Felix Bieker, Marit Hansen, Michael Friedewald

Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung

Die Europäische Union verfügt seit dem Inkrafttreten des Vertrags von Lissabon im Jahr 2009 über die rechtlich verbindliche Grundrechtecharta (GRC), die das Recht auf Privatsphäre, wie es seit den fünfziger Jahren aus Art. 8 der Europäischen Menschenrechtskonvention (EMRK) bekannt ist, um ein eigenständiges Recht auf den Schutz personenbezogener Daten erweitert. Allerdings klafft eine Lücke zwischen dem Schutz dieser Rechte und der Umsetzung neuer Technologien. Einen Ansatz, um die Lücke zu schließen, bietet die in der neuen Europäischen Datenschutz-Grundverordnung (DS-GVO) erstmals verbindlich geregelte Datenschutz-Folgenabschätzung (DSFA).[1]

Um Unternehmen und Behörden für die Einhaltung dieser Rechte zu sensibilisieren, schreibt Art. 35 DS-GVO die Durchführung einer DSFA vor, die dazu dient, Risiken für Individuen, die sich aus der Verwendung einer bestimmten Technologie oder eines bestimmten Systems ergeben, zu erkennen und zu analysieren. Auf der Grundlage dieser Analyse sind angemessene Maßnahmen auszuwählen und umzusetzen, um die festgestellten Risiken zu bewältigen.

Seit der Einführung von Folgenabschätzungen gab es immer wieder Ansätze, diese auch auf dem Gebiet des Privatsphären- und Datenschutzes fruchtbar zu machen.[2] *Auf freiwilliger Basis wurden diese jedoch in der Praxis oft nicht umgesetzt oder eher als Form des Produkt-Marketings verstanden. Wenn die Grundverordnung im Mai 2018 anwendbar wird, müssen Unternehmen und Behörden im Fall eines voraussichtlich hohen Risikos ihrer Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen den Datenschutzaufsichtsbehörden auf Anfrage ihre Datenschutz-Folgenabschätzungen vorlegen.*

I. Eine grundrechtskonforme Datenschutz-Folgenabschätzung

Der im Folgenden dargestellte Prozess für eine DSFA orientiert sich an den in Art. 35 DS-GVO formulierten Anforderungen und basiert auf ausführlichen Analysen bestehender Verfahren[3]. Er stellt sicher, dass die Ergebnisse reproduzierbar und überprüfbar sind. Zudem erlaubt er den Vergleich verschiedener möglicher Lösungen und ist technologieneutral formuliert.

Der Prozess ist in vier Phasen unterteilt (siehe Abb. 1): In der Vorbereitungsphase (1) ist zunächst das geplante Verfahren zur Datenverarbeitung zu beschreiben, das anschließend in der Bewertungsphase (2) aus der Perspektive der Betroffenen zu beurteilen ist. Sodann werden in der Maßnahmenphase (3) Vorkehrungen getroffen, um die identifizierten Risiken einzudämmen. Schließlich werden in der Berichtsphase (4) die Ergebnisse des DSFA-Verfahrens dokumentiert. Die anlassbezogen und regelmäßig erforderliche Fortschreibung der DSFA wird durch die Einbindung in das Datenschutz-Management des Verantwortlichen sichergestellt.

1. Vorbereitungsphase

1.1 Relevanzschwelle

Zunächst ist festzustellen, ob eine DSFA notwendig ist. Nach Art. 35 DS-GVO ist dies der Fall, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Die Formulierung „Rechte und Freiheiten" lehnt sich an Art. 52 Abs. 1 GRC an, der wiederum, der französischen Rechtstradition folgend, auf den Gebrauch in der EMRK zurückgeht.[4] Es besteht zwischen beiden kein qualitativer Unterschied; sie beziehen sich auf die europäischen Individualgrundrechte.[5]

Von den Verantwortlichen wird also die Einschätzung von Risiken gefordert, um festzustellen, ob es einer DSFA bedarf. Allerdings ist dabei zu beachten, dass es sich bei einer

1 Das in diesem Text vorgestellte Verfahren einer Datenschutz-Folgenabschätzung beruht in Teilen auf einem White Paper des Forums Privatheit für die Digitale Welt, an dem die Autoren mitgewirkt haben: Friedewald u.a., Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz, Fraunhofer ISI, Karlsruhe, 2016. Die Ausgestaltung der DSFA wird zurzeit auf europäischer Ebene zwischen den Aufsichtsbehörden diskutiert; der vorliegende Text ist daher „work in progress" und gibt den Stand vom 08.07.2016 wieder.

2 Vgl. etwa ICO (Information Commissioner's Office), Conducting privacy impact assessments code of practice, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf; CNIL (Commission Nationale de l'Informatique et des Libertés), Privacy Impact Assessment: Methodology (how to carry out a PIA), 2015, http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf; Wright/De Hert (Hrsg.), Privacy Impact Assessment, Dordrecht u.a. 2012.

3 Wright u.a., Privacy Impact Assessment and Smart Surveillance. A State of the Art Report, Deliverable 3.1 SAPIENT Project, 2013; Venier u.a., A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies. Deliverable 4 PRESCIENT Project, 2013, http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_deliverable_4_final.pdf; Wright/Friedewald, Integrating privacy and ethical impact assessment, Science and Public Policy Bd. 40, 2013, S. 755.

4 Borowsky, in: Meyer (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 52, Rn. 19.

5 Becker, in: Schwarze u.a. (Hrsg.), EU-Kommentar, 3. Aufl. 2012, Art. 52, Rn. 2.

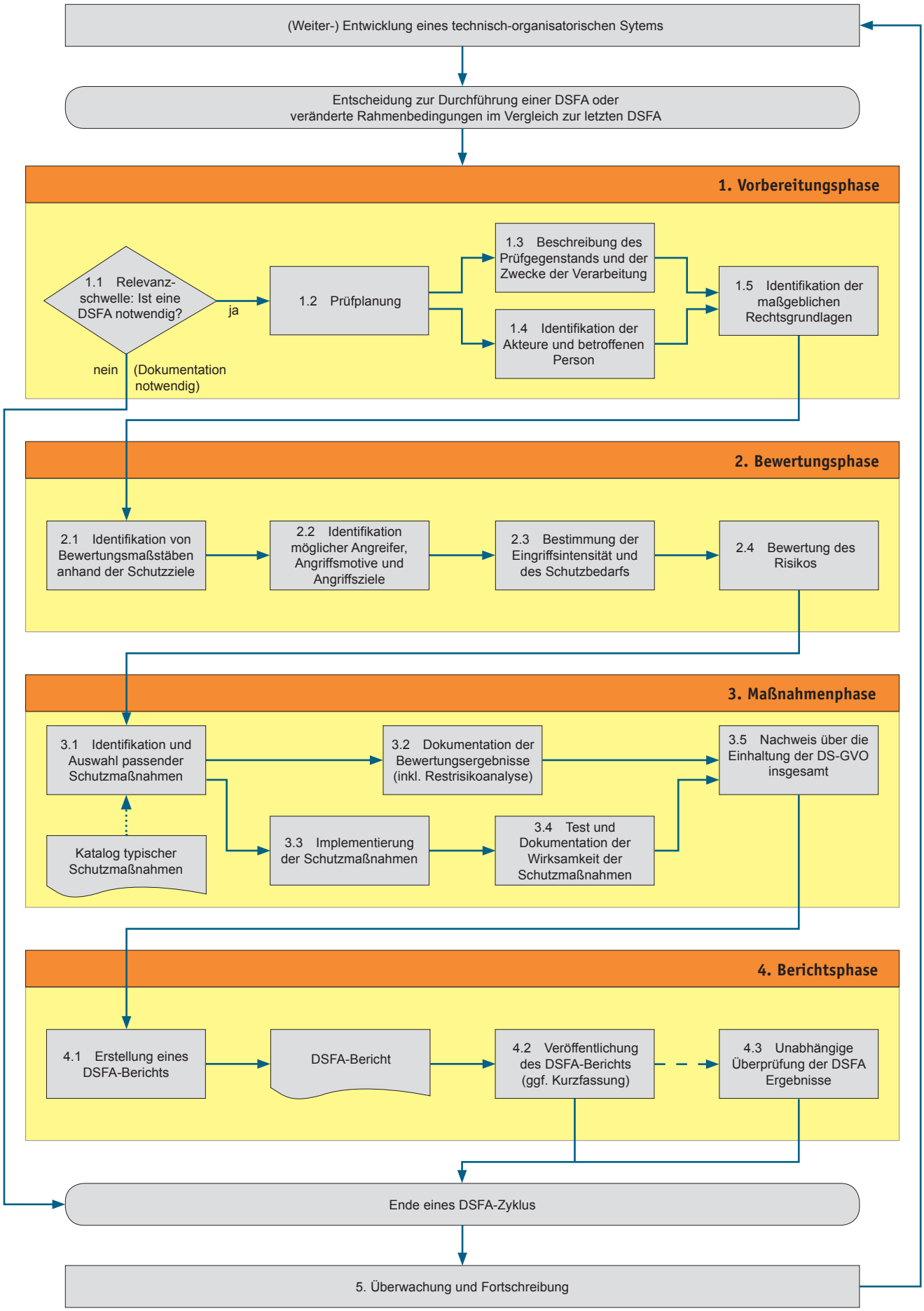

Abb. 1: Prototypischer Ablauf einer Datenschutz-Folgenabschätzung

DSFA nach DS-GVO nicht um das im Bereich der Informationssicherheit übliche Verfahren des Risikomanagements handelt. Dieses befasst sich mit Risiken für eine Organisation und ihren Aktivitäten. Art. 35 Abs. 1 DS-GVO liegt eine andere Art von Risikobeurteilung zugrunde: Im Fokus steht eine Bewertung des Risikos für die Rechte von Individuen. Damit ist insbesondere das Grundrecht auf den Schutz personenbezogener Daten gemeint.[6] Nach ständiger Rechtsprechung des Gerichtshofs der EU (EuGH) stellt jede Verarbeitung von personenbezogenen Daten einen Eingriff in Art. 8 GRC dar, der gerechtfertigt werden muss.[7] Folglich ist jeder Eingriff ein Risiko für die Rechte der betroffenen Personen. Den identifizierten Risiken müssen Maßnahmen entgegengesetzt werden. Können etwa bestimmte Risiken nicht (vollständig) beseitigt werden, müssen diese verbleibenden Restrisiken dokumentiert und gerechtfertigt werden. Sind diese allerdings als zu hoch einzustufen, darf das Verfahren nicht eingesetzt werden.

Die DS-GVO selbst gibt verschiedene Anhaltspunkte, wann ein solches hohes Risiko besteht. Nach der nicht abschließenden Aufzählung des Abs. 3 besteht ein solches Risiko insbesondere

- bei systematischer und umfassender Bewertung persönlicher Aspekte von Personen, die auf automatisierter Verarbeitung beruht und Grundlage von Entscheidungen ist, die diese Personen in erheblicher Weise beeinträchtigen;
- wenn besondere Kategorien personenbezogener Daten oder solche zu strafrechtlichen Verurteilungen oder Straftaten umfangreich verarbeitet werden;
- bei der systematischen und umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Zudem sind die von den Aufsichtsbehörden nach Art. 35 Abs. 4 u. 5 DS-GVO zu erstellenden Listen zu beachten, in denen diese Verarbeitungsvorgänge benennen, die stets einer DSFA bedürfen oder von einer solchen explizit ausgenommen sind. Allerdings ist die Aufstellung der Letzteren in das Ermessen der Datenschutzaufsichtsbehörden gestellt. Bei bestimmten Arten von Datenverarbeitungen generell und ohne weitere Prüfung von einer DSFA abzusehen, wäre jedoch dem umfassenden Grundrechtsschutz, den die DS-GVO ausdrücklich beabsichtigt, abträglich, so dass dieser Ansatz nicht weiter verfolgt werden sollte.

Unabhängig von der Entscheidung, ob eine DSFA durchgeführt werden soll, ist dieser Schritt in jedem Fall mit einer Begründung zu dokumentieren. Dies dient auch der Absicherung des Verantwortlichen gegenüber der zuständigen Aufsichtsbehörde, der eine Überprüfung so zudem erleichtert wird.

1.2 Prüfplanung

Zu den Zielen der DSFA nach der DS-GVO gehört es zu bewerten[8], ob ein definiertes Datenverarbeitungssystem die datenschutzrechtlichen Anforderungen erfüllt, und geeignete Schutzmaßnahmen für dieses System zu identifizieren. Die Überprüfbarkeit für die Öffentlichkeit und Aufsichtsbehörden kann durch den Rückgriff auf einen vordefinierten Katalog an Bewertungskriterien und -maßstäben sowie Schutzmaßnahmen erleichtert werden. Dies dient auch der Sicherstellung der von Art. 35 Abs. 9 DS-GVO geforderten Transparenz des Verfahrenlegts. Der Katalog sollte nicht mit einer einfachen Checkliste verwechselt werden, bei der einzelne Punkte abgehakt werden – vielmehr müssen die einzelnen Risiken detailliert in Bezug auf die konkreten Verarbeitungsvorgänge geprüft werden.

Das Team zur Durchführung der DSFA sollte über ausreichende Ressourcen und – idealerweise auch interdisziplinäre – Kompetenz verfügen, um eine objektive Analyse zu ermöglichen. Der für die Entwicklung und Umsetzung Verantwortliche sollte, mit der Unterstützung einer neutralen Partei, wie etwa aus der Qualitätssicherung, die DSFA durchführen. Zudem ist gem. Art. 35 Abs. 2 DS-GVO der Rat der/des Datenschutzbeauftragten einzuholen, soweit ein(e) solche(r) benannt ist.

1.3 Beschreibung des Prüfgegenstands und der Zwecke der Verarbeitung

Der Prüfgegenstand (engl. target of evaluation) bestimmt den Umfang der DSFA. Um einzuschätzen, ob voraussichtlich ein hohes Risiko besteht, muss der Verantwortliche einen Überblick über die geplante Datenverarbeitung haben. Aus diesem Grund fordert Art. 35 Abs. 7 Buchstabe a DS-GVO eine systematische Beschreibung der Verarbeitungsvorgänge, ihrer Zwecke sowie der berechtigten Interessen des Verantwortlichen. Dies beinhaltet insbesondere die Daten, ihre Formate beim Speichern oder Transferieren (Kommunikationsprotokolle), die verwendeten IT-Systeme und deren Schnittstellen sowie Prozesse und Funktionsrollen.

Eine DSFA nach Art. 35 DS-GVO 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. Die datenschutzrechtlichen Regeln zur Zweckbindung nach Art. 5 Abs. 1 Buchstabe b DS-GVO und der Datenminimierung gem. Art. 5 Abs. 1 Buchstabe c DS-GVO erfordern dabei eine abschließende Definition der verfolgten Zwecke und eine Güterabwägung zur Gewährleistung des Grundrechtsschutzes, die im nachfolgenden Verfahren bereits berücksichtigt ist. Bei dieser Verhältnismäßigkeitsprüfung ist zu beachten, dass sich auf das Europarecht als autonomer Rechtsordnung nicht einfach Instrumente des nationalen Rechts übertragen lassen. Folglich gibt es eine eigenständige europarechtliche Verhältnismäßigkeitsprüfung, die den Schwerpunkt auf die Prüfung der Erforderlichkeit und nicht, wie im deutschen Recht, auf die Angemessenheit legt.[9] Die Verarbeitung selbst unter-

6 Vgl. Erwägungsgründe 1 u. 2 DS-GVO.

7 EuGH v. 09.22.2010 – C-92/09 und C-93/09 (Schecke und Eifert); EuGH v. 08.04.2014 – C-293/12 und C-594/12 (Digital Rights Ireland und Seitlinger).

8 Obwohl alle Sprachfassungen von EU-Rechtsakten in gleichem Maße verbindlich sind, enthalten die englische und französische Version mit dem Begriff „assessment" / „évaluation" einen umfassenderen Begriff, als die deutsche Übersetzung. Die Ersteren beinhalten auch eine Beurteilung.

9 Trstenjak/Beysen, EuR 2012, S. 265.

liegt dem Zweckbindungsgrundsatzes des Art. 5 Abs. 1 Buchstabe b DS-GVO. Daher muss begründet werden, warum die Datenverarbeitung gerade für die verfolgten Zwecke notwendig ist.

1.4 Identifikation der Akteure und betroffenen Personen

Ebenso bedeutend wie die korrekte Beschreibung des Prüfgegenstands ist in dieser Phase die Identifikation der Akteure und betroffenen Personen. Die Rolle jeder dieser Gruppen bei der Datenverarbeitung, ihre rechtlichen Beziehungen und Interessen sind zu bestimmen. Relevant sind insbesondere

- der Hersteller[10] des Prüfgegenstands;
- der Betreiber des Prüfgegenstands, etwa als Dienstleister im Rahmen einer Auftragsverarbeitung (Rechenzentrum, Internet-Provider);
- Mitarbeiter der für den Einsatz des Prüfgegenstands verantwortlichen Organisation;
- Dritte, die im Zuge des Einsatzes des Prüfgegenstands Kenntnis von personenbezogenen Daten nehmen, entweder zufällig (etwa zufällig anwesende, mithörende Dritte) oder absichtlich (Sicherheitsbehörden);
- die betroffenen Personen gem. Art. 35 Abs. 9 DS-GVO in ihren (vom Anwendungskontext abhängigen) Rollen als Bürger, Patient, Kunde, Arbeitnehmer etc.

1.5 Identifikation der maßgeblichen Rechtsgrundlagen

Wie in Art. 5 Abs. 2 DS-GVO festgelegt, muss der Verantwortliche im Rahmen seiner Rechenschaftspflicht nachweisen können, dass die Verarbeitung der Daten rechtmäßig ist. Dies ist eine Voraussetzung für sämtliche Datenverarbeitungen und muss daher noch vor Beginn des DSFA-Verfahrens geprüft werden. Als Grundrechtseingriff ist die Datenverarbeitung nur zulässig, wenn einer der in Art. 6 Abs. 1 DS-GVO abschließend aufgezählten Gründe einschlägig ist. Zunächst muss die Verarbeitung der personenbezogenen Daten dazu geeignet sein, den damit verfolgten Zweck zu erreichen. Das ist der Fall, wenn sie der Erreichung des Zwecks jedenfalls dienlich ist. Dies ermöglicht eine Überprüfung, ob der Zweck systematisch und in einer kohärenten Weise verfolgt wird.[11]

Weiterhin muss die Verarbeitung erforderlich sein; es darf also keine weniger eingriffsintensive Maßnahme geben, die gleich geeignet zur Erreichung des verfolgten Zwecks sind. Die Erforderlichkeit umfasst das Schutzziel der Datensparsamkeit;[12] es dürfen also nicht mehr personenbezogene Daten verarbeitet werden, als für die Erreichung des Verarbeitungszwecks erforderlich ist.

Obwohl die wesentlichen Vorschriften zum Datenschutzrecht in der DS-GVO enthalten sind, lassen zahlreiche Regelungen den Mitgliedstaaten einen Spielraum bei der Umsetzung, etwa im öffentlichen Bereich gem. Art. 2 Abs. 2 DS-GVO oder im Gesundheitsbereich sowie den Sozialversicherungssystemen gem. Art. 9 Abs. 2 Buchstabe h DS-GVO. Daneben können auch sektorspezifische europäische oder nationale Regelungen zu beachten sein, zum Beispiel im Telekommunikationsbereich, bezüglich Berufsgeheimnissen oder dem Schutz von Minderjährigen. Soweit diese Vorschriften sich auf die Datenverarbeitungsvorgänge beziehen – auch in Bezug auf die Frage der Rechtmäßigkeit der Verarbeitung – sind sie im Verfahren der DSFA zu berücksichtigen.

2. Bewertungsphase

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

2.1 Identifikation von Bewertungsmaßstäben anhand der Schutzziele

Die datenschutzrechtlichen Anforderungen sind in Form des Standard-Datenschutzmodells[13] operationalisiert und haben sich in der IT- und Informationssicherheit bewährt.[14] Mithilfe dieser Methode können Risiken durch angemessene Maßnahmen und Verfahrensgestaltung behandelt werden.

Im Rahmen des Standard-Datenschutzmodells haben sich sieben Schutzziele etabliert: Vorgeschaltetes Schutzziel ist die Datensparsamkeit. Dazu gehören die klassischen drei Schutzziele der Informationssicherheit, nämlich Verfügbarkeit, Integrität und Vertraulichkeit, die allerdings in dem DSFA-Kontext aus der Perspektive der betroffenen Personen zu interpretieren sind.[15] Diese werden ergänzt durch drei zusätzliche datenschutzspezifische Schutzziele: Nichtverkettbarkeit, Transparenz und Intervenierbarkeit.

10 Der Hersteller könnte den Verantwortlichen auch mit einem „Beipackzettel", der bereits die wesentlichen Elemente einer DSFA benennt, unterstützen, s. unten II.

11 Trstenjak/Beysen, EuR 2012, S. 271.

12 Insofern ist die deutsche Fassung der DS-GVO missglückt: Während der deutsche Wortlaut („Notwendigkeit und Verhältnismäßigkeit") scheinbar ein weiteres Kriterium einführt, beziehen sich die englische und französische Fassung auf die „necessity"/„nécessité" und damit eigentlich die Erforderlichkeit, die ein Teil der Verhältnismäßigkeitsprüfung ist, vgl. Trstenjak/Beysen, EuR 2012, S. 269. Der Wortlaut von Art. 35 Abs. 1 DS-GVO ist dabei ebenfalls an Art. 52 Abs. 1 GRC angelehnt: „Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind […]".

13 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – der Weg vom Recht zur Technik. Ein Datenschutzwerkzeug für Aufsichtsbehörden und verantwortliche Stellen, Hannover 2015, https://www.datenschutzzentrum.de/uploads/sdm/SDM_Tagungsband2015_Hannover.pdf.

14 Hansen/Jensen/Rost, Protection Goals for Privacy Engineering, in: 2015 International Workshop on Privacy Engineering (IWPE), Security and Privacy Workshops (SPW), 2015, S. 159; Rost/Pfitzmann, DuD 2009, S. 353; Rost/Bock, DuD 2012, 743; Hansen, Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals, in: Camenisch u.a. (Hrsg.) Privacy and Identity for Life. IFIP AICT, Bd. 375, Springer, 2012, S. 14; Danezis u.a., Privacy and Data Protection by Design – from policy to engineering, ENISA 2014, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport.

15 Daneben erwähnt Art. 32 Abs. 1 Buchstabe b DSVGO neben den klassischen Sicherheitszielen der Vertraulichkeit, Integrität und Verfügbarkeit auch die Belastbarkeit der Systeme und Dienste.

Datensparsamkeit, die in der DS-GVO in Art. 5 Abs. 1 Buchstabe c DS-GVO als Prinzip der Datenminimierung ausdrücklich normiert ist, 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.[16] Danach gilt es, dass Erheben von personenbezogenen Daten von vornherein weitestgehend zu vermeiden und vorhandene personenbezogene Daten schnellstmöglich zu löschen. 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. Nichtverkettbarkeit 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.

Für den Bewertungsmaßstab, den die Schutzziele setzen, ist es im Rahmen der DSFA essenziell, die Perspektive der betroffenen Personen, deren Rechte geschützt werden müssen, einzunehmen. Wenn etwa die Transparenzanforderung verletzt wird, weil der Verantwortliche die betroffene Person nicht den gesetzlichen Anforderungen entsprechend informiert hat, muss eine DSFA auf diesen Mangel reagieren. Dies bedeutet: Nicht nur Sicherheitslücken stellen ein Risiko für die betroffene Person und ihre Daten dar, sondern auch andere datenschutzrechtliche Mängel. In dem Fall der fehlenden Information ist beispielsweise der betroffenen Person die Möglichkeit zur Intervention genommen, wenn sie nicht weiß, zu welchen Zwecken welche ihrer Daten verarbeitet werden.

2.2 Identifikation möglicher Angreifer, Angriffsmotive und Angriffsziele

Da die DSFA, wie Art. 35 Abs. 1 DS-GVO ausdrücklich regelt, die Perspektive der von der Datenverarbeitung betroffenen Person einnimmt, können Angriffe nicht nur seitens Dritter, sondern selbst durch regelkonform handelnde interne Anwender der Organisation erfolgen. Anders als in der Informationssicherheit, die die Perspektive der betroffenen Organisation einnimmt, ist das Ziel einer DSFA daher nicht der Schutz der Geschäftspraktiken, sondern der Schutz der Rechte der betroffenen Personen, also der zum Beispiel der Kunden oder auch der Beschäftigten in der Organisation. Folgerichtig muss in diesem Schritt des DSFA-Verfahrens jeder Eingriff in die Rechte der betroffenen Personen durch die Organisation ebenso betrachtet werden wie die Angriffe durch Unbefugte. Insoweit gehören also staatliche Stellen, wie Sicherheitsbehörden oder auch die Leistungsverwaltung, und Unternehmen, etwa IT-Dienstanbieter, Banken oder Interessenvereinigungen sowie Gesundheitsdienstleister oder Forschungsstellen, zu der Menge der potenziellen Angreifer, deren Motive und Angriffsziele zu analysieren sind. Beispielsweise bestünde in diesem Sinne ein Angriff darin, dass eine Abteilung der Organisation eine Nutzung der personenbezogenen Daten zu nicht kompatiblen Zwecken beabsichtigen würde.

Da die Organisation, die die DSFA durchführt, selbst als Risiko zu sehen ist, besteht natürlich ein Interessenskonflikt. Um tote Winkel in der Betrachtung auszuschließen, sollte es daher zumindest eine nachträgliche externe Aufsicht geben. Außerdem ist von der/dem Datenschutzbeauftragten, soweit ein(e) solche(r) ernannt ist, zu erwarten, dass sie/er den Standpunkt der von der Verarbeitung betroffenen Personen einnimmt.

2.3 Bestimmung der Eingriffsintensität und des Schutzbedarfs

Für die Abwägung der Rechte und Interessen der betroffenen Person und des Verantwortlichen ist die Intensität des Eingriffs festzustellen. Der Schutzbedarf ist dabei eng mit der Eingriffsintensität verknüpft: Die Eingriffsintensität blickt von außen auf die betroffene Person und bewertet die Folgen des Eingriffs für diese. Der Schutzbedarf wird aus Sicht der betroffenen Person, unabhängig davon, ob ein Eingriff tatsächlich erfolgt, festgestellt. Hat eine Person etwa eigene, sensible Daten auf einem System, so ergibt sich für sie ein hoher Schutzbedarf, unabhängig davon, was mit diesen Daten geschieht. Wie bereits einleitend ausgeführt, stellt jede, auch rechtmäßige, Verarbeitung personenbezogener Daten einen Eingriff in das Grundrecht auf Datenschutz gem. Art. 8 GRC der betroffenen Personen dar. Daher kann man im Falle einer DSFA den Eintritt eines Schadens – im Unterschied zum für den Bereich der Informationssicherheit entwickelten IT-Grundschutz des BSI[17] – nicht einfach nach Eintrittswahrscheinlichkeit und Schwere des

16 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.0.9, Darmstadt 2015, S. 9.

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

Schadens beurteilen. Stattdessen muss ein Eingriff in das Recht auf Datenschutz gem. Art. 8 Abs. 2 und Art. 51 Abs. 1 GRC gerechtfertigt werden. Daraus ist abzuleiten, dass der Schutzbedarf standardmäßig als normal eingestuft werden muss. Aufgrund der hervorgehobenen Stellung des Grundrechtsschutzes im Datenschutzrecht kommt ein niedriger Schutzbedarf nicht in Betracht. Der Datenschutz befasst sich mit der Machtasymmetrie zwischen der betroffenen Person, deren Daten verarbeitet werden, und dem Verantwortlichen, der diese Verarbeitung vornimmt, und kann daher keine geringeren Anforderungen stellen. Allerdings kann bei Verarbeitung besonderer Kategorien von Daten oder bei fehlender Transparenz oder Intervenierbarkeit für die betroffene Person der Schutzbedarf auf hoch oder sehr hoch steigen. Die drei Schutzbedarfsabstufungen werden daher wie folgt beschrieben:

- „Normal“: Personenbezogene Daten werden verarbeitet, und es gibt keine Anwendungsszenarien, bei denen die Verarbeitung eine hohe Eingriffsintensität erwarten lässt.
- „Hoch“:
  - Besondere Kategorien von Daten i.S.v. Art. 9 DS-GVO werden verarbeitet, so dass gesetzlich ein höheres Schutzniveau gefordert ist, oder
  - die betroffenen Personen sind auf die Entscheidungen/Dienste der Organisation angewiesen, soweit
    - die hohe Eingriffsintensität der Datenverarbeitung ernsthafte Folgen für die betroffenen Personen haben kann und/oder
    - es keine effektiven Sicherungsmaßnahmen oder Interventionsmöglichkeiten für die betroffenen Personen gibt (einschließlich der Möglichkeit Rechtsschutz zu erlangen).
- „Sehr hoch“: Personenbezogene Daten, die einen hohen Schutzbedarf aufweisen, werden verarbeitet und die betroffene Person ist in existenziellem Maße von der Entscheidung/dem Dienst der Organisation abhängig, und es bestehen weitere Risiken aufgrund mangelnder Datensicherheit oder unrechtmäßiger Zweckänderungen, die die betroffene Person nicht bemerken und/oder verhindern kann.

Zudem kann ein hoher Schutzbedarf aufgrund kumulativer Effekte verschiedener Aspekte bestehen, die allein keinen hohen Schutz erfordern. Dies kann etwa der Fall sein, wenn personenbezogene Daten über eine große Personengruppe gesammelt werden oder wenn personenbezogene Daten für verschiedene Zwecke erfasst und analysiert werden und die betroffenen Personen in verschiedenen Rollen betroffen sind.

2.4 Bewertung des Risikos

Kern der DSFA ist die Risikobewertung. Diese erfordert nach Art. 35 Abs. 7 Buchstabe c DS-GVO die Bewertung der Risiken für die Rechte der betroffenen Personen. In der Bewertung sind nach Erwägungsgrund 90 DS-GVO für jedes identifizierte Risiko auch die spezifische Eintrittswahrscheinlichkeit und die Schwere zu berücksichtigen. Dafür werden die in Phase 1 benannten Angriffsszenarien und der ermittelte Schutzbedarf aus Phase 2 miteinander in Beziehung gesetzt.

In der Informationssicherheit kennt man 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. Die Verwendung dieser Formel ist allerdings weder für Datenschutz- noch Informationssicherheitsrisiken praktikabel. So können in der Informationssicherheit üblicherweise keine exakten Werte angegeben werden: Beispielsweise würde die Eintrittswahrscheinlichkeit für ein Risiko eine ausreichende statistische Datenbasis für das betrachtete System erfordern. Für Datenschutzrisiken und die Perspektive der betroffenen Person gilt dies umso mehr. 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 einer Einheit wie Euro ausdrückbar. Auf Pseudo-Berechnungen sollte in der DSFA verzichtet werden. Stattdessen muss der Verantwortliche eine nachvollziehbare Argumentation für seine Bewertung in Abhängigkeit der Angriffsszenarien und Schutzzielanforderungen liefern.

Als Risiko für die Rechte natürlicher Personen wird in der DS-GVO insbesondere angeführt, dass aus der Verarbeitung personenbezogener Daten physische, materielle oder immaterielle Schäden resultieren könnten. Dabei ist zu berücksichtigen, dass bereits der Eingriff in das Recht auf Schutz der Daten der betroffenen Person aus Art. 8 GRC, wenn dieser nicht gerechtfertigt ist, einen immateriellen Schaden darstellt. Erwägungsgrund 75 nennt als Beispiele Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Auch das Risiko, dass die betroffenen Personen um ihre Rechte gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wird benannt. Zudem wird ein hohes Risiko dann angenommen, wenn personenbezogene Daten besonderer Kategorien (Art. 9) verarbeitet werden, wenn persönliche Aspekte (Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel) bewertet oder prognostiziert werden, oder wenn personenbezogene Daten schutzbedürftiger natürlicher Personen (z.B. von Kindern) verarbeitet werden. Mit Blick auf die Datensicherheit ergänzt Erwägungsgrund 83 „Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte“.

Nach Erwägungsgrund 76 sollen die Eintrittswahrscheinlichkeit und Schwere des Risikos in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das gesamte Verfahren (also Daten, Systeme und Prozesse) muss dabei im Blickfeld stehen und vom Verantwortlichen in Bezug auf die möglichen Risiken beurteilt werden. Soweit der in Phase 1 definierte Prüfgegenstand bereits implementierte oder geplante technisch-organisatorische Maßnahmen umfasst, wie sie auch in Art. 32 DS-GVO gefordert sind, unterfallen diese ebenfalls der Bewertung. Dies ist auch sinnvoll, da bestimmte Maßnahmen bereits in den verbreiteten Datenverarbeitungssystemen enthalten sind, beispielsweise Rollen- und Rechtekonzepte in Datenbanken und Betriebssystemen.

Bei der Bewertung des Risikos ist aber wesentlich, dass die vorhandenen Maßnahmen richtig umgesetzt werden, da singuläre Maßnahmen nicht ausreichen. So kann etwa die Vertraulichkeit eines Systems durch Rollen- und Rechtekonzepte gestärkt werden. Allerdings kann dies allein die Anforderungen der Vertraulichkeit nicht erfüllen. Denn wenn die eingeräumten Rechte zu weitgehend sind oder es keine klare Rollentrennung gibt, ist das Konzept nicht effektiv. Der Verantwortliche muss daher in der Risikobewertung darlegen, inwiefern das Rechte- und Rollenkonzept des konkreten Systems die Vertraulichkeit der Daten garantiert.

3 Maßnahmenphase

In der Maßnahmenphase werden die Ergebnisse der Risikobewertung umgesetzt und passende Schutzmaßnahmen identifiziert. Nach Art. 35 Abs. 7 Buchstabe d DS-GVO muss die DSFA Maßnahmen enthalten, die die identifizierten Risiken bewältigen, und es muss der Nachweis erbracht werden, dass die DS-GVO in ihrer Gesamtheit erfüllt wird, wobei die Rechte und berechtigten Interessen der betroffenen Personen sowie auch sonstiger Betroffener zu berücksichtigen sind. Hier ist die Angemessenheit der Datenverarbeitung zu beurteilen, wobei das Interesse des Verantwortlichen an der Datenverarbeitung zu den genannten Zwecken mit den Rechten und Interessen der betroffenen Person abgewogen werden muss.

3.1 Identifikation und Auswahl passender Schutzmaßnahmen

Die Auswahl der Maßnahmen lässt sich durch einen Katalog von Referenzschutzmaßnahmen unterstützen, wie er zurzeit vom AK Technik der Konferenz der unabhängigen Datenschutzbehörden entwickelt wird.[18] 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. Dafür ist eine Soll-Ist-Betrachtung hilfreich, durch die deutlich wird, inwieweit die geplanten Maßnahmen den Vorgaben des Standard-Datenschutzmodells entsprechen (siehe Abb. 2). Im Rahmen der Auswahl der Maßnahmen sind die Rechte und Interessen der betroffenen Personen sowie sonstiger Betroffener zu berücksichtigen.

18 AK Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder/Schulz/Rost, Das Standard-Datenschutzmodell – Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.0.9, Darmstadt 2015, Kapitel 7.

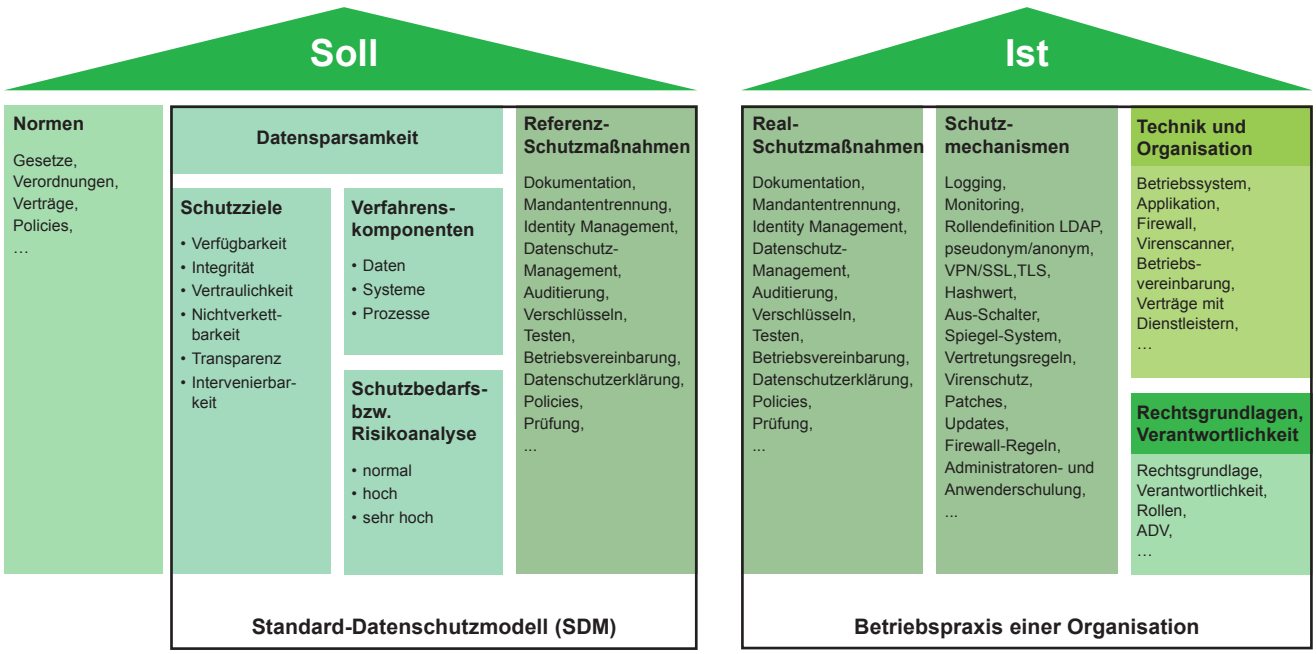

Abb. 2: Soll-Ist-Abgleich gemäß Standard-Datenschutzmodell

Auch in der Praxis erleichtert der Soll-Ist-Vergleich die Überprüfung der Risikobewertung. Hat ein Verantwortlicher zum Beispiel gar kein Rechte- und Rollenkonzept eingeplant, ist die Abweichung offensichtlich und muss begründet werden. Aber auch wenn es ein solches gibt, muss dies mitsamt seiner Funktion schlüssig dargelegt werden. Die ausgewählten Maßnahmen müssen dem Stand der Technik entsprechend gem. Art. 25 Abs. 1 u. Art. 32 DS-GVO regelmäßig aktualisiert werden.

Da die DSFA den Schutz von Individualrechte bezweckt, ist es nicht hinnehmbar, ein identifiziertes Risiko mit einer geringen Anzahl von betroffenen Personen als akzeptabel einzustufen und nur Maßnahmen zur Schadensminderung zu ergreifen. Es besteht jedoch die Möglichkeit, Risiken zu priorisieren und die Maßnahmen zu ergreifen, die den höchsten Nutzen für die betroffenen Personen haben und mit den rechtlichen Anforderungen übereinstimmen. Bei der Auswahl der Maßnahmen sollte der Verantwortliche insbesondere darlegen, welche Maßnahmen zur Verringerung oder Vermeidung von Eingriffen in die Rechte der betroffenen Personen oder um Schäden von ihnen abzuwenden, getroffen werden. Zudem sollte festgelegt sein, wer für die Umsetzung der Maßnahmen verantwortlich ist und welche Personen dabei einzubeziehen sind. Außerdem sollte der Verantwortliche bestimmen, bis wann die Maßnahmen umgesetzt sein sollen und welche Mittel dafür zur Verfügung stehen. Auch die Zuständigkeit für die Durchführung der Tests und Dokumentation der Wirksamkeit der Schutzmaßnahmen sind zu regeln.

3.2 Dokumentation der Bewertungsergebnisse

Nach der Bewertungsphase und Identifikation passender Schutzmaßnahmen müssen die Bewertungsergebnisse und die getroffene Auswahl dokumentiert werden. Diese Dokumentation umfasst nicht nur die erfolgreich eindämmbaren Risiken. Können etwa bestimmte Risiken nicht (vollständig) durch die Maßnahmen beseitigt werden, müssen diese verbleibende Restrisiken gerechtfertigt werden: Es muss dargestellt werden, aus welchen Gründen sie nicht oder nur zum Teil ausgeschlossen werden können. Sofern es sich bei den verbleibenden Restrisiken um hohe Risiken handelt, darf das untersuchte System nicht freigegeben werden und damit nicht zum Einsatz kommen. In dem Fall wären die Anforderungen der DS-GVO nicht erfüllt. Art. 36 der DS-GVO sieht jedenfalls in einem solchen Fall vor, dass der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde kontaktiert („vorherige Konsultation"), die die DSFA überprüfen und Empfehlungen abgeben muss.

3.3 Implementierung der Schutzmaßnahmen

Sofern die DSAF nicht nur ein Konzept für einen möglichen Einsatz, sondern ein konkretes Verarbeitungssystem betrifft, müssen die vorher ausgewählten Maßnahmen umgesetzt werden. Dies kann parallel zu der Dokumentation der Bewertungsergebnisse erfolgen. Die Umsetzung betrifft in der Regel technisch-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 Personen. 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 Funktionalität abgeschaltet wird.

3.4 Test und Dokumentation der Wirksamkeit der Schutzmaßnahmen

Die Implementierung der Schutzmaßnahmen allein reicht nicht aus. Zusätzlich muss die Wirksamkeit der Maßnahmen getestet und dokumentiert werden. Auch die Durchführung der Tests und die Testergebnisse sind zu dokumentieren.

3.5 Nachweis über die Einhaltung der DS-GVO insgesamt

Für den Nachweis, dass der betrachtete Prüfgegenstand – erweitert um die getroffenen Schutzmaßnahmen – die DS-GVO in ihrer Gesamtheit erfüllt, ist neben der Umsetzung der gewählten Schutzmaßnahmen eine Dokumentation der Verarbeitungsvorgänge, Risiken und Maßnahmen nötig. Die Gesamtheit der Dokumente dient nicht nur als Grundlage für den DSFA-Bericht, sondern auch der Freigabe der Datenverarbeitung durch den Verantwortlichen.[19] Datenverarbeitungssysteme für personenbezogene Daten sollten nicht eingesetzt werden, bevor die Freigabe auf Basis einer nachvollziehbaren Dokumentation erfolgt ist.

Änderungen der Maßnahmen können zu Änderungen des Prüfgegenstands oder der Akteure und betroffenen Personen führen. Es ist daher zu beachten, dass bei der Durchführung der DSFA nicht lediglich linear von Phase 1 bis 4 vorgegangen werden kann, sondern dass eine Rückkoppelung der jeweiligen Ergebnisse, im Sinne eines iterativen Vorgehens, sinnvoll ist. Beispielsweise kann es durch die Wahl entsprechender Maßnahmen zu einer weiteren Verarbeitung personenbezogener Daten kommen, für die wiederum die etwaigen Risiken zu betrachten sind. Eine ergebnisoffene Vorgehensweise wird daher üblicherweise verschiedene Maßnahmen-Sets beleuchten, bis das die DSFA durchführende Team davon überzeugt ist, dass die DS-GVO in ihrer Gesamtheit eingehalten wird und mit dem Ergebnis zufrieden ist.

19 So hat es etwa der Gesetzgeber in der Datenschutzverordnung Schleswig-Holstein geregelt, die auf dem Landesdatenschutzgesetz Schleswig-Holstein beruht.

4 Berichtsphase

4.1 Erstellung eines DSFA-Berichts

Für den Bericht zur DSFA bietet es sich die Orientierung an den einzelnen Phasen an, so dass der Prüfgegenstand, die Kriterien, die Bewertung und die Maßnahmenwahl in getrennten Abschnitten nachvollziehbar dargestellt werden. Die umfassende Dokumentation der Bewertungsergebnisse in einem DSFA-Bericht gewährleistet, dass die Ziele der DSFA erreicht werden. Dieser Bericht muss den Datenschutzaufsichtsbehörden gem. Art. 58 Abs. 1 Buchstabe a DS-GVO auf deren Verlangen vorgelegt werden.

4.2 Veröffentlichung des DSFA-Berichts

Der DSFA-Bericht sollte im Sinne der Transparenz veröffentlicht werden, zumindest in einer Kurzversion, die Geschäftsgeheimnisse sowie die Restrisikoanalyse, die sonst als Angriffsvorlage missbraucht werden könnte, schützt. Es sollten aber alle wesentlichen Informationen enthalten sein und keine (negativen) Ergebnisse der Untersuchung verschwiegen werden.

4.3 Unabhängige Überprüfung der DSFA-Ergebnisse

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. Dies umfasst insbesondere den Umgang mit Interessenskonflikten, die ausreichende Berücksichtigung der Rechte und Interessen der betroffenen Personen bei der Identifikation der Risiken, die Angemessenheit der ausgewählten Maßnahmen, genügende Information der Öffentlichkeit und die Sicherstellung, dass die gewählten Maßnahmen auch tatsächlich umgesetzt werden.

5. Überwachung und Fortschreibung

Eine DSFA ist kein strikt linearer oder abgeschlossener Prozess, sondern muss während des gesamten Lebenszyklus eines Projekts fortlaufend überwacht werden. Dementsprechend legt Art. 35 Abs. 11 DS-GVO fest, dass die DSFA jedenfalls dann zu wiederholen ist, wenn sich das mit der Verarbeitung verbundene Risiko ändert. Solche Änderungen können sich durch Veränderung der organisatorischen oder rechtlichen Rahmenbedingungen oder neue Risiken für den Datenschutz im Allgemeinen ergeben. Es gilt stets sicherzustellen, dass die Maßnahmen an solche 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.

II. Übergang in die neue Welt der DS-GVO

Die Datenschutz-Folgenabschätzung ist zwar in ihrer Beschreibung in der DS-GVO ein neues Instrument. Allerdings ist es auch gemäß der heutigen Rechtslage erforderlich, dass die Datenverarbeitung den Prinzipien der Zweckbindung und Erforderlichkeit genügt, dass die Verarbeitungsvorgänge dokumentiert vorliegen (z.B. im Verfahrensverzeichnis, das die/der Datenschutzbeauftragte führt) und dass die erforderlichen technisch-organisatorischen Maßnahmen getroffen und dokumentiert werden. Ziel ist die Beherrschbarkeit des Risikos, das mit der Datenverarbeitung einhergeht. Risikoanalysen sind zudem aus der Informationssicherheit bekannt.

Neu ist die Betonung der Rechte und Freiheiten der betroffenen Personen, die in herkömmlichen Risikoanalysen aus Organisationssicht zumeist unterreflektiert sind. Wer sich als verantwortliche Stelle heute datenschutzkonform aufgestellt hat, sollte auf Basis der vorhandenen Dokumente (Verfahrensverzeichnis, Sicherheitskonzept, Restrisikoanalyse, Test- und Freigabedokumente, sonstige Dokumentation) relativ schnell eine Datenschutz-Folgenabschätzung durchführen können – auch wenn der Fokus der DSFA deutlicher auf den Grundrechten statt auf Informationssicherheit liegen muss. Da die DS-GVO keine Meldepflicht der Datenverarbeitung (außer bezüglich der Informationspflicht im Fall von Datenpannen) an die Aufsichtsbehörde vorsieht,[20] besteht die Motivation für die Durchführung der DSFA darin, Risiken für die betroffenen Personen und indirekt auch für die Organisation (Sanktionierung durch Aufsichtsbehörden, Reputationsverlust) zu vermeiden und sich abzusichern.

Eine weitere interessante Nutzungsmöglichkeit der DSFA wird in Art. 35 Abs. 10 der DS-GVO angesprochen: Auch Rechtsgrundlagen, die Verarbeitungsvorgänge konkret regeln, können im Gesetzgebungsverfahren einer Folgenabschätzung unterzogen werden, in der die Anforderungen aus der DS-GVO berücksichtigt werden. In diesen Fällen können die Mitgliedstaaten regeln, dass eine nachfolgende DSFA durch den Verantwortlichen entbehrlich ist. Besser als ein Verzicht auf die DSFA ist es jedoch, wenn der Verantwortliche eine eigene DSFA für seinen Anwendungskontext mit seinen spezifischen Maßnahmen durchführt, die auf der abstrakten Gesetzes-DSFA beruht und sie konkretisiert. Eine solche DSFA wäre zügig durchführbar und hätte den Vorteil, dass die Einsatzbedingungen vor Ort geprüft werden und sich der Verantwortliche damit ein Bewusstsein über die Risiken und ihre Behandlung verschafft.

Ohnehin wäre es sehr sinnvoll, wenn die Datenverarbeitungssysteme – mindestens alle zertifizierten Produkte – als „Beipackzettel“ bereits die für die DSFA nötigen Informationen beinhalten würden. Beispielsweise könnte ein Muster für eine DSFA beigefügt sein, das die Anwender darauf hinweisen würde, welche Einsatzbedingungen zu garantieren sind, wo für die Durchführung der eigenen DSFA Angaben ergänzt werden müssen und wie die Risiken vor Ort zu bewerten sind.

20 Vgl. Erwägungsgrund 89 DS-GVO.

III. Fazit

Die DSFA hat großes Potenzial, den Schutz der Rechte von betroffenen Personen zu verbessern. Dabei ist insbesondere die Identifikation von Risiken durch neue Datenverarbeitungstechnologien für den Einzelnen hilfreich. Die Datenschutz-Folgenabschätzung dient dabei als Frühwarnsystem, dass alle Beteiligten in die Lage versetzt, potenzielle Schwachstellen in einem Verfahren systematisch zu finden und zu beseitigen. Das vorgestellte Verfahren bietet die Möglichkeit, den Schutz von Individuen, wie er von der DS-GVO beabsichtigt ist, im DSFA-Verfahren praktisch umzusetzen. Der Schutz der Grundrechte als das Leitmotiv des Datenschutzes, wie es auch in Art. 1 Abs. 2 DS-GVO normiert ist, rückt dabei endlich in den Vordergrund.

Danksagung

Wir danken den Teams im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und beim Forum Privatheit in der Digitalen Welt für die Diskussionen zum Thema. Speziell Rasmus Robrahn (ULD / Forum Privatheit) sowie Martin Rost (ULD) sei herzlich für eine kritische Durchsicht des Textes gedankt.

Felix Bieker, LL.M. Eur. (Edinburgh)
ist juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

Dipl.-Inform. Marit Hansen
ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das ULD.

Dr. Michael Friedewald
leitet am Fraunhofer-Institut für System- und Innovationsforschung in Karlsruhe das Geschäftsfeld Informations- und Kommunikationstechnik und koordiniert das BMBF Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Dr. Niels Lepperhoff

Dokumentationspflichten in der DS-GVO

Bisher galt das Prinzip, dass die Aufsichtsbehörde Verstöße eines Unternehmens gegen Datenschutzvorschriften belegen muss. Ein Unternehmen war nicht verpflichtet anlasslos eine Dokumentation zu erstellen und zu pflegen, mit der es sein gesetzeskonformes Handeln nachweisen konnte. Dies wird sich mit dem Inkrafttreten der Datenschutz-Grundverordnung grundlegend ändern. Dann müssen Unternehmen jederzeit in der Lage sein, die Rechtmäßigkeit ihrer Verarbeitung nachweisen zu können. So kann zukünftig auch eine fehlende Dokumentation mit einem Bußgeld belegt werden – sogar dann wenn die dazugehörige Verarbeitung rechtskonform erfolgt ist. Vor diesem Hintergrund sollte jedes Unternehmen ein Dokumentationssystem einführen oder das bereits vorhandene an die neue Rechtslage anpassen.

1. Einleitung

Der Dokumentation kommt in der Datenschutz-Grundverordnung (DS-GVO) eine größere Bedeutung zu als bisher. Die Bedeutung speist sich primär aus der in Art. 5 Abs. 2 DS-GVO eingeführten „Rechenschaftspflicht“:

„(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Art. 24 Abs. 1 S. 1 DS-GVO konkretisiert die Anforderungen zur Erfüllung der Rechenschaftspflicht wie folgt:

„(1) Der Verantwortliche setzt […] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. […]“

Die Nachweispflicht bezieht sich explizit auf die gesamte Verordnung und umfasst somit auch die die Grundsätze der DS-GVO (Art. 5 Abs. 1 DS-GVO):

- Rechtmäßigkeit, Verarbeitung[1] nach Treu und Glauben und Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung sowie
- Integrität und Vertraulichkeit.

Diese Grundsätze werden durch die weiteren Vorschriften der DS-GVO konkretisiert, so dass ein nicht geführter Nachweis

1 Art. 4 Nr. 2 DS-GVO fasst unter „Verarbeitung“ alle Phasen von der Erhebung über die Nutzung bis zur Löschung zusammen. Die Trennung von Erhebung und Verarbeitung aus § 3 Abs. 3 und 4 BDSG wird aufgegeben.