Handreichung „Anforderungen an ein PIA aus Sicht einer Datenschutzaufsichtsinstanz“

(V1.0, 2013-1014, Kontakt: Martin Rost, uld32@datenschutzzentrum.de)[1]

Gliederung

1. Das Problem

Im Bereich der Datenschutzaufsicht insbesondere über den privaten Sektor werden zunehmend Dokumente eingereicht, in denen die Durchführung eines „Privacy Impact Assessments“ (PIA) zu einem in der Regel neu entwickelten Produkt dokumentiert wird. Ein Produkt kann dabei sowohl ein klar umgrenzter Gegenstand oder auch ein komplexes Verfahren mit vielen Komponenten sein.

Die Durchführung von PIAs ist grundsätzlich zu begrüßen. Die bei den Aufsichtsbehörden eintreffenden PIA-Berichte sind dabei erfahrungsgemäß so angelegt, dass sie den möglichen oder den geplanten oder den faktisch getroffenen Zuschnitt eines Produkts sowie Schutzmaßnahmen gegenüber Aufsichtsbehörden rechtfertigen. Häufig entsteht dabei für eine Aufsichtsbehörde das Problem, dass ein PIA dann zwar methodisch korrekt durchgeführt wurde und im PIA-Bericht viele funktionale und sicherheitstechnische Details zutreffend beschrieben sind, aber trotzdem die wesentlichen Fragen bzgl. des Erfüllens datenschutzrechtlicher Anforderungen nicht beantwortet werden.

Diese Handreichung soll deshalb darlegen, welche Erwartungen eine Datenschutzaufsichtsbehörde an ein PIA und einen PIA-Bericht stellen muss, so dass der Bericht in einem datenschutzrechtlichen Prüfprozess als relevante Vorarbeit, im Sinne einer Vorabkontrolle, einfließen kann. Von einem PIA-Bericht ist dabei generell zu fordern, dass…

- die Methodik der Untersuchung,
- die Sachlage bzw. Fakten,
- die Ergebnisse und
- die Beurteilung der Ergebnisse und deren Begründung

jeweils sauber erkennbar geschieden sind.[2]

---

[1] In das Dokument flossen Kommentare ein von Kirsten Bock, Dr. Thomas Probst, Andreas Sachs, Gabriel Schulz, Michael Valersi, Dr. Ulrich Vollmer und Ursula Zabel.

[2] Beim Verfassen dieser Handreichung wurde Wert darauf gelegt, die Erläuterungen knapp zu halten. Wir empfehlen bei Vertiefungsbedarf den am Schluss des Dokuments aufgeführten Referenzen nachzugehen.

2. Eigenschaften eines datenschutzrechtlich relevanten PIAs

Damit ein PIA als sinnvolle Vorarbeit für eine Datenschutzprüfung genutzt werden kann, sollte es zu den nachfolgend aufgeführten Aspekten Aussagen enthalten.

2.1 Ausweis des TOE sowie des Scopes

Der Autor eines PIA sollte seinen

(1) Prüfungsgegenstand (engl. Target of Evaluation, ToE) sowie
(2) methodischen Anspruch und den Zweck (scope), mit dem das PIA durchgeführt wurde, darlegen.

Zu (1): Beim Ausweis des Prüfungsgegenstands ist darzulegen, ob ein Verfahren oder eine Komponente, aus einem Verfahren separiert, analysiert wird.

Die Besonderheit eines Datenschutz-Assessments besteht im Unterschied zu einem Sicherheits-Assessment darin, dass neben dem Risiko einer mißbräuchlichen Datennutzung etwa durch unbefugte Dritte, die kriminell agieren, auch das Risiko zu behandeln ist, das durch eine Organisation entsteht, die das Produkt befugt nutzt. Der ToE sollte insofern so abgefasst sein, dass auch die Datenschutz-Risiken durch eine zweckfremde Nutzung einer Komponente in den Blick geraten.

Ein PIA, das einer Datenschutzaufsichtsinstanz wie bspw. einem LfD oder dem BfDI vorgelegt wird, muss bei der Analyse einer einzelnen Verfahrenskomponente immer den Bezug zum Verfahren im Auge behalten, in dem die Komponente typischerweise zum Einsatz kommt oder kommen soll. Dieser Bezug sollte dann im Rahmen der Einsatzpraxis oder von use cases behandelt werden, in dem erwartbare Angreiferperspektiven und praxisrelevante Annahmen oder Fakten bzgl. des Kontextes ausgewiesen sind (siehe Seite 7: („2.4 Ausweis des Nutzungskontextes “)).

Zu (2): Beim Ausweis des Scopes sind zumindest drei unterschiedliche Interessen, Ansprüche an Methoden und Tiefe der Faktendarstellung, Ergebnisse und Kontexte zu unterscheiden, die durch eine Selbsttaxierung explizit gemacht werden sollten:

(a) PIA, das sich wissenschaftlich mit der Abschätzung des Privacy Impacts eines Gegenstands beschäftigt;
(b) PIA, das die Erfüllung der methodischen Anforderungen eines PIA-Frameworks mit Empfehlungscharakter anstrebt;
(c) PIA, das die Erfüllung bestehender datenschutzrechtlicher Vorgaben (bzw. dessen allgemein übergreifende Anforderungen) anstrebt.

Zu (a) Dieser Scope zeichnet sich insbesondere dadurch aus, dass die Methode, die theoretischen Annahmen, die Prüfkriterien und die Ergebnisse veröffentlicht und ohne Hürden zugänglich gemacht werden. Von einem wissenschaftlich angelegten PIA darf man erwarten, dass es bei den Beurteilungen von Technikfolgen immer auch eine gesamtgesellschaftliche Perspektive einzunehmen versucht. Insbesondere können in diesem Scope dann auch fehlende Rechtsgrundlagen angesprochen und entsprechende Empfehlungen gegeben oder auch geeignete Normentexte, seien diese Gesetzesentwürfe oder Einwilligungserklärungen, entworfen werden.

Wenn diese Bedingungen eingehalten sind und im Vorhinein feststeht oder festgelegt wurde, dass ein PIA zu einem Produkt auch im Falle eines negativen Ergebnisses veröffentlich wird und die Finanzierung des PIAs transparent ist, dann ist es legitim, wenn auch Hersteller und Betreiber diesen Scope ausweisen.

Zu (b): Dieser Scope trifft typischerweise auf PIAs zu, die von Herstellern von Produkten oder von Nutzern wie Unternehmen und Behörden vorgelegt werden. Die Kriterien zur Ermittlung des Privacy-Impacts können frei gewählt werden. Aber es ist inzwischen der typische Fall, dass bestehende Rahmenwerke zur Durchführung von PIAs herangezogen werden. Als Beispiele für solche Methodenrahmenwerke sind zu nennen das PIA-Framework der EU-Kommission (EU-Kommission 2009), der Art. 29 DS-Gruppe (Art. 29 Data Protection Working Party 2011), des BSI (BSI 2011) oder der inzwischen vorliegende Entwurf der ISO/IEC 29134 (ISO 2013). Diese Frameworks haben keine gesetzliche Grundlage, die Erfüllung konkreter rechtlicher Anforderungen beanspruchen sie nicht, ihr rechtlicher Bezug ist ungeklärt. Gleichwohl ist die Nutzung dieser Frameworks in methodischer Hinsicht hilfreich.

Von einem PIA-Bericht mit dem Scope (b) ist nicht zu erwarten, dass darin auch negative Ergebnisse dargelegt werden. Vielmehr ist damit zu rechnen, dass entweder das ToE so zugeschnitten ist, dass relevante Risiken für einen Betroffenen nicht in den Blick geraten oder heikle Aspekte nicht thematisiert oder verharmlost werden. Ein PIA mit dem Scope (b) kann trotzdem in einem Datenschutzprüfprozess relevant sein, wenn es zumindest zu klären hilft, welche Eigenschaft als datenschutzrechtlich besonders heikel anzusehen ist.

Zu (c): Dieser Scope signalisiert, dass ein PIA den Anspruch erhebt, im Sinne einer Vorarbeit zur Effektivierung einer Datenschutzprüfung beizutragen. Insbesondere wenn eine gesetzliche Vorschrift im Rahmen des Datenschutzrechts bestimmt, dass ein „Privacy-Impact-Assessment“ oder ein „Datenschutz-Impact-Assessment“ oder, in einer älteren Diktion, eine „Technikfolgenabschätzung“ durchzuführen ist, dann sind die Anforderungen gemäß Scope (c) zu erfüllen. Grundsätzlich muss eine Organisation, die ein PIA durchführt bzw. durchführen lässt, damit rechnen, dass eine Datenschutzaufsichtsinstanz zusätzliche Unterlagen anfordert. Dies ist insbesondere von länderspezifischen Details wie spezialgesetzliche Regelungen oder auch festgelegte Löschfristen oder gesetzlich festgeschriebene Schutzmaßnahmen abhängig.

Wenn gegenüber einer Datenschutzaufsichtsinstanz ein anderer PIA-Scope als (c) ausgewiesen ist, muss der Autor eines PIA-Berichts grundsätzlich damit rechnen, dass das vorgelegte PIA als „datenschutzrechtlich nicht-relevant“ eingestuft wird. Wenn einer Aufsichtsbehörde ausschließlich ein PIA mit Scope (b) vorgelegt wird, sollte ein Mapping vorgenommen werden, aus dem ersichtlich ist, wie eine Organisation, die den im PIA begutachteten Prüfungsgegenstand einsetzt, die datenschutzrechtlich bestehenden Anforderungen erfüllt.

Nachfolgend werden Anforderungen an ein PIA formuliert, das den Scope (c) einnimmt und den Anforderungen des Datenschutzrechts zu genügen beansprucht.[3]

2.2 Ausweis der Risiken und der eingenommenen Risikoperspektive

[3] In Anlehnung an den Entwurf in §33 der „General Data Protection Regulation“ der EU-Verordnung empfiehlt es sich, bei diesem scope anstatt von einem „privacy impact assessment“ genauer von einem „data protection assessment“ (vgl. EU-Parlament 2012) zu sprechen.

Die in einem am Datenschutzrecht orientierten PIA betrachteten Risiken müssen aus dem allgemeinen Datenschutzrecht heraus abgeleitet sein und vollständig behandelt werden (1). Dabei ist vornehmlich die Perspektive von Betroffenen einzunehmen (2) sowie auch die mittelbaren Auswirkungen zu behandeln, die auf Betroffene und deren Recht auf informationelle Selbstbestimmung rückwirken können (3).

Um Zeit und Kosten zu sparen ist es zu empfehlen, ein PIA durchzuführen, bevor wesentliche konstruktive und architektonische Entscheidungen bezüglich des Prüfungsgegenstands als Produkt bereits getroffen wurden. Wird das PIA als ein wesentlicher Bestandteil einer Vorabkontrolle angesehen, dann muss das PIA vor dem Beginn der Verarbeitung von personenbezogenen Daten bzw. vor der Einrichtung des Verfahrens durchgeführt werden (vgl. BDSG § 4d Abs. 5).

Zu (1): Die allgemeinen Datenschutz-Anforderungen betreffen im Wesentlichen die Legitimität und Korrektheit der Datenverarbeitung, die Vertraulichkeit der Verarbeitung ausschließlich durch Befugte, die Transparenz der Datenverarbeitung, der Datenflüsse, der Datenempfänger gegenüber Betroffenen und Aufsichtsbehörden, die Zweckbindung der Erhebung, Verarbeitung oder Weitergabe von Daten sowie die Umsetzung der Betroffenenrechte in Bezug auf Einsicht, Bearbeitung und Korrekturen oder Löschen von Daten. Alle Aktivitäten, die gegen diese Anforderungen verstoßen, bilden Datenschutzrisiken.

Es hat sich im Bereich der IT-Sicherheit bzw. Informationssicherheit bewährt, Anforderungen als Schutzziele zu formulieren.[4] Die Anforderungen des Datenschutzes sind rechtlich festgelegt. Diese Anforderungen lassen sich ebenfalls mit Hilfe von Schutzzielen umsetzen, die in kompakter und methodisch zugänglicher Form die operativen Risiken explizit machen, gegen die es durch eine angemessene Verfahrensgestaltung und Maßnahmen zu schützen gilt.

Sechs Schutzziele gelten derzeit im Bereich des Datenschutzes als etabliert. Den Risiken der IT-Sicherheit wird klassisch mit der Sicherung der drei Schutzziele

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit

begegnet. Die Risiken auch des Datenschutzes werden durch folgende Schutzziele formuliert, für die datenschutzspezifische Schutzmaßnahmen zur Verfügung stehen[5]:

- Transparenz,
- Nichtverkettbarkeit und
- Intervenierbarkeit.

Die Schutzziele thematisieren insgesamt wesentliche datenschutzrechtliche Risiken bzw. Anforderungen. Dabei stehen hinter jedem Schutzziel abgeleitete Schutzziele. So ist bspw. Revisionsfähigkeit ein ganz wesentlicher Aspekt der Sicherung der Transparenz und die Sicherung der Authentizität ist ein ganz wesentlicher Aspekt der Sicherung der Integrität in einer Kommunikationsbeziehung. Das Schutzziel Nichtverkettbarkeit nimmt die im Datenschutzrecht zentrale Anforderung der Zweckbindung einer Verarbeitung personenbezogener Daten auf, in einer Form, die der technischen und organisatorischen Umsetzung der Anforderung an

[4] Die neueren Datenschutzgesetze der Länder enthalten im Bereich technisch-organisatorischer Schutzmaßnahmen „Schutzziele“ (vgl. Rost 2012).

[5] Die PIA-Frameworks arbeiten entweder nur mit den drei klassischen Schutzzielen der IT-Sicherheit oder sie referenzieren die Datenschutz-„Prinzipien“ der „Global-Privacy-Standards“, die inzwischen in der ISO 29100 eingegangen sind. Das SDM beansprucht mit dem systematisch angelegten Konzept der Schutzziele, diese Prinzipien als Untermenge zu enthalten (vgl. Rost/Bock 2011),.

Zweckbindung, die wiederum die Anforderungen der Datensparsamkeit und Erforderlichkeit reguliert, entgegen kommt. Das Schutzziel der Intervenierbarkeit dient der operativ zugänglichen Gewährleistung der Betroffenenrechte. Hinter jedem dieser Schutzziele steht vor allem ein Katalog mit Maßnahmen zur Erreichung der Schutzziele in der Praxis. Das Schutzzielekonzept kann dabei jedoch nicht jede einzelne rechtliche Festlegung erfassen, was bspw. die Lösch- bzw. Aufbewahrungsfristen, Zustimmungserklärungen und ähnliches mehr, betrifft. Solche Regelungen im Detail sind insofern noch zusätzlich zu beachten.

Zu (2): Die Einnahme der Schutzperspektive muss ausgewiesen sein: Sind technische Funktionen für Geschäftsprozesse zu schützen oder gilt der Schutz dem Betroffenen und dessen Grundrechte? Zu unterscheiden sind insofern Risiken für das Verfahren der Organisation, die Informationssicherheit in den Blick nimmt, von den Risiken durch das Verfahren für den Betroffenen, die aus Datenschutzsicht zu beachten sind.

Beide Perspektiven liegen vielfach in einem Konflikt zueinander. Das Informationssicherheitsmanagement nach BSI 100-1 oder ISO 27001 nimmt vornehmlich die Sicherung von Geschäftsprozessen in den Blick und damit die Risikoperspektive einer Organisation ein. Sie sieht folglich grundsätzlich in externen Dritten und nicht regelkonform handelnden internen Nutzern Angreifer eines Verfahrens bzw. eines IT-Systems. Der Datenschutz legt darüber hinaus Wert darauf, dass auch die Organisation, unter deren Verantwortung ein IT-Verfahren betrieben wird, methodisch als eine Instanz thematisiert wird, von der Datenschutzrisiken ausgehen. Die Organisation, die den Prüfungsgegenstand einsetzt, darf sich insofern nicht in den blinden Fleck der Risikoanalysen eines PIAs setzen, sondern muss in jedem Falle selber zum Gegenstand der Risikoanalyse gemacht werden.

Zu (3): Bei großen Prüfungsgegenständen bzw. bei Produkten mit infrastrukturellen Ausmaßen (Beispiele: Mautsystem, Geldkarte, Kreditkarte, IT von Kraftfahrzeugen, Smart-Meter, Verwaltungsverfahren, Abrechnungssystem, Portale) sind die absehbaren negativen Rückwirkungen auf Betroffene auch dann zu beachten und darzulegen, wenn im bilateralen Verhältnis einer Organisation, die den Prüfungsgegenstand oder eine Komponente davon betreibt, und einem Betroffenen, der diese Komponente nutzt, die Rechtmäßigkeit festgestellt ist. Dieser Aspekt ist erfahrungsgemäß dann relevant, wenn pseudonymisierte oder anonymisierte Daten ohne Zweckbindungsschutz ausgewertet werden sollen, die durch Kontextierungen bzw. durch Hinzuziehen anderer Datenbestände, etwa im Rahmen typischer BigData-Strategien, jedoch wieder individualisierbar sind oder generell zur Diskriminierung von (Risiko-)Gruppen führen.

2.3 Ausweis des Schutzbedarfes und der Schutzmaßnahmen

Datenschutzrechtlich ist festgelegt, dass die Verarbeitung personenbezogener Daten nur auf einer Rechtsgrundlage erfolgen darf („Verbot mit Erlaubnisvorbehalt“, vgl. BDSG §4 ff). Damit Schutzmaßnahmen entsprechend der rechtlichen Abwägungen angemessen ausgewählt und in einem PIA berücksichtigt werden können, empfiehlt es sich methodisch, zunächst die Daten zu typisieren, die mit dem Prüfungsgegenstand erzeugt bzw. verarbeitet werden und deren Schutzbedarf zu ermitteln bzw. festzulegen (1). Im Anschluß an die Ermittlung des Schutzbedarfs für den Betroffenen können die angemessenen Schutzmaßnahmen bestimmt werden (2).

Zu (1): Als hinreichend differenziert haben sich folgende Schutzbedarfsabstufungen erwiesen: „normal“, „hoch“, „sehr hoch“. Zur Definition der Schutzbedarfe lassen sich die folgenden Definitionen heranziehen[6]:

- *Normal:* Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht zu heilen.
- *Hoch:* die Schadensauswirkungen werden von Betroffenen als beträchtlich eingeschätzt, z.B. weil eine von einer Organisation zugesagte Leistung wegfällt, die die Gestaltung des Alltags nachhaltig beeinflusst, und der Betroffene sie nicht aus eigener Kraft ersetzen kann sondern auf extern organisierte Hilfe angewiesen wäre.
- *sehr hoch:* Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, also: katastrophales Ausmaß für den Betroffenen an.[7]

Die Einstufung einer Schadensauswirkung ist auch an der Zahl der von dem Ereignis Betroffenen auszurichten. So ist von einem sehr hohen Schadenswert auszugehen, wenn ein Ereignis für eine sehr große Zahl von Betroffenen zu beträchtlichen Schäden führt.

Zu (2) Die Auswahl der Schutzmaßnahmen zur Bearbeitung der Risiken sollte drei Themenbereiche unterscheiden:

- *safety* thematisiert technisch bedingte Ausfälle der Funktionen von Systemen. Safety wird zumeist unter dem Schutzziel der Verfügbarkeit thematisiert.
- *security* thematisiert die technische und organisatorische Sicherheit funktionierender Systeme. Die wesentlichen Schutzziele sind die Sicherung der Integrität, die Vertraulichkeit der Geschäftsprozesse, die Transparenz des Systems und die Intervenierbarkeit für die Leitung der Organisation. Aspekte von Security werden zumeist aus der Perspektive der Sicherung der Geschäftsprozesse von Organisationen formuliert.
- *data protection* thematisiert die Sicherheit vor Mißbrauch von Daten bzw. Verfahren, der durch die Organisation, die die Komponente einsetzt, entstehen kann. Die wesentlichen Schutzziele sind die Sicherung der Vertraulichkeit der erhobenen und verarbeiteten Daten im Sinne des Betroffenen, die Sicherung der Integrität der Funktionen und Nutzungen der Daten, der Bindung der Datenverarbeitung an den ausgewiesen Zweck bzw. den Ausschluss der Verwendung von Daten zu anderen Zwecken ohne gesetzliche Legitimation inklusive der Weitergabe an andere Organisationen, die Transparenz der Prozesse für den Betroffenen, die ihn betreffen, einschließlich der unaufgeforderten und verständlichen Benachrichtigung über ablaufendeVerarbeitungen sowie die Möglichkeiten zum Eingriff darin, so durch Aufforderungen zur Berichtigung, Sperrung und Löschung der ihn betreffenden Daten.

Ein PIA muss schon begrifflich die Problemstellungen zum Thema „data protection“ prioritär in den Blick nehmen und darlegen, inwieweit der zu beurteilende Prüfungsgegenstand in dieser Hinsicht gegenstandsspezifische Risiken erzeugt. Es kann sich insbesondere dann vollständig auf die Behandlung dieses Themenbereichs konzentrieren, wenn Sicherheitsaspekte bereits in einem eigenständigen Security-Assessment behandelt werden. Allerdings ergeben sich auch aus den Themenbereichen safety und security eigenständige Folgen für die Betroffenen, die dann wiederum unter dem Aspekt data protection zu berücksichtigen sind.

Zu den Schutzzielen gibt es, wie bereits erwähnt, Kataloge mit Maßnahmen zum Erreichen der Schutzziele. In Bezug auf die Sicherung der Schutzziele der IT-Sicherheit (Verfügbarkeit,

---

[6] Diese Definitionen des Schutzbedarfs von Betroffenen befinden sich gegenwärtig in einem Abstimmungsprozess unter den deutschen Datenschutzaufsichtsbehörden (Stand: 2013/10).

[7] Diese Formulierungen lehnen sich an die Definition des Schutzbedarfes nach IT-Grundschutz an: https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf, S. 49

Integrität, Vertraulichkeit) lassen sich die Maßnahmenkataloge des BSI-Grundschutz heranziehen (BSI 2008), eingedenk der bereits erwähnten wesentlichen Bedingung, dass die Risikoperspektive auf die des Betroffenen anzupassen ist.

Als generische Schutzmaßnahmen des Datenschutzes zur Umsetzung der Schutzziele der Transparenz, Nichtverkettbarkeit und Intervenierbarkeit in Verfahren gelten die folgenden:[8]

- *Sicherung der Transparenz*: Dokumentation der technischen und organisatorischen Eigenschaften des Prüfungsgegenstands unter Beachtung der Wechselwirkung mit anderen Verfahren, revisionsfähige Protokollierung von Prozessen und Datenflüssen, die gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem welche personenbezogenen Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind bzw. der Bezug von welchen Einzelangaben zu welchen Personen hergestellt wurde, Dokumentation und fortgesetztes Controlling der Wirksamkeit der Sicherheitsmaßnahmen der IT-Sicherheit und des Datenschutzes.
- *Gewährleistung der Nichtverkettbarkeit*: In der Gestaltungsphase des Verfahrens: Einschränken der Datenerhebung auf die erforderlichen Daten. In der Betriebsphase: Nutzung der Möglichkeiten der Pseudonymisierung und Anonymisierung, frühest mögliches Löschen von Daten (auch auf Backup-Systemen).
- *Sicherung der Intervenierbarkeit*: Dem Betroffenen sind die ihnen zustehenden Rechte verständlich zu kommunizieren und kompetente und entscheidungsbefugte Ansprechpartner zu benennen, die für eine Durchsetzung dieser Rechte innerhalb der involvierten Organisationen sorgen können. Wenn irgend möglich ist den Betroffenen im Sinne eines Singlepoint of Contact ein operativer Zugriff auf ihre Daten einschließlich des Status ihrer Bearbeitung und der von ihnen erteilten Einverständniserklärungen zu geben und ihnen insbesondere die Möglichkeit zu eröffnen, erteilte Erklärungen zurückzuziehen. Organisationen haben Standardprozesse des Changemanagements auszuweisen.

Diese Maßnahmen sind seitens einer Organisation im Rahmen eines Datenschutzmanagements auf ihre Wirksamkeit hin zu kontrollieren.[9]

Die endgültige Festlegung des Schutzbedarfes und die konkrete Ausgestaltung des Prüfungsgegenstands sind von den realen Umständen abhängig, in denen dieser im Rahmen eines personenbezogenen Verfahrens eingesetzt wird. Deswegen muss ein PIA den Kontext bzw. das Verfahren, in dem der Untersuchungsgegenstand eingesetzt wird, thematisieren.

2.4 Ausweis des Nutzungskontextes

Die realen, praxisrelevanten Risiken für Betroffene und die Angemessenheit der zum Einsatz kommenden Sicherungsmaßnahmen können erst wirklich beurteilt werden, wenn der Prüfungsgegenstand nicht nur als solcher vereinzelt sondern eingebunden in Verfahren ganzheitlich betrachtet wird (1). Neben den Risiken durch den Gebrauch eines Verfahrens sind auch

[8] In Bezug auf die Sicherung der Schutzziele speziell des Datenschutz (Transparenz, Nichtverkettbarkeit, Intervenierbarkeit) wird derzeit unter den deutschen Aufsichtsinstanzen an einem abgestimmten Katalog zu spezifischen Datenschutzmaßnahmen gearbeitet (Stand: 2013/10). Ein erster Entwurf mit standardisierten Datenschutzmaßnahmen findet sich bei Probst (Probst 2012). Generell gilt es dabei zu bedenken, dass Maßnahmen der IT-Sicherheit und des Datenschutzes ihrerseits personenbezogene Verfahren sein können, die entsprechend zu gestalten sind. Dies gilt insbesondere für die Protokollierung der Aktivitäten von Mitarbeitern.

[9] Ein Entwurf zu einem Datenschutzmanagementsystem, das sich am Schutzzielkonzept des Datenschutzes und methodisch an die ISO27001 anlehnt findet sich bei Rost (Rost 2013).

die strukturell bestehenden Motive seitens der einsetzenden Organisationen zu berücksichtigen, die zur zweckfremden Nutzung oder zum Mißbrauch eines Verfahrens oder der Daten daraus verleiten (2).

Zu (1): Ein generisch oder prognostisch angelegtes PIA, das bspw. als Teil einer Privacy-By-Design-Strategie durchgeführt wird, trifft in der Regel auf einige Unwägbarkeiten bzgl. des Einsatzes des Prüfungsgegenstands. Methodisch sollten diese Unwägbarkeiten über die Formulierung von typischen *use cases* oder Einsatzszenarien abgefangen werden. Dagegen muss ein PIA für einen bereits existierenden Gegenstand in einem bereits bestehenden und einem weitgehend bekannten Kontext die Fakten bzgl. des Einsatzes des Prüfgegenstands und des Einsatzkontextes ausweisen. Hier würde man insofern, zur klaren Unterscheidung von use cases und Szenarien, von der *Einsatzpraxis* sprechen.

Bei der Darstellung eines Verfahrens sind dabei grundsätzlich drei Komponenten zu unterscheiden und einzeln anzusprechen:

- Daten und deren Formate beim Speichern oder Transferieren (Protokolle)
- IT-Systeme und deren Schnittstellen
- Prozesse und deren adressierbare Funktionsrollen

Eine Darstellung des Kontextes eines Verfahrens nimmt Bezug auf die Prozesse, an denen die *Rollen und Motive* sowie die rechtlichen Anforderungen und die Rechtsbeziehungen der Beteiligten untereinander darlegbar sind. Als handelnde Personen und Beteiligte sind zu nennen:

- die Betroffenen;
- die für den Einsatz des Prüfungsgegenstands verantwortlichen Organisationen;
- die Hersteller oder „Betreiber“ des Prüfungsgegenstands als Dienstleister etwa im Rahmen einer Auftragsdatenverarbeitung (RZ, Internet-Provider);
- ggf. Dritte, die im Zuge des Einsatzes des Prüfungsgegenstandes Kenntnis von personenbezogenen Daten nehmen, seien dies beiläufig (z.B. zufällig anwesende, mithörende Dritte) oder mit Vorsatz (Sicherheitsbehörden).

In der Praxis trifft man zunehmend auf zweistufig angelegte PIAs. Hersteller und Vertreiber führen ein generisch gehaltenes PIA gemäß Scope (b) durch. Darin sind dann Risikodimensionen ausgewiesen, die frei gewählt oder bspw. dem Privacy-Framework der ISO/IEC 29100 entnommen sein können. Die Risikolagen in konkreten Kontexten, in denen das Verfahren läuft oder laufen soll, werden dann durch ein ergänzendes zweites PIA geschildert. Dieses ergänzende PIA legt die verantwortlich datenverarbeitende Stelle vor. Ein derartiges „Ergänzungs-PIA“ ist dasjenige, das die Datenschutz-Aufsicht als das Wesentliche interessiert und das gemäß Scope (c) angelegt sein sollte. Als eine weitere bislang unerwähnte Komponente kann ein derartiges „Ergänzungs-PIA“ dann ggfs. auch eine auf die Komonenten abgestimmte Einwilligungserklärung als Legitimationsbasis enthalten, die die Risiken und deren Bearbeitung entlang der Schutzziele ausweist und darüber hinaus die Aspekte der Einholung, der Beachtung des Anwendungsbereichs sowie die Folgen eines Widerrufs behandelt.

Autoren die für Organisationen generische PIAs durchführen und entsprechende Berichte anfertigen, sollten für ihre Auftraggeber typische use cases formulieren, in denen die Strukturen vorgegeben und Empfehlungen für die Konfiguration und den datenschutzgerechten Einsatz des Prüfungsgegenstands enthalten sind. Darüber hinaus sollten auch Risiken angesprochen sein, die durch Auftragsdatenverarbeitung und Funktionsübertragungen entstehen und wie diese Risiken im Rahmen der Zusammenhang von IT-Securitymanagement und Datenschutzmanagement verringert werden können.

Zu (2): Ein PIA sollte neben kriminellen Angreifermotiven insbesondere die strukturell gegebenen „Angreifer"-Perspektiven thematisieren, die einen negativen Einfluss auf den Datenschutz von Personen in ihrer Rolle als Bürger, Kunde, Patient, Organisationsmitglied und MitarbeiterIn ausüben. Dazu zählen die Risiken der Zweckdurchbrechung bei der Nutzung von Daten durch andere Abteilungen einer Organisation sowie insbesondere der Zugriff auf Verfahren und deren Daten durch Sicherheitsbehörden, Konkurrenzunternehmen oder Forschungsinstitute.

3. Zusammenfassung

Ein datenschutzrechtlich als relevant einzustufendes Privacy-Impact-Assessment zeichnet sich durch folgende Eigenschaften aus:

- Ausweis des ToE und des angestrebten Scopes;
- Ausweis der Risiken anhand der datenschutzrechtlichen Anforderungen, insbesondere der sechs Schutzziele der IT-Sicherheit und des Datenschutzes,
- Ausweis von Verfahrensrisiken in Kontexten, in denen der Prüfungsgegenstand eingesetzt wird oder eingesetzt werden kann.

Erst wenn der Prüfungsgegenstand in einen Verfahrenszusammenhang gestellt wird, der bspw. nicht nur die Darstellung von Schnittstellen umfasst, sondern die strukturell gegebenen und absehbaren Angreifermotive berücksichtigt, können datenschutzrechtlich relevante Aussagen in Bezug auf die Risiken und deren Bearbeitung vorgenommen werden.

4. Anmerkungen

Allein die Existenz eines PIA enthebt eine Datenschutzaufsichtsbehörde nicht von einer Prüfung des zu analysierenden Gegenstands auf Datenschutzgerechtigkeit.

Liegen eine Rechtsgrundlage für oder eine Einwilligung in ein Verfahren vor, so bedeutet das nicht, dass von einem Gegenstand bzw. von einem Verfahren keine Risiken mehr für den Datenschutz bzw. die Privatssphäre von Betroffenen ausgehen und es keiner weiteren Prüfung des Verfahrens selber bedarf. Im Gegenteil: Das Bestehen einer Ermächtigungsregelung für eine personenbezogene Datenverarbeitung zeigt, dass hier regelungsbedürftige Risiken bestehen.

Anders als bei festgestellten Risiken nach IT-Grundschutz ist es aus einer grundrechtlichen Perspektive heraus nicht zu legitimieren, wenn wesentliche Risiken seitens einer datenverarbeitenden Organisation billigend in Kauf genommen werden. Wenn Risiken für Grundrechte bestehen und nicht materiell wirksam hinreichend verringert werden können, muss vom Einsatz eines solchen Produkts abgesehen werden.

5. Referenzen

- Art. 29 Data Protection Working Party, 2011: *Privacy and Data Protection Impact Assessment Framework for RFID-Applications*, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
- BSI 2008: *IT-Grundschutz*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- BSI / Oetzel / Spiekermann, 2011: *Privacy Impact Assessment Guideline*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guide-

line_Kurzfasssung.pdf;jsessionid=7DD3CC81A66012FFCE2625E610192A7A.2_cid359?__blob=publicationFile
- BSI, 2011: *Privacy Impact Assessments*, https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/RadioFrequencyIdentification/PIA/pia_node.html
- EU-Kommission, 2009: *EMPFEHLUNGEN vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF
- EU-Parlament, 2012: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- ISO-2013: ISO/IEC 29134**,** *Methodology for Privacy Impact Assessment (PIA)*, (Entwurf)
- Probst, Thomas, 2012: *Generische Schutzmaßnahmen für Datenschutz-Schutzziele*; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 439-444.
- 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.
- Rost, Martin, 2012: *Standardisierte Datenschutzmodellierung*; in: DuD - Datenschutz und Datensicherheit, 36. Jahrgang, Heft 6: 433-438.
- Rost, Martin, 2013: *Datenschutzmanagementsystem*; in: DuD - Datenschutz und Datensicherheit, 37. Jahrgang, Heft 5: 295-300.
- Wright, David / de Hert, Paul (Hrsg)., 2012: *Privacy Impact Assessment*, Springer