Martin Rost, Kirsten Bock

Impact Assessment im Lichte des Standard-Datenschutzmodells

Die bislang vorgestellten Privacy-Impact-Assessments (PIAs) werden den Anforderungen, wie sie vom modernen Datenschutz gestellt werden, nur zu einem geringen Teil gerecht. Sie sind zumeist entweder analytisch und suchend, also im weitesten Sinne wissenschaftlich motiviert und verlieren dadurch den Bezug zum Betroffenenschutz allzu oft aus den Augen. Oder PIAs sind als eine um Vertrauen werbende Marketingstrategie von Herstellern oder politischen Interessensvertretern einzuschätzen. Der Artikel nimmt einen aktuellen Vorschlag zur Ablaufstruktur eines PIA auf und schlägt eine ganze Reihe an konstruktiven Verbesserungen auf der Grundlage des standardisierten Datenschutzmodells (SDM) vor.

Einleitung

Die ersten Konzepte zum „Privacy Impact Assessment" lassen sich auf die Anfänge der Technikfolgenabschätzung der 1970er Jahre zurückführen. Seit etwa Mitte der 1990er Jahre gelten PIAs in Australien, England, Hong Kong, Kanada und USA als etabliert (vgl. Clarke 2011). Ein aktueller Überblick zur internationalen Situation findet sich bei Wright/De Hert (2012). Im deutschsprachigen Raum spielen aktuell insbesondere Beiträge zur Standardisierung (vgl. BSI 2011; DIN/ISO 2012) sowie zur Entwicklung einer praxisgerecht umsetzbaren Methode (Oetzel/Spiekermann 2012) eine sichtbare Rolle.

Analysiert man diese genannten Konzepte anhand des „standardisierten Datenschutzmodells" (Rost 2012), dann sind diese Konzepte und Strategien allerdings durchgängig verbesserungsfähig. Derzeit entsteht der Eindruck, als ob PIAs von der Industrie geradezu als Abwehrinstrumente gegen die Anforderungen seitens der offiziellen Datenschutzaufsicht eingesetzt werden, anstatt diese Anforderungen zu beachten. Ungeklärt ist oft die Unabhängigkeit der Autoren und die Verallgemeinerungsfähigkeit und Relevanz der Modelle, fragwürdig sind darin vor allem die Validität und Reliabilität der genutzten Kriterien, mit denen Datenschutzrisiken operationalisiert und analysiert werden. Zudem wird durchgängig keine Bestimmung des Verhältnisses von operativem Datenschutz und Informationssicherheit vorgenommen. Zwar ist operativer Datenschutz zweifelsfrei auf Maßnahmen der Informationssicherheit angewiesen, aber er erschöpft sich nicht darin. So sind bspw. Maßnahmen zur Pseudonymisierung oder Anonymisierung leicht ersichtlich genuine Schutzmaßnahmen des Datenschutzes. Das berechtigte Bedürfnis nach Systematik und methodischem Halt, den bspw. BSI-Grundschutz bietet, führte in den vergangenen Jahren auch bei Datenschutzbeauftragten dazu, dass unter der Hand die Risikoperspektiven und Sicherheitsinteressen von Organisationen übernommen und methodisch bearbeitet wurden, nicht aber die für den Datenschutz im Zentrum stehenden Risiken für die gesellschaftlichen Strukturen und Personen.[1]

Aus Datenschutzsicht besteht die Erwartung an ein PIA, dass es die Wirkungen transparent macht, die von dem zu beurteilenden Verfahren(sbestandteil) in Bezug auf die Risiken für die informationelle Selbstbestimmung durch die Machtasymmetrie zwischen Organisationen und Personen ausgehen bzw. ausgehen können.

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 (ULD) in Kiel.

E-Mail: martin.rost@datenschutzzentrum.de

1 Allerdings finden sich in einigen Landesdatenschutzgesetzen zumindest Spuren, die eine Durchführung von Assessments nahelegen. So verlangt bspw. das LDSG Schleswig-Holstein der Datenschutzaufsicht die Beratung öffentlicher Stellen im Hinblick auf die „Sozialverträglichkeit" von Verfahren ab (§ 39 Abs. 4 LDSG-SH).

Stand der PIA-Diskussion

Richard Clarke listet Kriterien zur Evaluation von PIA-Guidelines auf (vgl. Clarke 2011: 113). Daran gemessen attestiert er den Guidelines in den USA sowie den meisten kanadischen und australischen Provinzen eine geringe Qualität, u.a. weil diese sich nur auf die rechtliche Prüfung der Compliance zum Datenschutzrecht konzentrierten. Hohe Qualität attestiert er dagegen den Guidelines für Ontario, Alberta, England und der australischen Provinz Victoria, u.a. auch deshalb, weil sie auch Prozesse begutachteten (vgl. Clarke 2011: 118f).

Oetzel/Spiekermann, deren PIA-Prozessmodellierung wir gleich detailliert aufgreifen, verweisen zu Recht darauf, dass es viele unzulängliche Versuche zur Definition von Privacy und deren Operationalisierung gibt (2012), um sich dann trotzdem auf eine Auflistung von Privacy-Risiken bei Solove (2006) zu beziehen.[2]

Sowohl Clarke als auch Oetzel/Spiekermann vermeiden in ihren Ausführungen, einen verpflichtenden Kriterienkatalog zum Ausweis von Privacy-Risiken anzugeben. Das mag folgerichtig für ihre Ansätze sein, ist aber generell misslich, um die Transparenz und Integrität für PIAs einschätzen und Vergleichbarkeit unter ihnen herstellen zu können. Ebenso undefiniert bleiben die heranzuziehenden Kriterien im PIA-Framework seitens der DIN/ISO (vgl. ISO 2012). Das Forschungspapier zu diesem Framework verweist als inhaltliche Kriterien u.a. auf eine Ansammlung von unsystematischen „Prinzipien" und Maßnahmen des noch relativ jungen Privacy-Frameworks der ISO29100, die eine bedeutende Schnittmenge zu den „Global Privacy Standards" als Bestandteil des „Privacy By Design" aufweisen (vgl. Rost/Bock 2011). Darüber hinaus benennt das Papier die existierenden ISO-Standards zum Risk-Management sowie die empirisch orientierten PIAs zu RFID (BSI/ Oetzel/Spiekermann 2011) und zu Finanzsystemen (ISO22307:2008).

Das Referenzieren auf „Prinzipien" und Maßnahmen als Regelungsgrößen halten wir für problematisch. Im gelungenen Fall vermögen abstrakte Prinzipien zwar inkongruente Perspektiven von Stakeholdern zu fokussieren – man einigt sich zumindest darauf, dass es spezifizierbare Probleme gibt – allerdings ohne dass diese Fokussierung mit Umsetzungsdirektiven und der Aufforderung zu verbindlichen Regelungen ausgestattet ist. Und ein Festschreiben eines Maßnahmenbündels in einem Abschnitt über Regelungsgrößen weckt zwangsläufig Zweifel an den Motiven oder methodischen bzw. analytischen Kompetenzen der Autoren.

Das Referenzieren auf Schutzziele ist für Impact-Assessments im Bereich der Informationssicherheit seit Jahrzehnten verbindlich. Neben der Definition von Schutzzielen beinhaltet dieses Konzept einen Katalog sowohl mit Schutzmaßnahmen als auch mit Hinweisen zur methodischen Umsetzung in Organisationen. Für ein PIA bedeutet die Übernahme des Schutzziele-Konzepts, dass auf der Ebene konkreter Referenz-Schutzmaßnahmen ein PIA-Analyst bereits in der Planungsphase in der Lage ist, mögliche Risiken zu spezifizieren und dadurch in Bezug auf Wahrscheinlichkeit und Ausmaß von Auswirkungen abzuwägen und volks- und betriebswirtschaftlich zu kalkulieren.[3]

Diese guten Gründe mögen eine Rolle gespielt haben dafür, dass Oetzel/Spiekermann für ihr Modell das Konzept der Schutzziele, in Anlehnung an BSI-Grundschutz, übernehmen. Außerdem erweitern sie die im englischen Sprachraum etablierte PIA-Methodik um ein plausibles Schrittmodell und versuchen zumindest ansatzweise, auch der Betroffenenperspektive Geltung und operative Wirkung zu verschaffen.

Der Privacy-Impact eines PIA

Aus den Untersuchungen von Clarke lässt sich der Schluß ziehen, dass an PIAs berechtigt unterschiedliche Anforderungen gestellt werden können. Dann macht es allerdings auch Sinn, diese Anforderungen auszuweisen, um ein PIA für ein PIA zu ermöglichen.[4] Dass hier derzeit ein aktuelles Problem besteht, zeigt sich bspw. bereits in der Definition für PIA, wie sie Oetzel/Spiekermann (2012, Kap. 2.1) vorlegen. Ihnen zufolge muss ein PIA-Modell mindestens vier Anforderungen genügen: (1) Zusammenführung einer vorausschauenden Identifikation von Privatheits-Problemen (issues) oder Risiken, bevor Systeme und Programme etabliert oder verändert werden, (2) Einschätzung der Auswirkungen unter breiter ansetzenden Bedingungen als denen der Rechtskonformität, (3) mehr Prozess- als Output-Orientierung sowie (4) Systematizität.

Während wir den Aspekten (2), (3) und (4) ohne Weiteres zustimmen, ist die Bestimmung des ersten Teils problematisch, weil kontextabhängig. Während in einem interessegeleiteten oder wissenschaftlichen Kontext im Grundsatz eine Identifikation von möglichen Risiken offen gehalten sein kann, sind in einem rechtlich orientierten Kontext die Risikodimensionen bereits normativ festgelegt.

Zur Lösung dieses Problems schlagen wir vor, dass als erster Schritt in einem PIA dessen Anspruchstyp explizit gemacht wird. Der ausgewiesene Anspruchstyp steuert dann die Freiheitsgrade sowohl zur Identifikation von Risiken als auch den Grad der erwartbaren Neutralität und Unabhängigkeit der PIA-Autoren.

Eine Explikation des Anspruchstyps eines PIA macht dessen Risiken bzgl. der Transparenz und Integrität für den Leser abschätzbar. Denn es macht einen Unterschied, ob der Autor eines PIA seine Prüfkriterien oder Usecases nach Belieben wählt oder einen festgelegten, öffentlich zugänglichen Katalog übernimmt, der etwa aus dem Datenschutzrecht abgeleitet ist und damit beanspruchen kann, sowohl dem politisch festgestellten, verallgemeinerungsfähigen Willen sowie dem Grundgesetz zu entsprechen. Anstatt vom „Anspruchstyp" sprechen wir nachfolgend von einer „Policy", die sich die Autoren bzw. das PIA einzuhalten verpflichten.

2 Aus dem Umstand, dass a) keine allgemeine Definition von Privacy zur Verfügung steht, wohl aber für Datenschutz, b) Privacy einen aus Datenschutz heraus abgeleiteten Status hat (siehe Fußnote 7), und c) einem PIA eine strukturell-prophylaktische Wirkung zukommen soll, könnte man allein schon zu dem Schluss kommen, dass es angemessener wäre, von einem „data protection impact assessment" (DPIA) zu sprechen. Der Entwurf einer neuen EU-Verordnung sieht ein DPIA vor (siehe Fußnote 5).

3 In den ersten Entwürfen zur ISO29100 waren die sechs elementaren Schutzziele (siehe im weiteren Textverlauf) enthalten, die dann kurz vor Abschluss des mehrstufigen Standardisierungsverfahrens überraschend durch einen Prinzipienkatalog ersetzt wurden.

4 Die Policy eines PIA lässt sich nicht umstandslos aus der Bezeichnung der Organisation ableiten. Ein Institut mit ausgewiesen wissenschaftlichem Anspruch kann ein interessegeleitetes Auftrags-PIA erstellen, das wenig Transparenz gerade bei großen Risiken bringt, während ein Büro mit entschiedener Interessensperspektive durchaus wissenschaftlichen Ansprüchen an ein PIA genügen kann, wenn es Vollständigkeit beansprucht und Methodik und Ergebnisse gezielt dem wissenschaftlichen Diskurs aussetzt.

Drei Policies, deren Bezeichnungen wünschenswerter Weise standardisiert und deren Ausweis dann für ein PIA obligatorisch sein sollte, lassen sich unterscheiden:

(a) **Policy A**: Diese Policy ist einem solchen PIA vorbehalten, dessen Auftraggeber bzw. Autoren dem Anspruch genügen wollen, ein Produkt oder Verfahren in einem bestimmten Kontext in den Blick zu nehmen, ohne dass im Vorhinein ein bestimmtes Set an Kriterienkatalogen und Definitionen sowie Angreifermotive festgelegt sind. Die Autoren können dabei durchaus abhängig vom Auftraggeber agieren. Eine solche Policy kommt den Marketinginteressen insbesondere der Hersteller der zu evaluierenden Produkte entgegen. Diese Policy ist gut mit dem derzeit entwickelten PIA-Framework der ISO kompatibel.

(b) **Policy B**: Diese Policy erhebt den Anspruch, dass zur Evaluation die verallgemeinerbaren Anforderungen des Datenschutzrechts in operationalisierter Form als wesentliche Grundlage herangezogen werden.[5] Ein solches Vorgehen macht vor allem dann Sinn, wenn geplant ist, ein Verfahren oder eine Verfahrenskomponente einzusetzen und deshalb die Compliance mit dem Datenschutzrecht sicherzustellen ist. Als typischer Auftraggeber ist weniger der Hersteller als diejenige Organisation zu vermuten, die das Verfahren verantwortlich nutzen oder stellvertretend für andere evaluieren lassen will. Letzteres ist typisch für die öffentliche Verwaltung, wenn bspw. ein Bundesministerium neue Techniken oder Technikparadigmen wie bspw. „ubiquitäres computing", „cloud computing" oder „social networks" einschätzen muss.

Inhaltlich bietet sich zur Evaluation die Nutzung des „Standard-Datenschutzmodells" (SDM) an, weil es rechtlich verankert ist (vgl. Bock/ Meissner 2012). Dessen Nutzung hat u.a. zur Folge, dass das vollständige Set an Schutzzielen betrachtet wird, mit einem Risikoansatz, der vor allem die Betroffenenperspektive berücksichtigt.

(c) **Policy C**: Diese Policy erhebt den Anspruch, eine Evaluation mit wissenschaftlichem Anspruch durchzuführen. Eingelöst wird ein solcher Anspruch, wenn zumindest der Versuch unternommen wird, die Risiken vollständig, sowohl empirisch verlässlich als auch mit einem hohen prognostischen und spekulativen Anteil theoretisch gestützt und methodisch zu erfassen. Vollständigkeit heißt vor allem, dass neben den Perspektiven des Betroffenen und der Organisation(en) auch die der gesellschaftlichen Risiken zu analysieren und bewerten sind. Das setzt wiederum die Durchführung einer soziologischen Analyse von Datenschutz und Privatheit voraus.[6] Erst auf dieser Grundlage lässt sich theoretisch kontrolliert die gesamte Konfliktstruktur ausweisen, die mit dem Datenschutzrecht geregelt und mit den Schutzmaßnahmen behandelt werden kann.

Das bislang vollständigste Modell zur systematischen Operationalisierung von Privatheits- bzw. Datenschutzrisiken bietet dabei das SDM. Dieses Modell basiert im Wesentlichen auf dem Katalog der elementaren Schutzziele, die mit wissenschaftlicher Perspektive entwickelt wurden und zu denen eine sozialphilosophisch begründete Vollständigkeitsvermutung besteht (vgl. Rost/ Pfitzmann 2009).

Anhand der so vorgegebenen Risikodimensionen ließe sich dann beurteilen, wie mit Hilfe des zu evaluierenden Verfahrens(bestandteils) eine Aushebelung der Gewaltenteilung durch die Exekutive (typisch: Vorratsdatenspeicherung für Sicherheitsbehörden), ein Unterlaufen des Marktes (typisch: durch Bildung von Kartellen, Monopolbestrebungen u.a. mittels aggressiver Kundenbindungssysteme durch Kundenprofile und dem Verhindern der Mitnahme dieser Daten zur Konkurrenz), ein Verhindern einer diskursiven Behandlung von Forschungsergebnissen, die auch große Risiken ausweisen, sowie die Nichtbeachtung der Rechte von Arbeitnehmern möglich oder wahrscheinlich wäre. Im Methodenteil wären das Zustandekommen und die Angemessenheit der Operationalisierung von Privatheit durch das verwendete PIA-Modell zu reflektieren und dem wissenschaftlichen Diskurs auszusetzen.

Im Zusammenhang betrachtet darf von Auftraggebern und Autoren, die unter der Policy A agieren, schlicht nicht erwartet werden, dass sie ein vertrauenswürdiges PIA anstreben, das der Verpflichtung nachkommt, auch ein schlechtes Ergebnis öffentlich auszuweisen. Bei Policy C besteht dagegen zweifelsfrei die Pflicht zur Veröffentlichung gerade dann, wenn hohe Risiken bestehen. Bei Policy B besteht diese Pflicht nicht minder, doch ist grundsätzlich damit zu rechnen, dass PIAs unter Verschluss gehalten werden. Hier wäre deshalb obligatorisch im Vorhinein festzulegen, welche Informationen den Aufsichtsbehörden bzw. der Öffentlichkeit zugänglich zu machen sind.

Die sechs Schritte eines PIA

Nachfolgend werden die sechs Schritte des PIA-Modells von Oetzel/Spiekermann (2012) gemäß Policy B anhand der Ausführungen zum „Standard-Datenschutzmodell" (vgl. Rost 2012) diskutiert.

1) Die Phase des Einstiegs in ein PIA bezeichnen Oetzel/Spiekermann als „**Characterisation of the Application**". Im typischen Audit-Kontext spräche man vom „Target of Evaluation" (ToE).

Oetzel/Spiekermann zählen zur Festlegung des Objektbereichs die Darstellung der Applikation(en) und Systemkomponenten, Rollen, generische Geschäftsprozesse, detailierte Usecases, Flussdiagramme von Daten sowie Kategorien von Daten auf. Aus unserer Sicht sollte ein generisches PIA-Modell nicht auf Applikationen verengt werden. Es empfiehlt sich, „Verfahren" zu untersuchen – im ISO-Forschungspapier zu PIA ist die Rede von „Systemen", was wir für ebenso unzulänglich, weil zu unspezifisch halten. Denn es sind immer Verfahren, nicht nur einzelne Produkte, von denen Datenschutzrisiken ausgehen, sobald sie von Organisationen eingesetzt werden. Zur Konstruktion und Analyse von Risiken, die durch ein Objekt entstehen, müssen deshalb immer auch Annahmen über Prozesse, IT-Systeme und Daten getroffen werden (vgl. Rost 2012: 435f). Das geschieht typischerweise in Form von Szenarien oder Usecase-Betrachtungen. Oftmals müssen auch Annahmen bzgl. der organisatorischen und rechtlichen Struktur, über Rollen und Verantwortlichkeiten, Verträge und Rechtsgrundlagen ausgewiesen werden. Insofern ließe sich kompakt formulieren, dass die Darstellung eines ToE die Beschreibung zunächst der Funktionalität und des Zwecks, in Ab-

5 Grundlegende Anforderungen werden in Art. 33 Abs. 2 Buchstabe a – Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (KOM 2012) 11 formuliert.

6 Dass vor einer rechtlichen Regelung eine soziologische Analyse durchgeführt werden sollte, war der ersten Generation der professionellen Datenschützer, genannt seien Steinmüller, Lutterbeck, Podlech und Simitis, noch geläufig.

grenzung zu anderen denkbaren und verwandten Zwecken, eines Verfahrens verlangt. Anschließend sind die Komponenten eines Verfahrens darzustellen, entweder eine Beschreibung dessen, was in der realen Praxis technisch, organisatorisch und rechtlich bereits der Fall ist oder der Ausweis über die entsprechenden Annahmen einer möglichen Praxis in einem Usecase.

2) Der zweite Schritt eines PIA besteht in der „**Definition of Privacy Targets**". In den Ausführungen zu diesem Punkt zeigt sich, das Oetzel/Spiekermann nicht nur keinen Halt bei den vorgelegten Operationalisierungen von Privacy fanden, sondern trotz der entschiedenen Schutzziel-Orientierung über keine hinreichend operationalisierte Vorstellung von Privacy verfügen. Aber genau an diesem Punkt trägt das Konzept der Schutzziele, das allerdings konzeptionell besser zu Datenschutz als zum Privatheitsschutz passt, besonders gut, weil es die Freiheitsgrade gut begründet verringert.[7]

Ein seriöses Security-Assessment trifft Aussagen bzgl. der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Ein seriös ansetzendes PIA muss zumindest die sechs elementaren Schutzziele des Datenschutzes – Verfügbarkeit, Integrität, Vertraulichkeit sowie Transparenz, Nichtverkettbarkeit und Intervenierbarkeit – heranziehen. Anders als bei der Informationssicherheit müssen diese Schutzziele betrachtet werden, weil sie rechtlich verankert sind (vgl. Bock / Meissner 2012). Wenn ein PIA weniger oder andere Schutzziele verwendet, was bei Policy A legitim wäre, so sollte im Hinblick auf solche LeserInnen, die ungeübt in der Interpretation von PIAs sind, dieses begründet werden.

Die Schutzziele spannen die Dimensionen auf, die die Beobachtbarkeit von relevanten Datenschutzrisiken herstellen und systematische Analysen und letztlich standardisierte und damit vergleichbare Bewertungen ermöglichen (vgl. Rost 2012: 434f).[8] Gemäß SDM ist dabei keines der Schutzziele als prioritär oder als vernachlässigbar auszuweisen. Die Ziele stehen in einem systematischen, bei drei Achsen in einem bestimmt widersprüchlichen Verhältnis zueinander. Diese Widersprüchlichkeit ermöglicht rechtliche Abwägungen direkt im Medium der Schutzziele. So kann bspw. die Anforderung der Verfügbarkeit und zugleich Vertraulichkeit von Daten rechtlich abgewogen und unter normative, technische oder organisatorische Bedingungen gestellt werden. Außerdem müssen für die Beurteilung konkreter Risiken auch die wesentlichen (Referenz-)Maßnahmen jeweils zur Umsetzung der Schutzziele bekannt und ausgewiesen sein. Entweder geschieht dieser Ausweis bereits in diesem Schritt 2 mit, wofür wir plädieren, oder aber es muss der für Schritt 5 vorgesehene Maßnahmenbezug als unmittelbar nächster Schritt vorgezogen nachfolgen.

3) Oetzel/Spiekermann bestimmen den dritten Schritt als „**Evaluation of Degree of Protection Demand for each Privacy Target**". Sie markieren einen Unterschied zwischen dem Schutzbedarf von Privatheit und Informationssicherheit, indem sie die Schutzbedarfsanforderungen nicht nur aus der Perspektive der „verantwortlichen Stelle" formulieren, sondern zumindest auch aus der Perspektive der Betroffenen. Dabei identifizieren sie für die verantwortliche Stelle zwei Schutzanforderungen: Schutz vor a) Auswirkungen auf Reputationsverlust der Organisation und das Produkt („brand") sowie b) finanziellen Verlusten. Der Betroffene braucht zudem Schutz für c) seine soziale Reputation, d) seine finanzielle Situation sowie e) seine Freiheit. Dann unterscheiden sie, gemäß der BSI-Grundschutz-Methodik, normalen (begrenzte, kalkulierbare Schäden), hohen (beträchtliche Schäden) und sehr hohen (verheerende Schäden) Schutzbedarf.

An dieser Stelle bietet das SDM, das sich ebenfalls an BSI-Grundschutz anlehnt, Definitionen des Schutzbedarfs aus der Betroffenenperspektive (vgl. Rost 2012: 436). Während Oetzel/Spiekermann davon auszugehen scheinen, dass sich die beiden Perspektiven von Organisation und Person konfliktlos vereinbaren lassen, bezweifeln wir das. Es ist die Organisation, von der das Risiko ausgeht. Dieses Risiko ist transparent zu machen. Gerade dieses Konfliktverhältnis erzeugt erst Datenschutz-Anforderungen und hat das Datenschutzrecht historisch zur Bearbeitung dieses Konflikts entstehen lassen. Allein den Maßnahmen zur Sicherstellung der Informationssicherheit ist die Tendenz inhärent, Daten auf Vorrat zweckungebunden zu speichern, etwa in Form üppiger Protokolldaten, um bspw. die Organisationsinteressen gegenüber MitarbeiterInnen zu wahren.

4) Der vierte Schritt besteht in der "**Identifaction of Threats for each Privacy Target**". Fokussiert durch das SDM kann die Abgrenzung und Formulierung des Suchraums zur spezifischen Modellierung von Angriffen methodisch zunächst einmal anhand von zwei Dimensionen erfolgen:

a) Das Schutzziele-Set legt die Art der Angriffe durch Organisationen auf Personen nahe, wenn die Schutzziele mit deren Schutzmaßnahmen, jeweils für die drei Komponenten Daten, IT-Systeme und Prozesse, in Bezug auf das ToE negiert werden. Wie kann bspw. eine Applikation so eingesetzt werden, dass sie in Verfahren Intransparenz für Betroffene erzeugt, zur Vorratsdatenspeicherung beiträgt und die Nutzerkontrolle verhindert?

b) Außerdem sind die strukturell induzierten Beobachtungs- und Verwertungsinteressen zu berücksichtigen, wie sie Sicherheitsbehörden, Unternehmen und Forschungseinrichtungen – sowie insbesondere Organisationen wie Banken, Versicherungen, Logistik- und IT-Unternehmen, Krankenhäuser, Wissenschaftsinstitute der öffentlichen Hand sowie Arbeitgeber – ausbilden.. Dabei sind Verstöße gegen das Transparenzgebot der Betriebsabläufe bei einer Behörde, aufgrund des Rechtsstaatsgebots, anders zu bewerten als bei einem Unternehmen, sofern das Unternehmen dem Druck des Marktes ausgesetzt ist und Kunden die Wahl haben, welches Unternehmen sie für vertrauenswürdig halten. Beide genannten Dimensionen – Ziele/Maßnahmen sowie Organisationen – erzeugen die Analysegrundlage für ein sowohl theoretisches wie empirisch fundiertes Risk-Assessment.

Mit dieser Dimension der strukturell induzierten Angreiferperspektive hängt auch die Definition der Personenrolle bzw. des Menschenbilds einer Organisation zusammen, das eine Organisation als die Modellierungsgrundlage ihrer (automatisierten) Aktivitäten nimmt. Eine solche Explikation der in Technik auskristallisierten Personenmodellierung scheint uns inzwischen nötig zu sein, weil die gesellschaftlich bislang nur diffus verankerten allgemeinen Rollen-Schemata wie Bürger, Kunde, Patient, Mandant, Individuum, Subjekt, Mensch – oder mit or-

7 Während Datenschutz die Informationsverarbeitung bei Machtasymmetrien unter Bedingungen zu stellen versucht, so dass Organisationen überprüfbar den Anforderungen generischer Rollenschemata, wie sie sich durch Gewaltenteilung, Markt und Diskursfreiheit im Bürger, Kunden und Subjekt ausbilden, nachkommen, dient das Konzept des Privatheitsschutzes vornehmlich dazu, aus der Sicht dieser generischen Rollen die Zumutungen von Organisationen zu beobachten und auf Distanz zu halten. Über die Figur der „informationellen Selbstbestimmung" werden beide Konzepte miteinander vermittelt.

8 Zur Risikoanalyse spezieller Verfahren(sbestandteile) können andere, spezifisch zugespitzte, aus den sechs elementaren Schutzzielen abgeleitete Schutzziele hinzugenommen werden (vgl. Rost/Bock 2011).

ganisationsinternem Bezug: Mitarbeiter oder Mitglied – durch die Technisierung der Organisationen einseitig in deren Sinne definiert werden. Selbst in der öffentlichen Verwaltung oder in der Arztpraxis wird vom Kunden gesprochen. Die Spezifik bzw. Differenzierung der Freiheitsversprechen und unabdingbar bestehenden Rechtsansprüche, die mit diesen Rollen-Schemata verbunden sind, gehen schleichend verloren.

In der Praxis sind zudem noch zwei Risikolagen neueren Datums zu beachten: Auf der Basis von Internetnutzung können Aktivitäten privater Unternehmen offensichtlich gegen (Datenschutz-)Gesetze verstoßen, ohne dass diese Feststellung zur Abstellung rechtswidriger Aktivitäten führt. Und umgekehrt können Sicherheitsbehörden relativ umstandslos auf Datenbestände u.a. bei diesen Privatunternehmen zugreifen.

Entscheidend ist hier, dass in einem PIA verlässlich durch Organisationen erzeugte Risikoklassen ausgewiesen sind, bevor es zur Einschätzung der Realisierungswahrscheinlichkeiten kommt. Die Aufnahme und Festlegung eines Katalogs strukturell gegebener Angreifermotive verbesserte die Integrität und Vergleichbarkeit von PIAs, ohne dass der allgemeine Ansatz dadurch ungeeignet verengt wäre.

5) "**Identification and Recommendation of existing or new Controls suited to protect against Threats**". Schutzmaßnahmen sollten bereits in Schritt 2 oder 3 zur Modellierung von Angriffen auf der Ebene von Referenzmaßnahmen herangezogen werden (vgl. Probst 2012).

In diesem Schritt ließen sich Schutzmaßnahmen anführen, die im Katalog mit Referenzmaßnahmen nicht aufgeführt sind und die ganz spezifisch auf die Risiken des Verfahren(bestandteils) eingehen. Generell sollten auch die Schutzmaßnahmen selbst wiederum einer Art „Small-PIA" unterzogen werden. Dazu zählt auch die Evaluation des Changemanagements einer Organisation, um die im PIA empfohlenen Schutzmaßnahmen in der Organisation umzusetzen. Der Ausweis des Umsetzungsrisikos einer empfohlenen Schutzmaßnahme bildet eine weitere, für ein PIA gut umrissene Risikoklasse aus.

Auch wäre dieser Schritt der angemessene Ort, um einen spezifisch umrissenen Forschungsbedarf für Schutzmaßnahmen zu formulieren. Die Durchführung eines PIA ist bereits eine Maßnahme zum Schutz vor Verfahren(skomponenten) durch Verbesserung der Transparenz. Die Auditierung eines PIAs durch eine Datenschutzaufsichtsinstanz, die u.a. die ausgewiesene Policy des PIAs ggfs. bestätigte, bildet einen weiteren Vertrauensanker.

6) "**Assessment and Documentation of Residual Risks**" Dieser Punkt kann dazu dienen, all diejenigen Risiken zumindest zu erwähnen, die nicht behandelt wurden. Zum einen, weil sie als objektiv-nicht-behandelbar oder als zu unwahrscheinlich ausgewiesen sind oder weil ein bestimmtes Set an Schutzzielen/Risiken durch die Policy nicht abgedeckt wurden. Hier kann auch die Aufklärung darüber erfolgen, welche Instanz einer Organisation das Restrisiko entweder zu bearbeiten oder zu übernehmen und zu verantworten hat.

Fazit

Wenn ein PIA den Anspruch erhebt, (auch) die bestehenden allgemeinen datenschutzrechtlichen Anforderungen zu beachten, dann muss es folgende Eigenschaften aufweisen:

- Ausweis des Anspruchtyps bzw. der Policy, die für das PIA gelten soll.
- Darlegung der Datenschutzrisiken anhand der sechs elementaren Schutzziele, einschlielich des Referenz-Schutzmaßnahmenkatalogs.
- Definition von Schutzbedarfsabstufungen, die die Risiken primär und entschieden aus der Sicht von Betroffenen formuliert.
- Integration des zu begutachtenden Objekts in Usecases, die unter Ausweis von Annahmen bzgl. Daten, IT-Systemeigenschaften und Prozessen die Funktionen, Wirkungen und Nebenwirkungen des Objekts veranschaulichen.
- Bearbeitung absehbarer Angreiferperspektiven, wie sie insbesondere bei Sicherheitsbehörden, Versicherungen, Marketingabteilungen, IT- und Kommunikationsunternehmen, Forschungsinstituten sowie Arbeitsgebern typisch ausgebildet sind.

Literatur

Bock, Kirsten; Meissner, Sebastian; 2012: Datenschutz-Schutzziele im Recht – Zum normativen Gehalt der Datenschutz-Schutzziele; in: DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 425-431. https://www.european-privacy-seal.eu/results/articles/DuD-Bock-201206.pdf

BSI; Oetzel; Spiekermann, 2011: Privacy Impact Assessment Guideline. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile

Clarke, Roger, 2011: An evaluation of privacy impact assessment guidance documents; in: International Data Privacy Law, 2011: Vol. 1, No. 2, S. 111-120. http://www.rogerclarke.com/DV/PIAG-Eval.html

ISO 2012: Report "Study Period on Privacy Impact Assessment", Date: 26.03.2012, V1.0, Editor: Mathias Reinis. http://isotc.iso.org/livelink/livelink?func=ll&objId=8916258

Oetzel, Marie Caroline; Spiekermann, Sarah, 2012: Privacy-By-Design Through Systematic Privacy Impact Assessment – A Design Science Approach; published in June 2012 on "European Conference of Information Systems", Barcelona. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050872

Probst, Thomas, 2012: Generische Schutzmaßnahmen für Datenschutz-Schutzziele; in: DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444. https://www.european-privacy-seal.eu/results/articles/201206-DuD-Probst.pdf/view

Rost, Martin; Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353-358. http://www.maroki.de/ pub/privacy/DuD0906_Schutzziele.pdf

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. http://www.maroki.de/pub/privacy/DuD2011-01_RostBock_PbD_NSZ.pdf

Rost, Martin, 2012: Standardisierte Datenschutzmodellierung; in: DuD – Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438. http://www.maroki.de/pub/privacy/2012-06-DuD-SDM.pdf

Solove, Daniel J., 2006: A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol. 154, No. 3: S. 477-560. http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID920281_code249137.pdf?abstractid=667622&mirid=1

Wright, David; De Hert, Paul (ed.), 2012: Privacy Impact Assessment, Dordrecht Heidelberg London New York, Springer.