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

Dritte, überarbeitete Auflage

White Paper
DATENSCHUTZ-FOLGENABSCHÄTZUNG
Ein Werkzeug für einen besseren Datenschutz

Autorinnen und Autoren:
Michael Friedewald[1], Felix Bieker[2], Hannah Obersteller[4], Maxi Nebel[3], Nicholas Martin[1], Martin Rost[2], Marit Hansen[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
(4) Die Ausführungen der Mitautorin spiegeln ihre persönlichen Auffassungen wider

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

Inhalt

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[1] 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.[2]

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[3] auf die Rechte des Individuums als strukturell schwächeren Risikonehmer betrachtet, dessen faktisch notorische Übergriffe abgewehrt werden müssen.[4]

Definition:

Eine Datenschutz-Folgenabschätzung (DSFA) ist ein Prozess, um das Risiko zu erkennen, zu bewerten und zu bewältigen, 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 für dessen Grundrechte entsteht.

Ziel einer DSFA ist es, Kriterien des operationalisierten Grundrechtsschutzes zu definieren, die Folgen von personenbezogenen Verfahren möglichst umfassend zu erfassen sowie objektiv und nachvollziehbar mit Blick auf die verschiedenen Rollen und damit verbundenen Interessen so zu bewerten, dass 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 (DSGVO)[5] unter bestimmten Bedingungen verpflichtend sein, eine DSFA durchzuführen.

Der Text der DSGVO lässt freilich weitgehend offen, wie und nach welchen Kriterien eine solche DSFA durchzuführen ist. Es ist zu erwarten, dass nach Verabschiedung der DSGVO rasch Modelle für die Durchführung einer DSFA vorgelegt werden. Dabei wird voraussichtlich auf Vorschläge zurückgegriffen werden, die in den vergangenen Jahren 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.[6] 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.[7] 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.[8] Es folgten weltweite Nachfolger, etwa das *Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag* (TAB),[9] das zusammen mit anderen parlamentarischen Beratungsgremien europaweit vernetzt ist.[10] Spezielle Ausprägungen der Technikfolgenabschätzung gibt es überdies im Gesundheitssektor (Health Technology Assessment)[11] sowie im Bereich der Privatwirtschaft.[12]

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.[13] 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.[14]

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,[15] sondern galt darüber hinaus dem Schutz des verfassungsmäßigen Gefüges des Staates vor einer Veränderung durch automatisierte Datenverarbeitung.[16] Der Verantwortliche[17] hatte hierzu sicherzustellen, dass die vorgegebenen Ziele durch technische und organisatorische Maßnahmen eingehalten wurden.[18] § 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)[19] noch eine Vorabkontrolle im Umfang einer Technikfolgenabschätzung[20] 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[21] bzw. der informationellen Selbstbestimmung[22] 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.[23] 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.[24] Dadurch sollen besondere Risiken für die Rechte und Freiheiten der betroffenen Person durch automatisierte Verfahren identifiziert werden.[25] Auch diese Prüfung obliegt jedoch nicht einer unabhängigen Instanz, sondern dem Verantwortlichen selbst. Die Vorschrift geht auf Art. 20 Datenschutzrichtlinie (DSRL)[26] zurück; darin wird ein grundsätzlich weites Verständnis von »spezifischen Risiken für die Rechte und Freiheiten« zugrunde gelegt,[27] 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 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.[28] 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.[29]

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[30] 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 DSFAen in begrenztem Maße vor. Da jeder Verantwortliche selbst zur Durchführung der DSFA 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 Privacy Impact Assessments im angelsächsischer Rechtsraum

Im angelsächsischen Rechtsraum, genauer in Kanada, fanden Ansätze zu einem PIA bereits in den 1970er Jahren das erste Mal Erwähnung.[31] 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.[32] Infolgedessen erschienen in mehreren Ländern des angelsächsischen Rechtskreises Handreichungen zur Durchführung eines Privacy Impact Assessments, unter anderem in Kanada im Jahre 2002,[33] in Neuseeland erstmals 2002,[34] in den USA im Jahre 2004[35] und in Australien 2006.[36] In Europa erließ die britische Regierung im Dezember 2007 ein Handbuch zu Privacy Impact Assessments.[37]

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.[38] 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 nichtöffentliche Verantwortliche, sondern verpflichten nur öffentliche Stellen, also Behörden, beim Einsatz von Datenverarbeitungsanlagen. Schließlich werden kaum Kontrollen durch unabhängige Dritte vorgeschrieben; meist werden lediglich die Verantwortlichen selbst verpflichtet.[39]

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«[40] 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.[41] Um das Konzept des Datenschutzes durch Technikgestaltung (»Data Protection 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.[42]
2. Im Anschluss sollen die Datenflüsse von der Erhebung, Speicherung und Nutzung bis zur Löschung sowie die Zugangsrechte beschrieben werden.[43]
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.[44]
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.[45] 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.[46] Das ICO betont aber die Notwendigkeit der vollständigen Einhaltung der rechtlichen Anforderungen vor der Umsetzung des Projekts.[47]
6. Abschließend sollen die Ergebnisse gesichert und in den Projektplan eingearbeitet werden.[48]

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.[49] Bei den externen Konsultationen geht es um eine Einbindung der Betroffenen, um ihre Rechte und eine transparente Datenverarbeitung zu gewährleisten.[50]

In Bezug auf die eigentliche Bewertung der Datenschutzrisiken bleibt das ICO allerdings ausgesprochen unbestimmt: Neben dem Verweis auf fünf Datenschutz-Prinzipien und

einer daraus abgeleiteten Liste mit Screening-Fragen erschöpft sich die Anleitung in dem Hinweis, dass die Operationalisierung in jedem Einzelfall anders erfolgen kann. [51]

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[52], Maßnahmen[53] und bewährter Verfahren[54] 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 (»Data Protection 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.

Das Verfahren der CNIL ist im Vergleich zum ICO Code of Practice sehr viel stärker umsetzungsorientiert und greift dabei auf Methoden von EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*) zurück, einem vom französischen Verteidigungsministerium entwickelten Standard für Risikomanagement, das mit der verbreiteten ISO/IEC 27000-Reihe zur Informationssicherheit verwandt ist. Dies hat zwar den Vorteil, dass das Verfahren in vielen Organisationen an existierende Erfahrungen anknüpfen kann, es ist aber nicht zur Risikobewertung von Folgen für Bürgerrechte entwickelt worden. Darüber hinaus hat ein sehr formales und quantifizierendes Verfahren das Problem, dass es Datenschutzfolgen in ihrer Wahrscheinlichkeit und ihrem Schadensausmaß quantifizieren soll. Dies ist in der praktischen Umsetzung – insbesondere unter Einbeziehung von Betroffenen – kaum realisierbar und führt regemäßig zu wenig belastbaren Ergebnissen.

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

Trotz der fehlenden Pflicht zur Durchführung einer DSFA, verabschiedete die Europäische Kommission Empfehlungen im Zusammenhang mit der Einführung neuer Technologien wie RFID (RFID-Empfehlung)[55] und Smart Meters (Smart Meters-Empfehlung)[56], 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.[57]

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.[58] 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.[59] Weiterhin wurde hervorgehoben, dass eine Konsultation der Beteiligten, auf die sich der Einsatz der Technik auswirke, vorzunehmen sei.[60] 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.[61]

In ihrer Smart-Meter-Empfehlung befürwortete die Europäische Kommission, dass die Mitgliedstaaten ein Muster für eine DSFA annehmen und anwenden sollten, das die Kommission entwickeln und die Artikel-29-Datenschutzgruppe überprüfen sollte.[62] Die Kommission forderte, 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 angesichts des bereits von der Kommission vorgelegten Entwurfs der DSGVO, die eine solche Pflicht vorsah, 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.[63] Die Artikel-29-Datenschutzgruppe bemängelte am Muster, dass die Pflicht der Verantwortlichen, die Datenschutzaufsichtsbehörden vor der Durchführung der Abschätzung zu konsultieren, nicht vollständig im Entwurf umgesetzt wurde, hob aber hervor, dass – im Gegensatz zu der Beurteilung des für RFID-Anwendungen vorgeschlagenen Rahmens – die Risikoabschätzung der Folgen für die Rechte der Betroffenen besser umgesetzt werde, wobei Detailregelungen noch zu vereinheitlichen seien.[64] Auch 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 im vorgelegten Muster klarer formuliert werden sollte.[65] Abschließend stellte die Artikel-29-Datenschutzgruppe fest, dass das entwickelte Muster genauer ausgestaltet werden müsse, es aber, soweit dies anhand der Änderungsvorschläge erfolge, in Zukunft erfolgreich eingesetzt werden könne.[66]

3 Datenschutz-Folgenabschätzungen in der EU-Datenschutz-Grundverordnung

3.1 Anforderungen an eine Datenschutz-Folgenabschätzung

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

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). Nur wenn die DSFA ergibt, dass trotz der identifizierten Abhilfemaßnahmen ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, muss die Aufsichtsbehörde konsultiert werden (Art. 36 Abs. 1 DSGVO).

Es ist hervorzuheben, dass eine DSFA stets vor der Aufnahme eines Verarbeitungsvorgangs durchführen ist (Art. 35 Abs. 1 DSGVO). Zudem muss der Verarbeitungsvorgang fortlaufend überwacht werden und die DSFA »erforderlichenfalls« wiederholt werden. Gemäß Art. 35 Abs. 11 DSGVO ist das zumindest dann der Fall, wenn sich die mit der Verarbeitung verbundenen Risiken ändern. Die Artikel-29-Datenschutzgruppe benennt als relevante Änderungen von Risiken zum einen die Veränderung von Komponenten des Verarbeitungsvorgangs oder des Kontextes, zum anderen aber auch den organisationalen oder gesellschaftlichen Kontext, der sich aufgrund der Auswirkungen einer bestimmten Technologie verändern kann oder weil sich neue Schutzbedarfe ergeben.[67] Insofern ist der Verarbeitungsvorgang kontinuierlich zu überwachen, um überhaupt feststellen zu können, wann sich Risiken ändern. Um eine solche Überwachung sicherzustellen, empfiehlt es sich die DSFA in ein Datenschutz-Managementsystem einzubinden, um auf Änderungen adäquat reagieren zu können.

Verarbeitungsvorgänge, die bereits vor Inkrafttreten der DSGVO aufgenommen wurden, können jedoch auch unter die Pflicht einer DSFA fallen.[68] Dies gilt insbesondere bei Änderungen hinsichtlich des Verarbeitungsvorgangs selbst oder der damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen gemäß Art. 35 Abs. 11 DSGVO.

Hinsichtlich des Inhaltes einer DSFA formuliert Art. 35 Abs. 7 DSGVO eine Reihe von Mindestanforderungen. So enthält eine DSFA zumindest (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.

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«[69] (»genehmigte Verhaltensregeln«) durch den Verantwortlichen bzw. seinen Auftragsverarbeiter zu berücksichtigen sein (Art. 35 Abs. 8 DSGVO). »Gegebenenfalls« soll der Verantwortliche auch die Betroffenen oder ihre Interessenvertreter anhören (Art. 35 Abs. 9 DSGVO).[70]

Erfüllung der rechtlichen Vorgaben durch die Modelle von ICO und CNIL

Die DSGVO stellt nur sehr allgemeine Mindestanforderungen auf, es besteht aber erstmals eine konkrete Rechtspflicht zur Durchführung einer DSFA. 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 DSFA hervorhob.

Der vom ICO entwickelte PIA Code of Practice erfüllt die sehr allgemeinen Mindestanforderungen der DSGVO 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. Eine derartige Abwägung von Umsetzungskosten gegen Betroffenenschutz läuft der DSGVO allerdings zuwider: die DSGVO ist in jedem Fall einzuhalten und die Rechte der Betroffenen entsprechend zu schützen. Das Prinzip der datenschutzfreundlichen Voreinstellungen (»Data protection by design and by default«), wie es in Art. 23 DSGVO 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.[71] Die verpflichtenden Vorgaben der DSGVO 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. Wie erwähnt stellt der CNIL-Ansatz jedoch auf eine hohe Quantifizierbarkeit von Risiken ab, die in der Praxis nur selten gegeben sein wird. Ferner ist zu vermuten, dass der relativ starre und formale Ansatz der CNIL sich in der Praxis als eher unhandlich erweisen wird. Auch 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.

3.2 Risikoansatz vs. Grundrechtsgewährleistung

Mit der konsolidierten Fassung der DSGVO wurde der sogenannte Risikoansatz explizit formuliert.[72] 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.[73] Tatsächlich ist der Risikoansatz vom Risikomanagement zu unterscheiden; es gibt einige grundsätzliche Unterschiede zwischen den Prinzipien des Datenschutzes 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 betreffen, als akzeptabel eingeschätzt werden. Im Gegensatz dazu hat der Datenschutz zum Ziel, jede Beeinträchtigung der Rechte und Freiheiten natürlicher Personen durch Abhilfemaßnahmen auf ein möglichst geringes Maß zu reduzieren.[74] Im Grundsatz gilt für den Datenschutz, dass jede Verarbeitung personenbezogener Daten durch Organisationen, auch wenn diese durch Gesetz legitimiert ist, einen Eingriff in Art. 8 Abs. 1 Charta darstellt.[75]

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 DSGVO 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.

Exkurs: Gesetzes-DSFA

Art. 35 Abs. 10 DSGVO enthält eine weitere, besondere Art der DSFA: Die Gesetzes-Datenschutz-Folgenabschätzung. Soweit Daten aufgrund einer im konkreten Fall einschlägigen europäischen oder mitgliedstaatlichen Rechtsvorschrift verarbeitet werden, können die Mitgliedstaaten bestimmen, ob die Durchführung einer DSFA nach Art. 35 Abs. 1-7 DSGVO 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 sein, 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.
Erfolgt im Gesetzgebungsprozess bereits eine solche (notwendigerweise abstrakte) DSFA, kann der Gesetzgeber damit den Verantwortlichen bereits erheblich entlasten. Allerdings sollte dabei beachtet werden, dass sich aus dem konkreten Einsatz und der Umsetzung eines Verfahrens weitere Fragen ergeben, sodass von der Möglichkeit, auch in solchen Fällen eine DSFA zu fordern, dringend Gebrauch gemacht werden sollte. 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 immer in blaupausenartig-gleicher Qualität erfolgt.

4
Elemente eines Prozesses zur Datenschutz-Folgenabschätzung

Der Text der DSGVO stellt allgemeine Vorgaben hinsichtlich der Anforderungen an eine DSFA auf. Er formuliert in Art. 35 Abs. 7 DSGVO 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 Rechtsanwender ergebenden, tatsächlichen – inhaltlichen wie organisatorischen – Anforderungen in ein praktikables System zu bringen, wird der Rechtspraxis überlassen bleiben. Wie erläutert gibt es eine Vielzahl unterschiedlicher Ansätze für DSFAen 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.[76] 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 Verantwortliche, Auftragsverarbeiter und 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 vier Phasen, eine Vorbereitungsphase, die zur Organisation der DSFA dient, die eigentliche Durchführungsphase, eine Umsetzungsphase, in der die identifizierten Abhilfemaßnahmen nach erfolgreichem Durchlauf der DSFA umgesetzt und getestet werden, sowie eine Überprüfungsphase, die der Überwachung und Fortschreibung im Datenschutz-Managementsystem dient. Der hier vorgeschlagene Gesamtprozess auf Basis des SDM wurde zwischenzeitlich in einem Planspiel der DSK erprobt und u.a. auf Basis der dort erworbenen Erfahrung überarbeitet.[77] In den folgenden Abschnitten wird der Prozess mit seinen vier Phasen und den darin zu durchlaufenden Schritten näher erläutert.[78]

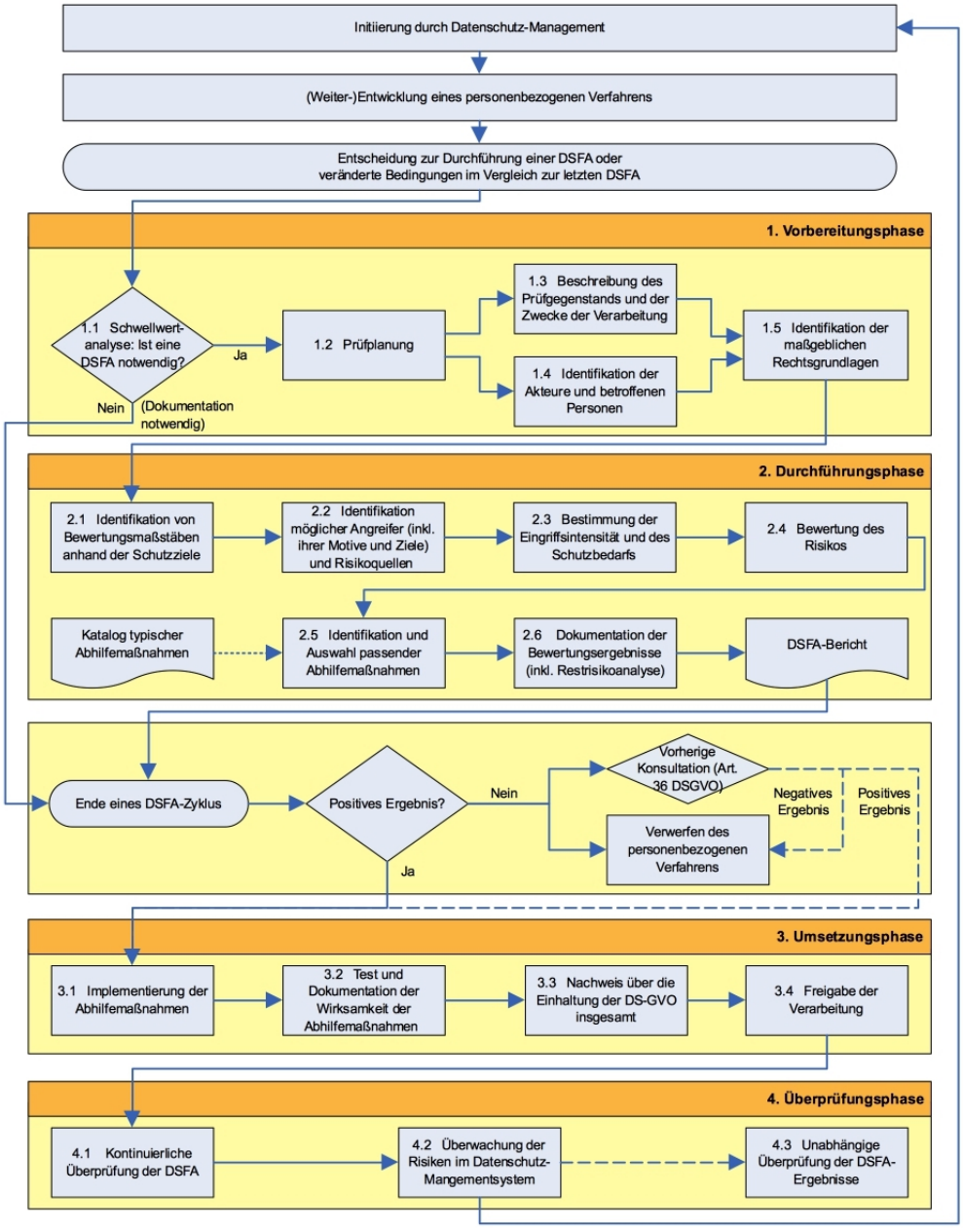

Abb. 01: Vorgehensweise für die Durchführung einer DSFA

4.1 Vorbereitungsphase

4.1.1 Schwellwertanalyse (1.1)

Zunächst muss der Verantwortliche prüfen, ob im konkreten Fall die Durchführung einer DSFA notwendig ist. Dies ist gemäß Art. 35 Abs. 1 DSGVO »insbesondere« der Fall, 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.

Der Verantwortliche muss also die Intensität der Beeinträchtungen für Betroffene und die Risiken für die Ausübung von Grundrechten abschätzen. Wird festgestellt, dass durch den geplanten Verarbeitungsvorgang voraussichtlich die Beeinträchtung nicht hoch und zudem kein hohes Risiko besteht, ist eine DSFA nicht zwingend durchzuführen. Entscheidet der Verantwortliche keine DSFA durchzuführen, ist diese Entscheidung unter Angabe der maßgeblichen Erwägungen zu dokumentieren.[79]

Es ist jedoch zu beachten, dass eine Analyse der eigenen Datenverarbeitung und deren Dokumentation, inklusive einer Beschreibung der technischen und organisatorischen Maßnahmen, nach Art. 30 DSGVO für das zu führende Verzeichnis über Verarbeitungstätigkeiten ohnehin gefordert ist.[80] Dies ist eine Umsetzung der allgemeinen Rechenschaftspflicht, nach der Verantwortliche die Einhaltung der rechtlichen Anforderungen der DSGVO nachweisen können müssen (Art. 5 Abs. 2 DSGVO).

Um festzustellen, ob die geplante Verarbeitungstätigkeit ein »hohes Risiko für die Rechte und Freiheiten natürlicher Personen« zur Folge hat, kann man in den drei nachfolgend skizzierten Schritten vorgehen.

1. Die Aufsichtsbehörden erstellen und veröffentlichen gemäß Art. 35 Abs. 4 DSGVO (im Rahmen ihres jeweiligen Zuständigkeitsbereichs) eine Liste der Verarbeitungsvorgänge, für die eine DSFA nach Abs. 1 verbindlich durchzuführen ist. An dieser Muss-Liste können sich Verantwortliche zunächst orientieren.

Zwar können die Aufsichtsbehörden eine Liste mit Arten von Datenverarbeitungsvorgängen erstellen, bei denen explizit keine DSFA durchgeführt werden muss (Art. 35 Abs. 1 DSGVO). Eine generelle Ausnahme einzelner Bereiche oder Verarbeitungsarten ist allerdings aufgrund des von der DSGVO bezweckten, umfassenden Grundrechtsschutzes (vgl. Art. 1 Abs. 2 DSGVO) kritisch zu beurteilen und sollte nicht weiter verfolgt werden.

Die Listen sind an den in Art. 68 DSGVO genannten Ausschuss (Europäischer Datenschutzausschuss) zu übermitteln. Sofern die gelisteten Verarbeitungstätigkeiten bestimmte europarechtliche Bezüge aufweisen (könnten), müssen die Aufsichtsbehörden vor ihrer Festlegung das Kohärenzverfahren nach Art. 63 DSGVO durchzuführen (Art. 35 Abs. 6 DSGVO).

2. Art. 35 Abs. 3 DSGVO enthält einen – nicht abschließenden – Katalog mit Anwendungsfällen, die eine DSFA erforderlich machen. Wenn das geplante Verarbeitungsverfahren nicht auf der Muss-Liste der Aufsichtsbehörde auftaucht, sollte der Verantwortliche im zweiten Schritt diese Regelbeispiele konsultieren. Liegt eines dieser Regelbeispiele vor, besteht ebenfalls eine Durchführungspflicht. Dies ist der Fall bei:

a) Systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen. Dies umfasst unter anderem Scoring, Profiling und automatisierte Einzelentscheidungen.

b) Umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10. Hierzu gehören wie bisher Angaben über die rassische

und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben sowie neuerdings genetische Daten.

c) Systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche, beispielsweise durch Videoüberwachung und Drohnen.

Aufbauend auf diesen Beispielen hat die Artikel-29-Datenschutzgruppe sich in ihren Leitlinien zur DSFA mit der Auslegung des hohen Risikos befasst und neun Kriterien aufgezählt, die sich an Art. 35 Abs. 3 und den Erwägungsgründen 71, 75, 91 DSGVO orientieren und die darauf hindeuten, dass bei einer Datenverarbeitung voraussichtlich ein hohes Risiko besteht. Durch diese Kriterien werden die Regelbeispiele des Art. 35 Abs. 3 weiter erläutert:[81]

1. Bewertung und Einstufung (Scoring) einschließlich Prognosen und Profilerstellung

Laut Erwägungsgründen 71, 91 DSGVO liegt dies insbesondere vor, wenn die Arbeitsleistung, wirtschaftliche Situation, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel beurteilt werden. Die Artikel-29-Datenschutzgruppe benennt hier das typische Beispiel der Bank, die die Kreditwürdigkeit eines Kunden bewertet, aber auch Gentests zur Bestimmung von Krankheiten oder das Tracking von Webseiten-Besuchern.

2. Automatische erfolgende Entscheidungen mit rechtlichen oder ähnlich signifikanten Auswirkungen für Betroffene

Bei automatischen Verarbeitungen droht eine Diskriminierung oder der Ausschluss bestimmter Individuen von Leistungen oder Angeboten, sodass diese besonders risikoreich sind.

3. Systematische Überwachung

Systematische Überwachung kann dazu führen, dass Daten von Betroffenen gesammelt werden, ohne dass ihnen dies oder die spätere Nutzung bewusst sind. Zudem ist es Individuen bei öffentlich zugänglichen Bereichen unter Umständen nicht möglich, diese zu umgehen.

4. Sensible personenbezogene Daten

Als sensibel sind insbesondere die die besonderen Kategorien von Daten gemäß Art. 9 Abs. 1 sowie Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO anzusehen. Nach der Artikel-29-Datenschutzgruppe fallen auch allgemeinere Daten, wie etwa Daten elektronischer Kommunikation, Aufenthaltsorte oder Finanzdaten unter dieses Kriterium. Dabei kann auch zu berücksichtigen sein, ob die Daten bereits öffentlich zugänglich sind. Weiterhin beziehen die Leitlinien auch Daten ein, die Privatpersonen ausschließlich für persönliche oder familiärer Tätigkeiten verarbeiten und benennt dabei ausdrücklich die Nutzung von Cloud-Diensten für die persönliche Dokumente-Verwaltung, E-Mail-Dienste, Tagebücher, E-Reader mit Anmerkungsfunktion und verschiedene Anwendungen, die Vitalfunktionen aufzeichnen.

5. Umfangreiche Datenmengen

Zur Bestimmung, ob es sich um umfangreiche Datenmengen handelt, empfiehlt die Artikel-29-Datenschutzgruppe in Anlehnung an Erwägungsgrund 91 zu berücksichtigen, wie viele Betroffene erfasst werden (entweder absolut oder als Anteil der betroffenen Bevölkerung), das Volumen der Daten und/oder die Breite der verschiedenen Daten, die verarbeitet werden, die Dauer oder der Bestand der Verarbeitungstätigkeit sowie die geografische Ausbreitung der Verarbeitungstätigkeit.

6. Vergleich oder Kombination von Datensätzen

Der Vergleich oder die Kombination von Datensätzen aus verschiedenen Quellen unter Einhaltung des Prinzips der Zweckbindung, die zu verschiedenen Zwecken von ver-

schiedenen Verantwortlichen erhoben wurden, begegnet der Gefahr, dass er die vernünftigen Erwartungen der Betroffenen übersteigt.

7. Daten schutzbedürftiger natürlicher Personen

Aufgrund des gesteigerten Machtungleichgewichts zwischen den Betroffenen und dem Verantwortlichen, kann die Verarbeitung von besonders schutzbedürftigen Personen die Durchführung einer DSFA nötig machen. Dies ergibt sich daraus, dass sich die Person einer Verarbeitung ihrer Daten nicht erwehren kann und gilt u.a. für Arbeitnehmer, Kinder, Menschen mit geistigen Behinderungen, Asylsuchende, ältere Menschen, Patienten.

8. Einsatz innovativer Technologien oder neuartiger organisatorischer Lösungen

Der Einsatz neuartiger Technologien kann neue Formen der Datensammlung und -verarbeitung beinhalten, da ihre persönlichen oder sozialen Folgen noch nicht bekannt sind. Dies gilt etwa für die Kombination von Fingerabdrücken und Gesichtserkennung für bessere physische Zugangskontrollen oder bestimmte Anwendungen des Internets der Dinge, die einen erheblichen Einfluss auf den Alltag und die Privatsphäre der Betroffenen haben können.

9. Verhinderung, dass die betroffene Person ein Recht ausüben, eine Dienstleistung in Anspruch nehmen oder einen Vertrag abschließen kann

Dieses letzte Kriterium umfasst etwa die Verarbeitung in öffentlichen Bereichen, die Betroffene nicht vermeiden können oder die das Recht der Betroffenen ändern, einen Vertrag einzugehen oder Zugang zu einer Dienstleistung zu erlangen, etwa durch eine Bonitätsauskunft.

Die Artikel-29-Datenschutzgruppe geht davon aus, dass ein hohes Risiko wahrscheinlicher ist, je mehr dieser Kriterien ein Verarbeitungsvorgang erfüllt, weist aber ausdrücklich darauf hin, dass dies auch der Fall sein kann, wenn nur eines der Kriterien erfüllt ist.[82] Die dargestellten Kriterien sind insofern eine Hilfestellung, es ist jedoch stets der Kontext der konkreten geplanten Verarbeitungstätigkeit und deren Auswirkungen auf die Rechte und Freiheiten natürlicher Personen zu beachten.

So ist z.B. auch die organisatorische und technologische Komplexität der Verarbeitungstätigkeit zu bedenken, d.h. die Zahl der Akteure und Organisationen, die mit der Verarbeitung betraut werden oder denen Daten offengelegt werden. Dieser Punkt wird zwar nicht direkt von der Artikel-29-Datenschutzgruppe adressiert, aber es ist davon auszugehen, dass eine Verarbeitung prinzipiell als umso risikoreicher einzuschätzen ist, je mehr Akteure an ihr beteiligt sind bzw. Zugriff auf die Daten bekommen, insbesondere wenn diese Akteure in separaten Organisationen beheimatet sind. Ebenso dürfte das zu vermutende Risiko mit der technischen Komplexität der Verarbeitung steigen, da die Gefahr des Auftretens von technischen Fehlern, Sicherheitslücken und Überschreitungen von Datenschutzprinzipien mit der Zahl der verwendeten Systeme, Komponenten und Schnittstellen, sowie der Zahl der Arbeitsschritte, steigen dürfte.

3. Schließlich muss der Verantwortliche, wenn keine der genannten Kategorien einschlägig ist, allgemein prüfen, ob sich aus der konkreten geplanten Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen ergeben könnte. Sollten dabei Zweifel bestehen bleiben, empfiehlt auch die Artikel-29-Datenschutzgruppe eine DSFA durchzuführen[83], da sie ein hilfreiches Werkzeug darstellt um die Einhaltung der datenschutzrechtlichen Bestimmungen sicherzustellen.

4.1.2 Prüfplanung (1.2)

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.

Die Durchführung einer DSFA ist nach Art. 35 Abs. 1 eine Managementaufgabe, verantwortlich ist also die Unternehmens- oder Behördenleitung. Diese kann die praktische Durchführung an Mitarbeiter oder einen externen Dienstleister delegieren. Dabei holt der Verantwortliche den Rat des betrieblichen oder behördlichen Datenschutzbeauftragten (DSB; sofern vorhanden) ein (Art. 35 Abs. 2 DSGVO). Art. 39 Abs. 1 Buchstabe c DSGVO sieht vor, dass der DSB bei der DSFA auf Anfrage berät und ihre die Durchführung überwacht. Die Artikel-29-Datenschutzgruppe hat in ihrem Leitfaden zum Datenschutzbeauftragten festgehalten, dass dieser bezüglich der Fragen, ob eine DSFA durchgeführt werden soll, nach welcher Methode dies erfolgen kann, ob sie intern oder extern durchgeführt wird, welche technischen und organisatorischen Maßnahmen zur Bewältigung der Risiken für die natürliche Personen angewandt werden und ob die DSFA ordnungsgemäß ausgeführt und ihre Schlussfolgerungen bezüglich der zu ergreifenden Maßnahmen in Übereinstimmung mit der DSGVO sind eingebunden werden kann.[84] Der Datenschutzbeauftragte ist nicht selbst für Verstöße gegen die DSGVO verantwortlich, sondern diese liegt gemäß Art. 24 Abs. 1 DSGVO beim Verantwortlichen.[85]

Ungeachtet ob das Management die operative Durchführung der DSFA an Mitarbeiter oder Externe delegiert oder selber in die Hand nimmt, kommt ihm eine besondere Verantwortung für den Erfolg der DSFA zu. Sinn der DSFA ist es, Prozesse und Anwendungen kritisch zu hinterfragen, verborgene Widersprüche aufzudecken, und problematische Elemente anzupassen oder zu beseitigen. Dafür muss gewährleistet sein, dass sich die DSFA nicht anderen Zielen der Organisation unterzuordnen hat.

Für die Durchführung sollte eine Projektmanagementmethode gewählt werden, die sicherstellt, dass alle relevanten Stakeholder ihre Interessen in das Projekt einbringen können und kein relevanter Aspekt übersehen wird. Typischerweise wird unterschieden zwischen einer Lenkungsgruppe und einem Expertenteam. Das Projekt wird zudem in Phasen unterteilt, die einen transparenten, integren und intervenierfähigen Projektfortschritt über gemanagte Phasenübertritte, etwa mit Tests und Freigaben sowie deren Dokumentation ermöglicht. Eine Projektmanagementmethode dient auch der Sicherung der Fokussierung des Projektauftrags und nutzt die Instrumente eines Lasten- und Pflichtenhefts, das zur Klärung einer legitimen Zwecksetzung, angemessenen Zweckttrennung und engen Zweckbindung beiträgt.

Teamzusammenstellung

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. Das Team sollte über eine möglichst große Bandbreite von Qualifikationen und Erfahrungen verfügen, da die Identifikation von Risiken für die Rechte und Freiheiten natürlicher Personen und die Erarbeitung passender Lösungen i.d.R. eine Mischung aus technischer, juristischer und betriebswirtschaftlicher Expertise erfordert.[86] Auf der anderen Seite muss gewährleistet sein, dass sich die DSFA 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.

Zudem sind – wie auch die Artikel-29-Datenschutzgruppen explizit fordert – Dritte, etwa Auftragsverarbeiter oder Hersteller von IT-Systemen, einzubeziehen[87], wenn dies notwendig ist, etwa um eine vollständige Beschreibung eines Systems zu gewährleisten.

4.1.3 Beschreibung des Prüfgegenstandes und der Zwecke der Verarbeitung (1.3)

Im ersten inhaltlichen Schritt ist zu definieren, was im Rahmen der DSFA geprüft wird, also der konkrete Prüfgegenstand (engl. *target of evaluation*). Dabei handelt es sich um das Verfahren, die verwendeten personenbezogenen Daten sowie die zur Erhebung und Verarbeitung herangezogenen IT-Systemen und Prozesse. Um dies bestimmen zu können, ist es wesentlich zunächst den Zweck des Verfahrens festzulegen. Die abschließende Festlegung des Zwecks ist rechtlich zur Umsetzung der Zweckbindung gemäß Art. 5 Abs. 1 Buchstabe b und der Datenminimierung gemäß Art. 5 Abs. 1 Buchstabe c DSGVO erforderlich.

Zur Beschreibung des Prüfgegenstandes gehört die systematische Beschreibung der Verarbeitungsvorgänge, ihrer Zwecke sowie der berechtigten Interessen des Verantwortlichen, wie dies auch von Art. 35 Abs. 3 DSGVO verlangt wird. Die Beschreibung beinhaltet insbesondere 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.

Eine DSFA nach Art. 35 DSGVO darf sich dabei nicht auf eine einzelne Komponente oder Funktion beschränken, sondern muss das gewählte Prüfobjekt in seiner Gesamtheit, inklusive der technischen und organisatorischen Umsetzung bei dem Verantwortlichen prüfen. Dies beinhaltet eine Beschreibung der generisch-technischen Architektur, in der der Prüfgegenstand detailliert beschrieben wird. Um dies zu erreichen, sollte ein Datenflussdiagramm, das die Subsysteme/Beteiligten, die Schnittstellen und Verbindungen zwischen diesen schematisch darstellt, erstellt werden. Auf dieser Basis können die (1.) Komponenten, (2.) die zu erhebenden Daten, (3.) die Schnittstellen der Komponenten und die darüber zugänglichen Daten und etwaige Sicherheitseigenschaften und (4.) die Eigenschaften zwischen den Verbindungen der Komponenten beschrieben werden.[88]

Sodann ist zu bewerten, ob das festgelegte Verfahren (also der Prüfgegenstand) im Hinblick auf den Zweck der Verarbeitung notwendig und verhältnismäßig ist (Art. 35 Abs. 7 Buchstabe b DSGVO).[89] Dabei ist zu prüfen, ob die Verarbeitungsvorgänge zum Erreichen des Zwecks geeignet und tatsächlich notwendig[90] sind – ob es keine alternativen Vorgehensweisen gibt, die weniger stark in die Rechte und Freiheiten natürlicher Personen eingreifen würden, und ob der durch die Verarbeitung erfolgende Eingriff in einem angemessenen Verhältnis zum angestrebten Zweck steht. Der Zweck wird meist über verschiedene Verfahren zu erreichen sein und innerhalb der jeweiligen Verfahren gibt es verschiedene Umsetzungsalternativen. Aus diesen Alternativen ist dementsprechende diejenige zu wählen, die am wenigsten Daten erfordert. Zudem können auch bestimmte Verarbeitungsvorgänge außer Verhältnis zu dem festgelegten Zweck stehen. So sind etwa an eine Verarbeitung von Kundendaten, die zur Abwicklung eines Kaufvertrages für beide Seiten notwendig sind und die auf der Basis von Art. 6 Abs. 1 Buchstabe b beruht, andere Anforderungen zu stellen, als an ein Tracking von Webseitenbesuchern, das im (im Einzelfall zu begründenden und mit den Interessen oder Rechten der betroffenen Personen abzuwägenden) berechtigten Interesses des Verantwortlichen gemäß Art. 5 Abs. 1 Buchstabe f DSGVO geschieht. Die hier vorzunehmende Güterabwägung kann also bereits Änderungen an dem geplanten Verarbeitungsvorgang nötig machen, etwa eine Beschränkung der zu verarbeitenden Daten, eine Änderung der beteiligten Akteure oder eingesetzter Technologien.[91]

Private und öffentliche Stellen, die ihre Datenverarbeitungsverfahren bereits heute in Form eines Verfahrensverzeichnisses bzw. einer Verfahrensübersicht dokumentieren, können diese für diesen Prozessschritt weiterverwenden. Weiterhin ist dieses Instru-

ment auch in der DSGVO vorgesehen: gemäß Art. 30 DSGVO ist ein Verzeichnis der Verarbeitungstätigkeiten zu führen, dass u.a. die Zwecke der Verarbeitung, eine Übersicht der Kategorien von Daten und die Datenflüsse beinhaltet.

4.1.4 Identifikation der Akteure und betroffenen Personen (1.4)

Ebenso wichtig wie die umfassende Beschreibung des Verfahrens und seines Einsatzkontextes ist die Identifikation der handelnden und betroffenen Akteure. Dies umfasst vor allem die Personen, die unmittelbar Einfluss auf das Verfahren nehmen können sowie solche Personen, die mittelbar oder unmittelbar durch den Einsatz betroffen sind. Es werden also nicht nur Organisationen und Personen, die im Rahmen der Entwicklung oder Verwendung eine bestimmte Rolle einnehmen und damit potenzielle Angreifer sind, betrachtet. Konkret fallen darunter:

- Mitarbeiter der für den Einsatz des Prüfgegenstands verantwortlichen Organisation[92];
- Betreiber des Prüfgegenstandes, z.B. wenn sie als Dienstleister im Rahmen einer Auftragsverarbeitung tätig werden (Rechenzentrum, Internet-Provider)
- 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).
- Schließlich ist auch die Einbeziehung des *Herstellers* des Prüfungsgegenstands sinnvoll, auch wenn dies von der DSGVO nicht explizit vorgesehen ist.

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 Konsultation der betroffenen Personen

Art. 35 Abs. 9 DSGVO sieht vor, dass der Verantwortliche «gegebenenfalls» die Standpunkte der «betroffenen Personen» einholt. Im angelsächsischen Raum gilt die Konsultation von Betroffenen und anderen interessierten Parteien (Stakeholder, z.B. Dienstleister, zivilgesellschaftliche Gruppen) im Rahmen von PIA-Prozessen ebenfalls als Best Practice.[93]

Die Konsultation der betroffenen Personen erfordert meist einen relativ hohen zeitlichen, organisatorischen und materiellen Aufwand. Gerade beim Einsatz von Technologien, die wesentliche Neuerungen für die Lebenswelten der Betroffenen darstellen, mit weitreichender Sammlung oder Verarbeitung personenbezogener Daten einhergehen, und für das Unternehmen strategischen Charakter haben bzw. erhebliches Konfliktpotential bergen (z.B. «Smart Home»-Produkte) kann eine solche Konsultation allerdings auch erheblichen Mehrwert stiften. Gerade bei der Verarbeitung von sensiblen Mitarbeiter-Daten (z.B. zur Leistungs- oder Verhaltenskontrolle) dürfte die Konsultation des Betriebsrats anzuraten sein.[94] Zu den Vorteilen, die durch Konsultationen realisierbar sind, zählen:

- Frühzeitige Erkenntnisse über Erwartungen, Verhalten und Prioritäten von Nutzern und anderen Betroffenen, auch zu vielschichtigen Themen wie etwa Vorstellungen von Fairness oder Sittlichkeit
- Unvorhergesehene Lösungen über den Einbezug externer Experten
- Steigerung der gesellschaftlichen Akzeptanz von Verarbeitungen, die zwar rechtlich zulässig sind aber erhebliche gesellschaftliche Neuerungen und somit Konfliktpotential bergen (z.B. «Smart Home»)
- Minimierung des Risikos unerwarteter und unkontrollierbarer Ablehnung und Proteste seitens der Betroffenen oder sonstiger gesellschaftlichen Akteure (z.B. Online-«Shitstorms»)

Wenn eine direkte Konsultation der betroffenen Personen oder ihrer Vertreter nicht möglich ist, können etwa Mitarbeiter der Geschäftsbereiche mit dem engsten Kontakt zu den Betroffenen (z.B. Vertrieb, Kundenbetreuung) einbezogen werden. Dies ist zwar keine Konsultation im Sinne des Art. 35 Abs. 9 DSGVO, kann aber wertvolle Einblicke in deren Erwartungen, Verhalten und Prioritäten geben.

Für eine direkte Konsultation von organisations-externen betroffenen Personen (Kunden, Nutzer, Bürger, etc.) stehen verschiedene partizipatorische Verfahren zur Verfügung. Etwa können Fokusgruppen – mit denen viele Unternehmen in den Bereichen Produktgestaltung und Marketing bereits Erfahrung haben – einberufen werden.[95] Auch können Interessensvertretungen wie Verbraucherschutz- oder Bürgerrechtsverbände einbezogen werden. Folgende Punkte haben sich in der Praxis als wichtig erwiesen, um eine erfolgreiche Konsultationen zu gewährleisten:[96]

- Klare Zusage des Managements, die Ergebnisse der Konsultation in die Projektgestaltung einfließen zu lassen.
- Der Zeitpunkt der Konsultation sollte früh angesetzt werden, damit die Ergebnisse die Gestaltung des Projekts noch sinnvoll beeinflussen können – d.h. bevor Schlüsselentscheidungen gefallen sind.
- Ausreichend Zeit muss für die Konsultation veranschlagt werden, um substantielle Ergebnisse erarbeiten zu können.
- Für die Auswahl der Teilnehmer müssen die relevanten Gruppen betroffener Personen ermittelt worden sein. Art. 35 Abs. 9 DSGVO ist dabei nicht auf die keine Betroffene im Sinne von Art. 4 Abs. 1 DSGVO beschränkt, sondern ist weiter zu verstehen. Es ist kann daher auch sinnvoll sein, Personen einzubinden, deren personenbezogene Daten nicht verarbeitet werden.
- Ggfs. erforderliches Fachwissen muss den Teilnehmern so vermittelt werden, dass es auch für technische oder rechtliche Laien verständlich wird. Hierbei ist auf die Wirkung unterschiedlicher Formulierungsweisen zu achten, die etwa technophile Teilnehmer oder solche mit Rechtskenntnissen unbeabsichtigt begünstigen können. Dies ist nicht nur aus normativen, sondern auch funktionalen Gesichtspunkten wichtig: es ist wenig sinnvoll, etwa eine Fokusgruppe durchzuführen, ohne sicherzustellen, dass alle Gruppenmitglieder auch beitragen können.
- Kommunikationsprozesse sowohl unter den Teilnehmern als auch zwischen ihnen und der Organisation müssen so gemanagt werden, dass Kommunikationsbarrieren abgebaut und Missverständnissen vorgebeugt werden, und möglichst alle in gleichem Umfang beitragen können. Wiederum ist dies ein ebenso funktionales wie normatives Gebot: Betroffenen-Konsultationen, die von einigen Wenigen dominiert werden, sind selten zweckmäßig. Hier kann die Verwendung externer Moderatoren mit Erfahrung in Konsultations-Prozessen hilfreich sein.
- Kommunikation der Konsultationsergebnisse an die Teilnehmer.

4.1.6 Identifikation der maßgeblichen Rechtsgrundlagen (1.5)

Auf Grundlage der vorherigen Schritte können nun die Rechtsgrundlagen der geplanten Verarbeitungsvorgänge bestimmt werden. Wie in Art. 5 Abs. 2 DSGVO festgelegt, muss der Verantwortliche die Einhaltung der Grundsätze des Abs. 1 im Rahmen seiner Rechenschaftspflicht nachweisen können. Zur Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchstabe a gehört die Identifikation der einschlägigen Rechtsgrundlagen im Sinne von Art. 6 DSGVO. Als Eingriff in das Grundrecht auf Schutz personenbezogener Daten der Betroffenen gemäß Art. 8 Charta bedarf jede Datenverarbeitung einer Rechtfertigung.[97]

Zur Erreichung eines Zwecks werden in der Regel verschiedene Rechtsbeziehungen bestehen, die jeweils eigene Rechtsgrundlagen erfordern. Es ist daher hilfreich eine Skizze der beteiligten Akteure und der jeweiligen Rechtsbeziehungen anzufertigen, um sicherzustellen, dass jede Datenverarbeitung einer Rechtsgrundlage zugeordnet wird.

Zunächst ist das anzuwendende Recht zu bestimmen. Die konkret zu identifizierenden Rechtsgrundlagen sind abhängig vom spezifischen Prüfgegenstand.

Die DSGVO ist gemäß Art. 2 sachlich anwendbar, wenn personenbezogene Daten verarbeitet werden und keine der in Abs. 2 definierten Ausnahmen einschlägig ist. Die örtliche Anwendbarkeit ist nach Art. 3 DSGVO gegeben, wenn personenbezogene Daten im Rahmen der Tätigkeit einer Niederlassung in der EU verarbeitet werden, unabhängig davon, ob die Verarbeitung in der EU erfolgt. Weiterhin ist sie auch anwendbar, wenn der Verantwortliche oder Auftragsverarbeiter nicht in der EU niedergelassen ist, aber personenbezogene Daten einer Person, die sich in der EU befindet verarbeitet werden und die Verarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen oder der Beobachtung von Verhalten, das in der EU erfolgt, steht.

Ist das europäische Datenschutzrecht anwendbar, ist eine Datenverarbeitung nur rechtmäßig, wenn einer der in Art. 6 Abs. 1 DSGVO abschließend aufgezählten Erlaubnistatbestände erfüllt ist.[98] Es bedarf folglich einer Rechtsgrundlage (auf gesetzlicher oder vertraglicher Grundlage oder über eine Einwilligung der Betroffenen). Gesetzliche Rechtsgrundlagen finden sich nicht nur in der DSGVO, sondern, soweit die DSGVO keine abschließende Regelung trifft, auch in anderen Spezialgesetzen auf europäischer oder nationaler Ebene. 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.

Die Gestaltung von Verträgen als Rechtsgrundlage unterliegt den allgemeinen Regelungen zur Vertragsgestaltung, wie sie sich etwa aus dem Bürgerlichen Gesetzbuch oder dem Allgemeinen Gleichbehandlungsgesetz ergeben. Für eine wirksame Einwilligung sind die Voraussetzungen der Art. 7 und 8 DSGVO zu beachten.

Schließlich ist zu beachten, dass auch für die Verarbeitung der Daten von Drittbetroffenen (etwa Familienmitglieder, die ein Produkt oder eine Dienstleistung mitnutzen), mit denen kein Vertrag geschlossen ist und keine eigene Einwilligung eingeholt wird, eine Rechtsgrundlage erforderlich ist. Dabei wird regelmäßig die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen gemäß Art. 6 Abs. 1 Buchstabe f DSGVO heranzuziehen sein. Allerdings ist dabei eine Abwägung mit den Interessen oder Grundrechten und Grundfreiheiten der (dritt-)betroffenen Person erforderlich. Eine Verarbeitung darf nur erfolgen, wenn diese das Interesse des Verantwortlichen an der Verarbeitung nicht überwiegen.

Weiterhin ist bei einer Datenübermittlung in Drittländer (also Staaten außerhalb der EU) oder internationale Organisationen im Rahmen einer Zweistufenprüfung gemäß Art. 44 S. 1 DSGVO zu beachten, dass neben einer wirksamen Rechtsgrundlage solche Übermittlungen nur zulässig sind, wenn die weiteren Bedingungen der Art. 44-50 DSGVO erfüllt sind. Das Ziel dieser Vorschriften ist, dass das durch die Verordnung gewährleis-

tete Schutzniveau nicht untergraben wird (Art. 44 S. 2 DSGVO). Es bedarf daher für die Datenübermittlung zusätzlich zu einer Rechtsgrundlage eines Angemessenheitsbeschlusses der Kommission (Art. 45), geeigneter Garantien (Art. 46), verbindlicher interner Datenschutzvorschriften (Art. 47) oder eines der Ausnahmegründe nach Art. 49 DSGVO.

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 Vorschriften zum Schutz Minderjähriger. Da im Rahmen der DSFA 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.

4.1.7 Dokumentation der Problem- und Aufgabendefinition und Relevanzfrage

Die Ergebnisse der Vorbereitungsphase sollten vom Durchführenden des DSFA-Prozesses dokumentiert und vom Verantwortlichen als verbindlich bestätigt werden. Die DSGVO sieht eine solche Zwischendokumentation zwar nicht explizit vor, sie wird aber als gute Verfahrenspraxis angesehen. Durch diesen Schritt kann am Ende der Vorbereitungsphase sichergestellt werden, dass alle relevanten Akteure und Prozesse erfasst sind, um eine erfolgreiche Bewertung des Prüfgegenstands vornehmen zu können. Die Darstellung sollte nach einer standardisierten Gliederung erfolgen, die auch später bei der Dokumentation der Prüfergebnisse verwendet wird. Dieser Bericht gibt den Rahmen für die nachfolgenden Bewertungsschritte vor.

4.2 Durchführungsphase

Die Durchführungsphase deckt die Anforderungen von Art. 35 Abs. 7 Buchstaben b und c DSGVO an die Bewertung der Verhältnismäßigkeit und des Risikos für die betroffenen Personen ab.

4.2.1 Identifikation von Bewertungsmaßstäben anhand der Schutzziele (2.1)

Es hat sich im Bereich der IT-Sicherheit bzw. Informationssicherheit bewährt, Anforderungen als Schutzziele zu formulieren.[99] Die Anforderungen des Datenschutzes sind gesetzlich normiert. Diese Anforderungen lassen sich ebenfalls mit Hilfe von Schutz-, bzw. Gewährleistungszielen[100] 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. Diese sind in das Standard-Datenschutzmodell[101] eingebettet, dass von der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) angenommen wurde und von der Artikel-29-Gruppe als ein Framework für die Durchführung einer DSFA empfohlen wird.[102]

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) Nichtver-

kettung, (5) Transparenz und (6) Intervenierbarkeit.[103] Diese werden ergänzt durch das grundlegende Gewährleistungsziel der Datensparsamkeit, das in der DSGVO in Art. 5 Abs. 1 Buchstabe c DSGVO als Prinzip der Datenminimierung ausdrücklich normiert ist.

Datenminimierung konkretisiert den Grundsatz der Erforderlichkeit, nach dem personenbezogene Daten nur in dem Umfang verarbeitet werden dürfen, wie es für das Erreichen des Zwecks erforderlich ist.[104] Danach gilt es, das Erheben von personenbezogenen Daten von vornherein weitestgehend zu vermeiden und vorhandene personenbezogene Daten schnellstmöglich zu löschen sind. Dies betrifft die Gestaltung der Verarbeitung insgesamt, d.h. nicht nur Technik und organisatorische Verfahren, sondern auch das Geschäftsmodell oder Geschäftsprozesse in der Organisation.

Verfügbarkeit bedeutet, dass personenbezogene Daten für die Berechtigten rechtzeitig zur Verfügung stehen und ordnungsgemäß verwendet werden können. Integrität beinhaltet die Anforderung, dass die Prozesse und Systeme der Datenverarbeitung gemäß Spezifikation funktionieren und die personenbezogenen Daten unversehrt, vollständig und aktuell sind. Vertraulichkeit betrifft Anforderungen an Geheimhaltung, das heißt, dass kein Unbefugter die personenbezogenen Daten zur Kenntnis nehmen kann. Nichtverkettung stellt sicher, dass Daten nicht zwischen verschiedenen, getrennt zu haltenden Bereichen verknüpft und nicht für andere als die ursprünglichen Zwecke verarbeitet werden. Transparenz bedeutet, dass die betroffenen Personen erkennen können, welche Umstände und Faktoren für die Verarbeitung der personenbezogenen Daten gelten. Intervenierbarkeit umfasst die Möglichkeit der betroffenen Person zur Kontrolle der sie betreffenden Daten und Verarbeitungen, beispielsweise durch effektive Wahrnehmung der Betroffenenrechte wie Auskunft, Berichtigung, Sperrung oder Löschung sowie Widerruf einer Einwilligung o. ä. Bei der Arbeit mit Schutzzielen ist stets zu berücksichtigen, dass sie und die sie umsetzenden Maßnahmen nicht unabhängig voneinander sind, sondern Wechselwirkungen bestehen und die Schutzziele in ihren Ausprägungen – je nach Kontext – unterschiedlich priorisiert werden müssen.

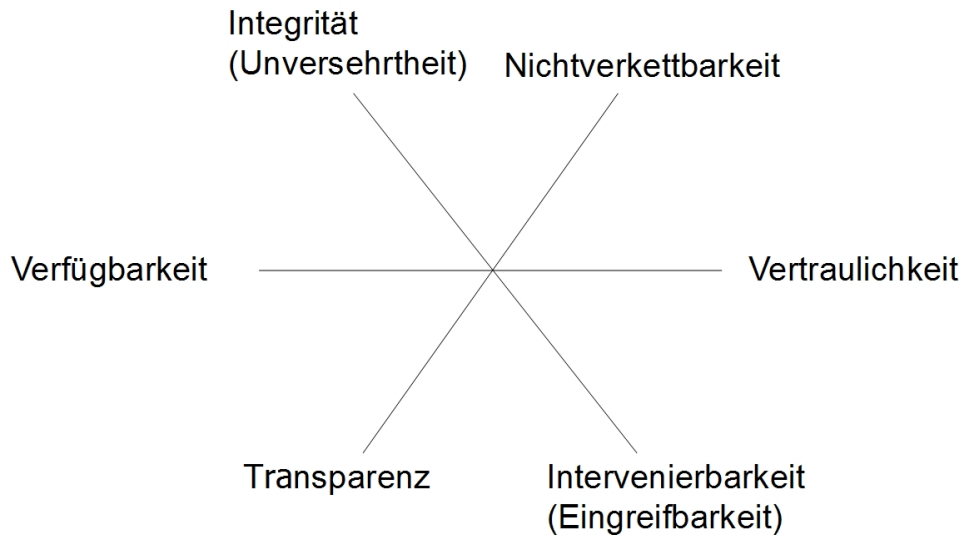

Abb. 02: Systematik der Schutzziele

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.[105] 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.

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 der DSGVO 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.

4.2.2 Identifikation möglicher Angreifer und Risikoquellen (2.2)

Bei der Betrachtung der Schutzziele ist 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. Im Unterschied zum Datenschutz sind die Angreifer in dieser Sichtweise grundsätzlich externe Dritte (oder kriminelle Innentäter) oder nicht regelkonform handelnde interne Nutzer.

Eine DSFA hat nicht zum Ziel, die Geschäftsprozesse einer Organisation zu schützen, sondern die Rechte und Freiheiten natürlicher Personen, also der Kunden, Arbeitnehmer etc. einer Organisation. Eine wesentliche Quelle des Risikos für diese Rechte und Freiheiten sind daher vor allem Organisationen, wie zum Beispiel Behörden und Unternehmen. Dies gilt auch, wenn diese oder ihre internen Anwender regelkonform handeln. Allein aus einer planmäßigen Datenverarbeitung können sich für Betroffene Nachteile ergeben. Es muss daher betrachtet werden, wie die Organisation Daten erfasst, verarbeitet und weitergibt, bzw. welche anderen Organisationen, sich Zugriff zu Daten verschaffen können.[106] Dabei geht es auch um Risiken, die aus der illegitimen Überdehnung des Zwecks durch den Betreiber selbst entstehen, sowie um Risiken, die aus dem potenziellen Interesse anderer Institutionen an den schon bei einem Betreiber vorliegenden Datenbestand resultieren. Darüber hinaus sind auch Risiken, die sich aus dem unbefugten Zugriff Dritter auf das Verfahren ergeben; dies können auch staatliche Stellen sein. Insofern muss im Rahmen einer DSFA standardmäßig überprüft werden, ob folgende Organisationen ein Risiko für die Rechte und Freiheiten natürlicher Personen (vgl. Art. 35 Abs. 1 DSGVO) und den Datenschutz 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[107], 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 in seiner Beratungsfunktion seine eigene Organisation »von außen« betrachtet.

4.2.3 Ermittlung der Eingriffsintensität und des Schutzbedarfs (2.3)

Um das Risiko bewerten zu können, muss festgestellt werden, wie schwer der Eingriff in die Rechte und Freiheiten natürlicher Personen wiegt. Dabei ist die *konkrete Verarbeitung* zu betrachten und der Verantwortliche muss den Eingriff in die Grundrechte *aus der Sicht der potenziell Betroffenen* bewerten. Dabei sind die Rechte auf Schutz personenbezogener Daten gemäß Art. 8 Charta und auf Achtung des Privatlebens gemäß Art. 7 Charta von besonderer Bedeutung. Zu beachten sind jedoch auch das Recht auf freie Meinungsäußerung gemäß Art. 11 Charta sowie das Recht auf Schutz vor Diskriminierung gemäß Art. 21 Charta. Der Verantwortliche muss nachweisen, dass die Eingriffe in die Rechte der Betroffenen auf das erforderliche Maß beschränkt und damit die Intensität des Eingriffs minimiert wurde, wie es etwa von Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO gefordert wird. Die Intensität des Eingriffs lässt sich folglich nur für eine konkrete Verarbeitungstätigkeit ermitteln.[108]

Ein Eingriff in die Grundrechte ist gemäß Art. 52 Abs. 1 Charta gerechtfertigt, wenn die Datenverarbeitung auf einer Rechtsgrundlage beruht, die verhältnismäßig ist. Im Rahmen dieser Verhältnismäßigkeitsprüfung steigen die Anforderungen an die rechtfertigenden Gründe in Abhängigkeit von der Schwere des Eingriffs.[109] Dabei lässt sich eine Einteilung nach der von *Alexy* entwickelten triadischen Skalierung vornehmen: dabei werden drei Stufen (leicht, mittel, schwer) unterschieden und die abstrakte Frage nach der Gewichtung eines Eingriffs operationalisiert.[110] Die somit ermittelte Abstufung ergibt den Schaden, der in der Verletzung der Selbstbestimmung des Betroffenen besteht.

Auf der Basis der Eingriffsintensität kann der Schutzbedarf festgestellt werden. Zur Unterscheidung der Schutzbedarfe haben sich haben sich die Abstufungen bewährt, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinen IT-Grundschutz-Katalogen empfiehlt.[111] Allerdings ist auch hier 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 Charta darstellt. Allein aus der Tatsache einer Datenverarbeitung 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.[112]

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 etwa den besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO 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.

Hoher Schutzbedarf besteht auch, wenn es nicht möglich ist, Konflikte unter zumutbaren Bedingungen für die Betroffenen gerichtlich klären zu lassen. Die folgenden beispielhaften Verarbeitungsszenarien führen zu einem hohen Schutzbedarf:

- Verarbeitung nicht veränderbarer Personen-Daten, die ein Leben lang als Anker für Profilbildungen dienen können bzw. zuordenbar sind (z. B. biometrische Daten, Gen-daten),
- Verbreitung eindeutig identifizierender, hoch verknüpfbarer Daten (z. B. lebenslang gültige Krankenversichertennummer, Steuer-ID),
- gesetzlich begründete oder anderweitig zu erklärende Intransparenz der Verfahrensweisen für Betroffene (z. B. Verfassungsschutz, Schätzwerte im Scoring),
- Verarbeitung von Daten in einem Verfahren mit möglichen gravierenden, finanziellen Auswirkungen für Betroffene,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf das An-sehen/die Reputation des Betroffenen,
- Verarbeitung von Daten in einem Verfahren mit möglichen Auswirkungen auf die körperliche Unversehrtheit des Betroffenen,
- Verarbeitung von Daten, die realistischer Weise zu erwartende Auswirkungen auf die Grundrechtsausübung einer Vielzahl Betroffener haben können (z. B. bei zunehmend flächendeckender, öffentlicher Videoüberwachung),
- Gefahr von Diskriminierung, Stigmatisierung (z. B. durch Algorithmen, intransparentes Zustandekommen von Entscheidungen eines Betroffenen),
- Eingriffe in besonders geschützten inneren Lebensbereich eines Betroffenen

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«).

Eine Festlegung auf »hohen Schutzbedarf« hat Folgen für die Ausgestaltung der funktionalen Aspekte des Verfahrens und der Schutzmaßnahmen, die aufgrund der Datenschutzgrundsätze aus Art. 5 DSGVO und insbesondere der Art. 24, 25 und 32 DSGVO mit Bezug zu technischen und organisatorischen Maßnahmen sowie der Betroffenenrechte der Art. 12 bis 22 DSGVO umzusetzen sind.

- *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. Es besteht Gefahr für Leib und Leben.

4.2.4 Bewertung des Risikos (2.4)

Kern der DSFA ist die Risikobewertung. Diese erfordert nach Art. 35 Abs. 7 Buchstabe c DSGVO die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen. Erwägungsgrund 75 stellt dabei klar, dass diese Risiken zu physischen, materiellen, aber eben auch immateriellen Schäden führen können. Immaterielle Schäden sind insbesondere ungerechtfertigte Eingriffe in die Grundrechte potenziell Betroffener, wie sie etwa

in Art. 7, 8, 11, 21 Charta verbürgt sind. Das spezifische Risiko für den Datenschutz und das Recht aus Art. 8 Charta besteht dabei in der Negierung der Schutzziele.[113]

Für die Bewertung des Risikos sind nach Erwägungsgrund 90 DSGVO für jedes identifizierte Risiko auch die Eintrittswahrscheinlichkeit und die Schwere zu berücksichtigen und nach Erwägungsgrund 76 DSGVO sind diese wiederum in Bezug auf die Art, den Umfang, die Umstände und Zwecke der Verarbeitung zu bestimmen. Dafür wird auch auf die in Phase 1 benannten Beschreibungen des Prüfgegenstands, die Angriffsszenarien und die soeben ermittelte Eingriffsintensität und den Schutzbedarf zurückgegriffen.

Die formelhafte Kalkulation des Gesamtrisikos für ein System: $Risk = \sum_{i=1}^{n} Impact_i \times p_i$ mit $Impact_i$ für das Schadensausmaß des Risikos *i* und p_i für dessen Eintrittswahrscheinlichkeit ist zwar weithin bekannt, aber weder für Datenschutz- noch Informationssicherheitsrisiken praktikabel. Es können in beiden Bereichen üblicherweise keine auch nur annähernd exakten Werte angegeben werden. Insbesondere gilt dies bei Risiken für Rechte und Freiheiten aus Perspektive der potenziell Betroffenen: Während das Schadensausmaß aus Sicht der Organisation häufig zumindest grob kalkulierbar ist, da finanzielle Auswirkungen abgeschätzt werden können, ist ein Risiko für Rechte der betroffenen Person oft kaum zu beziffern und nur in Ausnahmefällen seriös in monetären Einheiten ausdrückbar. Insofern ist zu beachten, dass in der englischen Version der DSGVO in Erwägungsgrund 90 konsequenterweise nicht die mathematische Wahrscheinlichkeit im Sinne von «propability», sondern «likelihood» verwendet wird. Insofern sollte auf Pseudo-Berechnungen in der DSFA verzichtet werden. Vielmehr muss der Verantwortliche eine nachvollziehbare Argumentation anhand objektiver Kriterien für die Bewertung der Risiken in Abhängigkeit der Angriffsszenarien und Schutzzielanforderungen liefern, wie dies auch in Erwägungsgrund 76 gefordert ist.

Bei diesem Schritt muss das gesamte Verfahren zur Verarbeitung betrachtet werde. Soweit der in Schritt 1.2 definierte Prüfgegenstand bereits implementierte oder geplante technische und organisatorische Maßnahmen enthält, sollen auch diese bewertet werden. Zum Beispiel gilt dies bei Einsatz bestimmter Datenverarbeitungssysteme, wie Betriebssystemen oder Datenbanken, die etwa Rollen- und Rechtekonzepte enthalten.

4.2.5 Identifikation und Auswahl passender Abhilfemaßnahmen (2.5)

Die ermittelten Risiken, müssen sodann durch passende Abhilfemaßnahmen, insbesondere technische und organisatorische Maßnahmen bewältigt werden (Art. 35 Abs. 7 Buchstabe d DSGVO).

Das Standard-Datenschutzmodell enthält nach Schutzzielen geordnete Referenzschutzmaßnahmen.[114] 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. Allerdings ist zu beachten, dass es sich dabei um keine Checkliste handelt, auf der man Maßnahmen abhakt. Dies wäre auf Basis der Risikobewertung unzureichend. Stattdessen müssen das gesamte Verfahren und die Schutzziele des Standard-Datenschutzmodells mit ihren Wechselwirkungen berücksichtigt werden.

Im Unterschied zum Risiko-Management darf bei der dem Grundrechtsschutz dienenden DSFA ein identifiziertes Risiko mit einer geringen Anzahl von betroffenen Personen nicht als akzeptabel eingestuft werden und nur durch Maßnahmen der Schadensminderung abgedeckt werden. Zwar besteht die Möglichkeit, Risiken zu priorisieren und solche Maßnahmen zu ergreifen, die den höchsten Nutzen für die Betroffenen haben und mit den rechtlichen Anforderungen übereinstimmen. Allerdings müssen bei der

DSFA Risiken ausdrücklich bewältigt und nicht nur gemanagt werden. Verbleibende Risiken (Restrisiken) müssen ebenfalls analysiert werden.

Der Verantwortliche sollte daher darlegen, welche Maßnahmen zur Eindämmung der Risiken für die Rechte und Freiheiten natürlicher Personen aus welchen Gründen ausgewählt werden. Zudem sollte in diesem Schritt festgelegt werden, wer für die Umsetzung der Maßnahmen innerhalb der Organisation verantwortlich ist und welche Personen einzubeziehen sind.

Tab. 01: Beispiele für generische Schutzmaßnahmen

Schutzziel	Komponente	Beispielhafte Maßnahmen
Sicherstellung von Verfügbarkeit	Daten, Systeme, Prozesse	Redundanz, Schutz, Reparaturstrategie
Sicherstellung von Integrität	Daten	Hash-Wert-Vergleich[115]
	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, Verschlüsselung
Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung	Daten	Anonymisierung, Pseudonymisierung, Nutzung attributbasierter Credentials
	Systeme	Trennung (Isolierung) von Datenbeständen, Systemen
	Prozesse	Identity Management, Anonymitätsinfrastrukturen, Audits, Trennung, Rollen und Berechtigungen
Sicherstellung von Transparenz durch Prüffähigkeit	Daten	Auskunft, Spezifikation, Dokumentation, Protokollierung
	Systeme	Spezifikation, Systemdokumentation, Protokollierung von Systemaktivitäten und Administrationaktivitäten.
	Prozesse	Auskunft, Spezifikation, Dokumentation von Prozessen, Protokollierung
Sicherstellung von Intervenierbarkeit durch Ankerpunkte	Daten	geregelte Berichtigung, Sperrung, Löschung
	Prozesse	Helpdesk/einheitlicher Ansprechpartner für Änderungen/Löschungen durch Single Point of Contact, Change Management

4.2.6 Dokumentation der Bewertungsergebnisse und DSFA-Bericht (2.6)

Nach der Durchführungsphase (inklusive der Identifikation geeigneter Abhilfemaßnahmen) müssen die Bewertungsergebnisse und die Entscheidung für die getroffene Maßnahmenauswahl dokumentiert werden. Damit eine DSFA die eingangs erwähnten positiven Effekte erzielen kann, ist es notwendig, dass der Prozess umfänglich dokumentiert wird. Es ist daher ein DSFA-Bericht zu erstellen, der Teil der allgemeinen Rechenschaftspflicht des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO und der auf Verlangen der Aufsichtsbehörde gemäß Art. 58 Abs. 1 Buchstabe a DSGVO vorgelegt werden kann. Der Bericht enthält auch die von Art. 30 DSGVO geforderten Angaben eines Verzeichnisses von Verarbeitungstätigkeiten und umfasst die Dokumentation von Verarbeitungsvorgängen, Risiken und Maßnahmen. Er umfasst nicht nur die erfolgreich eindämmbaren Risiken; können etwa bestimmte Risiken nicht (vollständig) durch die Maßnahmen beseitigt werden, müssen diese Restrisiken gerechtfertigt werden: Es muss

dargestellt werden, aus welchen Gründen sie nicht oder nur zum Teil ausgeschlossen werden können.

Ein DSFA-Bericht sollte einer einheitlichen Gliederung folgen, die es erleichtert, die Ergebnisse zu bewerten und zu vergleichen. Es bietet sich an, sich an den einzelnen Phasen dieses Prozesses zu orientieren, so dass der Prüfgegenstand, die Kriterien, die Bewertungen und die Maßnahmenwahl in getrennten Abschnitten nachvollziehbar dargestellt werden. Durch die umfassende Dokumentation der Bewertungsergebnisse wird gewährleistet, dass die Ziele der DSFA erreicht werden.

Die Veröffentlichung des DSFA-Berichts ist zwar gesetzlich nicht vorgeschrieben, dient aber der Transparenz und kann damit das Vertrauen in die Verarbeitungstätigkeit erhöhen. Wenn der Bericht Details über Betriebs- und Geschäftsgeheimnisse enthält oder wenn die Ergebnisse der Restrisikoanalyse als Angriffsvorlage missbraucht werden könnten, kann für die Öffentlichkeit eine gekürzte Fassung erstellt werden.[116] Eine solche Veröffentlichung wird auch von der Artikel-29-Datenschutzgruppe empfohlen.[117] Der Kurzbericht soll aber genau wie der vollständige Bericht alle Elemente der DSFA dokumentieren und darf keinesfalls mögliche negative Effekte verschweigen. Die Entscheidung, dass bestimmte Informationen nicht zu veröffentlichen sind, sollte nur aus berechtigten und zu dokumentierenden Gründen erfolgen.

Der Bericht sollte auf der Internetseite der Organisation leicht auffindbar und kostenlos zu beziehen sein.

4.3 Entscheidung über das Verfahren

Mit dem DSFA-Bericht endet die eigentliche DSFA und die Anforderungen des Art. 35 DSGVO sind erfüllt. Auf der Grundlage der Ergebnisse, entscheidet der Verantwortliche, ob die geplante Verarbeitung umgesetzt werden soll. Ist das Ergebnis negativ, weil hohe Restrisiken verbleiben,[118] darf das untersuchte System nicht freigegeben werden und damit nicht zum Einsatz kommen, da in diesem Fall die Anforderungen der DSGVO nicht erfüllt wären. Der Verantwortliche kann somit von dem Verfahren Abstand nehmen oder vor der Verarbeitung die Aufsichtsbehörde konsultieren (vorherige Konsultation gemäß Art. 36DSGVO). Die Aufsichtsbehörde ist nach Art. 36 Abs. 2 DSGVO verpflichtet, dem Verantwortlichen innerhalb von acht Wochen nach Übersendung der erforderlichen Unterlagen schriftliche Empfehlungen zu geben.

4.4 Umsetzungsphase

Erzielt die DSFA ein positives Ergebnis und soll die geplante Verarbeitung durchgeführt werden, müssen in der Umsetzungsphase die in der Durchführungsphase identifizierten Abhilfemaßnahmen umgesetzt, getestet und freigegeben werden. Nach Art. 35 Abs. 7 Buchstabe d DSGVO muss zudem der Nachweis erbracht werden, dass die DSGVO in ihrer Gesamtheit erfüllt wird.

4.4.1 Implementierung der Abhilfemaßnahmen (3.1)

Die Umsetzung betrifft in der Regel technische und organisatorische Maßnahmen, beispielsweise hardware- oder softwarebasierte Funktionalität für einen besseren Schutz der personenbezogenen Daten, Konfigurationsanpassungen, Konzepte mit Festlegungen der Rollen und Rechte, die in die Praxis umzusetzen sind, oder Prozesse zum Umgang mit Beschwerden der Betroffenen. Es ist auch möglich, dass dem Risiko dadurch begegnet wird, dass bei geeigneter technischer Realisierung auf personenbezogene Daten verzichtet werden kann oder dass bestimmte risikoträchtige Funktionalitäten abgeschaltet werden.

Elemente eines Prozesses zur Datenschutz-Folgenabschätzung

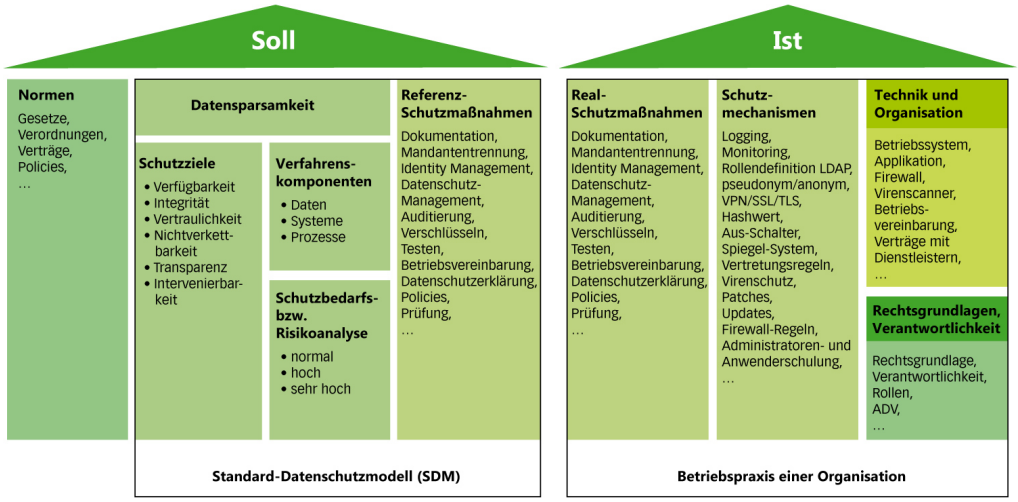

Abb. 03: Soll-Ist-Vergleich

Dafür ist eine Soll-Ist-Betrachtung hilfreich, durch die deutlich wird, inwieweit die geplanten Maßnahmen den Vorgaben des Standard-Datenschutzmodells entsprechen (siehe Abb. 03). Im Rahmen der Auswahl der Maßnahmen sind die Rechte und Freiheiten natürlicher Personen sowie sonstiger Betroffener zu berücksichtigen.

Der Soll-Ist-Vergleich ermöglicht zudem eine Überprüfung der Risikobewertung in der Praxis. Wenn nur ein rudimentäres Rollen- und Berechtigungskonzept vorliegt oder andere Lösungen, die vom Stand der Technik abweichen, genutzt werden, dann müssen die Alternativlösungen begründet und etwaige Lücken mit einer Konzeption zur Füllung etwa im Rahmen einer Projektplanung ergänzt werden. Ist ein Rollen- und Berechtigungskonzept vorhanden, muss dessen Funktion schlüssig dargelegt werden. Zudem ist zu beachten, dass die ausgewählten Maßnahmen stets dem aktuellen Stand der Technik gemäß Art. 25 Abs. 1 und Art. 32 DSGVO entsprechend aktualisiert werden müssen.

4.4.2 Test und Dokumentation der Wirksamkeit der Abhilfemaßnahmen (3.2)

Die Implementierung der Schutzmaßnahmen allein reicht nicht aus. Zusätzlich muss die Wirksamkeit der Maßnahmen durch Tests nachgewiesen werden. Dafür muss zunächst ein Testkonzept für Funktionen und die Abhilfemaßnahmen entwickelt werden, dessen Abläufe, wie auch die Testergebnisse, zu protokollieren sind. Zeigen sich dabei weitere Risiken, müssen diese ebenfalls bewältigt werden. Tests mit Echtdaten sind vor der Freigabe der Verarbeitung nur unter engen Bedingungen durchzuführen; auch Pilotphasen zählen bereits zum Echtbetrieb und müssen zeitlich begrenzt sein.

4.4.3 Nachweis der Einhaltung der DSGVO insgesamt (3.3)

Sind die Maßnahmen erfolgreich implementiert, ist darzulegen, dass die Verarbeitungstätigkeit die Anforderungen der DSGVO insgesamt einhält (Art. 35 Abs. 7 Buchstabe d DSGVO). Der DSFA-Bericht dient dabei als Grundlage. Darauf aufbauend wird die Erfüllung der rechtlichen Anforderungen etwa an die Umsetzung der technischen und organisatorischen Maßnahmen, wie sie durch Art. 25 und 32 DSGVO vorgegeben sind und die Bestätigung der Wirkung dieser Maßnahmen, behandelt.

4.4.4 Freigabe der Verarbeitung (3.4)

Der Nachweis der Einhaltung der DSGVO insgesamt ist auch die Grundlage für die Freigabe der Datenverarbeitung des Verantwortlichen. Ist der Nachweis erbracht, kann der Verantwortliche das Verfahren freigeben.

4.5 Überprüfungsphase

Die Abschätzung von Datenschutzfolgen ist kein einmaliger und strikt linearer Prozess, sondern muss während des gesamten Lebenszyklus eines Verfahrens fortlaufend überwacht werden.

4.5.1 Kontinuierliche Überprüfung der DSFA (4.1)

Dementsprechend legt Art. 35 Abs. 11 DSGVO fest, dass die DSFA jedenfalls dann zu wiederholen ist, wenn sich das mit der Verarbeitung verbundene Risiko ändert. Insofern ist kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischer, organisatorischer oder rechtlicher Weise verändern, die neue Datenschutzrisiken oder sonstige Risiken für die Rechte und Freiheiten natürlicher Personen nach sich ziehen. Veränderungen können sich aus dem Einsatz neuer Technologien, einer Zweckänderung oder auch Schwachstellen in der Informationssicherheit ergeben.[119]

4.5.2 Überwachung der Risiken im Datenschutz-Managementsystem (4.2)

Auch ist zu überwachen, ob die gewählten Abhilfemaßnahmen den erwarteten Nutzen haben oder ob andere Maßnahmen zu ergreifen sind. Es gilt stets sicherzustellen, dass die Maßnahmen an Veränderungen angepasst werden können. Um auf Veränderungen der Rahmenbedingungen möglichst effizient reagieren zu können, ist eine Einbindung in das allgemeine Datenschutz-Management der Organisation ratsam.

4.5.3 Unabhängige Prüfung der Prüfergebnisse (4.3)

Um zu gewährleisten, dass die DSFA ordnungsgemäß durchgeführt wurde, sollte die DSFA anhand des DSFA-Berichts von einem unabhängigen Dritten, etwa der zuständigen Datenschutzaufsichtsbehörde, überprüft werden können.

Insbesondere soll die Überprüfung sicherstellen, dass

- angemessen mit Interessenskonflikten umgegangen wurde,
- die Interessen der Betroffenen bei der Risikobewertung und der Auswahl von Schutzmaßnahmen angemessen berücksichtigt wurden,
- die Öffentlichkeit in ausreichendem Umfang über die Ergebnisse der DSFA informiert wird und
- die Abhilfemaßnahmen tatsächlich umgesetzt sind oder aber bei komplexen Schutzsituationen die Implementierung der vorgeschlagenen Schutzmaßnahmen tatsächlich in Angriff genommen wurde.

5
Diskussion – Was kann eine Datenschutz-Folgenabschätzung leisten?

Eine DSFA ist ein relativ neues Instrument zur Identifikation von Risiken, die durch den Einsatz von riskanten Verfahren, die zudem durch (neue) vorwiegend datenverarbeitende Technologien und Systeme 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 DSGVO 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 nach wissenschaftlichen Erkenntnissen und Erfahrungen aus der Praxis der Datenschutzbehörden die Analyse eines Verfahrens 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 DSGVO, muss die Perspektive der Betroffenen eingenommen werden, deren Grundrechte es durch entsprechende System- und Technikgestaltung zu schützen gilt.

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:[120] 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 DSGVO 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[121] hergestellt werden.

Anmerkungen

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

2 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

3 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.

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

5 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 Union L 119, 04. Mai 2016, S. 1-88.

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

7 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. München und Wien: Oldenbourg, S. 266 - 280., hier S. 266f.

8 Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos., S. 47 mit weiteren Nachweisen; Grunwald, A. (2010): Technikfolgenabschätzung - eine Einführung. 2. Aufl. 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. Zuletzt aufgerufen 10.03.2016.

9 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. Zuletzt aufgerufen 10.03.2016.

10 http://www.eptanetwork.org. Zuletzt aufgerufen 10.03.2016.

11 Grunwald, A. (2010): Technikfolgenabschätzung - eine Einführung. 2. Aufl. Berlin: Edition Sigma (Gesellschaft – Technik – Umwelt. Neue Folge, 1).S. 85ff.

12 Ibid., S. 82ff.

13 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.

Anmerkungen

14 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.

15 § 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«.

16 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.

17 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 DSGVO den Begriff »Verantwortlicher«.

18 Zum Beispiel § 6 Abs. 1 BDSG 1977; § 10 Abs. 1 HDSG 1978; § 6 Abs. 1 NDSG 1978.

19 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: RDV - Recht der Datenverarbeitung 15, Nr. 2, S. 65-69. hier S. 65f.

20 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. Zuletzt aufgerufen 10.03.2016.

21 § 1 Abs. 1 BDSG 1990 sowie 2003.

22 § 1 Satz 1 NDSG 2002.

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

24 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: RDV - Recht der Datenverarbeitung 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.

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

Anmerkungen

26 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.

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

28 Engelien-Schulz, T. (2003): Die Vorabkontrolle gemäß § 4d Abs. 5 und Abs. 6 Bundesdatenschutzgesetz (BDSG). In: RDV - Recht der Datenverarbeitung 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.

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

30 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.

31 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.

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

33 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.

34 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.

35 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.

36 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.

37 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. 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.

38 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.

39 Ein ausführlicher Vergleich ist nachzulesen in Ibid., S. 17ff.

40 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. Zuletzt aufgerufen 10.03.2016.

41 Ibid., S. 5.

42 Ibid., S. 20f.

43 Ibid., S. 22.

44 Ibid., S. 23-5.

45 Ibid., S. 28.

46 Ibid., S. 27.

47 Ibid., S. 28.

48 Ibid., S. 12-14.

49 Ibid., S. 16-18.

50 Ibid., S. 18f.

51 Ibid.,»The practical implementation of the basic prnciples will depend on the organisation's usual business practice« (S. 4) und » Each organisation will be best placed to determine how it considers the issue of privacy risks« (S. 6).

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

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

54 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; CNIL (Commission Nationale de l'Informatique et des Libertés) (2015b). Privacy Risk Assessment: Methodology (how to carry out a PIA). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf; CNIL (Commission Nationale de l'Informatique et des Libertés) (2015a). Privacy Risk Assessment: Tools (templates and knowledge bases). Paris. http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-2-Tools.pdf.

55 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 Zuletzt aufgerufen 10.03.2016.

56 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 Zuletzt aufgerufen 10.03.2016.

57 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; 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.

Anmerkungen

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.

58 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., S. 12.

59 Ibid., S. 7f.

60 Ibid., S. 11.

61 Ibid.

62 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. Zuletzt aufgerufen 10.03.2016.

63 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. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_de.pdf. Zuletzt aufgerufen 10.03.2016.

64 Ibid., S. 6f.

65 Ibid., S. 7f.

66 Ibid., S. 12f.

67 Artikel-29-Datenschutzgruppe (2017): Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 13 f. Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

68 Vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf. Zuletzt aufgerufen 10.11.2017.

69 Art. 38 DSGVO.

70 Zur DSFA sowie zu Regelungsoptionen durch die nationalen Gesetzgeber Marschall, in Roßnagel, Das neue Datenschutzrecht, 2018, § 5 Rn. 160 ff.

71 Das aus 2012 stammende Dokument bezieht sich insoweit selbstverständlich noch auf die DSRL. Eine Anpassung an die DSGVO ist jedoch zu erwarten.

72 Elemente des Risikomanagements waren allerdings implizit bereits in Art. 17 und 20 der DSRL formuliert. S. zum „Risikoansatz" kritisch Roßnagel, DuD 2016, 565, weil dieser Ansatz bewirkt, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter diese Pflichten erfüllen muss.

73 So zum Beispiel Jan Philipp Albrecht, Verhandlungsführer des Europäischen Parlaments für die geplante Datenschutzverordnung. https://www.janalbrecht.eu/presse/pressemitteilungen/eu-datenschutz.html. Zuletzt aufgerufen 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. Zuletzt aufgerufen 10.03.2016.

74 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Schulz, G.; Rost, M. (2016). Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfungauf der Basis einheitlicher Gewährleistungsziele. V.1.0 – Erprobungsfassung. https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_0.pdf. Zuletzt aufgerufen 16.11.2017.

Anmerkungen

75 Kingreen, T. (2016): EU-GRCharta Artikel 8. In: Calliess, C.; Ruffert, M. (Hrsg.): EUV/AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta – Kommentar, 5. Aufl. München: C.H. Beck, S. 2812-2816.

76 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. (2014b): Integrating privacy impact assessment in risk management. In: International Data Privacy Law 4, Nr. 2, S. 155-170.

77 Gonscherwoski, S.; Herber, T.; Robrahn, R.; Rost, M.; Weichelt, R. (2017): Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive"-Verfahrens (V 0.10). https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf. Zuletzt abgerufen 16.11.2017.

78 Wright, D.; Kroener, I.; Friedewald, M. et al. (2014a). 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. Zuletzt aufgerufen 10.03.2016.

79 Vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf. Zuletzt aufgerufen 10.11.2017.

80 Artikel-29-Datenschutzgruppe (2017). Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 12. Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

81 Ibid., S. 7-9.

82 Ibid., S. 11

83 Ibid., S. 7.

84 In jedem Fall haftet der (interne) DSB nicht persönlich, sondern nur im Rahmen der Arbeitnehmerhaftung für die ordnungsgemäße Durchführung der DSFA und deren Ergebnisse, vgl. Artikel-29-Datenschutzgruppe (2016). Guidelines on Data Protection Officers (DPOs). Working Paper 16/EN, WP 243. Brussels. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

85 Ibid.

86 Bamberger, K. A.; Mulligan, D. K. (2015): Privacy on the ground: Driving corporate behavior in the United States and Europe. Cambridge, Mass.; London: The MIT Press (Information policy series.

87 Ibid.(WP29); Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf. Zuletzt aufgerufen 10.11.2017.

88 Vgl. die Bearbeitung eine fiktiven Falles von Gonscherwoski, S.; Herber, T.; Robrahn, R.; Rost, M.; Weichelt, R. (2017): Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive"-Verfahrens (V 0.10). https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf. Zuletzt abgerufen 16.11.2017.

89 Die Erforderlichkeit dieser Bewertung ergibt sich ferner aus den datenschutzrechtlichen Regeln zur Zweckbindung nach Art. 5 Abs. 1 Buchstabe b DSGVO und der Datenminimierung gemäß Art. 5 Abs. 1 Buchstabe c DSGVO,

welche eine Güterabwägung zur Gewährleistung der Rechte und Freiheiten natürlicher Personen erfordern.

90 Der Begriff der Notwendigkeit bezieht sich dabei konkret auf den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchstabe c DSGVO. Dieser ist zwar in der deutschen Fassung unglücklich übersetzt (Während der deutsche Wortlaut »Notwendigkeit« lautet, beziehen sich die englische und französische Fassungen auf die »necessity«/»nécessité« und damit eigentlich die Erforderlichkeit), durch den insofern einheitlichen Wortlaut von Art. 35 Abs. 7 Buchstabe b und Art. 5 Abs. 1 Buchstabe b DSGVO ist der Bezug aber eindeutig.

91 Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

92 Mitarbeiter sind als Vertreter der datenverarbeitenden Organisation als potenzielle Angreifer und als Arbeitnehmer gleichzeitig als potenzielle Betroffene zu betrachten.

93 Vgl. z.B. Office of the Australian Information Commissioner (Hrsg.) (2014): Guide to undertaking privacy impact assessments. Sydney. https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf. Zuletzt aufgerufen 9. August 2017.

94 Wichtermann, M. (2016): Die Datenschutz-Folgenabschätzung in der DS-GVO: Die Folgenabschätzung als Nachfolger der Vorabkontrolle. In: DuD - Datenschutz und Datensicherheit 40, Nr. 12, S. 797-801.

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

96 Clarke, R. (2011): An Evaluation of Privacy Impact Assessment Guidance Documents. In: International Data Privacy Law 1, Nr. 2, S. 111-120.

97 Die Anforderungen des Art. 8 Abs. 2 Charta an die Rechtfertigung sind dabei in Art. 5 Abs. 1 und Art. 6 DSGVO einfachgesetzlich umgesetzt.

98 Es ist nach Art. 8 Abs. 2 Charta verboten, personenbezogene Daten zu verarbeiten. Dies setzt Art. 6 Abs. 2 auf einfachgesetzlicher Ebene um.

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

100 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.

101 Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder; Schulz, G.; Rost, M. et al. (2016). Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.0). Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder. https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methode_V_1_0.pdf.

102 Artikel-29-Datenschutzgruppe (2017). Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 21. Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

103 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.

104 Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder; Schulz, G.; Rost, M. et al. (2016). Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.0). Konferenz der unabhängigen

Anmerkungen

Datenschutzbeauftragten des Bundes und der Länder. https://www.datenschutz-mv.de/datenschutz/sdm/SDM-Methode_V_1_0.pdf.

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

106 Um dies festzustellen, kann es auch sinnvoll sein, in einem Vertrauensmodell darzustellen, welche Beziehungen zu anderen Organisationen bestehen und verdeutlicht, welchen Organisationen vertraut werden muss, da diese nur eingeschränkt kontrolliert werden. Angriffe seitens dieser Organisationen sind für den Verantwortlichen schwieriger zu erkennen und sollten daher explizit beschrieben werden.

107 Zu den Interessen verschiedener Akteure an personenbezogenen Daten in der Arbeitswelt vgl. Morlok, T.; Matt, C.; Hess, 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.; Matt, C.; Hess, T. (2015). Wertschöpfung in Datenmärkten: Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten. Forschungsbericht. Karlsruhe: Fraunhofer ISI. https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles_dokumente/Forschungsbericht-LMU-Wertschoepfung-in-Datenmaerkten_FP_3Sept15.pdf. Zuletzt aufgerufen 10.03.2016.

108 Alexy, R. (2003): Die Gewichtsformel. In: Jickeli, J.; Kreutz, P. et al. (Hrsg.): Gedächtnisschrift für Jürgen Sonnenschein (22. Januar 1938 bis 6. Dezember 2000). Berlin: de Gruyter, S. 771-792.

109 Jarass, H. D. (2016): Charta der Grundrechte der Europäischen Union: GRCh unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK –Kommentar. 3. Aufl. München: C. H. Beck, Rn. 34-36.

110 Alexy, R. (2003): Die Gewichtsformel. In: Jickeli, J.; Kreutz, P. et al. (Hrsg.): Gedächtnisschrift für Jürgen Sonnenschein (22. Januar 1938 bis 6. Dezember 2000). Berlin: de Gruyter, S. 771-792.

111 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. Zuletzt aufgerufen 10.03.2016.

112 Eine zusätzliche vierte Schadensklasse »gering« ist anders als bei der IT-Sicherheit nicht sinnvoll, da immer ein Risiko besteht, wenn personenbezogene Daten verarbeitet werden.

113 Vgl. Bieker, F. (2018): Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell. In: DuD - Datenschutz und Datensicherheit 42, Nr. 1 (im Erscheinen).

114 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder; Schulz, G.; Rost, M. (2016). Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfungauf der Basis einheitlicher Gewährleistungsziele. V.1.0 – Erprobungsfassung. https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_0.pdf. Zuletzt aufgerufen 16.11.2017.

115 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).

116 Bei öffentlichen Stellen besteht ggf. ein Anspruch auf Zugang aus dem Informationsfreiheitsrecht.

117 Artikel-29-Datenschutzgruppe (2017). Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a

Anmerkungen

high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 18. Brussels. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

118 Artikel-29-Datenschutzgruppe (2017): Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 19. Brussels. Online verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137. Zuletzt aufgerufen 11. August 2017.

119 Artikel-29-Datenschutzgruppe (2017): Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248, S. 15 f. Brussels. Online verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137. Zuletzt aufgerufen 11. August 2017.

120 Collingridge, D. (1980): The social control of technology. London: Pinter; Liebert, W.; Schmidt, J. C. (2010): Collingridge's dilemma and technoscience: An attempt to provide a clarification from the perspective of the philosophy of science. In: Poiesis & Praxis 7, Nr. 1-2, S. 55-71.

121 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
CNIL	Commission Nationale de l'Informatique et des Libertés
DPIA	Data Protection Impact Assessment
DSGVO	Datenschutz-Grundverordnung
DSB	Datenschutzbeauftragte_r
DSFA	Datenschutz-Folgenabschätzung
DSK	Datenschutzbeauftragten des Bundes und der Länder
DSRL	Datenschutzrichtlinie (Richtlinie 95/46/EG)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
EU	Europäische Union
HDSG	Hessisches Datenschutzgesetz
ISO	International Organization for Standardization
NDSG	Niedersächsisches Datenschutzgesetz
OTA	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
PIA	Privacy Impact Assessment
SDM	Standard-Datenschutzmodell
TA	Technikfolgenabschätzung
TAB	Büro für Technikfolgen-Abschätzung beim Deutschen
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

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

3. Auflage
November 2017

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 DUISBURG ESSEN

Offen im Denken

EBERHARD KARLS UNIVERSITÄT TÜBINGEN
INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein