forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Ein Werkzeug für einen besseren Datenschutz

White Paper

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Ein Werkzeug für einen besseren Datenschutz

Autorinnen und Autoren:
Michael Friedewald[1], Hannah Obersteller[2], Maxi Nebel[3], Felix Bieker[2], Martin Rost[2]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
(3) Universität Kassel, Institut für Wirtschaftsrecht

Herausgeber:
Peter Zoche, Regina Ammicht Quinn, Michael Friedewald, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

1 Einleitung 5

2 Datenschutz-Folgenabschätzungen – Entwicklung und gegenwärtige Praxis 7

2.1 Begriffsbestimmung 7

2.2 Folgenabschätzungen in den Bundes- und Landes-gesetzen Deutschlands 8

2.3 Angelsächsischer Rechtsraum 9

2.4 PIA in der Europäischen Union 10

2.4.1 Großbritannien: Der „Privacy Impact Assessment Code of Practice" des Information Commissioner's Office 10

2.4.2 Frankreich: Das „Privacy Impact Assessment" der Commission Nationale de l'Informatique et des Libertés 11

2.4.3 EU-Rahmen für Datenschutz-Folgenabschätzungen bei RFID-Anwendungen und Smart Meters Cloud Computing 12

3 Datenschutz-Folgenabschätzungen in der EU-Datenschutz-Grundverordnung 14

3.1 Gründe für die Durchführung einer Datenschutz- Folgenabschätzung 14

3.2 Anforderungen an eine Datenschutz-Folgenabschätzung 15

3.3 Risikoansatz vs. Grundrechtsgewährleistung 17

4 Elemente eines Prozesses zur Datenschutz-Folgenabschätzung 19

4.1 Vorbereitungsphase 20

4.1.1 Relevanzschwelle 20

4.1.2 Prüfplanung 20

4.1.3 Was wird betrachtet? 22

4.1.4 Wer sind die beteiligten Akteure? 23

4.1.5 Identifikation der maßgeblichen Rechtsgrundlagen 23

4.1.6 Dokumentation der Problem- und Aufgabendefinition 24

4.2 Bewertungsphase 24

4.2.1 Identifikation von Schutzzielen 24

4.2.2 Identifikation von möglichen Angreifern, Angriffsmotiven und -zielen 25

4.2.3 Identifikation von Bewertungskriterien und -maßstäben 26

4.2.4 Bewertung des Risikos 27

4.3 Bewertungsphase – ein alternatives Verfahren für wissenschaftliche Datenschutz-Folgenabschätzungen 29

4.4 Schutzmaßnahmen, Veröffentlichung und Überprüfung 31

4.4.1 Identifikation und Implementierung passender Schutzmaßnahmen 31

4.4.2 Dokumentation und Veröffentlichung des Ergebnisberichts 32

4.4.3 Unabhängige Prüfung der Prüfergebnisse 32

4.4.4 Überwachung und Fortschreibung 33

5 Diskussion – Was kann eine Datenschutz-Folgenabschätzung leisten? 34

Anmerkungen 36

Abkürzungsverzeichnis 44

1 Einleitung

Wir leben in einer zunehmend digitalisierten und vernetzten Welt. Viele privatwirtschaftliche und staatliche Angebote werden durch Angebote im Internet ergänzt oder gar ersetzt. Diese Angebote gehen überwiegend mit der Sammlung personenbezogener Daten einher. Die Spielregeln hierfür definieren vor allem die anbietenden Organisationen, während die Nutzer* meist nur entscheiden können, ob sie die Angebote nach diesen Regeln oder gar nicht nutzen wollen. Technik, mit der die Sammlung und Auswertung von Daten automatisiert und über breitbandige Netzwerke in alle Welt übermittelt werden kann, hat diese Machtasymmetrie weiter verstärkt. Dieser Zusammenhang und die Auswirkungen auf die Privatheit und Grundrechte sind den meisten Bürgern meist nur schemenhaft bewusst, obwohl die Medien bereits seit Jahren über „Datenpannen" und staatliche Überwachung berichten.[1]

Der Datenschutz thematisiert diese Machtasymmetrie zwischen Organisationen und Individuen und hat die Aufgabe, die Betroffenenrechte zu gewährleisten. Dabei wird zunächst jede Organisation als potenzieller Angreifer[2] auf die Rechte des Individuums als strukturell schwächeren Risikonehmer betrachtet, dessen faktisch notorische Übergriffe abgewehrt werden müssen.[3]

Definition:

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum in dessen unterschiedlichen Rollen (als Bürger, Kunde, Patient etc.) durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht.

Ziel einer DSFA ist es, Kriterien des operationalisierten Grundrechtsschutzes zu definieren, die Folgen von Datenverarbeitungspraktiken möglichst umfassend zu erfassen sowie objektiv und nachvollziehbar mit Blick auf die verschiedenen Rollen und damit verbundenen Interessen so zu bewerten, dass typischen Angriffen durch Organisationen mit adäquaten Gegenmaßnahmen begegnet werden kann.

Dass eine Folgenabschätzung vor dem Einsatz einer bestimmten Technologie, oder gar vor deren Entwicklung, sinnvoll ist, hat sich seit den 1960er Jahren unter dem Begriff der „Technikfolgenabschätzung" (TA) weitgehend durchgesetzt – allerdings zunächst vor allem mit Blick auf Folgen für Gesundheit und Umwelt. Die Ausweitung auf Fragen des Datenschutzes hat erst sehr viel später begonnen. Im Rahmen der Reform der Datenschutzvorschriften in der EU wurde die Idee aufgegriffen, Technikfolgen auch für das Recht auf Achtung des Privatlebens (Art. 7 Charta der Grundrechte der Europäischen Union; Charta) und den Schutz personenbezogener Daten (Art. 8 Charta) abzuschätzen. So wird es mit der Anwendbarkeit (Mai 2018) der Vorschriften der europäischen Datenschutz-Grundverordnung (DS-GVO)[4] unter bestimmten Bedingungen verpflichtend sein, eine DSFA durchzuführen.

Der Text der DS-GVO lässt freilich weitgehend offen, wie und nach welchen Kriterien eine solche DSFA durchzuführen ist. Es ist zu erwarten, dass nach Verabschiedung der DS-GVO rasch Modelle für die Durchführung einer DSFA vorgelegt werden. Dabei wird voraussichtlich auf Vorschläge zurückgegriffen werden, die in den vergangenen Jahren

* Aus Gründen der Lesbarkeit wird im Folgenden auf das Gendern von Personengruppen verzichtet. Die Verwendung des generischen Maskulinums schließt ausdrücklich alle Geschlechterformen mit ein.

in verschiedenen EU-Mitgliedstaaten, von staatlichen wie privatwirtschaftlichen Akteuren, für spezielle Datenverarbeitungen entwickelt wurden.

Mit diesem White Paper soll eine erste grundlegende Information für alle Akteure bereitgestellt werden, die sich in Kürze aus unterschiedlicher Perspektive mit dem Thema DSFA beschäftigen müssen:

- *Politische Entscheider* und *Datenschutzbehörden* sind gefordert zu definieren, welche Anforderungen an einen DSFA-Prozess gestellt werden.
- *Datenschutzbehörden* und *Datenschutzbeauftrage* müssen sich damit auseinandersetzen, wie das neue Instrument in ihre tägliche Arbeit integriert und produktiv für den Schutz der Betroffenen eingesetzt werden kann.
- *Forscher*, *Komponentenentwickler*, *Systemaggregatoren* sowie *Datenverarbeiter* müssen sich Klarheit darüber verschaffen, welche neuen Anforderungen auf sie zukommen, wie sie diesen gerecht werden können und wie sie ihre Tätigkeit ggf. ändern müssen.

Es soll dabei dafür geworben werden, die DSFA nicht nur als gesetzlich vorgeschriebene Pflichtaufgabe zu verstehen, derer man sich mit möglichst geringem Aufwand „entledigt". Sie soll vielmehr als Instrument vorgestellt werden, das hilft, ungewollte Datenschutzrisiken zu erkennen und im Sinne von „Privacy by Design" zu vermeiden. Damit können Organisationen nicht nur sicher sein, alle rechtlichen Anforderungen zu erfüllen, sondern auch damit werben, aktiv und nachvollziehbar die Interessen der Betroffenen zu schützen. Über eine Zertifizierung oder ein Datenschutzsiegel kann sich dies zu einem Wettbewerbsvorteil entwickeln.

2 Datenschutz-Folgenabschätzungen – Entwicklung und gegenwärtige Praxis

Mit dem Fortschritt insbesondere elektronischer Datenverarbeitungstechnologien und dem Aufkommen immer größerer Mengen personenbezogener Daten hat sich bereits seit frühester Zeit die Frage gestellt, wie die Folgen, die diese Technisierung auf die Persönlichkeitsrechte der Betroffenen und anderer Verfassungsziele wie Demokratie und Gewaltenteilung hat, systematisch analysiert und entsprechende Handlungsmaßnahmen ergriffen werden können. Hierzu werden sogenannte Folgenabschätzungen durchgeführt. Auch einige Rechtsordnungen haben sich in der Vergangenheit bereits mit dieser Frage beschäftigt. Der folgende Abschnitt erläutert kurz die Unterschiede der verschiedenen Begriffe sowie die Anfänge und Ausprägungen der sogenannten Privacy Impact Assessments (PIA) und Folgenabschätzungen.

2.1 Begriffsbestimmung

Folgenabschätzungen blicken auf eine lange Geschichte zurück. Erste Anfänge lassen sich bereits in den 1960er Jahren ausmachen, als Technologien zunehmend komplex wurden und damit potenzielle negative Auswirkungen auf Umwelt und Gesellschaft stiegen. Im Bereich der Informations- und Kommunikationstechnologien finden sich vorrangig die Begriffe Technikfolgenabschätzung, Datenschutz-Folgenabschätzung und Privacy Impact Assessment.

Technikfolgenabschätzung ist eine Wissenschaftsdisziplin, die sich mit dem wissenschaftlich-technischen Fortschritt und dessen Folgewirkungen auf die Gesellschaft und das Recht beschäftigt. Technikfolgenabschätzung hat eine zukunftsorientierte Technikanalyse und -bewertung zum Gegenstand.[5] Die Chancen und Risiken der Technik für die Gesellschaft sowie deren Akzeptanz werden unter einem ganzheitlichen und damit interdisziplinären Winkel erforscht und zum Beispiel durch verfassungs-, sozial-, oder umweltverträgliche Technikgestaltung methodisch gesteuert, so dass zum einen technische Sachzwänge vermieden, aber auch kumulative Folgewirkungen besser abgeschätzt werden können.[6] Bereits in den 1970er Jahren wurde Technikfolgenabschätzung in parlamentarischen Beratungsgremien institutionalisiert. Dies geschah zuerst 1973 in den USA, wo das *Office of Technology Assessment* (OTA) den US-amerikanischen Kongress beriet.[7] Es folgten weltweite Nachfolger, etwa das *Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag* (TAB),[8] das zusammen mit anderen parlamentarischen Beratungsgremien europaweit vernetzt ist.[9] Spezielle Ausprägungen der Technikfolgenabschätzung gibt es überdies im Gesundheitssektor (Health Technology Assessment)[10] sowie im Bereich der Privatwirtschaft.[11]

Wissenschaftliche Technikfolgenabschätzung hat in Deutschland eine lange Tradition. Bereits mit der kommerziellen Nutzung der Atomenergie stellte sich die Frage, welche Auswirkungen für die Gesellschaft zu erwarten seien.[12] Seit den 1990er Jahren werden Technikfolgenabschätzungen zunehmend auch für den Bereich der Informations- und Kommunikationstechnologien durchgeführt. Dabei geht es um die prospektive Bewertung der zu erwartenden Auswirkungen mit dem Ziel einer gesellschaftsverträglichen Technikgestaltung.[13]

Demgegenüber fokussieren sich Datenschutz-Folgenabschätzungen im engeren Sinne (s. u.) auf die Bewertung konkreter Datenverarbeitungsvorgänge. Sie sind häufig in gesetzlichen Bestimmungen oder behördlichen Empfehlungen niedergelegt und werden im Folgenden näher erläutert.

2.2 Folgenabschätzungen in den Bundes- und Landesgesetzen Deutschlands

Bereits seit den Anfängen der Datenschutzgesetzgebung in Deutschland waren Datenschutz-Folgenabschätzungen vorgesehen. Sie firmierten zwar nicht unter dieser Bezeichnung, waren aber als Institution angelegt. Als Prüfungsmaßstab der Folgenabschätzung diente der Gesetzeszweck. Zweck des Gesetzes war nicht nur der Schutz des Menschen vor Missbrauch seiner personenbezogenen Daten,[14] sondern galt darüber hinaus dem Schutz des verfassungsmäßigen Gefüges des Staates vor einer Veränderung durch automatisierte Datenverarbeitung.[15] Der Verantwortliche* hatte hierzu sicherzustellen, dass die vorgegebenen Ziele durch technische und organisatorische Maßnahmen eingehalten wurden.[16] § 7 Abs. 3 Niedersächsisches Datenschutzgesetz (NDSG 1993) schrieb beispielsweise ausdrücklich vor, dass automatisierte Datenverarbeitung nicht ohne umfassende Prüfung der Auswirkungen auf die Rechte der Betroffenen und Wirkmöglichkeiten der Verfassungsorgane zum Einsatz gelangen darf.

Im Zuge verschiedener Gesetzgebungsnovellen erfolgten umfangreiche Änderungen der gesetzlichen Zielbestimmungen. Während die Fraktion Bündnis 90/Die Grünen in ihrem Entwurf eines neuen Bundesdatenschutzgesetzes (BDSG)[17] noch eine Vorabkontrolle im Umfang einer Technikfolgenabschätzung[18] vorsah und der Zweck des Gesetzes im Bundesdatenschutzgesetz von 1978 noch der Schutz der Grundrechte war, fanden diese Vorschläge im Zuge der Gesetzesnovellierungen des Bundesdatenschutzgesetzes in den 1990er Jahren keinen Anklang; das neu gestaltete Bundesdatenschutzgesetz 2003 trug der Technikfolgenabschätzung keine Rechnung. Der Zweck des Gesetzes wurde auf den Schutz des Persönlichkeitsrechts[19] bzw. der informationellen Selbstbestimmung[20] reduziert. Statt einer umfassenden Technikfolgenabschätzung verpflichteten Landes- und Bundesdatenschutzgesetze lediglich den Verantwortlichen selbst dazu, technische und organisatorische Maßnahmen zu ergreifen, um Datensicherheit zu gewährleisten und so die informationelle Selbstbestimmung der Betroffenen zu wahren.[21] Selbst § 7 Abs. 3 NDSG 2002 reduzierte den Prüfungsmaßstab für die vorgesehene Technikfolgenabschätzung nur noch auf mögliche Gefahren für Rechte der Betroffenen. Die Auswirkungen auf Verfassungsorgane und damit zusammenhängende gesamtgesellschaftliche Gefahren, etwa für die demokratische Willensbildung, blieben nunmehr außer Betracht.

Daneben wurden neue Vorschriften eingeführt, die eine Technikfolgenabschätzung gleichwohl inhaltlich nicht ersetzen. So fordert § 4d Abs. 5 BDSG zwar eine Vorabkontrolle des Verfahrens.[22] Dadurch sollen besondere Risiken für die Rechte und Freiheiten der betroffenen Person durch automatisierte Verfahren identifiziert werden.[23] Auch diese Prüfung obliegt jedoch nicht einer unabhängigen Instanz, sondern dem Verantwortlichen selbst. Die Vorschrift geht auf Art. 20 Datenschutzrichtlinie (DSRL)[24] zurück; darin wird ein grundsätzlich weites Verständnis von „spezifischen Risiken für die Rechte und Freiheiten" zugrunde gelegt,[25] überlässt den Mitgliedstaaten bei der Umsetzung allerdings einen großen Handlungsspielraum. Die Umsetzung in § 4d Abs. 5 BDSG legt nahe, dass spezifische Risiken nur in besonderen Verarbeitungssituationen angenommen werden; § 4d Abs. 5 BDSG nennt die Verarbeitung besonderer personenbezogener Daten nach § 3 Abs. 9 BDSG sowie Datenverarbeitung zur Profilbildung. Selbst in

* Anstelle des in der bisherigen Datenschutzgesetzgebung in Deutschland bekannten Begriffs „Verantwortliche Stelle" für jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, verwendet die DS-GVO den Begriff „Verantwortlicher".

diesen Fällen sind jedoch weitreichende Rückausnahmen vorgesehen, wenn eine gesetzliche Pflicht oder Einwilligung des Betroffenen zur Datenverarbeitung besteht. Die Pflicht zur Vorabkontrolle besteht damit nur eingeschränkt; zudem ist die Prüfung lediglich auf das konkrete Verfahren beschränkt und erstreckt sich nicht auf die Entwicklung und Gestaltung eines Systems im Allgemeinen.[26] Dadurch fehlt es auch an einer Gesamtbetrachtung der Auswirkungen einer technologischen Entwicklung auf die verfassungsrechtlichen Schutzgüter. Unter diesen Voraussetzungen kommt der Vorabkontrolle statt einer Gestaltungswirkung eher eine Beanstandungswirkung zu, da diese erst vorgesehen ist, wenn das System bereits etabliert und einsatzfertig ist.[27]

Statt einer Vorabkontrolle sieht zum Beispiel § 6 Abs. 1 Nr. 11 in Verbindung mit § 7 Abs. 6 Satz 3 Hessisches Datenschutzgesetz (HDSG) lediglich vor, Auswirkungen eines Verfahrens[28] auf die Rechte der Betroffenen im Sinne des § 1 Abs. 1 Nr. 1 HDSG zu prüfen und das Ergebnis in einem Verfahrensverzeichnis niederzulegen. Dieser Prüfung kommt keine vergleichbare Wirkung wie eine Folgenabschätzung zu, da sie sich nur auf bestimmte Datenverarbeitungsvorgänge und Verantwortliche beschränkt sowie auf die Risiken, die direkt mit den Rechten der Betroffenen verbunden sind, nicht jedoch den größeren Gesamtzusammenhang in den Blick nimmt.

Festhalten lässt sich, dass die Technikfolgenabschätzung in der deutschen Gesetzgebung hoffnungsvoll begonnen hat, durch verschiedene Gesetzgebungsnovellen jedoch bis zur Unkenntlichkeit verwässert wurde. Die geltenden gesetzlichen Vorschriften sehen allenfalls Datenschutz-Folgenabschätzungen in begrenztem Maße vor. Da jeder Verantwortliche selbst zur Durchführung der Datenschutz-Folgenabschätzung für die von ihm konkret durchgeführten Datenverarbeitungsvorgänge verpflichtet ist, bleiben insbesondere kumulative Wirkungen auf Persönlichkeitsrechte und andere Verfassungsziele, die sich aus dem Zusammenspiel verschiedener Technologien ergeben können, außer Betracht. Vorgaben, die eine unabhängige, nicht von Einzelinteressen geleitete Technikfolgenabschätzung mit Blick auf übergeordnete Verfassungsziele zum Ziel haben, fehlen indes.

2.3 Angelsächsischer Rechtsraum

Im angelsächsischen Rechtsraum, genauer in Kanada, fanden Ansätze zu einem PIA bereits in den 1970er Jahren das erste Mal Erwähnung.[29] Erste behördliche Stellungnahmen und Empfehlungen zum Einsatz eines Privacy Impact Assessments wurden allerdings erst Mitte der 1990er Jahre abgegeben, 1996 durch die US-amerikanische Steuerbehörde sowie 1999 durch die kanadische Verwaltungsbehörde.[30] Infolgedessen erschienen in mehreren Ländern des angelsächsischen Rechtskreises Handreichungen zur Durchführung eines Privacy Impact Assessments, unter anderem in Kanada im Jahre 2002,[31] in Neuseeland erstmals 2002,[32] in den USA im Jahre 2004[33] und in Australien 2006.[34] In Europa erließ die britische Regierung im Dezember 2007 ein Handbuch zu Privacy Impact Assessments.[35]

Trotz der Verbreitung quer durch den angelsächsischen Rechtsraum herrscht allerdings kein einheitliches Verständnis über die Methode „Privacy Impact Assessment". Zwar weisen die Empfehlungen einige Gemeinsamkeiten etwa hinsichtlich des Prüfungsgegenstands „privacy" und des Ziels der Risikovorsorge auf, unterscheiden sich aber doch in speziellen Aspekten.[36] So stellt jedes Land eigene Anforderungen an die Umsetzung eines Privacy Impact Assessments. Viele Länder verstehen darunter zudem keinen interdisziplinären Ansatz, in dem neben Technologieexperten weitere Expertisen einfließen. Auch wird ein PIA nicht immer als Prozess verstanden, der die Technik begleitet, sondern nur als abschließende Evaluation vor Inbetriebnahme einer Technologie. Nur selten ist ein PIA gesetzlich vorgeschrieben; häufig handelt es sich lediglich um Empfehlungen, denen jedoch Kontroll- und Durchsetzungsmechanismen fehlen. Überdies richten sich diese Gesetze oder Empfehlungen nicht immer an öffentliche und nicht-öffentliche Verantwortliche, sondern verpflichten nur öffentliche Stellen, also Behör-

den, beim Einsatz von Datenverarbeitungsanlagen. Schließlich werden kaum Kontrollen durch unabhängige Dritte vorgeschrieben; meist werden lediglich die Verantwortlichen selbst verpflichtet.[37]

Zusammenfassend ist festzustellen, dass PIAs im angelsächsischen Raum bereits seit Mitte der 1990er Jahre vielfach Erwähnung gefunden hat. Allerdings verbergen sich dahinter weder eine einheitliche Methode noch einheitliche Anforderungen an die Umsetzung. In jedem Fall beschränkt sich Privacy Impact Assessment jedoch auf die Prüfung von Auswirkungen spezifischer datenverarbeitender Projekte, Programme, Produkte oder Dienstleistungen auf „privacy" und den Schutz personenbezogener Daten, ohne übergeordnete Auswirkungen auf die gesellschaftliche Ordnung und andere Rechtsgüter mit in den Blick zu nehmen.

2.4 PIA in der Europäischen Union

2.4.1 Großbritannien: Der „Privacy Impact Assessment Code of Practice" des Information Commissioner's Office

Die britische Datenschutzaufsichtsbehörde *Information Commissioner's Office* (ICO) hat ein eigenes generisches, d. h. nicht nur auf eine Technologie anwendbares, PIA-Modell entwickelt. In dem 2014 veröffentlichten Handbuch „Conducting privacy impact assessments – code of practice"[38] des ICO wird ein PIA als Prozess definiert, der einer Organisation hilft, die Risiken eines Projektes für die Privatheit zu identifizieren und zu reduzieren.

Laut ICO ist ein effektives PIA während der gesamten Entwicklung und Umsetzung eines Projektes im Rahmen etablierter Projektmanagementprozesse anzuwenden. Die Organisation kann so systematisch und umfassend analysieren, welche Auswirkungen ein bestimmtes Projekt oder System auf die Privatheit der Betroffenen hat. „Projekt" ist hierbei als jeder Plan oder Vorschlag innerhalb einer Organisation zu verstehen.[39] Um das Konzept des Datenschutzes durch Technikgestaltung („Privacy by Design") bestmöglich umzusetzen, ist ein PIA so früh wie möglich durchzuführen, wozu das ICO sechs Phasen vorschlägt:

1. Zunächst ist die Notwendigkeit eines PIA zu prüfen. Dabei betont das ICO, dass der Umfang eines PIA variieren kann. Dies hängt insbesondere davon ab, inwieweit sensible persönliche Daten verarbeitet werden oder wie viel Personal und Ressourcen zur Verfügung stehen.[40]
2. Im Anschluss sollen die Datenflüsse von der Erhebung, Speicherung und Nutzung bis zur Löschung sowie die Zugangsrechte beschrieben werden.[41]
3. Sodann können Risiken für die Privatheit sowie ihre Lösungen identifiziert werden. Als Risiken führt das ICO solche für die Privatheit von Individuen und Compliance sowie andere Risiken für die Organisation selbst auf.
4. Beim Zugang Unbefugter oder der Nutzerüberwachung drohen nicht nur dem Individuum Schaden, sondern die Organisation setzt sich auch Haftungsrisiken aus.[42]
5. Die Organisation soll im nächsten Schritt Lösungen für die identifizierten Risiken erarbeiten, etwa die Vermeidung von Datenerhebungen, die Schulung von Mitarbeitern im Umgang mit personenbezogenen Daten oder die Umsetzung technischer Sicherheitsmaßnahmen zum Schutz der Daten.[43] Dabei soll nach einem dreistufigen Schema beurteilt werden, ob das Risiko dadurch beseitigt, verkleinert oder akzeptiert wird, wobei der Nutzen von Maßnahmen auch mit deren Kosten in Relation gesetzt werden darf.[44] Das ICO betont aber die Notwendigkeit der vollständigen Einhaltung der rechtlichen Anforderungen vor der Umsetzung des Projekts.[45]
6. Abschließend sollen die Ergebnisse gesichert und in den Projektplan eingearbeitet werden.[46]

Während all dieser Phasen unterstreicht das ICO die wichtige Rolle interner sowie externer Konsultationen. Bei der internen Konsultation geht es darum, alle Ebenen des Projekts vom Beschaffungswesen und der IT, bis in das Management einzubinden.[47] Bei den externen Konsultationen geht es um eine Einbindung der Betroffenen, um ihre Rechte und eine transparente Datenverarbeitung zu gewährleisten.[48]

2.4.2 Frankreich: Das „Privacy Impact Assessment" der Commission Nationale de l'Informatique et des Libertés

Die *Commission Nationale de l'Informatique et des Libertés* (CNIL) ist die französische Behörde für Datenschutz und Informationsfreiheit. Auch sie hat sich wiederholt mit den Anforderungen an ein PIA beschäftigt und gibt in aktuell drei Dokumenten Empfehlungen hinsichtlich Methodologie[49], Maßnahmen[50] und sog. „good practices"[51] zum Umgang mit Datenschutzrisiken, insbesondere Risiken für die (Freiheits-)Rechte der Betroffenen.

Einleitend führt die CNIL in ihrem im Sommer 2015 veröffentlichten Dokument zur Methodologie eines PIA aus, dass fundamentale Prinzipien und Rechte unabhängig von Art, Schwere oder Wahrscheinlichkeit eines Risikos unverzichtbar seien und nicht abdingbar. Bei einem PIA geht es demnach darum, mittels technischer und organisatorischer Kontrollen Risiken, die für die Betroffenenrechte bestehen, zu begegnen. Das Dokument richtet sich in erster Linie an alle Verantwortlichen (als Haftungspflichtige), sowie an Produktentwickler, die dem Ansatz des Datenschutzes durch Technik („Privacy by Design") folgen wollen.

Die CNIL beschreibt ihren PIA-Prozess als Kreislauf, der kontinuierlich wiederholt werden muss: Zunächst ist der Zusammenhang, in dem personenbezogene Daten verarbeitet werden, zu definieren und beschreiben. Es sind insbesondere die Zwecke, Beteiligten, personenbezogenen Daten (Kategorien), der Prozess und Hilfsmittel zu benennen.

Dann müssen existierende oder geplante Kontrollmechanismen betrachtet werden, um eine Einhaltung der Datenschutzgesetze und die Verhältnismäßigkeit zu gewährleisten. Der rechtlichen Überprüfung unterliegen hierbei insbesondere Zweck, Information der Betroffenen und Gewährleistung der Rechte der Betroffenen. Daneben ist zu überprüfen, ob und wie geplant ist, Risiken im Hinblick auf den Umgang mit personenbezogenen Daten zu begegnen. Angesprochen sind hiermit insbesondere organisatorische Maßnahmen, Datensicherheits- und Zugangskontrollmaßnahmen.

Im Anschluss sind die Datenschutzrisiken einzuschätzen, um sicherzustellen, dass ihnen in geeigneter Weise begegnet wird. Dazu müssen zunächst die Risikoquellen („wer" und „wieso") ausgemacht werden. Dann ist festzustellen, welche Handlungen/Unterlassungen/Umstände genau eintreten könnten, wie, bzw. wie schwer diese jeweils die Persönlichkeitsrechte der Betroffenen verletzen würden und inwiefern eine Bedrohung im Zusammenhang mit den konkret verwendeten (technischen) Hilfsmitteln liegen kann. Aus Schwere und Wahrscheinlichkeit des Eintritts des Ereignisses bzw. der Bedrohung sind die individuellen Risiken zu ermitteln. Über die identifizierten Risiken, geordnet nach ihrer Schwere, ist eine Übersicht zu erstellen.

Schließlich ist eine Entscheidung zu treffen, die das geplante (bzw. bestehende und durch das PIA nur überprüfte) Vorgehen bestätigt oder die dazu auffordert, die vorangegangenen Schritte zu wiederholen. Ergibt die Evaluation, dass das Ergebnis zufriedenstellend ist, muss ein Umsetzungsplan erstellt und beschlossen werden. Wenn nicht, müssen die Ziele, deren Behandlung als nicht zufriedenstellend befunden wurde, (neu) betrachtet werden.

Jedenfalls ist bei signifikanten Änderungen des Zusammenhangs, der Kontrollmaßnahmen, der Risiken etc. der Prozess zu wiederholen. Im Übrigen aber ist dies in regelmäßigen Abständen erforderlich, um Veränderungen bemerken zu können.

Über die Durchführung des PIAs ist zudem ein Report anzufertigen, der (auf Anfrage) der zuständigen Datenschutzbehörde zur Verfügung gestellt werden muss. Der Report soll den fraglichen Datenverarbeitungsvorgang beschreiben, Rahmen, rechtliche und Risikokontrollmaßnahmen sowie eine Darstellung der Risiken enthalten und die nach dem PIA gefallene Entscheidung dokumentieren. Im Anhang sollen sich detaillierte Beschreibungen dieser Punkte und der Umsetzungsplan befinden.

2.4.3 EU-Rahmen für Datenschutz-Folgenabschätzungen bei RFID-Anwendungen und Smart Meters Cloud Computing

Trotz der fehlenden Pflicht zur Durchführung einer DSFA, verabschiedete die Europäische Kommission Empfehlungen im Zusammenhang mit der Einführung neuer Technologien wie RFID (RFID-Empfehlung)[52] und Smart Meters (Smart Meters-Empfehlung)[53], die die Durchführung einer DSFA durch die Unternehmen und die Bereitstellung der Ergebnisse an die nationalen Datenschutzbehörden fordern. Die Ergebnisse der auf diesen Empfehlungen basierenden Vorschläge wurden jeweils von der Artikel-29-Datenschutzgruppe kritisch beurteilt, wobei diese auch erstmals allgemeine Anforderungen an DSFAen stellte.[54]

Der Kommission zufolge sollten die Mitgliedstaaten in Zusammenarbeit mit der Zivilgesellschaft einen Rahmen für solche Abschätzungen entwickeln. In dem von Branchenvertretern im März 2010 vorgelegten Rahmen zur Abschätzung des Einsatzes von RFID-Anwendungen wurden diese in vier verschiedene Stufen unterteilt, je nachdem in welchem Ausmaß personenbezogene Daten verarbeitet werden. Je nach Stufe musste in dem vorgeschlagenen Rahmen eine vierteilige Abschätzung vorgenommen werden, deren Prüfungsdichte in Abhängigkeit von den Auswirkungen der Datenverarbeitung stieg: Auf eine Beschreibung der Anwendung folgten Vorschläge zu Kontroll- und Sicherheitsmaßnahmen, während der dritte Teil die Benachrichtigung der Nutzer über ihre Rechte vorsah. Abschließend sollte festgestellt werden, ob die Anwendung durchgeführt werden dürfe.

Die Artikel-29-Datenschutzgruppe lehnte den vorgeschlagenen Rahmen insgesamt in dieser Form jedoch ab.[55] Sie kritisierte insbesondere, dass er keinerlei verbindliche Vorgaben zur Ermittlung der mit der Anwendung verbundenen Datenschutzrisiken enthalte, obwohl dies ein zentrales Element einer DSFA sein müsse.[56] Weiterhin wurde hervorgehoben, dass eine Konsultation der Beteiligten, auf die sich der Einsatz der Technik auswirke, vorzunehmen sei.[57] Zudem müsse der Prozess in Übereinstimmung mit Art. 8 DSRL die Voraussetzungen für die Verarbeitung von besonderen Datenkategorien, z. B. die ethnische Herkunft, politische oder religiöse Überzeugungen sowie Gesundheitsdaten, erfüllen.[58]

In ihrer Smart-Meter-Empfehlung befürwortete die Europäische Kommission, dass die Mitgliedstaaten ein Muster für eine DSFA annehmen und anwenden sollten, das von der Kommission entwickelt und der Artikel-29-Datenschutzgruppe überprüft werden sollte.[59] Die Kommission stellte als Anforderung auf, dass das Muster, neben Abfragen bezüglich der Erfüllung der Anforderungen der Datenschutzrichtlinie, eine Beschreibung der Verarbeitungsprozesse und eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen enthalten sollte. Die Artikel-29-Datenschutzgruppe hielt zunächst allgemein fest, dass aufgrund der gewählten Handlungsform der Kommission – Empfehlungen sind gemäß Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) nicht rechtsverbindlich – auch mit der Smart-Meter-Empfehlung keine Rechtspflicht zur Durchführung einer DSFA bestehe. Allerdings könne es mit Blick auf den damals schon von der Kommission vorgelegten Entwurf der DS-GVO, die eine solche Pflicht erstmals in den Gesetzestext aufnahm, für die Branchenvertreter sinnvoll sein, das vorgeschlagene Muster als eine frühzeitige Umsetzung dieser zukünftigen Rechtspflicht anzusehen. Aus diesem Grund seien auch Beurteilungsspielräume hinsichtlich der Durchführung einer solchen Abschätzung eng auszulegen.[60] Die Artikel-29-Datenschutzgruppe bemängelte an dem Muster, dass die Pflicht der Ver-

antwortlichen, die Datenschutzaufsichtsbehörden vor der Durchführung der Abschätzung zu konsultieren, nicht vollständig in dem Entwurf umgesetzt wurde, hob aber hervor, dass – im Gegensatz zu der Beurteilung des für RFID-Anwendungen vorgeschlagenen Rahmens – die Risikoabschätzung bezüglich der Folgen für die Rechte der Betroffenen besser umgesetzt werde, wobei Detailregelungen noch zu vereinheitlichen seien.[61] Außerdem wurde die Bedeutung des Umgangs mit Datenschutzzielen als einer der wichtigsten Schritte einer DSFA hervorgehoben. Die Artikel-29-Datenschutzgruppe betonte zudem, dass es im Rahmen des Datenschutzrechts einen entscheidenden Unterschied zum Sicherheitsbereich, für den Risikofolgenstrategien ursprünglich entwickelt wurden, gibt: Zwar könne man grundsätzlich diesen Ansatz auch auf das Datenschutzrecht übertragen, allerdings seien Bereiche, die durch die Datenschutzrichtlinie geregelt sind, ausgeschlossen. Im Rahmen geltenden Rechts bestünde bezüglich dessen Umsetzung kein Beurteilungsspielraum und es gebe auch keine annehmbaren Abweichungen von den bindenden Vorschriften. Die Anforderungen der Datenschutzrichtlinie müssten in jedem Fall vollständig umgesetzt werden, was in dem vorgelegten Muster noch klarer formuliert werden sollte.[62] Abschließend stellte die Artikel-29-Datenschutzgruppe fest, dass das entwickelte Muster genauer ausgestaltet werden müsse, aber dass es, soweit dies anhand der Änderungsvorschläge erfolge, in Zukunft erfolgreich eingesetzt werden könne.[63]

3 Datenschutz-Folgenabschätzungen in der EU-Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung wurde am 4. Mai 2016 im Amtsblatt der EU veröffentlicht. Sie ist ab dem 25. Mai 2018 nach einer zweijährigen Übergangsfrist anwendbar und wird die bisherige DSRL ablösen. Als Verordnung hat sie grundsätzlich direkt in allen Mitgliedstaaten Geltung (Art. 288 Abs. 2 AEUV).

Wie auch schon in allen Entwurfsfassungen vorgesehen, ist mit dem konsolidierten Gesetzestext nunmehr erstmals die ausdrückliche Normierung einer DSFA (die englische Fassung verwendet den Begriff „Data Protection Impact Assessment"; DPIA) im europäischen Recht vorgesehen. Aus den Erwägungsgründen der Verordnung ist zu erkennen, dass die DSFA insbesondere gedacht ist, um die bislang obligatorische, verwaltungsintensive und dennoch datenschutzrechtlich nicht als förderlich erwiesene, generelle Benachrichtigung der Aufsichtsbehörden vor Aufnahme bestimmter Datenverarbeitungsvorgänge zu ersetzen (Erwägungsgrund 89), bzw. zu optimieren: Die Verantwortlichen sollen bei kritischen (geplanten) Datenverarbeitungen zunächst eine DSFA durchführen und das Ergebnis sodann ggf. der Aufsichtsbehörde übermitteln (Erwägungsgrund 94). Ergibt die DSFA, dass ohne Maßnahmen des Verantwortlichen zur Eindämmung des Risikos ein hohes Risiko für die Betroffenenrechte bestünde, besteht eine Rechtspflicht, die Aufsichtsbehörde zu konsultieren (Art. 36 Abs. 1 DS-GVO).

3.1 Gründe für die Durchführung einer Datenschutz-Folgenabschätzung

Gemäß Art. 35 Abs. 1 DS-GVO ist eine DSFA „insbesondere" durchzuführen, wenn durch die Verwendung neuer Technologien, wobei Art, Umfang, Umstände und Zwecke der Datenverarbeitung zu berücksichtigen sind, voraussichtlich ein hohes Risiko besteht, dass Rechte und Freiheiten Betroffener verletzt werden. Art. 35 Abs. 2 nennt sodann Regelbeispiele für Datenverarbeitungen, bei denen eine Durchführungspflicht besteht. Dies soll der Fall sein bei:

- (a) systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;
- (b) umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10, sowie
- (c) systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

Die Aufsichtsbehörden haben zudem gemäß Art. 35 Abs. 4 DS-GVO (im Rahmen ihres jeweiligen Zuständigkeitsbereichs) eine Liste der Verarbeitungsvorgänge zu erstellen und zu veröffentlichen, für die eine DSFA nach Abs. 1 durchzuführen ist. Art. 35 Abs. 5 DS-GVO enthält auch eine Ermächtigung der Aufsichtsbehörden, eine Liste mit Arten von Datenverarbeitungsvorgängen zu erstellen und zu veröffentlichen, bei denen explizit keine DSFAen durchgeführt werden müssen. Beide Listen sind an den in Art. 68 DS-GVO genannten Ausschuss (Europäischer Datenschutzausschuss) zu übermitteln. Sofern die gelisteten Verarbeitungstätigkeiten bestimmte europarechtliche Bezüge aufweisen (könnten), ist vor ihrer Festlegung das Kohärenzverfahren nach Art. 63 DS-GVO durchzuführen (Art. 35 Abs. 6 DS-GVO). Durch Art. 35 Abs. 10 DS-GVO wird indes bereits verordnungsseitig eine große Ausnahme von der Durchführungspflicht im

Einzelfall getroffen: Soweit Daten aufgrund einer im konkreten Fall einschlägigen europäischen oder mitgliedstaatlichen Rechtsvorschrift verarbeitet werden, wird es weitestgehend ins Ermessen der Mitgliedstaaten gestellt, ob die Durchführung einer DSFA nach Art. 35 Abs. 1-7 DS-GVO im Einzelfall „erforderlich" ist. Hierzu müssen die folgenden Voraussetzungen kumulativ gegeben sein: Es muss sich um Verarbeitungsvorgänge handeln, die entweder zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, der der Verantwortliche unterliegt (Bsp.: Speicherung zur Erfüllung von Aufbewahrungspflichten), oder die zur Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Bsp.: Steuerverwaltung). Die zu beurteilende Verarbeitung muss auf einer anwendbaren europäischen oder mitgliedstaatlichen Rechtsvorschrift beruhen, die diese Verarbeitung(en) auch konkret regelt. Zu fordern dürfte insofern eine Bestimmung der jeweiligen Verarbeitung(en) nach Art, Umfang, Umständen und Zweck sein. Schließlich muss im Rahmen der allgemeinen Folgenabschätzung bei Erlass der Rechtsvorschrift bereits eine DSFA vorgenommen worden sein.

Im Ergebnis wird es damit insbesondere in das Ermessen der Mitgliedstaaten gestellt, ob sie an sich selbst – ihre eigenen Behörden und Ämter – die gleichen Datenschutzanforderungen stellen wie an die private Wirtschaft. Zugleich wird die staatliche Verwaltung immer mehr digitalisiert, und die Bürger haben in diesen Fällen in aller Regel auch nicht die Möglichkeit, auf einen „datenschutzfreundlicheren Anbieter" auszuweichen. Weiterhin ist eine gewisse Eindimensionalität in der Betrachtung der DSFA zu erkennen: Auch wenn man im Gesetzgebungsverfahren die „Folgen" für den „Datenschutz" – letztlich: die Rechtmäßigkeit eines gesetzlich definierten Datenverarbeitungsvorgangs – im Grundsatz wird abschätzen können, heißt das nicht, dass die Anwendung im Einzelfall – d. h. in der ausführenden Behörde – immer in blaupausenartig-gleicher Qualität erfolgt. Die Regelung konterkariert insofern das eigentliche Ziel einer DSFA, den Schutz der Daten des Einzelnen gegenüber einer Institution zu gewährleisten, indem die Institution angehalten wird, sich selbst zu hinterfragen. Eine umfassende DSFA wird auf abstrakter, legislativer Ebene nur eingeschränkt möglich sein. Dennoch sollte der hier vorgeschlagene Prozess soweit wie möglich im Gesetzgebungsverfahren adaptiert und in der Gesetzesbegründung entsprechend dokumentiert werden.

3.2 Anforderungen an eine Datenschutz-Folgenabschätzung

Der Text der DS-GVO stellt allgemeine Vorgaben hinsichtlich der Anforderungen an eine DSFA auf. Er formuliert in Art. 35 Abs. 7 DS-GVO klar, dass es sich insofern um Mindestanforderungen handelt. Demnach hat der Verordnungstext nicht den Anspruch, sich insbesondere praktisch stellende Fragen abschließend zu beantworten. Die, sich für den Rechtsanwender ergebenden, tatsächlichen – inhaltlichen wie organisatorischen – Anforderungen in ein praktikables System zu bringen, wird der Rechtspraxis überlassen bleiben.

Abs. 3 verlangt (a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; (b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck; (c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Abs. 1; sowie (d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Generell zielt die DS-GVO mit dem Instrument der DSFA darauf ab, dass der Verantwortliche bei Verarbeitungsvorgängen, die aufgrund ihrer Art, ihres Umfangs, ihrer

Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, eine Bewertung vornimmt. Anhand dieser Abschätzung sollen sodann – entsprechend – geeignete Maßnahmen zur Eindämmung des identifizierten Risikos gefunden werden (Erwägungsgrund 90). Dies soll auch die – in einigen Mitgliedstaaten sehr umfangreich bestehenden – allgemeinen Meldepflichten ablösen (Erwägungsgrund 89).

Neben diesen inhaltlichen Vorgaben werden weitere Regelungen bzgl. zu berücksichtigender Punkte getroffen. So soll bei der Einschätzung der datenschutzrechtlichen Auswirkungen etwa die Einhaltung allgemeiner – noch aufzustellender – „codes of conduct"[64] („genehmigte Verhaltensregeln") durch den Verantwortlichen bzw. seinen Auftragsverarbeiter zu berücksichtigen sein (Art. 35 Abs. 8 DS-GVO). "Gegebenenfalls" soll der Verantwortliche auch die Betroffenen oder ihre Interessenvertreter anhören (Art. 35 Abs. 9 DS-GVO).

Nach Art. 35 Abs. 11 DS-GVO ist schließlich „erforderlichenfalls" durch den Verantwortlichen zu überprüfen, ob die Verarbeitung gemäß der DSFA durchgeführt wird. Zumindest gilt dies, wenn eine Änderung des mit den Verarbeitungsvorgängen bestehenden Risikos eintritt. Unabhängig davon ist es empfehlenswert, in regelmäßigen Abständen die Rechtskonformität der betreffenden Verarbeitungsvorgänge zu überprüfen, auch um Änderungen des Risikos zeitnah feststellen zu können.

Hinsichtlich der Dokumentation der DSFA oder auch der Zusammenfassung ihrer Ergebnisse in einem Bericht werden explizit keine Vorgaben gemacht. In Art. 36 DS-GVO wird bestimmt, in welchen Fällen die Aufsichtsbehörde – im Anschluss an die DSFA, aber vor Aufnahme der Verarbeitung – zu konsultieren ist. Hierbei geht es um Fälle, in denen ohne die von dem Verantwortlichen getroffenen Schutzmaßnahmen ein hohes Risiko bestünde (Art. 35 Abs. 1 DS-GVO). Art. 35 Abs. 3 DS-GVO listet dazu auf, welche Angaben gegenüber der Aufsichtsbehörde zu machen sind und macht so – scheinbar – mittelbar auch Vorgaben zum Inhalt des Berichts: Der Verantwortliche soll „gegebenenfalls" die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen und beteiligten Auftragsverarbeiter mitteilen; insbesondere im Falle der Verarbeitung innerhalb einer Gruppe von Unternehmen (a). Auch die Zwecke und die Mittel der beabsichtigten Verarbeitung (b), die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DS-GVO vorgesehenen Maßnahmen und Garantien (c) und die Kontaktdaten des Datenschutzbeauftragten – soweit vorhanden – (d) sind mitzuteilen. Weiterhin heißt es dann jedoch, dass „die Datenschutz-Folgenabschätzung gemäß Artikel 35" (e) und „alle sonstigen von der Aufsichtsbehörde angeforderten Informationen" (f) zu übermitteln sind. Im Ergebnis werden also lediglich Vorgaben hinsichtlich mitzuteilenden „organisatorischen Informationen" gemacht. Über Art. 35 DS-GVO hinausgehende Anhaltspunkte für den Aufbau einer DSFA oder den über sie anzufertigenden Bericht ergeben sich nicht.

Erfüllung der rechtlichen Vorgaben durch die Modelle von ICO und CNIL

Die DS-GVO stellt nur sehr allgemeine Mindestanforderungen auf, es besteht aber erstmals eine konkrete Rechtspflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Es werden auch die (ebenfalls allgemein formulierten) Punkte der Artikel-29-Datenschutzgruppe aufgegriffen, die die Ermittlung der Datenschutzrisiken für die Rechte der Betroffenen als zentrales Element der Datenschutz-Folgenabschätzung hervorhob.

Der vom ICO entwickelte PIA Code of Practice erfüllt die sehr allgemeinen Mindestanforderungen der Entwürfe teilweise. Allerdings ist zu beachten, dass es sich aufgrund der bisher fehlenden Rechtspflicht bezüglich der Durchführung einer DSFA nur um Empfehlungen handelt.

Ein zentraler Punkt des Code of Practice ist die Identifizierung der Risiken für die Betroffenen. Darauf aufbauend sollen Lösungen, die den Schutz der Privatheit sicherstellen, gefunden und bewertet werden. Dabei wird auch explizit darauf hingewiesen, dass es eine Lösung sein kann, bestimmte Daten nicht zu erheben, wie es in Punkt 2 der Mindestanforderungen vorgesehen ist, und auch eine Festlegung von Löschfristen wird erwähnt. Allerdings haben diese Punkte einen Empfehlungscharakter und sollen mit den Kosten, die durch die Umsetzung entstehen, abgewogen werden. Das Prinzip der datenschutzfreundlichen Voreinstellungen („Data protection by design and by default"), wie es in Art. 23 DS-GVO nunmehr festgeschrieben wird, ist in dem Code of Conduct noch nicht berücksichtigt.

Die Dokumente der CNIL zur Durchführung eines PIAs haben zum Ziel, die Einhaltung bestehender Datenschutzgesetzgebung zu systematisieren und zu dokumentieren. Nach der Feststellung, dass die Grundrechte der Betroffenen nicht verhandelbar seien, ist auch dieser Ansatz vornehmlich als Empfehlung formuliert. Lediglich darauf, dass die Vorgaben des Datenschutzrechts und ihre Einhaltung obligatorisch und daher zu kontrollieren sind, wird hingewiesen.[65] Die verpflichtenden Vorgaben der der DS-GVO hinsichtlich des Inhalts eines PIAs werden durch das Modell der CNIL voraussichtlich unproblematisch erfüllt: Es zielt auf die Risiken für die Betroffenenrecht ab, betont insoweit den Unterschied zu Risiken für die Organisation selbst (etwa Imageverlust, finanzieller Schaden etc.) und fordert eine Beschreibung der Verarbeitungsvorgänge sowie eine Risikoeinschätzung. Auch nennt es mögliche Maßnahmen für diverse konkrete Anwendungsfälle und schreibt die Dokumentation des gesamten Prozesses und eine regelmäßige Wiederholung vor. Für alle vorzunehmenden Schritte werden Beispielsfälle und -maßnahmen genannt. Allerdings ist bislang nicht ersichtlich, wie die CNIL in der Praxis nicht unübliche widersprüchliche Ergebnisse des Analyseprozesses auflösen will. Es wird keine Systematik an die Hand gegeben, die es ermöglicht, planvoll – im Sinne eines Gesamtkonzeptes – auf widersprüchliche Anforderungen zu reagieren und in jedem Einzelfall eine gute Balance zu erreichen.

3.3 Risikoansatz vs. Grundrechtsgewährleistung

Mit der konsolidierten Fassung der DS-GVO wurde der sogenannte Risikoansatz explizit formuliert.[66] Der Verantwortliche muss demnach mögliche Risiken analysieren und je nach Ergebnis der Analyse unterschiedliche Auflagen erfüllen, beispielsweise die Durchführung einer DSFA, soweit die beabsichtigte Art der Datenverarbeitung wahrscheinlich zu einem hohen Risiko für die Betroffenenrechte führen wird (vgl. soeben unter 3.1). Insbesondere im Rahmen der Verhandlungen des Verordnungstexts im Rat der EU wurde darüber spekuliert, ob mit dem Risikoansatz „die Rechte der Betroffenen beschnitten und die Pflichten für Unternehmen und Behörden reduziert werden" sollten.[67] Tatsächlich ist der Risikoansatz vom Risikomanagement zu unterscheiden; es gibt einige grundsätzliche Unterschiede zwischen den Prinzipien des Datenschutz und des Risikomanagements: Datenschutz stellt das Individuum als Betroffenen von Datenverarbeitung in den Fokus und betrachtet jede Organisation als potenziellen Angreifer auf die Betroffenenrechte. Das klassische Risikomanagement adressiert hingegen Risiken für die Organisation und deren Tätigkeit. Im Rahmen einer umfassenden DSFA ist es aber sinnvoll, Organisationen zusätzlich auf die Risiken hinzuweisen, die durch die Verletzung von Betroffenenrechten entstehen – direkt durch Sanktionen der Aufsichtsbehörden oder indirekt durch Imageverlust o. ä.

Während es dem Datenschutz darum geht, die Rechte jedes Einzelnen zu garantieren, ist das Ziel des Risikomanagements die Reduktion von Risiken auf ein für die Organisation akzeptables Maß. Was für eine Organisation akzeptabel ist, hängt dabei davon ab, welche Mittel zur Abstellung von Risiken zur Verfügung stehen und wie risikofreudig die Organisation (bzw. deren Entscheider) ist. Dies führt dazu, dass Risiken, die selten eintreten, nur mit geringem Schaden verbunden sind oder nur wenige Personen betref-

fen, als akzeptabel eingeschätzt werden. Im Gegensatz dazu hat der Datenschutz zum Ziel, jede Beeinträchtigung von Betroffenenrechten vollständig zu vermeiden oder zu beseitigen (es sei denn, eine gesetzliche Erlaubnis oder Einwilligung liegt vor).[68] Im Grundsatz gilt für den Datenschutz, dass jede Verarbeitung personenbezogener Daten durch Organisationen, auch wenn diese durch Gesetz legitimiert ist, einen Grundrechtseingriff darstellt.

Eine DSFA, zumal wenn sie von dem Verantwortlichen selbst durchgeführt werden soll, sollte eine systemische Perspektive haben, bei der alle Akteure mit ihren spezifischen Interessen im Blick sind. Auch eine Grundrechtsgewährleistung ist im Rahmen einer Risikoanalyse wie sie in der DS-GVO gefordert wird möglich, wenn berücksichtigt wird, dass die Erfüllung der sich aus den Grundrechten der Betroffenen ergebenden Anforderungen nicht von der Verfügbarkeit finanzieller und personeller Mittel abhängig sein darf.

Der im folgenden Kapitel skizzierte Prozess zur Durchführung von DSFAen versucht den Brückenschlag zwischen dem Risikoansatz sowie dem Ansatz zur Grundrechtsgewährleistung und kombiniert die als sinnvoll erachteten Elemente mit dem Ziel, ein für alle Beteiligten nützliches Werkzeug zu schaffen.

4
Elemente eines Prozesses zur Datenschutz-Folgenabschätzung

Wie erläutert gibt es eine Vielzahl unterschiedlicher Ansätze für Datenschutz-Folgenabschätzungen sowie Prozesse zu deren Durchführung. Abb. 01 zeigt einen prototypischen Prozess, der auf einer umfangreichen Analyse bestehender organisatorischer Abläufe basiert und solche Elemente kombiniert, mit denen in der Praxis die bestmöglichen Resultate erzielt wurden.[69] Obwohl der Prozess als weitgehend linear dargestellt ist, kann es notwendig sein, bestimmte Schritte mehrfach zu durchlaufen, bis eine akzeptable Lösung gefunden ist.

Der Ansatz stellt die Reproduzierbarkeit und *Überprüfbarkeit* der Ergebnisse sicher. Damit ist es für Dritte (u.a. die zuständigen Datenschutzbehörden) möglich zu kontrollieren, ob rechtliche Vorgaben eingehalten werden. Ein standardisiertes Verfahren versetzt Kunden bzw. Betroffene zudem in die Lage, die Datenschutzfolgen verschiedener Lösungen miteinander zu *vergleichen*. Schließlich fokussiert das Verfahren nicht nur auf eine Technologie oder Anwendung, sondern ist technologieneutral formuliert. Dies hilft, den *Aufwand* für die wiederholte Durchführung gering zu halten.

Der Gesamtprozess (Abb. 01) gliedert sich in drei Phasen, eine Vorbereitungsphase, die zur Organisation der Datenschutz-Folgenabschätzung dient, die eigentliche Bewertungsphase sowie eine Berichts- und Maßnahmenphase. In den folgenden Abschnitten werden die drei Phasen und die darin zu durchlaufenden Schritte näher erläutert.[70]

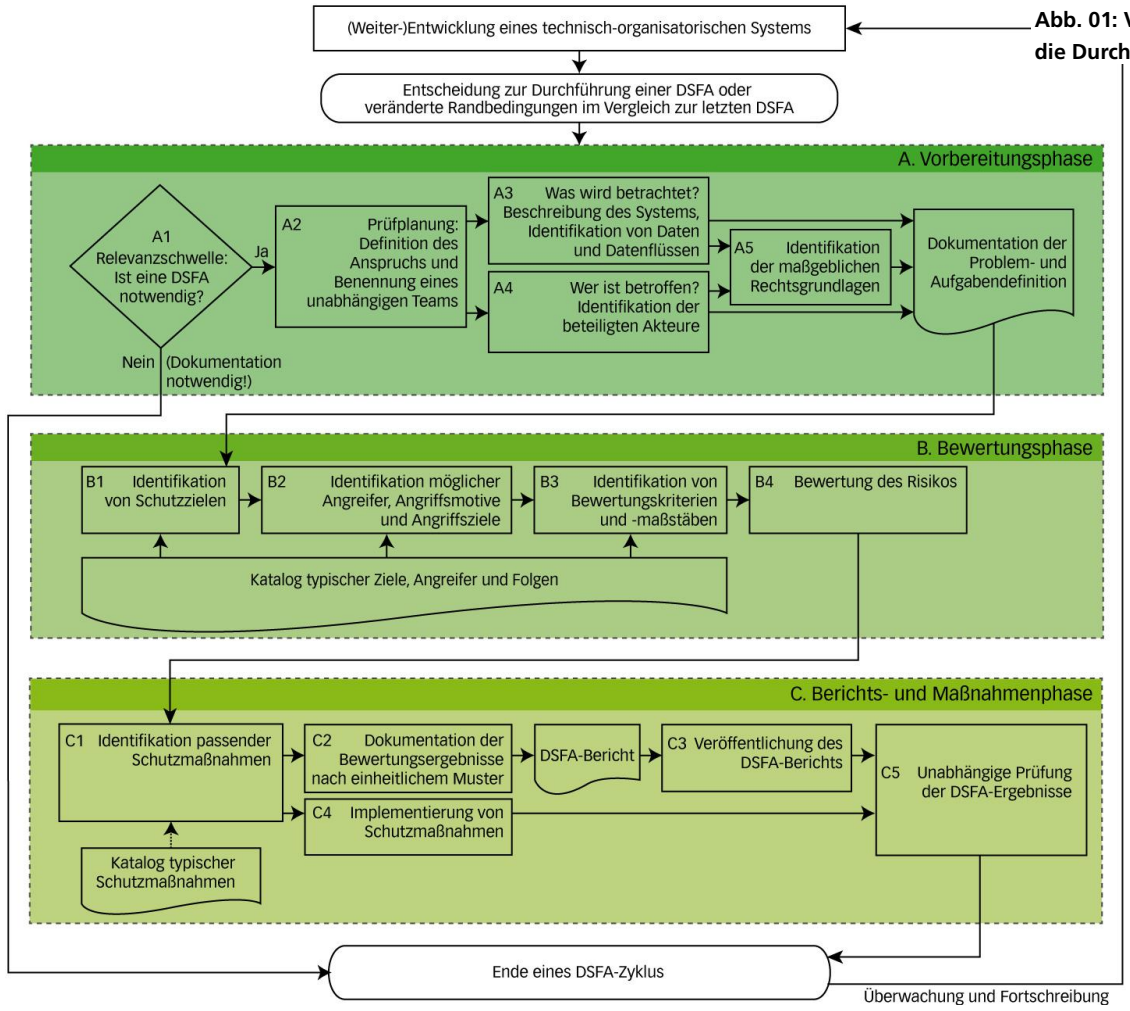

Abb. 01: Vorgehensweise für die Durchführung einer DSFA

4.1 Vorbereitungsphase

4.1.1 Relevanzschwelle

Zunächst muss sich der Verantwortliche mit der Frage auseinandersetzen, ob im konkreten Fall die Durchführung einer DSFA überhaupt notwendig ist.

DS-GVO definiert die gesetzliche Relevanzschwelle in Art. 35 Abs. 1 und nennt in Art. 35 Abs. 3 sodann einen nicht abschließenden Katalog mit Anwendungsfällen. Art. 35 Abs. 1 DS-GVO bestimmt, dass wenn „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" der Betroffenen besteht, eine DSFA durchzuführen ist. Dies impliziert, dass die bloße Datenverarbeitung als solche keine Rechtspflicht auslöst. Allerdings ist zu bedenken, dass um überhaupt seriös feststellen zu können, ob ein „hohes Risiko" besteht, bereits eine Abschätzung vorgenommen werden muss. Auch eine solche kann in Form des im Folgenden dargestellten Prozess erfolgen. Weiterhin ist zu beachten, dass Verantwortliche selbstverständlich bestehende Gesetze einzuhalten haben und dies auch gegenüber der Aufsichtsbehörde nachweisen können müssen. Die Analyse der eigenen Datenverarbeitung im Vorfeld und die Dokumentation dieser können die Kommunikation mit der Aufsichtsbehörde wesentlich erleichtern.

Verpflichtend ist eine DSFA gemäß Abs. 3 insbesondere bei folgenden Verarbeitungsvorgängen durchzuführen:

- bei systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen;
- bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10;
- bei systematischer weiträumiger Überwachung öffentlich zugänglicher Bereiche.

Darüber hinaus werden die Aufsichtsbehörden verpflichtet, weitere Fälle von Datenverarbeitungen festzulegen und zu veröffentlichen, in denen vorab eine DSFA vorzunehmen ist (Art. 35 Abs. 4 DS-GVO). Ebenso werden Aufsichtsbehörden ermächtigt, Fälle zu definieren und zu veröffentlichen, in denen eine DSFA explizit nicht vorzunehmen ist (Art. 35 Abs. 5 DS-GVO). Zu weiteren Ausnahmen von der Durchführungspflicht vgl. 3.1.

4.1.2 Prüfplanung

Wenn sich bei der Prüfung der Relevanzschwelle ergeben hat, dass eine DSFA durchzuführen ist, sollten zunächst die damit verbundenen Ziele und Rahmenbedingungen festgelegt und ein geeignetes Team zusammengestellt werden.

Anspruch der Datenschutz-Folgenabschätzung

Zunächst ist der Charakter der DSFA festzulegen. Dies ist später auch bei der Veröffentlichung der Ergebnisse zu kommunizieren. In der bisherigen Praxis finden sich drei Typen von DSFA.[71] Dabei ist zu betonen, dass von den im Folgenden genannten Typen nur die DSFA im engeren Sinne die Anforderungen der DS-GVO an eine rechtlich gebotene DSFA vollumfänglich kann.

Marketing-DSFA haben i. d. R. das Ziel, mit geringem Aufwand Kunden (und Aufsichtsbehörden – die sich indes nicht mit diesen vergleichsweise oberflächlichen Analysen zufriedengeben sollten) einen Nachweis über die Erfüllung datenschutzrechtlicher

Anforderungen zu erbringen. Zu diesem Zweck wird häufig ein formal korrekt durchgeführtes Verfahren nach einem der vielen in Europa gebräuchlichen Vorgehensweisen (z. B. ISO-Standard, ICO Handbook etc.) durchgeführt, allerdings wird meist eine sehr enge Systemdefinition verwendet. Die darauf angewendeten Kriterien sind vielfach intransparent, häufig werden dabei auch die Kriterien der Informationssicherheit mit denen des Datenschutzrechts gleichgesetzt. Die Ergebnisse von Marketing-DSFAen versuchen in der Regel, Aufsichtsbehörden und die Öffentlichkeit von der Risikolosigkeit einer Technologie oder eines Systems zu überzeugen. Die Identifikation negativer Folgen wird meist von vorherein vermieden und schon gar nicht veröffentlicht. Aus rechtlicher Sicht ist fraglich, welche Relevanz diese Art von DSFA besitzt bzw. ob sie den Anforderungen der DS-GVO genügen wird.[72] Nach zutreffender Ansicht ist dies zu verneinen, da ein effektiver Schutz der Betroffenenrechte so keinesfalls erreicht werden kann.

Standard-Datenschutz-Folgenabschätzungen (DSFA im engeren Sinne) sind solche, die am ehesten den Vorstellungen des europäischen Gesetzgebers entsprechen dürften und die das Ziel haben, den Nachweis zu liefern, dass ein konkretes Datenverarbeitungssystem konform mit den datenschutzrechtlichen Anforderungen ist, oder geeignete Schutzmaßnahmen für dieses System zu identifizieren. Bei solchen DSFAen wird auf einen vordefinierten Katalog an Bewertungskriterien und -maßstäben sowie Schutzmaßnahmen zurückgegriffen, um die Bewertung für die Aufsichtsbehörden und die Öffentlichkeit nachvollziehbar zu machen. Die Ergebnisse einer DSFA im engeren Sinne werden in einer standardisierten Form dokumentiert und veröffentlicht (ggf. unter Weglassung von Teilen, die Betriebs- und Geschäftsgeheimnisse enthalten).

Schließlich gibt es auch wissenschaftliche *Datenschutz-Folgenabschätzungen (DSFA im weiteren Sinne),* die sich eher in der Tradition wissenschaftlicher Technikfolgenabschätzungen verstehen. Sie haben den Zweck, unbekannte Eigenschaften und Risiken einer Technologie oder eines Systems aufzudecken. Zu diesem Zweck ist eine wissenschaftliche DSFA meist sehr breit angelegt, beschränkt sich nicht auf einen konkreten Anwendungsfall und bewertet nicht nur Aspekte des Daten- und Privatheitsschutzes, sondern auch weitere Aspekte. Dazu gehören vor allem ethische, ökonomische und Sicherheits-Aspekte.[73] In diesem Zusammenhang gibt es Bestrebungen, unterschiedliche Verfahren der Technikbewertung in einem integrierten Bewertungsrahmen zusammenzufassen.[74] Da die Datenschutz-Folgenabschätzung nicht nur aktuelle, sondern auch künftige Risiken adressiert, ist das Vorgehen prospektiv und arbeitet häufig mit (spekulativen) Szenarien, die oftmals keiner so engen Zweckbindung wie für Forschungsdaten unterworfen werden können, wie es rechtlich vielfach gefordert ist. Allerdings ist zur Kompensation möglicherweise für Einzelpersonen riskanter Folgen und Forschungen zu fordern, dass die Ergebnisse der Folgenabschätzungen allgemein öffentlich zugänglich sind und einen gewissen kompensatorischen Nutzen für diese Personen entfalten können. Das Wissen aus einer wissenschaftlichen DSFA darf dann nicht exklusiv gehalten und nur wenigen Organisationen vorbehalten sein.

Wegen der prognostischen Unsicherheiten ist es nicht ausreichend, einen fest definierten Katalog an Kriterien und Maßnahmen abzuarbeiten (was nicht bedeutet, dass Informationssicherheits- und/oder Datenschutzstandards ignoriert werden sollten); stattdessen sind ein partizipatives Vorgehen und ein risikoorientierter Ansatz sinnvoll. Insbesondere können fehlende Rechtsgrundlagen angesprochen und entsprechende Empfehlungen gegeben oder auch geeignete Normentexte, seien diese Gesetzesentwürfe oder Einwilligungserklärungen, entworfen werden. Eine wissenschaftliche Datenschutz-Folgenabschätzung ist ergebnisoffen angelegt und auch negative Prüfergebnisse werden publiziert.

Team

Bei der Zusammenstellung des Teams ist es wichtig, eine Balance zwischen Unabhängigkeit und Verantwortlichkeit herzustellen. Zum einen ist es für die Objektivität und

Glaubwürdigkeit der Ergebnisse entscheidend, dass das Team in der Lage ist, eine wirkungsvolle Prüfung vorzunehmen. Dafür ist zum einen sicherzustellen, dass ausreichend Ressourcen (Zeit, Personal, Kompetenzen) zur Verfügung stehen: Auf der anderen Seite muss gewährleistet sein, dass sich die Datenschutz-Folgenabschätzung nicht anderen Zielen der Organisation unterzuordnen hat. Damit die Prüfung die gewünschten Ziele erreichen kann, insbesondere die Änderung von als kritisch bewerteten Elementen, ist gleichzeitig zu gewährleisten, dass die für die Entwicklung oder Einführung verantwortlichen Personen in den Prozess eingebunden sind, idealerweise als Verantwortlicher für die Durchführung der DSFA. Um Interessenkonflikte zu vermeiden, ist die Einbeziehung einer neutralen Stelle (z. B. Qualitätssicherung) zu erwägen. Verpflichtend ist nunmehr gem. Art. 35 Abs. 2 DS-GVO (sofern vorhanden) den Rat des internen Datenschutzbeauftragten einzuholen. Zumindest sollte dies Gegenstand einer (nachträglichen) Überprüfung sein.

4.1.3 Was wird betrachtet?

Im ersten inhaltlichen Schritt ist zu definieren, was im Rahmen der DSFA geprüft wird, also der Prüfgegenstand (engl. *target of evaluation*). Zur Beschreibung des Prüfgegenstandes gehören neben Zweck und Kontext vor allem drei Komponenten, die zu unterscheiden und einzeln abzuhandeln sind:

- Daten und deren Formate beim Speichern oder Transferieren (Protokolle),
- verwendete IT-Systeme und deren Schnittstellen sowie
- Prozesse und Funktionsrollen.

Mit Blick auf das durch die DSFA angestrebte Ziel bzw. den Grund ihrer Durchführung lassen sich auch hier unterschiedliche Typen von DSFA unterscheiden:

- Eine *konkrete DSFA*, wie sie einer Datenschutzaufsichtsbehörde gem. Art. 35 DS-GVO vorgelegt werden muss, darf sich nicht auf einzelne Komponenten oder Verfahrensweisen beschränken, sondern muss den vorab definierten Prüfungsgegenstand in seiner Gesamtheit beschreiben. Dazu zählt nicht nur die technische Realisierung, sondern auch die organisatorische Gestaltung und Einbettung bei dem Verantwortlichen. Um eine ganzheitliche Perspektive auch bei der Bewertung von Einzelverfahren und Komponenten beibehalten zu können, müssen die Anwendungsfälle innerhalb der Organisation des Verantwortlichen möglichst realistisch und präzise beschrieben werden. Insbesondere müssen die Zwecke der Datenverarbeitung abschließend definiert werden, um den datenschutzrechtlichen Prinzipien der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) und der Datensparsamkeit, bzw. „Datenminimierung“, (Art. 5 Abs. 1 lit. c DS-GVO) genügen zu können und – soweit erforderlich – eine rechtliche Güterabwägung zur Gewährleistung des Grundrechtsschutzes vornehmen zu können.
- *Generische DSFA* betrachten dagegen Technologie, Verfahren oder Komponenten ohne Berücksichtigung eines konkreten Einsatzkontexts. Meist handelt es sich hierbei um prognostische wissenschaftliche DSFAen. Dabei werden grundsätzliche Risiken untersucht, die sich nicht auf Fragen des Datenschutzes beschränken müssen. Um den damit verbundenen prognostischen Unsicherheiten zu begegnen, werden normalerweise mehrere für typisch erachtete Szenarien für Einsatzkontexte definiert. Bei der Bewertung kann dann auf existierendes Wissen über diese Einsatzkontexte zurückgegriffen und für das zu prüfende Verfahren extrapoliert werden. Diese Form der DSFA kann in zweierlei Weise genutzt werden: intern im Rahmen einer Privacy-by-Design-Strategie für die technische Weiterentwicklung und extern in Form von Empfehlungen für die Konfiguration und den datenschutzgerechten Einsatz.

In der Praxis bietet sich allerdings eine *Kombination beider Formen* an. Hersteller und Vertreiber führen eine generische DSFA durch und weisen darin auf generelle Risiken in verschiedensten Kategorien hin. Für die Nutzung in einem konkreten Kontext – und zur

Erfüllung ihrer gesetzlichen Pflicht nach Art. 35 DS-GVO – führt der Verantwortliche dann eine konkrete DSFA durch, die ggf. auf der generischen DSFA aufbaut.

4.1.4 Wer sind die beteiligten Akteure?

Ebenso wichtig wie die umfassende Beschreibung des Systems und seines Einsatzkontextes ist die Identifikation der handelnden und betroffenen Akteure. Darunter fallen nicht nur Organisationen und Personen, die im Rahmen der Entwicklung oder Verwendung eine bestimmte Rolle einnehmen und damit potenzielle Angreifer sind, sondern vor allem die Personen, die mittelbar oder unmittelbar durch den Einsatz betroffen sind. Konkret fallen darunter:

- die *Hersteller* des Prüfungsgegenstands;
- *Betreiber* des Prüfungsgegenstands als Dienstleister etwa im Rahmen einer Auftragsdatenverarbeitung (Rechenzentrum, Internet-Provider);
- Mitarbeiter der für den Einsatz des Prüfungsgegenstands verantwortlichen Organisation[75];
- die *betroffenen Personen* in ihren Rollen als Bürger, Patient, Kunde, Arbeitnehmer etc. (je nach Anwendungskontext);
- *Dritte*, die im Zuge des Einsatzes des Prüfungsgegenstandes Kenntnis von personenbezogenen Daten nehmen, entweder zufällig (z. B. zufällig anwesende, mithörende Dritte) oder absichtlich (Sicherheitsbehörden).

Für jede dieser Akteursgruppen ist zu beschreiben, welche Rolle sie bei der Datenverarbeitung spielen, welche Rechtsbeziehungen zwischen ihnen bestehen und welche Interessen bei ihnen vorliegen. Die Besonderheit einer DSFA besteht darin, dass neben dem Risiko missbräuchlicher Datennutzung durch unbefugte Dritte vor allem das Risiko betrachtet wird, das durch die missbräuchliche, den eigentlichen Zweck überdehnende oder überschreitende – sowie sogar bestimmungsgemäße – Nutzung von Daten durch die Organisation selbst entsteht. Insofern ist bei der Identifikation der Betroffenen stets zu eruieren, welche Motive zur Nutzung von Daten durch andere Abteilungen einer Organisation sowie insbesondere der Zugriff auf Verfahren und deren Daten durch Sicherheitsbehörden, Konkurrenzunternehmen oder Forschungsinstitute bestehen können.

4.1.5 Identifikation der maßgeblichen Rechtsgrundlagen

Die Identifikation der maßgeblichen Rechtsgrundlagen ist der nächste Schritt in der Vorbereitungsphase. Diese soll nicht nur die Gewährleistung der Rechte der Betroffenen sicherstellen, sondern liegt auch im Interesse des Verantwortlichen, eigenen Pflichten nachzukommen.

Zunächst ist das anzuwendende Recht zu bestimmen. Werden personenbezogene Daten im Rahmen der Tätigkeit einer Niederlassung in der Europäischen Union verarbeitet oder werden personenbezogene Daten einer in der Union ansässigen Person verarbeitet, ist der Anwendungsbereich der DS-GVO eröffnet und mithin europäisches Recht anzuwenden.[76] So kann nicht-europäisches Recht anwendbar sein, wenn ein Verantwortlicher seinen Sitz in einem anderen Staat hat und keine personenbezogenen Daten von in der Union ansässigen Personen verarbeitet.

Die konkret zu identifizierenden Rechtsgrundlagen sind abhängig vom spezifischen Prüfgegenstand. Zunächst immer zu beachten ist das Datenschutzrecht. Das einschlägige Datenschutzrecht bestimmt sich nach der DS-GVO.[77] Diese hat zukünftig Anwendungsvorrang vor nationalem Datenschutzrecht. Über entsprechende Öffnungsklauseln, also Vorschriften, die die Ausgestaltung oder Beschränkung des Regelungsinhalts den Mitgliedstaaten überlassen,[78] zur Ausfüllung unbestimmter Rechtsbegriffe oder durch Regelungslücken[79] in der DS-GVO, können gegebenenfalls auch weiterhin natio-

nale Vorschriften Anwendung finden, soweit die DS-GVO keine abschließende Regelung trifft. Diese können sich zum Beispiel aus dem Bundesdatenschutzgesetz, den Landesdatenschutzgesetzen, aus dem Telemedien- oder Telekommunikationsgesetz ergeben, aber auch aus weiteren bereichsspezifischen Vorschriften, etwa den Sozialgesetzen oder dem Strafrecht. Die Beachtung der Rechtsgrundlagen dient auch dem Verantwortlichen, um die Verwirklichung von Straftatbeständen zu verhindern. Besonders relevant ist dies etwa für diejenigen Verantwortlichen, die dem Berufsgeheimnis unterliegende personenbezogene Daten verarbeiten. Diese müssen sicherstellen, dass keine Daten unbefugt offenbart werden können.

Je weiter der Prüfgegenstand, desto mehr zusätzliche Rechtsgrundlagen sind potenziell zu beachten. Dazu gehören alle rechtlichen Vorschriften, die im Rahmen der elektronischen Datenverarbeitung Anwendung finden können, etwa Vorgaben zu AGB- und sonstigem Verbraucherrecht oder Minderjährigenschutz. Da im Rahmen der Datenschutz-Folgenabschätzung jedoch vorrangig Prozesse und technische Abläufe geprüft werden, kommen solche Rechtsgrundlagen im Rahmen der DSFA nur dann in Betracht, wenn deren Anforderungen direkt im technischen Prozess umgesetzt sind. Andernfalls sind diese vorrangig im Rahmen der Compliance sicherzustellen.

4.1.6
Dokumentation der Problem- und Aufgabendefinition

Die Ergebnisse der Vorbereitungsphase sind vom Verantwortlichen des DSFA-Prozesses in Form eines „Scoping-Berichts" zu dokumentieren. Die Darstellung sollte nach einer standardisierten Gliederung erfolgen, die auch später bei der Dokumentation der Prüfergebnisse verwendet wird. Dieser Bericht gibt den verbindlichen Rahmen für die nachfolgenden Bewertungsschritte vor.

4.2 Bewertungsphase

4.2.1 Identifikation von Schutzzielen

Es hat sich im Bereich der IT-Sicherheit bzw. Informationssicherheit bewährt, Anforderungen als Schutzziele zu formulieren.[80] Die Anforderungen des Datenschutzes sind gesetzlich normiert. Diese Anforderungen lassen sich ebenfalls mit Hilfe von Schutz-, bzw. Gewährleistungszielen[81] umsetzen, die in kompakter und methodisch zugänglicher Form die operativen Risiken explizit machen, vor denen es durch eine angemessene Verfahrensgestaltung und Maßnahmen zu schützen gilt.

Sechs Schutzziele gelten derzeit im Bereich des Datenschutzes als etabliert (Abb. 02). Den Risiken der Informationssicherheit wird klassisch mit der Sicherung der drei Schutzziele (1) Verfügbarkeit, (2) Integrität und (3) Vertraulichkeit begegnet. Aufbauend hierauf werden zusätzlich als spezifische Datenschutzschutzziele formuliert: (4) Nichtverkettbarkeit, (5) Transparenz und (6) Intervenierbarkeit.[82]

Die Schutzziele thematisieren insgesamt wesentliche datenschutzrechtliche Risiken bzw. Anforderungen. Dabei stehen hinter jedem Schutzziel weitere, von ihnen abgeleitete Schutzziele. So nimmt das Schutzziel Nichtverkettbarkeit die im Datenschutzrecht zentrale Anforderung der Zweckbindung einer Verarbeitung personenbezogener Daten auf, in einer Form, die der technischen und organisatorischen Umsetzung der Anforderung an Zweckbindung, die wiederum die Anforderungen der Datensparsamkeit und Erforderlichkeit reguliert, entgegenkommt.[83] Die Revisionsfähigkeit ist ein wesentlicher Aspekt der Sicherung der Transparenz, und die Sicherung der Authentizität ist ein wesentlicher Aspekt der Sicherung der Integrität in einer Kommunikationsbeziehung. Das Schutzziel der Intervenierbarkeit dient der operativ zugänglichen Gewährleistung der Betroffenenrechte.

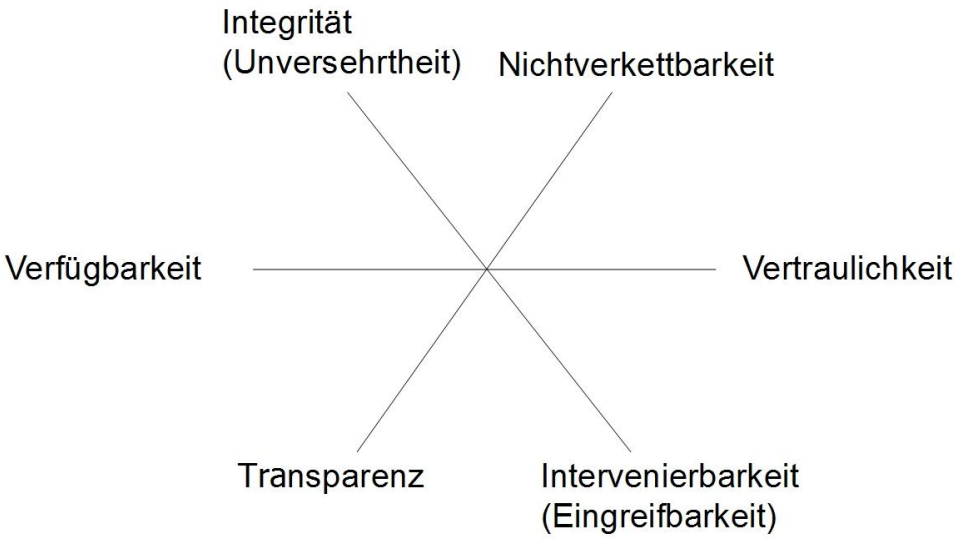

Abb. 02: Systematik der Schutzziele

Hinter jedem dieser Schutzziele steht vor allem ein Katalog mit Maßnahmen zur Erreichung der Schutzziele in der Praxis. Generell lassen sich alle Schutzziele aus verschiedenen Normen des BDSG ableiten bzw. die zentralen Grundsätze des Datenschutzrechts jeweils einem oder mehreren Schutzzielen zuordnen. 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 zusätzlich zu beachten.

Die Schutzziele befinden sich in einem doppelten Spannungsfeld. Jeweils zwei Schutzziele können als entgegengesetzte Pole auf einem Graphen betrachtet werden. Das Spannungsfeld entsteht, da bei dem Fokus auf ein Schutzziel, z. B. durch besonders hohe Anforderungen, die umzusetzen sind, beim gegenüberstehenden Schutzziel zwangsläufig Abstriche gemacht werden müssen. Im Rahmen der Bewertung ist im Einzelfall eine Abwägung zu treffen, in welchem Umfang die Erreichung eines Schutzziels zu Lasten des konkurrierenden Schutzziels erfolgen soll. Beispielsweise kann ein System, mit dem als sehr vertraulich eingeschätzte Daten verarbeitet werden, nicht gleichzeitig in hohem Maß Verfügbarkeit für die Daten garantieren. Das erforderliche hohe Maß an Vertraulichkeit bedingt die Notwendigkeit der Implementierung strenger personeller und räumlicher Zugangskontrolle, was die Verfügbarkeit einschränkt.

4.2.2 Identifikation von möglichen Angreifern, Angriffsmotiven und -zielen

Bei der Betrachtung der Schutzziele ist darüber hinaus zu berücksichtigen, dass konsequent die Betroffenenperspektive eingenommen wird. Insbesondere die Schutzziele der Informationssicherheit werden in der Regel aus der Risikoperspektive der Organisation betrachtet, bei der die Sicherung der Geschäftsprozesse im Vordergrund steht. Die Angreifer sind in dieser Sichtweise grundsätzlich externe Dritte und nicht regelkonform handelnde interne Nutzer.

Bei einer DSFA muss aber von einer anderen Konstellation ausgegangen werden: Zu schützen sind in diesem Fall nicht die Geschäftsprozesse, sondern die Interessen und Rechte der Kunden, Arbeitnehmer etc. einer Organisation. Als Risiko für den Datenschutz müssen hingegen vor allem Organisationen, wie zum Beispiel Behörden und Unternehmen, betrachtet werden, die Daten erfassen, verarbeiten und weitergeben, bzw. solche Organisationen, die sich Zugriff zu Daten verschaffen können. Dabei geht es vor allem um Risiken, die aus der illegitimen Überdehnung des Zwecks durch den Betreiber selbst entstehen, aber auch um Risiken, die aus dem potenziellen Interesse anderer Institutionen an den schon bei einem Betreiber vorliegenden Datenbestand resultieren. Insofern muss im Rahmen einer DSFA standardmäßig überprüft werden, ob

folgende Organisationen ein Risiko für die Rechte des Einzelnen und die Privatheit darstellen:

- Staatliche Stellen, z. B.
  - Sicherheitsbehörden: Innenministerien, Polizei, Geheimdienste, Militär etc.
  - Staatliche Leistungsverwaltung: Leistungsträger für Arbeitslosengeld II („Hartz IV"), Rentenversicherungsträger etc.
  - Statistische Ämter
  - Versagende Aufsichtsbehörden, die durch das Hinterlassen rechtsfreier Räume Angriffe anderer Akteure ermöglichen
- Unternehmen[84], z. B.
  - Technologiehersteller, Systemintegratoren, IT-Diensteanbieter (Zugang, Inhalte etc.)
  - Banken, Versicherungen
  - Wirtschaftsauskunfteien, Adress- und Datenhandel, Marktforschung
  - Werbebranche
  - Interessenvereinigungen, Verbände
  - Arbeitgeber
- Gesundheitswesen, z. B.
  - Krankenhäuser, Ärzte
  - gesetzliche und private Krankenversicherungen
- Forschung, z. B.
  - Medizinforschung
  - Sozialforschung
  - Universitäten

Es ist offensichtlich, dass es einen Interessenkonflikt gibt, wenn die Organisation, die die DSFA durchführt, gleichzeitig ein gewichtiges Risiko für den Datenschutz darstellt. Um auszuschließen, dass sich die Organisation in den blinden Fleck der Risikoanalysen setzt, sollte wenigstens eine nachträgliche Überprüfung durchgeführt werden. Auch vom internen Datenschutzbeauftragten ist zu erwarten, dass er die Betroffenenperspektive einnimmt und seine eigene Organisation „von außen" betrachtet. Idealerweise sollte die DSFA aber von einer unabhängigen Instanz (jedoch in enger Kooperation mit der den Prüfgegenstand betreibenden Organisation) durchgeführt werden.

4.2.3 Identifikation von Bewertungskriterien und -maßstäben

Für die Bewertung eines Risikos haben sich die Schutzbedarfsabstufungen bewährt, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinen IT-Grundschutz-Katalogen empfiehlt.[85]

Allerdings ist eine direkte Übertragung dieser auf Informationssicherheit abzielenden Sichtweise auf Datenschutzaspekte nicht zielführend. Um dem auf Grundrechtsschutz angelegten Datenschutz gerecht zu werden, kann der Schutzbedarf nicht allein anhand von Schadenshöhen und Eintrittswahrscheinlichkeiten bestimmt werden. Vielmehr ist primär anzuerkennen, dass jede – auch eine völlig rechtskonforme – Datenverarbeitung einen Eingriff in die Grundrechte der Betroffenen aus Art. 7 und 8 der EU-Grundrechtecharta darstellt. Allein daraus folgt bereits ein „normaler" Schutzbedarf. Aufgrund spezifischer Arten der Datenverarbeitung bzw. Verarbeitung von speziellen Arten von Daten kann sodann eine noch höhere Eingriffsintensität und damit die Annahme eines hohen oder sogar sehr hohen Schutzbedarfs impliziert sein.[86] Die Schutzbedarfsabstufungen lassen sich wie folgt zusammenfassen:

- *Normal*: Es werden personenbezogene Daten verarbeitet, ohne dass Verarbeitungsszenarien mit potenziell erhöhter Eingriffsintensität gegeben sind.
- *Hoch*: Es werden personenbezogene Daten verarbeitet, die der Kategorie „besonderer Arten personenbezogener Daten" zuzuordnen sind und als solche de lege lata

hohen Schutzbedarf aufweisen, und/oder die Betroffenen sind von den Entscheidungen bzw. Leistungen der Organisation abhängig, wobei

- die hohe Eingriffsintensität der Datenverarbeitung zu erheblichen Konsequenzen für die Betroffenen führen kann und/oder
- keine effektiven Interventions-/Selbstschutzmöglichkeiten für die Betroffenen bestehen; hierzu zählt auch das Fehlen realistischer Möglichkeiten gerichtlicher Überprüfung.

- *Sehr hoch*: Es werden personenbezogene Daten mit hohem Schutzbedarf verarbeitet, und zusätzlich sind die Betroffenen von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existenziell abhängig und es bestehen zusätzliche Risiken durch unzureichende Informationssicherheit oder unzulässige Zweckänderung seitens der Organisation, ohne dass die Betroffenen solche direkt bemerken und/oder korrigieren können.

Zudem kann sich durch „Kumulierungseffekte" ein hoher Schutzbedarf auch bei Datenverarbeitungen mit – einzeln betrachtet – nur normalem Schutzbedarf ergeben. Dies kann der Fall sein, wenn Daten von sehr vielen Personen erhoben werden („Kumulierung vieler Daten") oder aber wenn Daten durch einzelne Personen (z. B. Administratoren) zu verschiedenen Zwecken erhoben werden, wobei sich die betroffenen Personen jeweils in verschiedenen Rollen befinden („Kumulierung vieler Berechtigungen").

4.2.4 Bewertung des Risikos

Der Kern des Bewertungsvorgangs besteht im Vergleich der, von den Verantwortlichen, geplanten bzw. in der Prüfung festgestellten Maßnahmen mit einem Katalog von Referenzmaßnahmen. Probst (2012) hat einen ersten Vorschlag zu einem Katalog mit generischen Schutzmaßnahmen vorgelegt. Gegenwärtig (2016) erarbeitet eine Arbeitsgruppe des Arbeitskreises Technik („AK Technik") der Datenschutzbeauftragten des Bundes und der Länder einen solchen Katalog mit, unter den deutschen Aufsichtsbehörden abgestimmten, Datenschutzmaßnahmen.[87]

Tab. 01: Beispiele für generische Schutzmaßnahmen

Schutzziel	Komponente	Maßnahmen
Sicherstellung von Verfügbarkeit	Daten, Systeme, Prozesse	Redundanz, Schutz, Reparaturstrategie
Sicherstellung von Integrität	Daten	Hash-Wert-Vergleich[88]
	Systeme	Einschränkung von Schreibrechten, regelmäßige Integritätsprüfungen
	Prozesse	Festlegung von Referenzwerten (min/max), Steuerung der Regulation
Sicherstellung von Vertraulichkeit	Daten, Systeme	Verschlüsselung
	Prozesse	Rechte- und Rollenkonzepte
Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung	Daten	Anonymität, Pseudonymität, attributbasierte Credentials
	Systeme	Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen
	Prozesse	Identity Management, Anonymitätsinfrastrukturen, Audits

Schutzziel	Komponente	Maßnahmen
Sicherstellung von Transparenz durch Prüffähigkeit	Daten	Dokumentation, Protokollierung
	Systeme	Systemdokumentation, Protokollierung von Konfigurationsänderungen
	Prozesse	Dokumentation von Verfahren, Protokollierung
Sicherstellung von Intervenierbarkeit durch Ankerpunkte	Daten	Zugriff auf Daten für den Betroffenen (Auskunft, Berichtigung, Sperrung, Löschung)
	Prozesse	Helpdesk/einheitlicher Ansprechpartner für Änderungen/Löschungen, Change Management

Tab. 01 (Fortsetzung): Beispiele für generische Schutzmaßnahmen

Diese Liste führt auf, welche Maßnahmen zur Gewährleistung der verschiedenen Schutzziele ergriffen werden können. Der bislang noch in Erarbeitung befindliche Maßnahmenkatalog des AK Technik sieht eine Reihe von Maßnahmen vor (ähnlich Tab. 01). Es ist künftig sicherzustellen, dass die Liste stets die technisch besten verfügbaren Maßnahmen aufführt.[89]

Im Rahmen der Risikobewertung sind Abweichungen danach zu gewichten und zu beurteilen, inwieweit sie das Erreichen der Schutzziele gefährden (Abb. 03). Aus Sicht der Aufsichtsbehörden besteht ein datenschutzrechtlicher Mangel, wenn eine solche Analyse ergibt, dass die Schutzziele nicht in ausreichendem Maße erfüllt werden. Im Rahmen ihres Beratungsauftrags kann die Aufsichtsbehörde zur Beseitigung eines solchen Mangels dann konkrete Hilfestellung leisten.

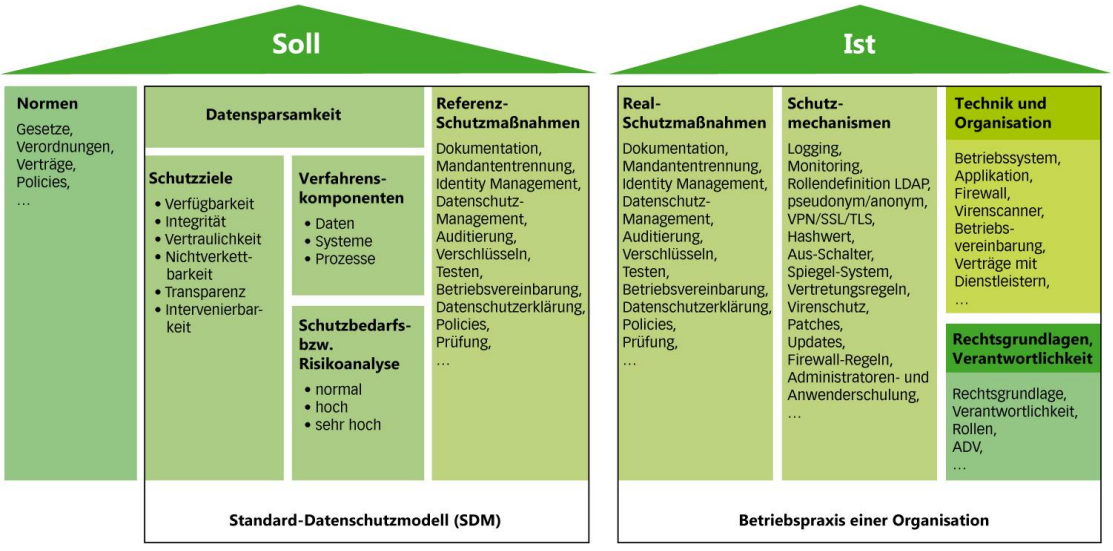

Abb. 03: Soll-Ist-Vergleich im Rahmen der Risikobewertung

In der Praxis lässt sich mit nur geringem Aufwand feststellen, dass Anforderungen nicht erfüllt werden, weil die zugeordneten Maßnahmen und die gebotene Qualität der Umsetzung entsprechend dem Schutzbedarf sofort ersichtlich fehlen. Komplizierter ist der Fall, wenn die zu prüfende Stelle andere als die Referenz-Schutzmaßnahmen gewählt hat. Auch wenn diese als grundsätzlich geeignet beurteilt werden können, kann in Zweifel stehen, dass sie in ihrer konkreten Ausgestaltung dem festgestellten Schutzbedarf entsprechen. Hier ist dann der Nachweis zu führen, dass die getroffene Schutzmaßnahme mindestens denselben Schutz wie die Referenz-Schutzmaßnahme bietet.[90]

Aufbauend auf den bisherigen Ergebnissen ist sodann abschließend eine „klassische" Risikoanalyse vorzunehmen, d. h. zu fragen, ob und mit welcher Wahrscheinlichkeit die

Organisation die Datenschutzbestimmungen nicht einhalten wird (organisationsinterne Gründe). Insbesondere folgende Aspekte sollten betrachtet werden:

- Motivation der Organisation, den Verarbeitungszweck unbefugt zu ändern
- Operative Möglichkeiten der Organisation, den Zweck unbefugt zu ändern
- (Auftrags-)Verarbeitung der Daten in Drittstaaten (möglicherweise abweichendes Schutzniveau, weniger Kontroll- und Rechtsschutzmöglichkeiten)
- Erreichen der festgelegten Anforderungen durch die getroffenen Schutzmaßnahmen, insbesondere Vorliegen von Prozessen zur Konfliktresolution zwischen Informationssicherheit (für Geschäftsprozesse) und operativer Sicherung der Betroffenenrechte.

4.3 Bewertungsphase – ein alternatives Verfahren für wissenschaftliche Datenschutz-Folgenabschätzungen

Für eine wissenschaftliche DSFA bietet sich neben der oben dargestellten Bewertung anhand von standardisierten Katalogen ein offeneres Bewertungsverfahren an, das an Methoden des Risikomanagements nach ISO 31000:2009[91] angelehnt ist und auf einer intensiven Einbeziehung alle Beteiligten basiert. Reines Risikomanagement erfüllt allerdings nach zutreffender Ansicht nicht die Anforderungen der DS-GVO. Ein solcher Bewertungsprozess wird im Folgenden kurz skizziert (vgl. Abb. 04).[92]

Ausgangspunkt einer partizipativen wissenschaftlichen DSFA ist die Überlegung, auf welche Weise welche Akteursgruppen und Interessen im Evaluationsprozess einer Technik- oder Datenschutz-Folgenabschätzung repräsentiert werden können. Dem trägt auch Art. 35 Abs. 9 DS-GVO Rechnung, der vorsieht, dass der Verantwortliche gegebenenfalls die Standpunkte der betroffenen Personen einholt. Mit der elaborierten Expertise technischer Experten allein geht die Gefahr einer verengten Sichtweise und folglich einer technokratisch-paternalistischen Bevormundung Technik-nutzender Bürger einher. Technikfolgenabschätzungsverfahren sind damit immer auch politische Veranstaltungen und die Frage nach dem Einbezug von Betroffenen ist entsprechend als Frage nach der demokratischen Qualität von Technikgestaltung zu verstehen. Schon das Prozedere der relevanten Gruppen weist insofern politische Qualität auf. Wir stellen im Folgenden ein alternatives Modell vor, d. h. ein offeneres Bewertungsverfahren, das zumindest versucht, auf die Frage nach der Demokratisierung von Bewertungsverfahren Antworten zu finden.

Vor allem bei neuen Technologien ist es häufig nicht ausreichend, diese anhand eines bereits existierenden Katalogs zu überprüfen, da sich die Datenschutz- und Privatheitsrisiken mit der technischen Entwicklung erheblich verändern.[93] Darüber hinaus kann sich nicht nur die Bewertung von Risiken zwischen unterschiedlichen Akteursgruppen erheblich unterscheiden, häufig entspricht auch das von den Bürgern wahrgenommene nicht dem tatsächlich vorhandenen Risiko.[94] Beide Effekte sollten aber für die Gestaltung von gesellschaftlich akzeptablen technischen Systemen berücksichtigt werden.

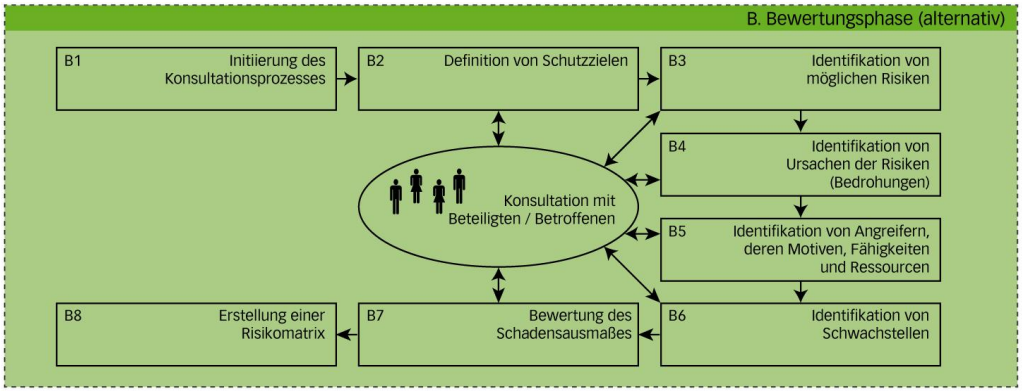

Abb. 04: Elemente eines partizipativen Bewertungsprozesses

Zentral für diesen Ansatz ist die Einbeziehung möglichst aller relevanten Akteure, die bereits während der Vorbereitungsphase identifiziert wurden. Dabei sollte die Frage im Blick behalten werden, welche Akteure überhaupt als „relevant" gelten und wer darüber entscheidet.

Solch eine partizipative Bewertung stellt allerdings Anforderungen an Zeitpunkt und Umstände:

- Bei einer DSFA, die vor der Markteinführung bzw. parallel zum Entwicklungsprozess durchgeführt wird, kann die Einbeziehung von externen Personengruppen u. U. unerwünscht sein, nicht nur weil Betriebs- und Geschäftsgeheimnisse betroffen sind, sondern auch weil aus Imagegründen keine unausgereiften Lösungen präsentiert werden sollen. Es ergibt sich daraus die Anforderung, frühzeitig eine konstruktive Form der Einbindung zu wählen.
- Die Einbeziehung von Betroffenen kann problematisch sein, da eine sorgfältige und systematische Bewertung meist Fachwissen erfordert, das bei technischen Laien nicht vorausgesetzt werden kann. Hier ist somit die Frage maßgeblich, wie sich dieses Fachwissen vermitteln lässt.
- Das für das Bewertungsverfahren verwendete Vokabular hat Folgen für die Intensität und Qualität der Einbeziehung unterschiedlicher Akteursgruppen. So dürften bestimmte Formulierungsweisen etwa besonders technophile Akteure oder solche mit Rechtskenntnissen begünstigen. Fraglich ist daher, wie sich Übersetzungsprozesse zwischen den beteiligten Gruppen erfolgreich gestalten lassen.

Partizipative DSFAen unter Einbeziehung von Externen werden vermutlich schon deswegen eher die Ausnahme bleiben, da dieser Prozess zeitaufwendiger ist und es ansonsten bei bestimmten Akteursgruppen rasch zu einer „Konsultationsmüdigkeit" kommen könnte.

Methodisch stehen verschiedene partizipatorische Verfahren zur Verfügung, wobei sich beispielsweise die Nutzung von Fokusgruppen anbietet, mit denen viele Unternehmen in den Bereichen Produktgestaltung und Marketing Erfahrung haben.[95]

Im Rahmen der Konsultation wird mit allen Beteiligten Folgendes analysiert:

- Welche Werte bzw. Schutzziele werden bei der betrachteten Technologie bzw. dem betrachteten System als besonders relevant erachtet? Dabei sind die Schutzziele des Datenschutzes (Abschnitt 4.2.1) Ausgangspunkt der Analyse. Sie sollte sich allerdings nicht darauf beschränken. Vielmehr sollen auch andere Werte diskutiert werden, die durch die Technik berührt werden und ggf. im Wechselverhältnis zueinander stehen. Dazu können etwa Fragen der Gerechtigkeit bzw. Diskriminierungsfreiheit, der Kosten oder der Sicherheit gehören, die von den verschiedenen Beteiligten durchaus als unterschiedlich wichtig erachtet werden können.[96]
- Was sind Risiken (Schadensereignisse), die es mit Blick auf die Schutzziele zu vermeiden gilt?[97]
- Was sind die Ursachen eines Risikos (Bedrohung): Wer ist bei diesen Schadensereignissen der Angreifer? Was sind die Motive des Angreifers? Über welche Schwachstelle findet der Angriff statt? Welche Fähigkeiten und Ressourcen sind für die erfolgreiche Durchführung eines Angriffs notwendig? Wie groß ist die Wahrscheinlichkeit eines erfolgreichen Angriffs?
- Welche Folgen hat die Realisierung eines Risikos: Auf welche Weise treten Schäden auf? Wer wird geschädigt? Welchen Charakter haben die Schäden? Welches Schadensausmaß ist zu erwarten?

Auch die Bewertungskriterien und -maßstäbe können im Austausch zwischen den beteiligten Gruppen festgelegt werden. Da es sich allerdings meist um qualitative Bewertungen handelt, ist auch bei einer partizipativen Bewertung der Datenschutzfolgen die Nutzung der in Abschnitt 4.2.3 erläuterten Skala für die Beurteilung des Schadensaus-

maßes sinnvoll. In ähnlicher Granularität sollte auch die Eintrittswahrscheinlichkeit der verschiedenen Angriffe bewertet werden (beispielsweise in fünf Stufen von unwahrscheinlich bis sehr wahrscheinlich). Die Größe des Risikos wird dann als Produkt von Eintrittswahrscheinlichkeit und Schadensausmaß bestimmt.

Im abschließenden Schritt werden die Wahrscheinlichkeit und das Schadensausmaß für jedes Risiko in einer Risikomatrix eingetragen (vgl. Abb. 05).

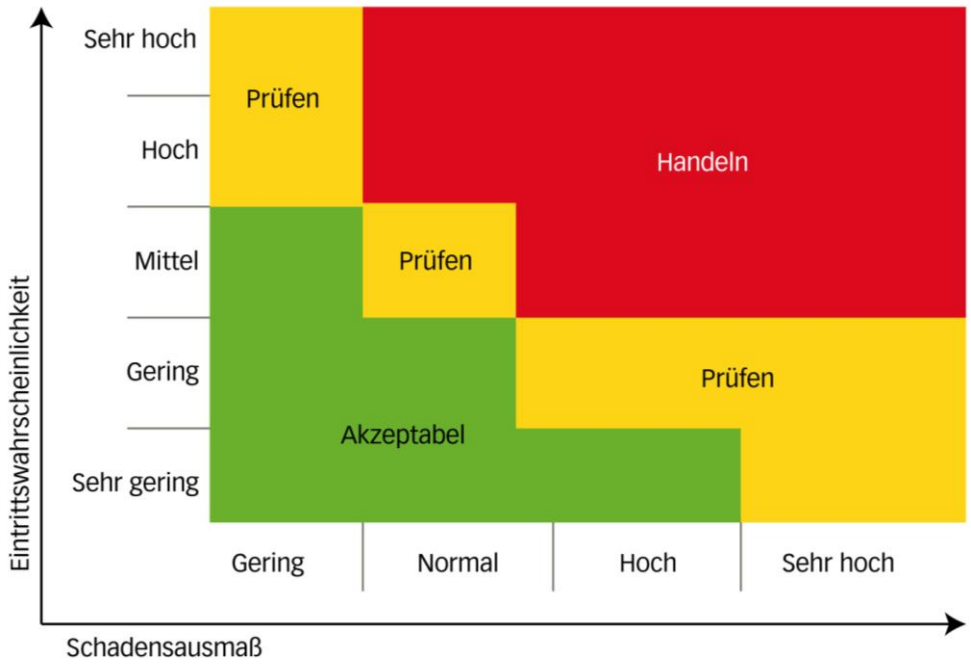

Abb. 05: Risikomatrix

Je nach der Lage innerhalb der Matrix kann dann festgelegt werden, welchen Risiken prioritär zu begegnen ist und welche Risiken ggf. akzeptabel sind. Dabei kann auch berücksichtigt werden, dass in der Regel die finanziellen und/oder personellen Ressourcen begrenzt sind, die zur Vermeidung von Risiken zur Verfügung stehen (sog. ALARP-Prinzip – *as low as reasonably practicable*). Eine hohe Priorität des Handelns besteht bei solchen Risiken, die eine hohe Eintrittswahrscheinlichkeit haben und potenziell großen Schaden verursachen können. Akzeptabel können solche Risiken sein, die entweder wenig wahrscheinlich sind oder nur geringen Schaden nach sich ziehen.

Eine solche Bewertung lässt die Einhaltung gesetzlicher Vorgaben unberührt. So kann die Risikobewertung zu dem Schluss führen, dass das Risiko aus Sicht einer Organisation akzeptabel ist, weil nur die Rechte Einzelner betroffen sind. Das genau widerspricht aber dem Verständnis des Datenschutzes als Grundrechtsschutz.

Dennoch kann die probabilistische Bewertung des Risikos hilfreich sein, da sie es ermöglicht, unterschiedliche Interessen und Rahmenbedingungen im Wechselspiel zu betrachten. Im Fall von fundamentalen Konflikten zwischen Werten und/oder Akteuren können so Anstöße zur Um- oder Neugestaltung entstehen.

4.4 Schutzmaßnahmen, Veröffentlichung und Überprüfung

4.4.1 Identifikation und Implementierung passender Schutzmaßnahmen

Auf Grundlage der Bewertungsergebnisse ist ein Plan zur Risikobehandlung zu erstellen. Dabei ist zu beachten, dass es in vielen Fällen – insbesondere bei Auswirkungen auf verfassungsmäßig geschützte Individualrechte – nicht möglich ist, ein Risiko mit Hinweis auf die u. U. geringe Zahl der Geschädigten als akzeptabel einzustufen und

nur Maßnahmen zur Verminderung der Schäden zu ergreifen. Insbesondere bei dem in Abschnitt 4.3 geschilderten Bewertungsverfahren besteht allerdings die Möglichkeit, Risiken zu priorisieren, um dann im Rahmen der rechtlichen Vorgaben und der zur Verfügung stehenden Ressourcen diejenigen Maßnahmen zu ergreifen, die zusammengenommen den größten Nutzen für die Betroffenen haben.

Der Maßnahmenplan sollte explizit benennen,

- welche Schutzmaßnahmen ergriffen werden sollen, um den Grundrechtseingriff und konkrete Schäden für Betroffene zu vermeiden oder zu verringern,
- wer für die Umsetzung der Schutzmaßnahmen verantwortlich und wer daran zu beteiligen ist,
- bis wann diese Schutzmaßnahmen umgesetzt sein sollen und welche Mittel dafür zur Verfügung gestellt werden,
- nach welchen Kriterien der Erfolg einer Schutzmaßnahme beurteilt werden soll und
- wer diese Beurteilung durchführt und dokumentiert.

Um die Wahl geeigneter Schutzmaßnahmen zu erleichtern, kann die Liste der generischen Schutzmaßnahmen genutzt werden, die bereits für die Bewertung des Risikos (vgl. Abschnitt 4.2.4) eingesetzt wurde.

4.4.2 Dokumentation und Veröffentlichung des Ergebnisberichts

Damit eine DSFA die anfangs erwähnten Effekte erzielen kann, ist es notwendig, dass der Prozess umfänglich dokumentiert und in Form eines Berichts öffentlich zugänglich gemacht wird. Ein solcher DSFA-Bericht sollte – wie schon der Scoping-Bericht – einer standardisierten Gliederung folgen, die es Aufsichtsbehörden, Unternehmen und der Öffentlichkeit erleichtert, die Ergebnisse zu bewerten und zu vergleichen.

Wenn der Bericht auch Details über Betriebs- und Geschäftsgeheimnisse enthält, kann für die Öffentlichkeit eine gekürzte Fassung erstellt werden. Der Kurzbericht soll aber genau wie der vollständige Bericht alle Elemente der DSFA dokumentieren und darf keinesfalls mögliche negative Effekte verschweigen.[98] Die Entscheidung, dass bestimmte Informationen nicht zu veröffentlichen sind, sollte nur aus berechtigten und zu dokumentierenden Gründen erfolgen.

Aus Gründen der Transparenz ist es angeraten, den DSFA-Bericht zu veröffentlichen; er sollte auf der Internetseite der Organisation leicht auffindbar und kostenlos zu beziehen sein, obwohl dies nicht explizit in der DS-GVO gefordert ist. Ggf. kommt auch eine Hinterlegung von DSFA-Berichten bei der zuständigen Aufsichtsbehörde in Betracht.

Der vollständige Bericht ist Grundlage der Prüfung der DSFA und sollte auch als Grundlage für Kontrollen durch Datenschutzaufsichtsbehörden dienen können.

4.4.3 Unabhängige Prüfung der Prüfergebnisse

DSFA-Berichte sollten in der Regel durch eine unabhängige dritte Stelle – ggf. auch durch die zuständige Datenschutzaufsicht – geprüft werden, um sicherzustellen, dass der DSFA-Prozess ordnungsgemäß durchgeführt wurde. Insbesondere soll die Überprüfung sicherstellen, dass

- angemessen mit Interessenkonflikten umgegangen wurde,
- die Interessen der Betroffenen bei der Risikobewertung und der Auswahl von Schutzmaßnahmen in ausreichendem Umfang berücksichtigt wurden,
- die Öffentlichkeit in ausreichendem Umfang über die Ergebnisse der DSFA informiert wird und
- die Implementierung der vorgeschlagenen Schutzmaßnahmen tatsächlich in Angriff genommen wurde.

4.4.4 Überwachung und Fortschreibung

Die Abschätzung von Datenschutzfolgen ist kein einmaliger und linearer Prozess, sondern muss über die Lebensdauer eines Prüfgegenstands ggf. mehrfach wiederholt werden. Insofern ist kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischer, organisatorischer oder rechtlicher Weise ändern, die neue Datenschutzrisiken nach sich ziehen. Auch ist zu überwachen, ob die gewählten Schutzmaßnahmen den erwarteten Nutzen haben oder ob andere Maßnahmen zu ergreifen sind. Die Dokumentation der DSFA ist mit solchen Informationen kontinuierlich fortzuschreiben.

5
Diskussion – Was kann eine Datenschutz-Folgenabschätzung leisten?

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein relativ neues Instrument zur Identifikation von Risiken, die durch den Einsatz von (neuen) vorwiegend datenverarbeitenden Technologien und Systemen für die Grundrechte der Bürger auf Achtung des Privatlebens und den Schutz personenbezogener Daten nach Art. 7 und 8 Charta entstehen. Die Nutzung dieses Instruments wird durch die Datenschutz-Grundverordnung in bestimmten Fällen obligatorisch vorgeschrieben. Da es bislang keinen allgemein akzeptierten Standard für die Durchführung einer DSFA gibt, haben wir in diesem White Paper Vorschläge für einen Prozess gemacht, mit dem – je nach angewandtem Modell – nach wissenschaftlichen Erkenntnissen bzw. Erfahrungen aus der Praxis der Datenschutzbehörden die Analyse einer Technologie oder eines Systems auf Einhaltung der Datenschutzgesetze erfolgen kann. Im Folgenden soll kurz diskutiert werden, welchen Nutzen eine DSFA für die unterschiedlichen Akteure haben kann, aber auch, wo die Grenzen eines solchen Instruments liegen.

Die DSFA ist in erster Linie ein „Frühwarnsystem", das es den beteiligten Akteuren ermöglicht, über die Folgen technischer Entwicklungen und deren Nutzung systematisch nachzudenken sowie mögliche Mängel zu erkennen und zu beseitigen. Dabei ist es entscheidend, vorab festzulegen, welches Ziel mit der DSFA verfolgt wird. Geht es um Erfüllung der neuen gesetzlichen Pflicht nach DS-GVO, muss die Perspektive der Betroffenen eingenommen werden, deren Grundrechte es durch entsprechende System- und Technikgestaltung zu schützen gilt (Standard-DSFA). Aber auch bei einer wissenschaftlichen DSFA sind die Interessen und Befindlichkeiten anderer Gruppen und insbesondere der Betroffenen zu berücksichtigen, die nicht unmittelbar in den Entwicklungsprozess einer Technik oder in die Entscheidung über deren Einsatz beteiligt sind, jedoch in erster Linie von den Folgen berührt sind.

Je nach Zielsetzung, kann eine gute DSFA dabei – über die bloße Pflichterfüllung hinaus – verschiedene Aufgaben erfüllen:

- Für Technikanbieter und Systembetreiber:
  - Eine DSFA stellt eine zuverlässige und nachvollziehbare Quelle dar, die eine informierte Diskussion über Risiken und deren Ursachen ermöglicht.
  - Die Analysen im Rahmen einer DSFA machen Verantwortlichkeiten und Zuständigkeiten zur Gewährleistung von Datenschutzvorkehrungen auf unterschiedlichsten Ebenen in einer Organisation klar.
  - Eine frühzeitige Durchführung einer DSFA ermöglicht bessere Entscheidungen schon in der Entwurfsphase einer Technologie oder eines Systems und verhindert so, dass später aufwändige (und oftmals dennoch unzureichende) Nachbesserungen vorgenommen werden müssen.
  - Eine DSFA kann Datenpannen vorbeugen, die Kosten für deren Behebung, Schadensersatzansprüche, einen Imageschaden in der Öffentlichkeit oder ggf. Sanktionen durch die Aufsichtsbehörden nach sich ziehen können.
  - Zusammengenommen ist eine DSFA ein nützliches Instrument, mit dem Unternehmen nachweisen können, dass sie rechtskonforme Produkte und Dienstleistungen anbieten. Damit fördert sie das Vertrauensverhältnis zwischen Unternehmen, Kunden und Bürgern und kann somit zum Wettbewerbsvorteil werden.
- Für die Öffentlichkeit:
  - Eine DSFA macht deutlich, in welcher Weise ein Anbieter oder Betreiber Betroffenenrechte berücksichtigt hat, insbesondere wenn die DSFA unabhängig überprüft oder sogar mit einer Zertifizierung kombiniert wurde.

- Auf diese Weise können Bürger und Kunden eine (besser) informierte Entscheidung darüber treffen, ob sie bestimmte Angebote nutzen wollen oder nicht.
- Für die Aufsichtsbehörden:
  - Standardisierte DSFA erleichtern den Aufsichtsbehörden die Erfüllung ihrer Aufsichtspflicht, d. h. mögliche Schwächen oder Rechtsverstöße zu erkennen und
  - den Anbietern im Rahmen ihrer Beratungsaufgabe Hilfestellung zur Verbesserung ihrer Produkte bzw. Datenverarbeitung zu geben.

Diskussion – Was kann eine Datenschutz-Folgenabschätzung leisten?

Damit sich das volle Potenzial wirklich entfalten kann, muss allerdings sichergestellt werden, die DSFA nicht nur als einmalige Aktion zu verstehen, sondern als kontinuierlichen Prozess, der während des Produktlebenszyklus bzw. der Durchführung der konkreten Datenverarbeitung ganz oder teilweise mehrfach durchgeführt werden sollte. Der Grund hierfür liegt im sogenannten Steuerungsdilemma, das aus dem Bereich der klassischen Technikfolgenabschätzung bekannt ist:[99] Kern dieses Dilemmas ist die Forderung, dass eine Folgenabschätzung möglichst frühzeitig erfolgen sollte, um noch Änderungen in der Gestaltung vornehmen zu können. Gleichzeitig ist es aber notwendig, die zu bewertende Technologie oder den zu bewertenden Prozess so genau wie möglich zu beschreiben und zu charakterisieren, was erst in späteren Entwicklungsphasen möglich ist, wenn grundsätzliche Gestaltungsentscheidungen längst gefallen sind und nicht mehr ohne Weiteres geändert werden können.

Wenig zielführend sind aus diesem Grund auch in großer Eile und unmittelbar vor Produkteinführung durchgeführte DSFAen, die vor allem den Zweck haben, der Öffentlichkeit und den Aufsichtsbehörden ein positives Bild zu vermitteln, indem bestimmte Probleme ausgeklammert werden. Dies kann etwa durch einen zu engen Fokus beim Prüfgegenstand wie die Ausklammerung technischer und organisatorischer Fragen und die Fokussierung auf rein rechtliche Fragestellungen erfolgen.

Es darf allerdings nicht unerwähnt bleiben, dass eine DSFA (wie jedes formalisierte Verfahren) auch festlegt, was *außerhalb* des Bewertungsrahmens bleiben muss. Aus diesem Grund sind wissenschaftlich orientierte DSFAen z. B. für den Bereich der Forschung und Entwicklung sinnvoll, auch wenn sie die Anforderungen der DS-GVO an eine DSFA nicht unbedingt erfüllen. Sie ermöglichen es aber, Fragen des Datenschutzes in das Risikomanagement der Technikproduzenten und Systembetreiber zu integrieren. Damit kann eine in der Technikfolgenabschätzung häufig vermisste Balance zwischen dem Verlangen nach Normativität auf der einen und nach Operationalisierung auf der anderen Seite[100] hergestellt werden.

Anmerkungen

[1] Hallinan, D.; Friedewald, M. (2012): Public Perception of the Data Environment and Information Transactions: A selected-survey analysis of the European public's views on the data environment and data transactions. In: Communications and Strategies Nr. 88, S. 61-78. http://ssrn.com/abstract=2374358 (10.03.2016).

[2] Der Begriff des „Angreifers" ist im Kontext von Datenschutz und Informationssicherheit die gängige Bezeichnung für jeden Akteur, der – absichtlich oder unabsichtlich – die jeweiligen Schutzziele verletzt. Der Begriff beschränkt sich nicht nur auf unautorisierte externe Angreifer, die ein System vorsätzlich und häufig mit kriminellen Absichten angreifen. Gerade im Kontext des Datenschutzes entstehen Angriffe auf die Betroffenenrechte häufig aus dem bestimmungsgemäßen Betrieb eines Systems durch autorisierte Personen.

[3] Rost, M. (2013): Zur Soziologie des Datenschutzes. In: DuD - Datenschutz und Datensicherheit 37, Nr. 2, S. 85-91.

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) . In: Amtsblatt der Europäischen Gemeinschaften L 119, Mai 2016, S. 1-88.

[5] Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos, S. 47.

[6] Ausführlich zum Beispiel Roßnagel, A. (Hrsg.) (1989): Freiheit im Griff, Informationsgesellschaft und Grundgesetz. Stuttgart: Hirzel., S. 9ff.; Roßnagel, A. (1997): Rechtswissenschaftliche Technikfolgenabschätzung am Beispiel der Informations- und Kommunikationstechnik. In: Schulte, M.; Di Fabio, U. (Hrsg.): Technische Innovation und Recht, Antrieb oder Hemmnis? Heidelberg: C.F.Müller, S. 139-162, hier S. 139ff.; Roßnagel, A. (1997): Verfassungsverträglichkeit der Informations- und Kommunikationstechniken. In: Westphalen, R. G. v. (Hrsg.): Technikfolgenabschätzung als politische Aufgabe, 3. Aufl. München und Wien: Oldenbourg, S. 266 - 280, hier S. 266f.

[7] Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos, S. 47 mit weiteren Nachweisen; Grunwald, A. (2010): Technikfolgenabschätzung - eine Einführung. Berlin: Edition Sigma (Gesellschaft – Technik – Umwelt. Neue Folge, 1)., S. 67;Grunwald, A.; Hennen, L.; Sauter, A. (2014): Parlamentarische Technikfolgenabschätzung. In: Aus Politik und Zeitgeschichte (APuZ) 64, Nr. 6/7, S. 17-24. http://www.bpb.de/apuz/177763/parlamentarische-technikfolgenabschaetzung?p=all (10.03.2016).

[8] Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) mit wechselnden Partnern betrieben. http://www.tab-beim-bundestag.de (10.03.2016).

[9] http://www.eptanetwork.org (10.03.2016).

[10] Grunwald, A. (2010): Technikfolgenabschätzung - eine Einführung. Berlin: Edition Sigma (Gesellschaft – Technik – Umwelt. Neue Folge, 1), S. 85ff.

[11] Ebd., S. 82ff.

[12] Roßnagel, A. (1983): Bedroht die Kernenergie unsere Freiheit: Das künftige Sicherungssystem kerntechnischer Anlagen. München: C. H. Beck; Zweck, A. (1993): Die Entwicklung der Technikfolgenabschätzung zum gesellschaftlichen Vermittlungsinstrument. Opladen: Westdeutscher Verlag (Studien zur Sozialwissenschaft, 128). Kuhlmann, S. (2013): Strategische und konstruktive

Technikfolgenabschätzung. In: Simonis, G. (Hrsg.): Konzepte und Verfahren der Technikfolgenabschätzung. Wiesbaden: Springer VS, S. 129-143.

[13] Zum Beispiel Riehm, U.; Wingert, B. (1995): Multimedia - Mythen, Chancen und Herausforderungen. Mannheim: Bollmann. Ein Ein Überblick über Studien im europäischen Ausland findet sich in Gieguth, G.; Wingert, B. (1996). TA-Studien im Bereich Informationstechnologie - eine Auswertung von sechs Studien eurpäischer parlamentarischer TA-Einrichtungen. TAB-Arbeitsbericht 38. Bonn: Büro für Technikfolgen-Abschätzung bei Deutschen Bundestag.
Mit den Fragen der Auswirkungen von Technikfolgen auf Rechtsnormen (einschließlich Freiheitsrechten und Folgen für die Demokratie) befasst sich zudem systematisch die rechtswissenschaftliche Technikfolgenforschung, Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos.

[14] § 1 Abs. 1 Nr. 1 Hessisches Datenschutzgesetz (HDSG). Im HDSG 1970 fand sich noch keine entsprechende Formulierung, in den Hessischen Datenschutzgesetzen 1978, 1986 sowie 1999 dann schon. Ähnlich auch § 1 Abs. 1 Niedersächsisches Datenschutzgesetz (NDSG) 1978: „Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken".

[15] Gemäß § 1 Abs. 1 Nr. 2 HDSG. Im HDSG 1970 fand sich noch keine entsprechende Formulierung, in den Hessischen Datenschutzgesetzen 1978, 1986 sowie 1999 dann schon. Die Überwachung der Einhaltung obliegt dem Hessichen Landesdatenschutzbeauftragten, § 23 Abs. 2, später § 24 Abs. 2 HDSG. Ähnliche Wortlaute finden sich auch in anderen Datenschutzgesetzen, etwa in § 1 Nr. 2 NDSG 1993.

[16] Zum Beispiel § 6 Abs. 1 BDSG 1977; § 10 Abs. 1 HDSG 1978; § 6 Abs. 1 NDSG 1978.

[17] Such, M.; Fraktion Bündnis 90/Die Grünen (1997). Entwurf eines Bundesdatenschutzgesetzes (BDSG). Drucksache 13/9082 Bonn: Deutscher Bundestag, S. 9; dazu auch Weichert, T. (1999): Der Entwurf eines Bundesdatenschutzgesetzes von Bündnis 90/Die Grünen. In: Recht der Datenverarbeitung (RDV) 15, Nr. 2, S. 65-69, hier S. 65f.

[18] Siehe dazu Roßnagel, A.; Pfitzmann, A.; Garstka, H. (2001). Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern Berlin: Bundesministeriums des Innern. http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile (10.03.2016).

[19] § 1 Abs. 1 BDSG 1990 sowie 2003.

[20] § 1 Satz 1 NDSG 2002.

[21] Zum Beispiel § 9 BDSG 1990 und 2003; § 10 HDSG 1986; § 10 Abs. 1, 2 HDSG 2001.

[22] Zum Begriff „Verfahren" und dessen Umfang vgl. Spindler, G.; Schuster, F.; Döpkens, H.-R. (2015): Recht der elektronischen Medien. 3. Aufl. München: Beck., § 4d BDSG, Rn. 10. Zur Vorabkontrolle vgl. Voßbein, R. (2003): Vorabkontrolle gemäß BDSG, Anwendungsgebiete und Zusammenhang mit IT-SEC und CC. In: DuD - Datenschutz und Datensicherheit 27, Nr. 7, S. 427-432, hier S. 427; Voßbein, R. (2002): Vorabkontrolle und Datenschutzaudit - Gemeinsamkeiten und Unterschiede. In: Recht der Datenverarbeitung (RDV) 18, Nr. 6, S. 322-325, hier S. 322; Schild, H.-H. (2001): Meldepflichten und Vorabkontrolle. In: DuD - Datenschutz und Datensicherheit 25, Nr. 5, S. 282-286, hier S. 282

[23] Simitis, S. (2014): Kommentar zum Bundesdatenschutzgesetz. 8. Aufl. Baden-Baden: Nomos., § 4d BDSG, Rn. 35.

Anmerkungen

[24] Richtlinie 95/46/EG (1995): Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. In: Amtsblatt der Europäischen Gemeinschaften L 281, Nr. 23. November 1995, S. 31-50.

[25] Dammann, U.; Simitis, S. (1997): EG-Datenschutzrichtlinie, Kommentar. Baden-Baden: Nomos, Art 20, Rn. 2.

[26] Engelien-Schulz, T. (2003): Die Vorabkontrolle gemäß § 4d Abs. 5 und Abs. 6 Bundesdatenschutzgesetz (BDSG). In: Recht der Datenverarbeitung (RDV) 19, Nr. 6, S. 270-278, hier S. 271f., 274, dort insbesondere Fn. 25. Zur Umsetzung des Art. 20 DSRL in den einzelnen Mitgliedstaaten der Europäischen Union siehe Le Grand, G.; Barrau, E. (2012): Prior Checking, a Forerunner to Privacy Impact Assessments. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 97-116.

[27] Engelien-Schulz, T. (2003): Die Vorabkontrolle gemäß § 4d Abs. 5 und Abs. 6 Bundesdatenschutzgesetz (BDSG). In: Recht der Datenverarbeitung (RDV) 19, Nr. 6, S. 270-278, hier S. 276ff.

[28] Verfahren = Gesamtheit aller Verarbeitungsschritte zur Erfüllung eines Zwecks. Vgl. Nungesser, J. (Hrsg.) (2001): Hessisches Datenschutzgesetz, unter Berücksichtigung der EG-Datenschutzrichtlinie. Kommentar für die Praxis. Stuttgart: Deutscher Gemeindeverlag, § 6 HDSG, Rn. 4.

[29] Wright, D.; De Hert, P. (2012): Introduction to Privacy Impact Assessment. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 3-32, hier S. 8, jeweils mit weiteren Nachweisen.

[30] Ebd., S. 9; Clarke, R. (2011): An Evaluation of Privacy Impact Assessment Guidance Documents. In: International Data Privacy Law 1, Nr. 2, S. 111-120.

[31] Bayley, R. M.; Bennett, C. J. (2012): Privacy Impact Assessments in Canada. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 161-185.

[32] Edwards, J. (2012): Privacy Impact Assessment in New Zealand - A Practitioner's Perspective. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 187-204.

[33] Bamberger, K. A.; Mulligan, D. K. (2012): PIA Requirements and Privacy Decision-making in US Government Agencies. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 225-250.

[34] Clarke, R. (2012): PIAs in Australia: A Work-in-Progress Report. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 119-148.

[35] ICO (Information Commissioner's Office) (2007). Privacy impact assessment handbook. Wilmslow: UK Information Commissioner's Office.; ersetzt durch ICO (Information Commissioner's Office) (2014). Conducting privacy impact assessments code of practice. Wilmslow: UK Information Commissioner's Office. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (10.03.2016). Die britische Datenschutzaufsichtsbehörde empfiehlt PIA darüberhinaus in ihrem Datenschutz-Handbuch als Bestandteil des Privacy-by-Design-Ansatzes, https://ico.org.uk/for-organisations/guide-to-data-protection/ (10.03.2016). Vgl. auch Warren, A.; Charlesworth, A. (2012): Privacy Impact Assessment in the UK. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact

Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 205-224.

[36] Im Einzelnen Wright, D.; De Hert, P. (2012): Introduction to Privacy Impact Assessment. In: Wright, D.; De Hert, P. (Hrsg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer (Law, Governance, and Technology, 6), S. 3-32, hier S. 6f. Die Autoren verstehen PIA als Prozess, der die Technikentwicklung begleiten soll, bis diese einsatzfähig ist und dabei die betroffenen Beteiligten in die Bewertung mit einbindet.

[37] Ein ausführlicher Vergleich ist nachzulesen in ebd., S. 17ff.

[38] ICO (Information Commissioner's Office) (2014). Conducting privacy impact assessments code of practice. Wilmslow: UK Information Commissioner's Office. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (10.03.2016).

[39] Ebd., S. 5.

[40] Ebd., S. 20f.

[41] Ebd., S. 22.

[42] Ebd., S. 23-5.

[43] Ebd., S. 28.

[44] Ebd., S. 27.

[45] Ebd., S. 28.

[46] Ebd., S. 12-14.

[47] Ebd., S. 16-18.

[48] Ebd., S. 18f.

[49] CNIL (Commission Nationale de l'Informatique et des Libertés) (2015). Privacy Impact Assessment: Methodology (how to carry out a PIA). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (10.03.2016).

[50] CNIL (Commission Nationale de l'Informatique et des Libertés) (2015). Privacy Impact Assessment: Tools (templates and knowledge bases). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-2-Tools.pdf (10.03.2016).

[51] CNIL (Commission Nationale de l'Informatique et des Libertés) (2012). Measures for the Privacy Risk Treatment. Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-3-GoodPractices.pdf (10.03.2016).

[52] Europäische Kommission (2009): Empfehlung vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. In: Amtsblatt der Europäischen Union vom 16.05.2009, S. 47-51. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009H0387&from=DE (10.03.2016).

[53] Europäische Kommission (2012): Empfehlung vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme. In: Amtsblatt der Europäischen Union vom 13.03.2012, S. 9-22. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012H0148&from=DE (10.03.2016).

[54] Artikel-29-Datenschutzgruppe (2010). Stellungnahme 5/2010 zum Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen Arbeitspapier 00066/10/DE, WP 175. Brüssel. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp175_de.pdf (10.03.2016); Artikel-29-Datenschutzgruppe (2013). Stellungnahme 07/2013 zum Muster für die Datenschutzfolgenabschätzung für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der

Anmerkungen

Kommission für intelligente Netze Working Paper 2064/13/DE, WP 209. Brüssel. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_de.pdf (10.03.2016).

55 Ebd., S. 12.

56 Ebd., S. 7f.

57 Ebd., S. 11.

58 Ebd.

59 Europäische Kommission (2012): Empfehlung vom 9. März 2012 zu Vorbereitungen für die Einführung intelligenter Messsysteme. In: Amtsblatt der Europäischen Union vom 13.03.2012, S. 9-22, hier Punkt 5, S. 11. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32012H0148&from=DE (10.03.2016).

60 Artikel-29-Datenschutzgruppe (2013). Stellungnahme 07/2013 zum Muster für die Datenschutzfolgenabschätzung für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze Working Paper 2064/13/DE, WP 209. Brüssel, S. 5. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_de.pdf (10.03.2016).

61 Ebd., S. 6f.

62 Ebd., S. 7f.

63 Ebd., S. 12f.

64 Art. 38 DS-GVO

65 Das aus 2012 stammende Dokument bezieht sich insoweit selbstverständlich noch auf die Richtlinie 95/46/EG. Eine Anpassung an die DS-GVO ist jedoch zu erwarten.

66 Elemente des Risikomanagements waren allerdings implizit bereits in Art 17 und 20 der Richtlinie 95/46/EG formuliert.

67 So zum Beispiel Jan Philipp Albrecht, Verhandlungsführer des Europäischen Parlaments für die geplante Datenschutzverordnung. https://www.janalbrecht.eu/presse/pressemitteilungen/eu-datenschutz.html (10.03.2016). Ähnliche Bedenken formulierte die Artikel-29-Datenschutzgruppe (2014). Statement on the role of a risk-based approach in data protection legal frameworks. Working Paper 14/EN, WP 218. Brüssel. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (10.03.2016).

68 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Schulz, G.; Rost, M. (2015). Das Standard-Datenschutzmodell - der Weg vom Recht zur Technik: Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen. https://www.datenschutzzentrum.de/uploads/sdm/SDM_Tagungsband2015_Hannover.pdf (10.03.2016).

69 Clarke, R. (2011): An Evaluation of Privacy Impact Assessment Guidance Documents. In: International Data Privacy Law 1, Nr. 2, S. 111-120; Wadhwa, K. (2012): Privacy impact assessment reports: a report card. In: Info - The Journal of policy, regulation and strategy for telecommunications, information and media 14, Nr. 3, S. 35 - 47; Wright, D.; Gellert, R.; Bellanova, R. et al. (2013). Privacy Impact Assessment and Smart Surveillance: A State of the Art Report. Deliverable 3.1. SAPIENT Project; Wright, D.; Wadhwa, K.; Lagazio, M. et al. (2014): Integrating privacy impact assessment in risk management. In: International Data Privacy Law 4, Nr. 2, S. 155-170.

70 Wright, D.; Kroener, I.; Friedewald, M. et al. (2014). A guide to surveillance impact assessment - How to identify and prioritise for treatment risks arising from

surveillance systems. Deliverable 4.4. SAPIENT Project. http://www.sapientproject.eu/SIA_Manual.pdf (10.03.2016).

71 Rost, M. (2013). Anforderungen an ein PIA aus Sicht einer Datenschutzaufsichtsinstanz. Handreichung 2013-1014. Kiel: Unabhängiges Landesdatenschutzzentrum Schleswig-Holstein.

72 Stellvertretend sei hier das Privacy Impact Assessment genannt, das Anfang 2008 vom britischen Unternehmen Phorm in Auftrag gegeben wurde. Phorm ist ein Online-Werbeanbieter, der für seine Angebote Internet-Datenpaketen (sog. *Deep Packet Inspection*) untersuchte und Nutzerprofile erstellte. Der unter Fachleuten und Datenschutzbehörden kontrovers diskutierte DSFA-Bericht kam zu dem Schluss, Phorm verarbeite dabei überhaupt keine personenbezogenen Daten. Vgl. 80/20 Thinking Ltd. (2008). [Phorm] Privacy Impact Assessment. London. http://web.archive.org/web/20110701052220/http://www.phorm.com/assets/reports/Phorm_PIA_Final.pdf (10.03.2016).

73 Wright, D.; Friedewald, M. (2013): Integrating privacy and ethical impact assessment. In: Science and Public Policy 40, Nr. 6, S. 755-766; Wright, D.; Friedewald, M.; Gellert, R. l. (2015): Developing and Testing a Surveillance Impact Assessment Methodology. In: International Data Privacy Law 5, Nr. 1, S. 40-53.

74 von Schomberg, R. (2013): A vision of Responsible Research and Innovation. In: Owen, R.; Bessant, J. et al. (Hrsg.): Responsible Innovation. London: John Wiley, S. 51-74; Stahl, B. C. (2013): Responsible Research and Innovation: The Role of Privacy in an Emerging Framework. In: Science and Public Policy 40, Nr. 6, S. 708-716.

75 Mitarbeiter sind als Vertreter der datenverarbeitenden Organisation als potenzielle und als Arbeitnehmer als potenzielle Betroffene zu betrachten.

76 Art. 3 DS-GVO

77 Art. 6 DS-GVO

78 Für den öffentlichen Bereich in Art. 1 Abs. 2a DS-GVO-Rat; Beschränkungen der Betroffenenrechte in Art. 21 DS-GVO-Rat; Gesundheits- und Sozialbereich in Art. 9 Abs. 2 lit. h DSGVO-Rat oder auch Art. 80 ff. DS-GVO-Rat, um nur einige zu nennen.

79 Etwa dann, wenn delegierte Rechtsakte für die Kommission vorgesehen wurden, die aber ersatzlos entfallen sind, ohne die Voraussetzungen in der DS-GVO selbst zu regeln.

80 Rost, M. (2012): Standardisierte Datenschutzmodellierung. In: DuD - Datenschutz und Datensicherheit 35, Nr. 6, S. 433-438.

81 Die Entwicklung erfolgte aufbauend auf den bereits etablierten Schutzzielen der IT-Sicherheit. U. a. zur Vermeidung von Begriffskollisionen ist in der deutschen Datenschutzkonferenz die offizielle Bezeichnung „Gewährleistungsziele" vereinbart worden. Dies entspricht dem materiellen Gehalt der Ziele als bei der Datenverarbeitung „zu gewährleistende" Maßgaben.

82 Rost, M.; Bock, K. (2011): Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. In: DuD - Datenschutz und Datensicherheit 35, Nr. 1, S. 30-35; Rost, M.; Pfitzmann, A. (2009): Datenschutz-Schutzziele—revisited. In: DuD - Datenschutz und Datensicherheit 33, Nr. 6, S. 353-358.

83 Hinweis: Das Standard-Datenschutzmodell (SDM), das den Kriterienkatalog für ein an Grundrechten orientiertes DPIA anliefert, weist Datensparsamkeit als ein eigenständiges, siebentes Gewährleistungsziel aus.

84 Zu den Interessen verschiedener Akteure an personenbezogenen Daten in der Arbeitswelt vgl. Hess, T.; Matt, C.; Morlok, T. (Hrsg.) (2015): Privatheit und Datenflut in der neuen Arbeitswelt – Chancen und Risiken einer erhöhten Transparenz. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). Zur Wertschöpfung in Datenmärkten vgl. Bründl, S.;

Anmerkungen

Matt, C.; Hess, T. (2015). Wertschöpfung in Datenmärkten: Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten. Forschungsbericht. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/Forschungsbericht-LMU-Wertschoepfung-in-Datenmaerkten_FP_3Sept15.pdf (10.03.2016).

85 BSI (Bundesamt für Sicherheit in der Informationstechnik) (2008). BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise (Version 2.0). Bonn. https://www.bsi.bund.de/gshb (10.03.2016).

86 Eine zusätzliche vierte Schadensklasse „gering" hat sich in der Praxis bewährt, wenn keinerlei Risiken zu erwarten sind.

87 Probst, T. (2012): Generische Schutzmaßnahmen für Datenschutz-Schutzziele. In: DuD - Datenschutz und Datensicherheit 36, Nr. 6, S. 439-444.

88 Um nicht jedes Zeichen eines Datensatzes einzeln vergleichen zu müssen, werden Prüfsummen, sogenannte Hash-Werte gebildet und miteinander verglichen. Die dabei zum Einsatz kommenden mathematischen Funktionen haben Eigenschaften, die einen Schutz gegen bestimmte Angriffe bieten (Kollisionsresistenz) bieten und keine Rekonstruktion der Daten aus dem Hashwert ermöglichen (Einwegfunktionen).

89 Hansen, M.; Jensen, M.; Rost, M. (2015): Protection Goals for Privacy Engineering. In: Proceedings 2015 IEEE Security and Privacy Workshops (SPW 2015), San Jose, Calif., 21 May 2015. Los Alamitos, CA: IEEE Computer Society, S. 159-166; Roussopoulos, M.; Langheinrich, M.; Beslay, L. et al. (2008). Technologiebedingte Herausforderungen für den Datenschutz in Europa. Bericht der ENISA Ad-Hoc-Arbeitsgruppe zu Datenschutz und Technologie.Heraklion: ENISA https://www.enisa.europa.eu/activities/risk-management/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe-german-version (10.03.2016).

90 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder; Schulz, G.; Rost, M. (2015). Das Standard-Datenschutzmodell: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (V0.9) Empfohlen von der 90. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 30. September und 1. Oktober 2015 in Darmstadt. https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf (10.03.2016); Rost, M.; Bock, K. (2012): Impact Assessment im Lichte des Standard-Datenschutzmodells. In: DuD - Datenschutz und Datensicherheit 36, Nr. 10, S. 743-747.

91 ISO/IEC (2009). Risk management — Principles and guidelines. ISO/IEC 31000:2009(E). Genf: International Standardisation Organisation.

92 Das hier erläuterte Verfahren wurde im Rahmen des EU-Projekts SAPIENT entwickelt. Vgl. Wright, D.; Kroener, I.; Friedewald, M. et al. (2014). A guide to surveillance impact assessment — How to identify and prioritise for treatment risks arising from surveillance systems. Deliverable 4.4. SAPIENT Project. Dieses basiert seinerseits auf einem Verfahren der französischen Datenschutzbehörde CNIL sowie einem Prozess, der im Auftrag der englischen Datenschutzbehörde ICO entwickelt wurde. Vgl. CNIL (Commission Nationale de l'Informatique et des Libertés) (2015). Privacy Impact Assessment: Methodology (how to carry out a PIA). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (10.03.2016); CNIL (Commission Nationale de l'Informatique et des Libertés) (2015). Privacy Impact Assessment: Tools (templates and knowledge bases). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-2-Tools.pdf (10.03.2016); Wright, D.; Wadhwa, K.; Lagazio, M. et al. (2013). Privacy impact

assessment and risk management. Report for the Information Commissioner's Office. London: Trilateral Research & Consulting.

93 Finn, R. L.; Wright, D.; Friedewald, M. (2013): Seven types of privacy. In: Gutwirth, S.; Leenes, R. et al. (Hrsg.): European Data Protection: Coming of Age. Dordrecht: Springer, S. 3-32.

94 Vgl. etwa Friedewald, M.; van Lieshout, M.; Rung, S. et al. (2015): Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model. In: Camenisch, J.; Fischer-Hübner, S. et al. (Hrsg.): Privacy and Identity Management for the Future Internet in the Age of Globalisation: 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, Patras, Greece, September 7-12, 2014, Revised Selected Papers. Heidelberg, Berlin: Springer (IFIP Advances in Information and Communication Technology, 457), S. 39-53; Lusoli, W.; Miltgen, C.; Compañó, R.; Maghiros, I. (2009). Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks. JRC Scientific and Technical Reports EUR 23765 EN. Luxembourg: Office for Official Publications of the European Communities. http://ftp.jrc.es/EURdoc/JRC50089.pdf (10.03.2016); Spiekermann, S. (2009): RFID and Privacy - What Consumers Really Want and Fear. In: Personal and Ubiquitous Computing 13, Nr. 6, S. 423-434.

95 Steyaert, S.; Lisoir, H.; Nentwich, M. et al. (2006): Leitfaden partizipativer Verfahren: Ein Handbuch für die Praxis. Wien: Österreichische Akademie der Wissenschaften.

96 Ein umfangreicher Katalog möglicher Schutzziele und Bewertungskriterien findet sich im Anhang von Wright, D.; Kroener, I.; Friedewald, M. et al. (2014). A guide to surveillance impact assessment — How to identify and prioritise for treatment risks arising from surveillance systems. Deliverable 4.4. SAPIENT Project.

97 Zur möglichst umfassenden Identifikation aller relevanten Risiken können ebenfalls unterschiedliche Methoden genutzt werden, die vom Abgleich existierender Risikokategorien/-listen bis zu Kreativtechniken reichen können.

98 Ein momentan (Dezember 2015) verhandelter ISO-Standard gibt eine mögliche Gliederung des DSFA Berichts vor und legt auch die Minimalanforderungen an den Kurzbericht fest. Vgl. ISO/IEC (2016). Information technology - Security techniques - Privacy impact assessment - Guidelines. ISO/IEC 29134. Geneva, Switzerland: International Standardisation Organisation.

99 Collingridge, D. (1980): The social control of technology. London: Pinter; Liebert, W.; Schmidt, J. C. (2010): Collingridge's dilemma and technoscience. In: Poiesis & Praxis 7, Nr. 1-2, S. 55-71.

100 Grunwald, A. (1999): Technology Assessment or Ethics of Technology? Reflections on Technology Development between Social Sciences and Philosophy. In: Ethical Perspectives 6, Nr. 2, S. 170-182.

Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DPIA	Data Protection Impact Assessment
DS-GVO	Datenschutz-Grundverordnung
DSFA	Datenschutz-Folgenabschätzung
DSRL	Datenschutzrichtlinie (Richtlinie 95/46/EG)
EU	Europäische Union
HDSG	Hessisches Datenschutzgesetz
ISO	International Standards Organisation
NDSG	Niedersächsisches Datenschutzgesetz
PIA	Privacy Impact Assessment
SDM	Standard-Datenschutzmodell
TA	Technikfolgenabschätzung

IMPRESSUM

Kontakt:
Michael Friedewald
Geschäftsfeldleiter „Informations- und Kommunikationstechnik“

Telefon +49 721 6809-146
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

2. Auflage: 250 Stück
Mai 2016

Druck
Stober GmbH Druck und Verlag, Eggenstein

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein