 Der Würfel

Der Würfel versammelt die Prozesseigentümer, die Daten und Technik sowie die Anforderungen des Datenschutzes und der Datensicherheit in einem Bild. Der Würfel verspricht allen Beteiligten, durchaus im Sinne des Paradigmas der mehrseitigen Sicherheit, dass sowohl bei der Planung als auch beim Prüfen von Systemen jedes Schutzinteresse bzw. jeder wesentliche Datenschutz-Aspekt in den Blick gerät und im Hinblick auf eine **Gesamtstimmigkeit** thematisiert werden kann.[8] Insbesondere Systemplaner können nichts „vergessen" oder von Anforderungen überrascht werden. Sie können sichergehen, sich auf das Richtige zu fokussieren und dann aber auch nicht mehr zu tun als notwendig ist.

Durch die Anordnung zu einem Gesamtmodell, mit sozusagen doppelt belegten Dimensionen, ist zudem sichergestellt, dass verschiedene Einstiege in eine System-Planung oder -Prüfung möglich sind. So gerät ein technischer Prüfer oftmals zunächst an (Dokumente über) technische Systeme, und arbeitet sich dann zu den Daten der Fachapplikationen und den verschiedenen Sicherheitsmaßnamen auf unterschiedlichen Ebenen vor. Ein interner Datenschutzbeauftragter vollzieht oftmals als erstes die Geschäftsverteilungspläne sowie die Rollen- und Zugriffskonzepte der Organisationen nach und rekonstruiert so die Rechtsbeziehungen, Rechtsgrundlagen, Zuständigkeiten und Verantwortungsbereiche. Speziell bei Planungsaktivitäten wird demgegenüber üblicherweise zumeist bei Verfahren bzw. Prozessen eingestiegen und es werden anhand von Usecases die Erforderlichkeit der dafür notwendigen Daten, der Zuständigkeiten und der rechtlichen Regelungen analysiert bzw. festgelegt.

Der Datenschutzwürfel ist auch eine gute Modellierungsgrundlage, um die differenzierten operativen Anforderungen des Datenschutzmanagements zu erforschen und zu formulieren: In der Prozessdomäne des Betroffenen wäre das nutzerkontrollierte Identitätenmanagement anzusprechen.[9] In der Prozessdomäne der Organisation wäre das Datenschutzmanagementsystem innerhalb einer Organisation zu verorten. Und in der Prozessdomäne der gesellschaftlichen Organisations-Infrastruktur zur Gesamtregulierung des „Datenschutzes" eines Rechtsstaates sind zuvorderst, neben den gesetzlichen Regelungen, insbesondere die Techniken und Methoden zur effektiven Durchführung von Aufsichts- und Prüfungstätigkeiten sowie Datenschutz-Audits und Forschungsprojekte zum Datenschutz anzuführen. Hier liegen die Infrastrukturgestaltungsaufgaben des Staates.

Am Beispiel von AAL dargestellt zeigt sich die Funktionalität einer solchen kompakten Anordnung der Daten, Prozesse und Schutzziele. Die Gesamtansicht führte dazu, dass erstens die Beteiligten ihre Rolle bei der Gestaltung ihrer Systeme fanden, indem sie sich primär gegen andere Rollen und Verantwortlichkeiten abgrenzen konnten. Und zweitens entwickelten sie konkrete Vorstellungen, welche spezifischen Anforderungen der Datenschutz, auch im Unterschied zu den Anforderungen der Datensicherheit, an sie in ihrer gefundenen Rolle – als Hersteller, als Betreiber, als Vertreter von Betroffenen – gestellt wurden. Wir trafen mehrfach auf Verantwortliche, denen an einem in die Systeme eingebauten Datenschutz deshalb gelegen war, weil sie davon überzeugt waren, dass ohne Datenschutz die Betroffenen kein Vertrauen in die Überwachungssysteme entwickeln werden, selbst wenn sie tatsächlich freiwillig und informiert in deren Betrieb eingewilligt haben. Trotz eines derart ausgewiesenen Bemühens sah sich niemand in der Lage, datenschutzrechtliche Anforderungen umzusetzen. Hinzu kam der häufig zu hörende Vorwurf, dass sie Datenschutzbehörden ausgeliefert seien, deren Entscheidungen sie vielfach als intransparent, nicht nachvollziehbar und deshalb letztendlich als willkürlich empfanden. Die Arbeit von Datenschutzbehörden hat sich an ihren eigenen Kriterien, wie sie in den Schutzzielen zum Ausdruck kommen, messen zu lassen.

5 Fazit

Der generische Datenschutzwürfel stellt a) den Schutzbedarf von Daten und IT-Systemen; b) von vermessenen Prozessen, Rechtsbeziehungen und Verantwortlichkeiten; sowie c) von rechtlich zunächst abzuwägenden Schutzzielen und den daraus dann abzuleitenden Schutzmaßnahmen in eine untereinander kontrollierbare Beziehung vor Augen. Mit den Schutzzielen sind Vorgaben formuliert, die mit den jeweiligen Fachlogiken und Fachinstrumenten der Juristen, Techniker, Organisatoren oder Betriebswirte für Systemplanungen oder Systemprüfungen aufeinander abgestimmt umsetzbar sind. Am Würfel lässt sich zeigen, dass im Zentrum der Betrachtungen das Datenschutzmanagement der Organisationen steht, das den Anforderungen sowohl des nutzerkontrollierten Identitätenmanagement als auch der externen Datenschutzaufsicht genügen muss.

8 Vgl. Pfitzmann, Andreas, 2006: Multilateral Security: Enabling Technologies and Their Evaluation; in: G. Müller (Hrsg.): Emerging Trends in Information and Communication Security , LNCS 3995, Springer-Verlag, Berlin/Heidelberg: 1-13.

9 Vgl. Meints, Martin / Zwingelberg, Harald, 2009: Identity Management Systems – recent developments; http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf.