ANFORDERUNGEN AN PRIVACY IMPACT ASSESSMENTS AUS SICHT DER DATENSCHUTZAUFSICHTSBEHÖRDEN

EINE HANDREICHUNG DES AK TECHNIK

Version 1.0 vom 11.11.2013

Kontakt: Gabriel Schulz, *gabriel.schulz@datenschutz-mv.de*

INHALT

1 ZIELSTELLUNG

Unter der Bezeichnung Privacy Impact Assessment (PIA) werden Werkzeuge und Vorgehensweisen zusammengefasst, mit denen die Auswirkungen der Datenverarbeitung mit neuen Verfahren und Technologien beurteilt und Methoden zur Begrenzung negativer Folgen für die informationelle Selbstbestimmung der betroffenen Personen bestimmt werden. In verschiedener Ausprägung kommen sie in der anglophonen Welt bereits seit den 70er Jahren zum Einsatz.

Die Europäische Kommission forderte im Jahr 2009 die Erarbeitung eines PIA-Rahmenwerks, mit dem Ziel, einen datenschutzfreundlichen Einsatz der RFID-Technologie zu befördern. Das von der Industrie erarbeitete Rahmenwerk und die ihm zugrunde liegende Methodik wurde 2010 von der Artikel-29-Arbeitsgruppe der europäischen Datenschutzbehörden befürwortet. Der im Jahr 2012 veröffentlichte Entwurf einer Datenschutzgrundverordnung sieht in Artikel 33 eine Verpflichtung zur Durchführung von Datenschutz-Folgeabschätzungen (*data protection impact assessments*) für Verarbeitungen vor, die mit besonderen Risiken für die betroffenen Personen einhergehen.

Im Zuge dieser Entwicklung werden bei den Datenschutzaufsichtsbehörden zunehmend Dokumente eingereicht, in denen die Durchführung eines PIA zu neu entwickelten Produkten oder Verfahren dokumentiert wird. Damit wird beabsichtigt, die Gestaltung des Gegenstands des PIA und die bei seinem

Einsatz vorgesehenen Schutzmaßnahmen im Kontext einer datenschutzrechtlichen Beratung oder Kontrolle zu rechtfertigen.

Dieses Vorgehen ist grundsätzlich zu begrüßen. Rechtzeitig durchgeführt können PIAs dazu beitragen, nicht nur Rechtskonformität zu erreichen, sondern im Sinne eines *privacy by design* auch einen gelungenen Ausgleich zwischen den Interessen der Anwender und der Personen zu finden, deren Daten sie verarbeiten. Hiermit geht sie über die bei bestimmten Verarbeitungen gesetzlich geforderte Vorabkontrolle hinaus.

Häufig wird das gewünschte Ziel der PIA-Vorlage jedoch nicht erreicht, trotz formal korrekter Durchführung des PIA und zutreffender Beschreibung vieler funktionaler und sicherheitstechnischer Details, weil wesentliche datenschutzrechtliche Anforderungen nicht behandelt wurden.

Es ist daher Zielstellung dieser Handreichung, die Erwartungen der Datenschutzaufsicht an Struktur und Inhalt eines PIA zu formulieren, deren Erfüllung sichert, dass sein Ergebnis eine valide und relevante Grundlage für einen datenschutzrechtlichen Prüfprozess bilden kann.

2 GLIEDERUNG DES PIA-BERICHTS

Grundsätzlich soll ein PIA-Bericht

1. Methodik und Zweck der Untersuchung,
2. die Sachlage, insbesondere die Eigenschaften des Prüfungsgegenstandes und den Kontext seines Einsatzes,
3. die Ergebnisse und
4. die Beurteilung der Ergebnisse und deren Begründung

sauber voneinander getrennt darlegen.[1]

Es ist nicht erforderlich, dass ein PIA-Bericht vollständig in sich geschlossen ist. Verweise auf weiterführende Dokumente sind zulässig. Es muss jedoch möglich sein, die wesentlichen Inhalte und Schlussfolgerungen unmittelbar aus dem Text des Berichts heraus nachzuvollziehen. Umgekehrt steht es der prüfenden Behörde frei, insbesondere bei Unklarheiten im Detail den Einreicher des PIA um die Vorlage zusätzlicher Unterlagen zu bitten.

3 METHODIK UND ZWECK DES PIA

PIAs werden mit weit variierenden Zielstellungen durchgeführt, die unterschiedliche Ansprüche an Methoden und Tiefe der Faktendarstellung, Ergebnisse und Kontexte bedingen. Zweck eines PIAs kann sein,

1. die Auswirkungen einer Technologie oder eines Verfahrens auf die Privatsphäre der Betroffenen wissenschaftlich abzuschätzen;
2. den Prüfgegenstand entsprechend der methodischen Anforderungen eines PIA-Rahmenwerks zu analysieren und im Interesse der Betreiber Konsequenzen in Bezug auf Gestaltung und Einsatz zu ziehen;

[1] Beim Verfassen dieser Handreichung wurde Wert darauf gelegt, die Erläuterungen knapp zu halten. Wir empfehlen bei Vertiefungsbedarf den zum Schluß aufgeführten Referenzen nachzugehen.

3. die Erfüllung datenschutzrechtlicher Vorgaben nachzuweisen.

Zu 1. PIAs mit dieser Zielstellung zeichnen 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 fehlende Rechtsgrundlagen angesprochen und entsprechende Empfehlungen gegeben oder auch geeignete Normentexte entworfen werden.

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

Zu 2. Dieser Zweck trifft typischerweise auf PIAs zu, die von Herstellern von Produkten oder von Betreibern wie Unternehmen und Behörden vorgelegt werden. Beispiele für geeignete Methodenrahmenwerke sind die PIA-Rahmenwerke der EU-Kommission (EU-Kommission 2009), der Artikel-29-Gruppe (Art. 29 Data Protection Working Party 2011), des BSI (BSI 2011) oder der inzwischen vorliegende Entwurf der ISO/IEC 29134 (ISO 2013). Diese Rahmenwerke haben keine rechtliche Wirkung und beanspruchen nicht, die Erfüllung konkreter rechtlicher Anforderungen zu garantieren. Gleichwohl ist die Nutzung der Rahmenwerke in methodischer Hinsicht hilfreich.

Ein PIA-Bericht mit diesem Zweck steht in der Gefahr, negative Ergebnisse zu vermeiden, und relevante Risiken für die Betroffenen nicht in den Blick zu nehmen. Je umfassender im PIA Prüfungsgegenstand und der Kontext seines Einsatzes, wie auch Auswirkungen und Risiken behandelt werden, desto größer die Relevanz, mit welcher der PIA-Bericht in den Datenschutzprüfprozess eingebracht werden kann.

Zu 3. PIAs mit dieser Zweckbestimmung dienen explizit der Prüfung der Bedingungen eines rechtskonformen Einsatzes des untersuchten Verfahrens durch Hersteller und Betreiber selbst, aber auch der Effektivierung von Prüfungen durch die Datenschutzaufsicht. Derartige PIAs müssen insbesondere dann durchgeführt und dokumentiert werden, wenn durch Gesetz bestimmt ist, dass ein Privacy Impact Assessment, ein Datenschutz-Folgenabschätzung oder, in einer älteren Diktion, eine Technikfolgenabschätzung auszuführen ist.

Um Zeit und Kosten zu sparen, ist es zu empfehlen, ein PIA dieser Art 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, vgl. § 4d Abs. 5 Bundesdatenschutzgesetz (BDSG), dann muss das PIA vor dem Beginn der Verarbeitung von personenbezogenen Daten bzw. vor der Einrichtung des Verfahrens durchgeführt werden.

Wird ein PIA, das mit anderer Zweckbestimmung erarbeitet wurde, zum Zweck der Prüfung der Rechtskonformität bei der Datenschutzaufsicht vorgelegt, so muss damit gerechnet werden, dass der Bericht von der Behörde als datenschutzrechtlich nicht relevant eingestuft wird. Um dies zu vermeiden, sollte der Bericht zumindest um eine explizite Aufstellung ergänzt werden, aus der ersichtlich ist, wie ein Betreiber des im PIA betrachteten Prüfungsgegenstands die datenschutzrechtlich bestehenden Anforderungen erfüllt.

In der Praxis trifft man auch auf zweistufig angelegte PIAs: Hersteller und Vertreiber führen ein generisch gehaltenes PIA durch. Darin sind Risiken ausgewiesen, die frei gewählt oder einem Rahmenwerk wie dem Datenschutz-Rahmenstandard 29100 von ISO und IEC entnommen wurden. Die Risikolagen in konkreten Kontexten, in denen das Verfahren laufen soll, werden dann durch ein ergänzendes zweites

PIA geschildert. Dieses ergänzende PIA legt die verantwortlich datenverarbeitende Stelle vor. In diesem Fall muss sich zumindest das zweite, das Anwendungs- oder Ergänzungs-PIA an der dritten Zweckbestimmung ausrichten.

Im Folgenden formuliert die vorliegende Handreichung Anforderungen ausschließlich an PIA, die auf die Erfüllung der Anforderungen des Datenschutzrechts ausgerichtet sind.

4 AUSWEIS DES PRÜFUNGSGEGENSTANDES UND DES NUTZUNGSKONTEXTS

Beim Ausweis des Prüfungsgegenstands (engl. *target of evaluation, ToE*) ist darzulegen, ob ein vollständiges Verfahren analysiert wird, das einen Geschäftsprozess als Ganzes oder in wesentlichen Teilen abbildet, oder eine Komponente, die aus ihrem Einsatzumfeld separiert wurde.

Auch im zweiten Fall muss bei der Analyse immer der Bezug zu den Gesamtverfahren im Auge behalten werden, in denen die Komponente typischerweise zum Einsatz kommt oder kommen soll. Dies ermöglicht erst eine umfassende Darstellung der Annahmen zum Einsatzkontext, zu erwartbaren Angreiferperspektiven und den realen, praxisrelevanten Risiken für die Betroffenen sowie eine Beurteilung der Angemessenheit der vorgesehenen Sicherungsmaßnahmen.

Ein generisch 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 *Anwendungsfällen* oder *Einsatzszenarien* abgefangen werden. Dagegen muss ein PIA für den Einsatz des Prüfungsgegenstandes in einem bereits bestehenden und weitgehend bekannten Kontext diese vorgesehene *Einsatzpraxis* darlegen. Für die Abbildung des oder der unterstützten Geschäftsprozesse empfiehlt es sich, auf etablierte Modelle zurückzugreifen und in der Darstellung der Prozessabläufe den mit ihnen verbundenen Fluss personenbezogener Daten hervorzuheben.

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

1. die *Verarbeitungsprozesse* und deren adressierbare Funktionsrollen,
2. die zu verarbeitenden personenbezogenen *Daten* und deren Formate beim Speichern oder Transferieren,
3. die hierbei zum Einsatz kommenden informationstechnischen *Systeme* und Geräte, sowie deren Schnittstellen.

An Hand der Verarbeitungsprozesse lassen sich die *Rollen und Motive* der Beteiligten, die Rechtsbeziehungen unter ihnen und die sich ergebenden rechtlichen Anforderungen darstellen. Als handelnde Personen und Beteiligte sind zu nennen:

1. die Betroffenen,
2. die für den Einsatz des Prüfungsgegenstands verantwortlichen Organisationen,
3. Dienstleister, die das Verfahren oder Teile davon im Rahmen einer Auftragsdatenverarbeitung betreiben (z. B. Rechenzentren) oder die an der Verarbeitung beteiligte Systeme und Geräte warten, dies schließt oft auch die Hersteller des Prüfungsgegenstands ein, sowie
4. ggf. Dritte, die im Zuge des Einsatzes des Prüfungsgegenstandes Kenntnis von personenbezogenen Daten nehmen können, beiläufig (z. B. zufällig anwesende, mithörende Dritte) oder beabsichtigt (z. B. Sicherheitsbehörden).

Autoren, die für Organisationen generische PIAs durchführen und entsprechende Berichte anfertigen, sollten für ihre Auftraggeber typische Anwendungsfälle 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 dargelegt werden, wie diese Risiken im Zusammenspiel von Informationssicherheits- und Datenschutzmanagement beherrscht werden können.

5 AUSWEIS DER RISIKEN UND DER EINGENOMMENEN RISIKOPERSPEKTIVE

Die in einem am Datenschutzrecht orientierten PIA betrachteten Risiken müssen aus den rechtlichen Anforderungen heraus abgeleitet sein und vollständig behandelt werden. Dabei ist vornehmlich die Perspektive von Betroffenen einzunehmen, wobei auch mittelbare Auswirkungen zu behandeln sind, die auf Betroffene rückwirken können. Als Risikoquellen sind neben Dritten und unbefugt handelnden Verfahrensanwendern auch die einsetzenden Organisationen selbst zu berücksichtigen.

5.1 ANFORDERUNGEN UND SCHUTZZIELE

Die allgemeinen Datenschutzanforderungen betreffen im Wesentlichen die Legitimität (materielle Rechtmäßigkeit) der Datenverarbeitung, die Vermeidung unerwünschter Ereignisse, welche die Betroffenen in ihrem Persönlichkeitsrecht beeinträchtigen (in Form unmittelbarer Schäden oder unrechtmäßiger Verarbeitung oder Offenbarung ihrer Daten), die Transparenz gegenüber Betroffenen und Aufsichtsbehörden, sowie die Umsetzung der Betroffenenrechte. Alle Aktivitäten, die gegen diese Anforderungen verstoßen, stellen im PIA zu betrachtende Bedrohungen dar.

Die Voraussetzungen für die materielle Rechtmäßigkeit der mit dem Prüfungsgegenstand durchzuführenden Verarbeitung ergeben sich aus den Umständen der Einsatzpraxis, vgl. die Ausführungen zum Nutzungskontext auf Seite 4. Sie liegen in der Regel außerhalb des Prüfungsgegenstandes selbst, können jedoch von seiner Ausgestaltung und der Art und Weise des Einsatzes abhängen.

Besonders deutlich wird dies, wenn beabsichtigt ist, sich auf Einwilligungen der Betroffenen als Rechtsgrundlage zu stützen und Einholung und Management der Einwilligungen durch den Prüfungsgegenstand unterstützt werden. Einwilligungen sind nur als freie, willentliche Entscheidungen auf informierter Grundlage wirksam. Eine PIA muss in dieser Konstellation untersuchen, ob Betroffene im Rahmen des untersuchten Verfahrens die zur Beurteilung der vorgesehenen Erhebung und Verarbeitung relevanten Informationen wahrnehmen, ihren Willen eindeutig und frei Ausdruck geben können (schriftlich, soweit nicht besondere Umstände ein anderes Vorgehen rechtfertigen) und erteilte Einwilligungen einsehen und widerrufen können.

Umgekehrt können sich Bedingungen und Ausmaß der rechtlichen Zulässigkeit einer Verarbeitung im Laufe des Verarbeitungsprozesses ändern, z. B. bei Änderung der Rechtsverhältnisse zwischen den Beteiligten. Entsprechend den Umständen der Einsatzpraxis muss die PIA betrachten, ob derartige Änderungen im Umgang mit dem Prüfungsgegenstand abgebildet werden können.

Es hat sich im Bereich der Informationssicherheit bewährt, Anforderungen als Schutzziele zu formulieren. Auch die über die Wahrung der materiellen Rechtmäßigkeit hinausgehenden datenschutzrechtlichen Anforderungen lassen sich als Schutzziele formulieren, die zugleich in kompakter und methodisch zugänglicher Form die Risiken ausweisen, gegen die es durch angemessene Produkt- und Verfahrens-

gestaltung sowie eigens hierzu ergriffene technische und organisatorische Maßnahmen zu schützen gilt. [2]

Den Risiken der Informationssicherheit werden klassisch durch Sicherung der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit begegnet. Bezogen auf die Verarbeitung personenbezogener Daten lauten sie:

1. Nur Befugte nehmen personenbezogene Daten zur Kenntnis.
2. Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell.
3. Personenbezogene Daten stehen zeitgerecht zur Verfügung und werden ordnungsgemäß verarbeitet.

Folgende Schutzziele sind datenschutzspezifisch:

4. Es werden so wenige personenbezogene Daten wie möglich erhoben und verarbeitet und hierbei an einen so kleinen Kreis von Personen wie möglich bekanntgegeben.
5. Personenbezogene Daten werden nicht für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt.
6. Den Betroffenen ist die Ausübung der ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung wirksam möglich.
7. Die Verarbeitung von personenbezogenen Daten kann anhand aktueller und vollständiger Dokumentation mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden.

In das letztgenannte Schutzziel einbezogen sind die Teilziele:

8. Personenbezogene Daten können ihrem Ursprung zugeordnet werden.
9. Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Für die Schutzziele 4 bis 9 haben sich die Bezeichnungen Datensparsamkeit, Zweckbindung oder auch Nichtverkettbarkeit, Intervenierbarkeit, Transparenz, Authentizität und Revisionsfähigkeit eingebürgert. Für jedes der genannten Schutzziele stehen spezifische Schutzmaßnahmen zur Verfügung, die sowohl bei der Planung als auch bei dem Betrieb des Verfahrens zu berücksichtigen sind.

5.2 SCHUTZPERSPEKTIVE UND RISIKOQUELLEN

Die Einnahme der Schutzperspektive muss ausgewiesen sein: Sind technische Funktionen für Geschäftsprozesse zu schützen oder gilt der Schutz den Betroffenen und dessen Grundrechten in ihrer Rolle als Bürger, Kunde, Patient, Organisationsmitglieder und Beschäftigte?

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 den Angreifer eines Verfahrens bzw. des 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.

[2] Die neueren Datenschutzgesetze der Länder legen durch die Vorgabe von Schutzzielen die Zielrichtung der technischen und organisatorischen Maßnahmen fest, die von den verantwortlichen Stellen zu treffen sind.

Die Organisation, die den Prüfungsgegenstand einsetzt, muss daher in den Gegenstand der Risikoanalyse einbezogen werden. Dies ist bereits bei der Definition und Abgrenzung des Prüfungsgenstandes zu berücksichtigen. Neben den Risiken durch den Gebrauch eines Verfahrens sind auch die strukturell bestehenden Motive seitens der einsetzenden Organisationen zu berücksichtigen. So kann z. B. ein Interesse an der Nutzung einmal erhobener Daten in anderen Kontexten bestehen, das zu einer Durchbrechung der Zweckbindung verleitet. Dazu zählen auch die absehbaren Risiken die entstehen, wenn Sicherheitsbehörden oder marktbeherrschende Unternehmen oder dominante Forschungsinstitute den Prüfungsgegenstand bei Verfahren mit Personenbezug zur Festigung ihres Machtvorteils einsetzen.

Bei großen Prüfungsgegenständen bzw. bei Produkten mit infrastrukturellem Charakter (Beispiele: Mautsystem, Geldkarte, Kreditkarte, IT von Kraftfahrzeugen, Smart-Meter, Verwaltungsverfahren, Abrechnungssystem) sind darüber hinaus die absehbaren negativen Rückwirkungen auf Betroffene auch dann zu beachten und darzulegen, wenn sie außerhalb des Kontexts des bilateralen Verhältnisses einer Organisation, die den Prüfungsgegenstand oder eine Komponente davon einsetzt, und einem Betroffenen liegen. Dies ist erfahrungsgemäß u. a. dann relevant, wenn anonymisierte Daten ohne Zweckbindungsschutz ausgewertet werden sollen, deren Personenbezug durch Kontextualisierung bzw. durch Hinzuziehen anderer Datenbestände wieder hergestellt werden könnte.

6 AUSWEIS DES SCHUTZBEDARFES

Damit Schutzmaßnahmen für die weitergehenden Schutzziele entsprechend der rechtlichen Abwägungen angemessen ausgewählt und in einem PIA beurteilt werden können, empfiehlt es sich methodisch, zunächst die Daten zu typisieren, die mit dem Prüfungsgegenstand erhoben, erzeugt bzw. verarbeitet werden und dann deren Schutzbedarf festzulegen. Die Einstufung darf hierbei nicht allein abstrakt erfolgen, sondern muss die Spezifika der Einsatzpraxis berücksichtigen.

Als hinreichend differenziert hat sich eine dreistufige Kategorisierung des Schutzbedarfs in die Klassen „normal", „hoch" und „sehr hoch" erwiesen[3]:

> *Normal:* Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht zu heilen. Der Bedarf, personenbezogenen Daten gegen jedwede unrechtmäßige Verarbeitung zu schützen, ist mindestens in diese Kategorie einzuordnen.
>
> *Hoch:* Die Schadensauswirkungen werden von den 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 hierfür auf externe Hilfe angewiesen ist.
>
> *Sehr hoch:* Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches Ausmaß für die Betroffenen an.[4]

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

[4] 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

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, wenn auch nicht existenzbedrohlichen Schäden führt.

7 AUSWEIS DER SCHUTZMASSNAHMEN

In Bezug auf die Sicherung der Schutzziele der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) lassen sich die Maßnahmenkataloge des BSI-Grundschutz-Katalogs (BSI 2008) sowie des ISO-Standards 27002 heranziehen, unter Beachtung der bereits erwähnten Einschränkung, dass dabei die Risikoperspektive auf die der Betroffenen anzupassen ist.

Generische Schutzmaßnahmen des Datenschutzes zur Umsetzung der in Abschnitt 5.1 aufgeführten Schutzziele sind u. a.:[5]

Zur Gewährleistung der Datensparsamkeit: In der Gestaltungsphase des Verfahrens: Einschränkung der Datenerhebung auf das minimale erforderliche Maß. In der Betriebsphase: Dezentrale Datenhaltung, Pseudonymisierung und Anonymisierung, privacy preserving data mining, frühestmögliches Löschen von Daten.

Zur Sicherung der Transparenz, Revisionsfähigkeit und Authentizität: 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. Wirksame Methoden zur Feststellung unrechtmäßiger Kenntniserlangung durch Dritte oder nicht autorisierte Beschäftigte und angemessener Reaktion auf derartige Vorfälle einschließlich der ggf. erforderlichen Information an Aufsichtsbehörden und Betroffene. Bereitstellung spezifischer Information über den Prüfungsgegenstand und die aus seinem Einsatz entstehenden Risiken für einzelne Betroffene und zum Abruf durch die Allgemeinheit. Effektive Verfahren zur Erstellung von kompletten Aufstellungen der Daten, die sich auf einen Betroffenen beziehen, zum Zweck der Auskunft an diese.

Zur Gewährleistung von Zweckbindung bzw. Nichtverkettbarkeit: Kennzeichnung von Daten in Bezug auf die Zwecke, zu deren Erfüllung sie zur Verfügung stehen, Trennung von Datenbeständen (physisch oder logisch), zweck-, prozess- und betroffenenorientierte Rollen- und Rechtekonzepte, informationelle Gewaltentrennung, Verwendung verfahrensspezifischer Pseudonyme.

Zur Sicherung der Intervenierbarkeit: Verständliche Kommunikation der ihnen zustehenden Rechte an die Betroffenen. Benennung kompetenter und entscheidungsbefugter Ansprechpartner, die für

[5] In Bezug auf die Sicherung der für den Datenschutz spezifischen Schutzziele wird derzeit unter den deutschen Aufsichtsinstanzen an einem abgestimmten Katalog zu regelmäßig zu ergreifenden 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 Informationssicherheit und des Datenschutzes ihrerseits personenbezogene Verfahren sein können, die entsprechend zu gestalten sind. Dies gilt insbesondere für die Protokollierung der Aktivitäten von Mitarbeitern.

eine Durchsetzung dieser Rechte innerhalb der involvierten Organisationen sorgen können. Operativer Zugriff der Betroffenen auf ihre Daten einschließlich des Status ihrer Bearbeitung und auf die von ihnen erteilten Einverständniserklärungen. Bereitstellung von Verfahren, erteilte Erklärungen zurückzuziehen. Voraussetzung der Effektivität dieser Maßnahmen sind Standardprozesse des Change Managements.

Die vorgesehenen Maßnahmen sind stets seitens jeder Organisation, die am Einsatz des Prüfungsgegenstands beteiligt ist, im Rahmen ihres Datenschutzmanagements auf Wirksamkeit hin zu kontrollieren.[6]

8 ZUSAMMENFASSUNG

Ein datenschutzrechtlich relevantes Privacy Impact Assessment zeichnet sich dadurch aus, dass es folgendes ausweist:

1. die Methodik und den Zweck des Assessments,
2. den Prüfungsgegenstand und den Nutzungskontext,
3. die Voraussetzungen der materiellen Rechtmäßigkeit der Anwendung des Prüfungsgegenstandes,
4. die Risiken der Anwendung unter Berücksichtigung der Schutzziele der IT-Sicherheit und des Datenschutzes,
5. die vorgesehenen Maßnahmen zur Gewährleistung der Rechtmäßigkeit und Begrenzung der Risiken.

Datenschutzrechtlich relevante Aussagen in Bezug auf die Risiken und deren Bearbeitung können nur vorgenommen werden, wenn der Prüfungsgegenstand in seinen Verfahrenszusammenhang gestellt wird.

Drei Anmerkungen zum Schluss:

Allein die Existenz eines PIA enthebt eine Datenschutzaufsichtsbehörde nicht der Aufgabe, das analysierte Verfahren auf Rechtskonformität zu prüfen.

Liegen eine gesetzliche Ermächtigung für oder eine Einwilligung in ein Verfahren vor, so bedeutet das nicht, dass keine Risiken mehr für die Privatsphäre der Betroffenen ausgehen. Im Gegenteil: Dass eine personenbezogene Datenverarbeitung einer Rechtsgrundlage bedarf, zeigt, dass Risiken bestehen.

Anders als bei festgestellten Risiken der Informationssicherheit ist es aus einer grundrechtlichen Perspektive heraus nicht zu legitimieren, wenn wesentliche Risiken für die Betroffenen als Dritte seitens einer datenverarbeitenden Organisation in Kauf genommen werden. Wenn die Risiken nicht wirksam und in ausreichendem Maß verringert werden können, muss vom Einsatz des Prüfungsgegenstandes abgesehen werden.

[6] Ein Entwurf zu einem Datenschutzmanagementsystem, das sich am Schutzzielkonzept des Datenschutzes und methodisch an die ISO 27001 anlehnt findet sich bei Rost (Rost 2013).

9 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_Guideline_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 1. 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, 35. 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, 36. 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.): *Privacy Impact Assessment*. Springer-Verlag, 2012.