Martin Rost, Kirsten Bock

Privacy By Design und die Neuen Schutzziele

Grundsätze, Ziele und Anforderungen

„Privacy by Design" versammelt sieben Grundsätze, die einen modernen proaktiven Datenschutz mit weltweiter Perspektive versprechen. Die „Neuen Schutzziele" beanspruchen die Operationalisierbarkeit eines modernen, proaktiven Datenschutzes anhand sechs elementarer Schutzziele, die systematisch aufeinander bezogen sind und universell gelten sollen. Während Privacy by Design von den zehn auf Praxis zielenden Anforderungen der Global Privacy Standards ergänzt wird, fügen sich die Neuen Schutzziele in die bewährte Methodik der Risikoanalysen und Schutzmaßnahmen nach BSI ein. Beide Paradigmen setzen auf Privacy-Enhancing-Technologies. Die Autoren argumentieren für eine Zusammenführung der Ansätze zu einem umfassenden Gesamtkonzept.

1 Einleitung

Privacy by Design (PbD) und die Global Privacy Standards (GPS)[1] sind spätestens seit der *Madrider Erklärung*[2] zu einem breit akzeptierten Bestandteil der europäischen Datenschutzbestrebungen, insbesondere durch die Aktivitäten der Artikel 29-Datenschutzgruppe, geworden.[3] Ann Cavoukian, Datenschutzbeauftragte der kanadischen Provinz Ontario, gilt seit Jahren als die treibende Kraft hinter PbD.[4] Sie weist PbD als eine Art Sediment der weltweit gemachten Erfahrungen mit bislang vereinzelten Strategien und Paradigmen für einen wirkungsvollen Datenschutz aus. PbD sei ein Versuch, den eher ingenieurswissenschaftlichen Arbeiten und Techniken, die im Rahmen von Privacy Enhancing Technologies (PETs) entwickelt wurden, ein Prozesse betonendes Rahmenwerk und deren wesentliche Komponenten zur Seite zu stellen.

Schutzziele und Schutzmaßnahmen zählen seit Jahren zum bewährten Instrumentarium der Datensicherheit. Einige Landesdatenschutzgesetze sowie die Europäische Datenschutzrichtlinie kennen bereits Schutzziele, die auch über reine Sicherheitsaspekte hinausgehen. Die Neuen Schutzziele (Data-Protection Goals, DPG) schließen an diesen Standards an und sind das Ergebnis theoretischer Überlegungen zu deren innerer Systematik[5]. Eingeflossen sind zudem praktische Erfahrungen mit Kriterienkatalogen für Beratungen von großen IT-Projekten, Prüfungen und Auditierungen.[6] Die Neuen Schutzziele wurden von einer Unterarbeitsgruppe des AK-Technik der Datenschutzbeauftragten der Länder und des Bundes auf die spezifischen Anforderungen des Datenschutzes zugespitzt.[7] Sie bildeten die konzeptionelle Grundlage für die Entschließung der DSB-Konferenz vom März 2010, in der als erste Forderung die Aufnahme

Kirsten Bock

leitet das Referat EuroPriSe – Europäisches Datenschutz Gütesiegel beim Unabhängigen Landeszentrum für Datenschutz (ULD) in Kiel.
E-Mail: kbock@datenschutzzentrum.de

Martin Rost

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

1 The 7 Foundational Principles – Implemen- tation and Mapping of Fair Information Practices – http://www.privacybydesign.ca/content/uploads/2010/05/pbd-implement-7found-principles.pdf.

2 „Globale Datenschutz Standards für eine globale Welt" – Erklärung der Zivilgesellschaft, Madrid, Spanien, 3. November 2009 – http://thepublicvoice.org/madrid-declaration/ german/

3 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp170_de.pdf

4 Ann Cavoukian, Commissioner@ipc.on.ca Information and Privacy Commissioner of Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario, Canada, M4W 1A8, info@ipc.on.ca

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

6 Schleswig-holsteinisches Gütesiegel und Europäisches Datenschutzgütesiegel EuroPriSe

7 Die sechs elementaren Schutzziele sind Bestandteil sowohl des Entwurfs des neuen Landesdatenschutzgesetzes in Schleswig-Holstein als auch des bislang unveröffentlichten Entwurfs der ISO29101 – Privacy Reference Architecture, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45124

von Schutzzielen in ein novelliertes Bundesdatenschutzgesetz formuliert wird.[8]

2 Privacy by Design

Der 1. Grundsatz **Proactive not Reactive; Preventative not Remedial** betont die Notwendigkeit eines proaktiv auch beratenden, im Unterschied zu einem bloß reaktiv sanktionierenden Datenschutz. Dieser Grundsatz beinhaltet die Aufforderung insbesondere an Datenschutzbeauftragte, sich bereits an der Planungsphase von neuen IT-Projekten, ob in der eigenen Organisation oder im Rahmen von IT-Projekten in der öffentlichen Verwaltung, einzubringen. Der 2. Grundsatz **Privacy as Default** betont den maximal erreichbaren Grad von Privatssphäre, der dann gegeben ist, wenn in jedem System in der Standardeinstellung zunächst einmal keinerlei personenbezogene Daten verarbeitet werden (dürfen). Wenn eine Person von sich aus nicht agiert, soll sie sicher davon ausgehen können, dass ihre Privatsphäre intakt ist und bleibt. Der 3. Grundsatz **Privacy Embedded into Design** betont, dass der Schutz der Privatssphäre in die Systeme ganzheitlich und integrativ eingebaut sein muss, ohne deren Funktionalität zu beeinträchtigen. Ganzheitlichkeit zielt darauf ab, dass in den Systemen von vornherein verschiedene Kontexte berücksichtigt und darüber hinaus auch alle Interessen der Beteiligten integriert sind. Der 4. Grundsatz **Full Functionality – Positive Sum, not Zero-Sum** soll ermutigen, dass es durch Abstimmung aller Interessen zu einer Win-Win-Situationen kommen und Mehrsummengewinne eingestrichen werden können. Es wird empfohlen, sich dabei auch von falschen Dichotomien, wie bspw. der zwischen Datensicherheit und Privatsphärenschutz, zu verabschieden. Der 5. Grundsatz **End-to-End-Security -- Lifecycle Protection** betont die Angewiesenheit des Privatsphärenschutzes auf die Mechanismen zur Herstellung von Datensicherheit. Auf der Prozessebene bedeutet dies, dass die Prozesse der Datenverarbeitung immer von Anfang bis Ende zu betrachten sind. In diesem Sinne meint Ende-zu-Ende-Sicherheit nicht nur ein Ende-zu-Ende-Verschlüsseln und Signieren, sondern umfasst den gesamten „Lebenszyklus" eines IT-Prozesses. Der 6. Grundsatz **Visibility and Transparency** stellt auf die Notwendigkeit der Prüfbarkeit von Systemen und Prozessen der Verarbeitung personenbezogener Daten ab. Transparenz mit Blick auf die Prozesse und technischen Systeme in den Organisationen ist eine Voraussetzung für jede Prüfbarkeit bzw. Prüffähigkeit. Der 7. Grundsatz lautet **Respect for User Privacy**. Dieser Grundsatz bildet den Abschluss der Auflistung der Grundsätze, und zugleich den Anfang von allem, was im Zentrum der Bemühungen von PbD stehen soll. Aber dieser Grundsatz ist nicht nur Appell, sondern hat wiederum eine operative Seite und den Anspruch, dass Techniken nutzerzentriert funktionieren sollen.

2.1 Global Privacy Standards

Die 1. GPS-Anforderung **Consent** zielt auf die übereinstimmende Einwilligung als Voraussetzung für die Sammlung und Nutzung von Daten. Die 2. Anforderung **Accountability** betrifft die Aspekte der Verantwortung, Zurechenbarkeit und Haftung für Prozesse der Datenverarbeitung personenbezogener Daten. Die 3. Anforderung **Purposes** stellt auf die Zweckbindung, die Anforderung 4 **Collection Limitation** auf Mechanismen der Datensparsamkeit und die Erforderlichkeit ab, wonach die Sammlung von Daten fair, rechtskonform und begrenzt zu geschehen hat. Die knappen Ausführungen zu Anforderung 5 **Use, Retention, and Disclosure Limitation** stellen Anforderungen bzgl. der Nutzung, Speicherung und Weitergabe von Daten. Anforderung 6 **Accuracy** zielt auf die Korrektheit von Daten entsprechend dem Verarbeitungszweck. Die Anforderung 7 **Security** versammelt Anforderungen der Datensicherheit gemäß internationalen Standards. Die Anforderung 8 **Openness** steht für die Operationalisierung von Transparenz als Voraussetzung für Zurechenbarkeit und Verantwortbarkeit von Datenverarbeitung. Gefordert wird, dass interessierte Personen Informationen über die Leitlinien und Arbeitspraktiken in Bezug auf den IT-Betrieb erhalten. Die Anforderung 9 **Access** verlangt, dass Personen Zugriff auf ihre Daten bekommen und über deren Verwendung informiert werden. Die Personen sollen in der Lage sein, selbsttätig die Korrektheit ihrer Daten bestätigen oder bestreiten zu können. Und letztlich fordert die Anforderung 10 **Compliance** von Organisationen, dass sie die notwendigen Schritte unternehmen, um ihre Prozesse, Leitlinien und Grundsätze bezüglich Schutz der Privatsphäre zu überwachen und zu bewerten.

2.2 Diskussion PbD / GPS

Geht man die Grundsätze und Anforderungen durch, so gibt es nur wenige Überraschungen: Proaktiver Datenschutz ist bei vielen Datenschutzbeauftragten in Deutschland seit nunmehr mindestens zehn Jahren wenn nicht geübte so doch angestrebte Praxis. Privacy by Default ist eine aus der Datensicherheit bekannte klassische „Firewall-Strategie" (man schließt zunächst alle Ports und öffnet dann nur die, die man wirklich braucht). In Bezug auf marktwirtschaftliche Realitäten als auch auf das Verhältnis staatlicher Verwaltung und Bürger ist dies jedoch eine unrealistische Maximal-Vorstellung[9], die den Unterschied zwischen dem nordamerikanischen Verständnis von Privacy als „Abwehrformel" (Spiros Simitis) und der europäischen Datenschutz-Auffassung des Gestaltens von ohnehin notwendiger Kommunikation zeigt, auch unter Berücksichtigung der erstrangigen Stellung der Einwilligung im Rahmen von Fair-Practises im PbD/GPS-Konzept. Der Grundsatz des in Technik eingebauten Datenschutzes ist der paradigmatische Kern der Privacy-Enhancing-Technologies (PETs), deren Konzeptionen und Herstellung in Deutschland und der EU ebenfalls seit nunmehr gut zehn Jahren bekannt ist. Der 4. Grundsatz verspricht die Aussicht auf ein Mehrsummenspiel, wenn Organisationen Datenschutz beherzigen. Der ökonomische Beweis, dass sich Datenschutz rechnet, zeigt die stetig steigende Zahl von Datenschutz-Audits in den letzten Jahren, nicht nur in Deutschland. Mit dem Grundsatz der Ende-zu-Ende-Sicherheit ist weniger eine klassische Sicherheits-Maßnahme zu verstehen, sondern die sehr berechtigte Aufforderung an Systemdesigner, dass bei Verfahren mit der Initiierung immer auch die Terminierung in den Blick zu nehmen ist.

Zwischenfazit: PbD lässt sich als „PETs plus datenschutzfördernde Prozesse" verstehen. Das sind keine neuen Komponenten, aber das ist State of the Art eines modernen Verständnisses, welche Kompo-

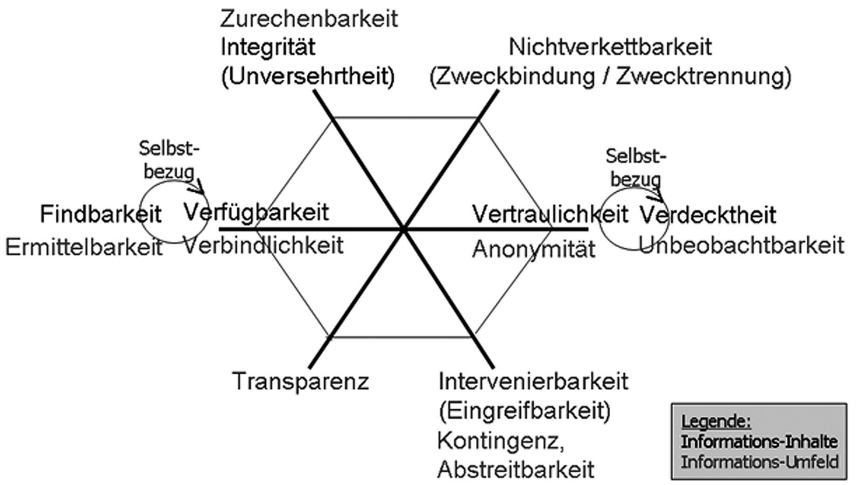
8 http://www.datenschutz-berlin.de/.../665/ DSB_Konferenz_Entschliessungen.pdf

9 Albers, Marion, 2010: Grundrechtsschutz der Privatheit; in: Deutsches Verwaltungsblatt, Heft 17, 2010: 1068

nenten ein wirkungsvoller Datenschutz umfassen sollte. Deshalb sollte den PbD-Grundsätzen auch in Deutschland und Europa mehr Aufmerksamkeit zukommen und diese in bereits vorhandene Konzepte integriert werden. Der Mehrwert von PbD besteht aus unserer Sicht zum einen darin zu (er)klären, dass Datenschutz und Privatheit „gesellschaftliche" Projekte sind, die sich weder in Datenschutzrecht noch in Datensicherheitstechnik aufteilen oder darin auflösen lassen. Recht und Technik reagieren auf vorgängige, latente Konflikte der Gesellschaftsstruktur. Viele auch professionelle Datenschützer haben diesen, dem Recht vorgängigen Aspekt des Datenschutzprojekts, aus dem Auge verloren, wenn sie jede weitere Aktivität einstellen, und dies für einen professionellen Habitus halten, sobald ihnen allein eine Rechtsgrundlage präsentiert wird, aber materiell das Problem fortbesteht. Und zweitens versammelt PbD weltweit zustimmungsfähig aufeinander abgestimmt die unverzichtbaren Komponenten für einen wirkungsvollen Datenschutz über Grenzen hinweg und in der Weltgesellschaft.[10]

Zu einem relevanten Resümee zum „Privacy by Design"-Ansatz[11] kommt Simon Davies (London School auf Economics & Privacy International). Davies stellt PbD in eine gewisse evolutionäre Entwicklungslogik entlang der Datenschutzherausforderungen seit Beginn der 70er Jahre. Unter anderem verweist er darauf, dass „Privacy by Design" auf die Provokation des „Surveillance by Design" reagiert, das 1994 im Rahmen von „Communications Assistance for Law Enforcement ACT (CALEA)" thematisiert wurde. Davies stellt fest, dass die Intentionen von PbD bis in die 90er Jahre zurückreichen und bereits tief in den Konzepten von Verschlüsselungstechniken oder auch PETs verankert waren bzw. sind und listet entsprechende Techniken auf, die den Grundsätzen von PbD folgen. Davies Fazit lautet: PbD entspricht mehr einer Einigung bezüglich der Herausforderungen an den Datenschutz als einer Einigung auf die dafür anzustrebenden technischen Lösungen. PbD biete zwar eine signifikante Schnittmenge zwischen den beiden Domänen, der regulativen und der ingenieurstechnischen, und die Grundsätze seien auch motivierend, passen aber eher in den regulativen Horizont. Sie böten zu wenig technische Substanz und zu wenig Ankopplungspunkte auch für ökonomische Interessen. Die sieben Grundsätze seien motivierend und inspirierend, zeigten aber nicht das Potential für alle Interessenten auf.[12] Technisch umsetzbare Grundsätze müssen spezifischer zugeschnitten sein. An diesem von Davies herausgehobenen kritischen Punkt setzen, so denken wir, die Neuen Schutzziele an.

Abb. 1 | Tableau der Schutzziele



3 Die Neuen Schutzziele

Die Arbeit mit Schutzzielen ist den meisten IT-Verantwortlichen vertraut: Seit vielen Jahren schon werden Schutzziele in Katalogen gelistet, deren Reichweite kommentiert und schließlich mit Maßnahmen zu deren Erreichen hinterlegt. Die Arbeit mit ihnen hat sich bewährt. Sie sind so formuliert, dass sie die Anforderungen an technische und organisatorische Systeme sowohl abstrakt überblickbar als auch in Form von Maßnahmen hinreichend konkret fassbar machen.

Die „klassischen" Schutzziele der Datensicherheit, nämlich **Verfügbarkeit, Integrität und Vertraulichkeit,** fokussieren primär solche Anforderungen, die an eine sichere Aufrechterhaltung des Betriebs und der Infrastruktur einer Organisation zu stellen sind. Dagegen spezifiziert Datenschutz diese fokussierten Erfordernisse an organisierte Datensicherheit primär aus der Perspektive der personenbezogenen Daten betroffener Menschen (genauer: Bürger, Kunden und Nutzer, Patienten) und reichert diese Perspektive außerdem mit weiteren spezifischen Anforderungen an, die sich aus den übergeordneten Grundrechten von Menschen ergeben. Die spezifischen Anforderungen lassen sich ebenfalls als Schutzziele formulieren. Die spezifischen Datenschutz-Schutzziele sind **Transparenz** – als Voraussetzung für die Steuerung und Regulation technisch-organisatorischer Prozesse sowie für Abwägungen bezüglich des Zwecks der Datenverarbeitung, der Erforderlichkeit, der Datensparsamkeit, des Informationsbedarfs der Betroffenen usw. – **Nichtverkettbarkeit** – als Operationalisierung von Zweckbindung/Zwecktrennung sowie der Erforderlichkeit – und **Intervenierbarkeit** – als Operationalisierung insbesondere von Betroffenenrechten und der Fähigkeit der informationsverarbeitenden Stellen bzw. Betreibern von Systemen, dass diese nachweislich tatsächlich ihre Systeme steuernd beherrschen. Und nicht von den System beherrscht werden. Diese sechs Schutzziele sind mit Schutzmaßnahmen hinterlegt.

Die Maßnahmen für die drei klassischen Schutzziele der Datensicherheit sind bekannt. Um Verfügbarkeit sicherzustellen, erhöht man die Redundanz verfügbarer Systeme oder hält ausgeklügelte Fallback- und/oder Reparaturstrategien vor.

10 Rundle/Glueck haben 10 „Data Protection Principles" aus weltweiten Quellen kondensiert (u.a. APEC, OECD, FTC, EU-Directive), die ebenfalls einer näheren Betrachtung unterzogen werden sollten. http://www.microsoft.com/mscorp/ twc/endtoend-trust/vision/lop.aspx

11 Davies, Simon, 2010: Why Privacy by Design is the next crucial step for privacy protection – A disccussion paper, (Stand: 2010-10-27) http://www.i-comp.org/blog/wp-content/uploads/ 2010/10/ privacy-by-design.pdf

12 vgl Davies 2010: 4

Integritätssicherungen bedeuten in der Regel gut organisierte Hashwert-Checks. Und Vertraulichkeit von Datenbeständen oder Kommunikationen stellt man durch Abschottungen und insbesondere Verschlüsselungstechniken her. Diese Maßnahmen sind dann, in Bezug auf Datenschutz-Anforderungen, in vielen Fällen näher zu spezifizieren. Ebenso bekannt – und in einem gewissen Rahmen vorbildlich auch für eine systematische Bearbeitung von Datenschutzrisiken – sind die Systematik und Methoden zur Modellierung von Systemen zur Schutzbedarfsfeststellung der Daten (die sich dann auf die Systeme vererben) sowie zur Risikoanalyse und Risikobearbeitung. In diese Methodik können dann auch die spezifischen Schutzmaßnahmen des Datenschutzes eingepasst werden.

3.1 Schutzmaßnahmen

Das Schutzziel **Transparenz**, das mehr als nur „Prüfbarkeit" meint, ist mit solchen Maßnahmen herzustellen, die gewährleisten, dass die Erhebung und Verarbeitung von Daten in Verfahren und deren Nutzung mit zumutbarem Aufwand geplant, nachvollzogen, überprüft und bewertet werden können. Das Maßnahmenbündel umfasst in diesem Sinne ein methodisches *Projektmanagement*, einschließlich stufenweiser Tests- und Freigaben; die *Dokumentation* der IT-Infrastruktur eines Verfahrens, der Daten und der Datenflüsse, der Sicherheitsmaßnahmen der die *Unterrichtung* von Betroffenen, unter Umständen Publikation eines „Datenbriefs". Die in einem Verfahren beteiligten Entitäten, Daten und Operationen sind in ihrem Zusammenspiel auch über rechtliche Grenzen hinweg zu planen, im Sinne eines Monitorings zu überwachen und zwecks Analysier- und Nachweisbarkeit zu protokollieren. Es sollte ein Quickfreeze einer Datenverarbeitung (gesamtverfahrens- oder einzelfallbezogen) möglich sein, um jederzeit einen Systemzustand feststellen zu können.

Das Schutzziel **Nichtverkettbarkeit** soll die Zweckbindung und Zwecktrennung von Verfahren operationalisieren. Die Zweckbindung eines Verfahrens setzt immer auch die Kenntnis thematisch verwandter Verfahren voraus, gegen die ein herausgehobener Zweck abzugrenzen ist, um die Logik und Erforderlichkeit einer Verkettung von Daten oder Subverfahren unter einem spezifischen Zweck bestimmen und festlegen zu können. Nichtverkettbarkeit ist durch solche Maßnahmen umzusetzen, mit denen die Daten des Verfahrens nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. Das Maßnahmenbündel zur Umsetzung dieses Zieles umfasst vor allem Rollen- und Strukturkonzepte. Das bedeutet im Einzelnen zumindest angemessene *Funktions- und Rollentrennungen* zwischen und innerhalb von Organisationen mit Verantwortungszuweisungen an kompetente Belegschaftsangehörige; eine kontrollierte *Konzeption*, Implementierung, Konfiguration, Betriebnahme und Außerbetriebnahme, mit Tests und Simulationen in den jeweiligen Phasen, nach Best-Practice Gesichtspunkten; den Einsatz von *Techniken loser Kopplungen* oder eng zugeschnittener Dienste (Metadirectory, Federation-Services, Service-orientierte Architekturen etc.); das *Steuern von regulierten Prozessen* des Erhebens, Nutzens, Löschens von Daten mit Techniken jeweils auf dem aktuellen Stand.

Das Schutzziel **Intervenierbarkeit** ist mit Maßnahmen umsetzbar, die dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. Das bedingt letztlich einen operativen Zugriff auf Verfahren und Daten. Das kann im Einzelnen zumindest die Einrichtung eines SPOC (Single-Point-Of-Contact) für Betroffene zur Adressierung einer Intervention mit Verfolgbarkeitsoption bedeuten. Betroffene müssen auf Daten und laufende Verfahren zugreifen können und diese müssen entsprechend einsehbar, änderbar, korrigierbar, sperrbar und löschbar ausgelegt sein. Im Sinne der Transparenz wäre es dann beispielsweise wesentlich, dass dem Betroffenen nachgewiesen werden kann, dass das von ihm initiierte Löschen von Daten sich auch tatsächlich auf sämtliche Generationen von Kopien und Backups erstreckt hat. Im IT-Design müssen Prozesse dafür fallbezogen eingerichtet bzw. separiert sein, damit sich Interventionen oder „Systemstörungen" nicht systemweit auswirken, trotzdem aber zumindest Teile aus der Produktion rausgenommen werden können. Sinnvoll sind ferner feingranulare statt pauschale Einwilligungen aus Verfahren heraus sowie zeitliche Beschränkungen erteilter Einwilligungen. Wünschenswert wäre, weil konsequent fortgedacht, der Einsatz von *Personal Agents innerhalb einer Organisations-IT,* die die Verfahren mit Personenbezug aus der Interessenslage der davon betroffenen Personen überwachen und über entsprechende Benachrichtungs- und Einwirkungswerkzeuge verfügen. Es obläge externen unabhängigen Prüfinstanzen, solche Agents darauf zu überprüfen, dass diese den gesetzlichen Vorschriften genügen und die Interessen der Nutzer und Organisationen in einem ausgewogenen Verhältnis berücksichtigen.

Aus den sechs elementaren Schutzzielen lassen sich weitere ableiten, die in dem Tableau der Schutzziele ersichtlich sind, aber an dieser Stelle nicht weiter ausgeführt werden können.

Die Grundsätze, die die Schutzziele operationalisieren, sind im Wesentlichen zwei: 1. Sie operationalisieren die allgemein gesellschaftlich bestehende Anforderung, dass Systembetreiber in der Lage sein müssen – und dies auch nachweisen können müssen-, dass sie ihre Systeme, als Teile einer gesellschaftlichen Infrastruktur, *beherrschen*. 2. Sie operationalisieren die Anforderung an ein Systemdesign, das für alle Beteiligte *fair* nutzbar sein soll. Die Umsetzung beider Grundsätze ist eine Voraussetzung dafür, dass alle Akteure vernünftigerweise in das korrekte Funktionieren beherrschter Systemen bzw. in die Fairness gesellschaftsweit implementierter Infrastrukturen vertrauen dürfen. Vertrauenswürdigkeit macht Kommunikation schnell. Dies ist eine wesentliche Eigenschaft moderner Gesellschaften. Der Nachweis der Beherrschbarkeit von Systemen ist, im Unterschied zum Fair-Practice ein Aspekt, der bei PbD bislang keine herausgehobene Rolle spielte, sich aber logisch daraus ergibt.

Mit diesen sechs elementaren Zielen lassen sich Anforderungen für Prozesse formulieren, die für drei unterschiedliche Domänen zu konzipieren sind und bei denen verschiedenen Typen von PETs aufeinander abgestimmt zum Einsatz kommen können.

4 Drei Prozessdomänen

Die wesentliche konzeptionelle Idee, die hinter dem Konzept der Datenschutz-Prozessdomänen steckt, läuft zunächst darauf hinaus, dass jede gesellschaftlich relevante Kommunikation, die insbesondere zwischen Organisationen und Personen stattfindet, ausschließlich in technisierter Form, also typischerweise auf

der Basis von Computern (Smartphones) und Internet geschieht. Wenn ubiquitäres Computing Realität wird – und im Internet ist diese bereits Realität -, dann sollte diese Realität, die bislang Organisationen gegenüber Personen einen operativen Vorteil verschafft, auch zum Vorteil der Nutzer angewendet werden können. Für eine durchtechnisierte, datenschutzfreundliche Kommunikationsinfrastruktur sind mindestens drei Komponenten erforderlich, die wir zu den operativen Bestandteilen der Prozess-Domänen zählen: Ein Programm, dessen Aktivitäten ausschließlich der Hoheit des Nutzers im Sinne eines persönlichen „Identity-Protectors" (John Borking) unterliegen, sowie ein IT-gestütztes *Datenschutz-Management* für Organisationen, das sowohl das *nutzerkontrollierte Identitätenmanagement Typ3*[13] als auch die Interessen einer Organisation bedient. Und diese beiden Prozess-Domänen, einmal kontrolliert vom Nutzer einmal kontrolliert von einer Organisation, setzen dann auf einer dritten Prozessdomäne, nämlich der basalen *gesellschaftlichen Informationsverarbeitungs- und Kommunikationsinfrastruktur* auf, für die das Internet mit dessen Services paradigmatisch steht. Von dieser Infrastruktur ist dann in einer Analogie zu Verkehrsstraßen zu fordern, dass diese gesellschaftsweit neutral jeder und jedem, ohne eingebaute Machtasymmetrie zugunsten von Organisationen, zur Verfügung steht, als operative Voraussetzung für faire Marktbedingungen, wirksame Rechtsstaatlichkeit und offene Wahrheits-Diskurse.

Das **nutzerkontrollierte Identitätenmanagement** (user-controlled Identitymanagement – ucIM) basiert bekanntlich im Wesentlichen darauf, mit Hilfe eines Programms eine differenzierte Nutzung verschiedener Pseudonymtypen[14] – die vom nur einmal verwendbaren Transaktionspseudonym, über anonyme Credentials und nichtverkettbare Pseudonyme des „Neuen Personalausweises", über Rollen- und Beziehungspseudonyme bis zum Personenpseudonym reichen – zu unterstützen, die das Verkettungsrisiko zwischen verschiedenen Nutzeraktivitäten durch Organisationen so gering wie möglich halten. Voraussetzung für eine wirklich wirksame Nutzung von Pseudonymen im Internet ist allerdings, dass die genutzte Kommunikationsinfrastruktur zunächst anonyme Kommunikationsbeziehungen zulässt. Entscheidend ist, dass der Nutzer, im Sinne des Schutzziels Intervenierbarkeit, die Kontrolle über die Preisgabe der Zuordnungsregel zwischen Pseudonym und den Echtdaten seiner Person innehat. Darüber hinaus sollte eine Applikation für Identitätenmanagement ggfs. Personal Agents steuern können sowie über ein Einwilligungsmanagement im Rahmen bestehender Kommunikationsbeziehungen verfügen.

Im Bereich des **organisationsinternen Datenschutzmanagements** hat sich seit 2007, im Windschatten der ISO27001 (Informationssicherheitsmanagementsystem) und des ITIL-Paradigmas (zur Koordination der Schnittstelle von Organisation und Technik) und deren Standardprozesse einiges getan. Datenschutz wird hierbei auf alle standardisierten Prozesse bezogen. Und man findet zunehmend erste Versuche, Vorfälle im Rahmen des Incident-, Problem- und Changemanagements nicht nur in Bezug auf Sicherheit sondern auch auf Datenschutz hin zu taxieren und zu behandeln. Auch hier erweisen sich die Neuen Schutzziele als überaus nützlich. Wichtig wäre, dem nutzerkontrollierten Identitätenmanagement einen Anker auf der Organisationsseite im Sinne eines „enterprise-controlled-Identity-Management" (ecIM) zu bieten. Solche Entwicklungen finden in Deutschland aktuell faktisch beiläufig im Rahmen der Anpassungen von Workflows an die Bedingungen, die im Zuge der Zuteilung von Berechtigungszertifikaten für den Zugriff auf die EID-Funktionen des „Neuen Personalausweises" durch Organisationen zu erfüllen sind, statt. Es zeigt sich, dass es in vielen Fällen der Interaktion von Organisationen und Personen vollkommen ausreicht, dass Personen sich mit einem Pseudonym authentifizieren und eine Vollidentifikation erst bei einigen hoheitlichen Konstellationen sowie beim Bestehen eines kreditorischen Risikos auf Seiten eines Unternehmens nötig wird. Ein wesentliches Element des Datenschutzmanagements besteht darin, dass dieses, wie sämtliche anderen Prozesse einer Organisation auch, letztlich vom Management kontrolliert, reguliert und gesteuert erfolgt. Das hat z.B. für Prozesse mit Datenschutz-Schutzmaßnahmen zur Folge, dass zur Steigerung der Transparenz und Intervenierbarkeit sog. Key Performance Indicators (kpi) oder besser noch, Key Risk Indicators (kri)[15] zu bilden sind. In diesem Rahmen wäre eine auch maschinelle Unterstützung nicht nur wünschenswert sondern unumgänglich. Es gilt zu prüfen, ob eine Renaissance der Automatisierungs-Ansätze, wie sie zum ersten Mal nachdrücklich mit P3P[16] (im Rahmen des ucIM/ecIM) und EPAL[17] (im Rahmen des organisationsinternen Datenschutzmanagements) verfolgt wurden, infrage kommt.

Die gesellschaftliche Datenschutzinfrastruktur, in der die anderen beiden Prozessdomänen eingebettet sind, umfasst die gesellschaftsweite Anreiz-, Sanktions-, politische und wissenschaftliche Diskurs- und Reflexions-Infrastruktur. Das Instrument der freiwilligen externen Auditierung von Unternehmen und Dienstleistungen zählt dabei zur Anreiz-Struktur, mit der Marktteilnehmer weltweit insbesondere ihrer Konkurrenz signalisieren können, dass sie Produkte und Verfahren anbieten, die einen überdurchschnittlichen Datenschutz bieten. Die Schutzziele sind dabei sowohl auf den Auditierungsprozess selber zu beziehen – der seinerseits insbesondere den Anforderungen an Transparenz (durch offen zugängliche Kriterienkataloge und Ergebnisprotokolle), Integrität (Fachkunde, finanzielle Unabhängigkeit und Unparteilichkeit der Zertifizierungsstelle) und Zweckbestimmtheit (Compliance plus) zu erfüllen hat – als auch darauf, dass die Schutzziele und deren Maßnahmen selbstverständlich den wesentlich Bestandteil des Prüfkriterien-Katalogs ausmachen. Die aus Datenschutzsicht zentrale Controlling-Funktion externer Audits besteht darin, dass von den Organisationen finanziell unabhängige Stellen mit Hilfe von fachkundigen Experten die Prozesse von Organisa-

13 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

14 Hansen, Marit / Pfitzmann, Andreas, 2010: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version v0.34 Aug. 10, 2010,http://dud.inf.tu-dresden.de/literatur/Anon_ Terminology_v0.34.pdf.

15 Einen Überblick mit verschiedenen Dokumenten zu den verschiedenen Steuerungsparadigmen und Steuerungsinstrumenten nach CoBIT und ITIL findet sich unter http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

16 http://www.w3.org/TR/P3P/

17 http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

tionen begutachten, deren Datenschutzrisiken von den betroffenen Personen nicht abgeschätzt werden (können) und die zudem die Geschäftsgeheimnisse bzw. Sicherheitsinteressen von Organisationen berühren können.

5 Fazit

Das selbstverständlich prozessorientierte und auf PET zurückgreifende Konzept der „Neuen Schutzziele" nimmt nicht nur die Grundsätze und Anforderungen von Privacy by Design und Global Privacy Standards vollständig auf, sondern behebt auch deren von Simon Davies herausgearbeiteten Schwächen in Bezug auf die Integrationsfähigkeit von regulatorischen, technischen und betriebswirtschaftlichen Anforderungen an ein modernes globales Datenschutz-Konzept. Durch die Neuen Schutzziele gerät, im Zusammenspiel mit modernen Auditierungsinstrumenten, neben der Orientierung an Fairness auch die Beherrschbarkeit (und deren Nachweisbarkeit) von Systemen in den Blick. (Schutz-)Ziele lassen sich von unterschiedlichen Ausgangspunkten anstreben. Und ob sie erreicht wurden, ist anhand vermessener Schutzmaßnahmen dann nicht nur kontrollierbar, sondern mehr noch anhand von kpi/kri messbar! Und dadurch rechtlich, betriebswirtschaftlich und technisch zugänglich. Kontrollierbarkeit ist eine Voraussetzung für den Betrieb spezifischer Datenschutz-Prozesse. Es ist plausibel, die selben Schutzziele dann an drei unterschiedlich zu regelnde Datenschutz-Prozessdomänen anzulegen, die sich in ihrer Controlling-Struktur unterscheiden: a) Nutzerkontrolliertes Identitätenmanagement, b) Datenschutzmanagement einer Organisation entlang von Prozesssteuerung sowie c) die gesellschaftsweite Gesamtdatenschutzinfrastruktur mit ihren Verbreitungsmedien sowie ihren organisierten Beratungs-, Auditierungs- und Prüfungsstrukturen. Mit der Umsetzung der Schutzziele gelingt es, sowohl dem nationalen als auch dem europäischen Datenschutzrecht sowie den globalen Grundsätzen und Anforderungen von PbD/GPS vollumfänglich zu genügen.