Fraunhofer ISI

FRAUNHOFER-INSTITUT FÜR SYSTEM- UND INNOVATIONSFORSCHUNG

Nicholas Martin, Michael Friedewald, Ina Schiering, Britta A. Mester, Dara Hallinan, Meiko Jensen

DIE DATENSCHUTZ-FOLGENABSCHÄTZUNG NACH ART. 35 DSGVO

Ein Handbuch für die Praxis

FRAUNHOFER VERLAG

Kontaktadresse
Dr. Michael Friedewald
Fraunhofer-Institut für
System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe
Telefon 0721 6809-146
Telefax 0721 6809-315
E-Mail michael.friedewald@isi.fraunhofer.de
URL www.isi.fraunhofer.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
http://dnb.de abrufbar.

ISBN (Print) 978-3-8396-1594-2

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Die dieser Veröffentlichung zu Grunde liegenden Arbeiten wurden mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 03VP03551, 03VP03552 und 03VP03553 gefördert. Die Verantwortung für den Inhalt der Veröffentlichung liegt bei den Autoren.

Typografische Gestaltung und Grafiken
scientific design gbr, Neustadt an der Weinstraße

Titelbild
Composing: Stefanie Ziegler, Foto: © bannosuke/fotolia, Piktogramm (Paar): © pixabay

Druck und Weiterverarbeitung
BoschDruck Solutions GmbH, Ergolding
Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

© by Fraunhofer Verlag, 2020
Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 800469, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

DIE DATENSCHUTZ-FOLGENABSCHÄTZUNG NACH ART. 35 DSGVO

Ein Handbuch für die Praxis

Autorinnen und Autoren:
Nicholas Martin, Michael Friedewald, Ina Schiering,
Britta A. Mester, Dara Hallinan, Meiko Jensen

Herausgeber:
Michael Friedewald und Nicholas Martin
Fraunhofer-Institut für System- und Innovationsforschung ISI
Karlsruhe

In Zusammenarbeit mit

FIZ Karlsruhe
Leibniz-Institut für Informationsinfrastruktur

Fachhochschule Kiel
Hochschule für Angewandte Wissenschaften

Ostfalia
Hochschule für angewandte Wissenschaften

datenschutz nord

FRAUNHOFER VERLAG

INHALTSÜBERSICHT

VORWORT

Dieses Handbuch stellt eine Weiterentwicklung eines vom „Forum Privatheit“ in einem White Paper vorgestellten Ansatzes zur Durchführung von Datenschutz-Folgenabschätzungen dar.[1]

Die Grundlage für die Operationalisierung und methodische Weiterentwicklung des Ansatzes waren zwölf Workshops und Interviews mit Unternehmen und Behörden, die 2018/19 im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts durchgeführt wurden.

Wichtige Orientierung boten auch die Kurzpapiere Nr. 5 und Nr. 18 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder,[2] das DSFA-„Planspiel“ der Datenschutz-Aufsichtsbehörden Schleswig-Holstein, Mecklenburg-Vorpommern und Niedersachsen[3] und das Standard-Datenschutzmodell,[4] sowie die deutsche und englische Textversion der Datenschutz-Grundverordnung (DSGVO),[5] und einschlägigen Kommentierungen.

Schließlich möchten wir dem Projektbeirat und allen beteiligten Gesprächspartnern und -partnerinnen noch einmal unseren großen Dank für ihre Bereitschaft zur Teilnahme an den obengenannten Workshops und Interviews aussprechen.

Karlsruhe, im Februar 2020

KURZFASSUNG DATENSCHUTZ-FOLGENABSCHÄTZUNG

Die vorliegende Kurzfassung bietet eine stark komprimierte Übersicht zu einer möglichen Vorgehensweise bei einer Datenschutz-Folgenabschätzung (DSFA) im Sinne des Art. 35 DSGVO.

DSFA-Ablauf

Insgesamt ist die durchzuführende Datenschutz-Folgenabschätzung (DSFA) in fünf Phasen zu unterteilen:

I **Initialisierungsphase**

II **DSFA-Vorbereitungsphase**

III **DSFA-Durchführungsphase**

IV **DSFA-Umsetzungsphase**

V **Nachhaltigkeitsphase**

Folgende Untergliederung der einzelnen Phasen hat sich als sinnvoll herausgestellt:

- Ziel
- Input
- Rollen/Verantwortlichkeit
- Umsetzung
- Output und Ergebnis

In jeder Phase sollten bestimmte Dokumente vorgehalten werden. Diese werden im Folgenden als:

- Input oder Output einer Phase bezeichnet und durch Ziffern [N] gekennzeichnet und durchlaufend nummeriert.

Alle dabei genannten Dokumente werden am Schluss der Kurzfassung zur Übersicht zusammengestellt. Die benannten Phasen, deren Gliederung und die jeweils notwendigen Dokumente sowie zu dokumentierenden Ergebnisse, werden nachfolgend noch einmal für jede Phase näher dargestellt. Dabei werden die zur Grundlage dienenden rechtlichen Rahmenbedingungen der DSGVO benannt, um gegebenenfalls Interessierten eine detailliertere Aufbereitung des jeweiligen Themas zu ermöglichen. Es handelt sich bei diesem Schema bewusst um eine sehr abstrakte Darstellung der für die Durchführung einer DSFA sinnvollen Vorgehensweise. Vorausgesetzt wird daher ein konkretes Hintergrundwissen zum Thema Datenschutz-Folgenabschätzung. Die Kapitel 4 bis 8 in diesem Handbuch geben ausführlichere Informationen zu den einzelnen Schritten. Erfahrungsgemäß setzt die Umsetzung der Datenschutz-Folgenabschätzung darüber hinaus aber zumindest ein Grundwissen zu Datenschutz- und Datensicherheitsfragen (je nach Zusammensetzung des DSFA-Teams) voraus.

Initialisierungsphase

Ziel:

Schwellwertanalyse: Klärung, ob eine DSFA erforderlich ist (Art. 35 Abs. 1 DSGVO).

Input:

1 *Dokumentation* der neuen, geplanten oder geänderten *Verarbeitungsvorgänge* (mit den für das Verzeichnis der Verarbeitungstätigkeiten aufzunehmenden Angaben, gemäß Art. 30 Abs. 1 DSGVO), *Dokumentation der Sicherstellung der Rechtmäßigkeit* (i. S. d. Art. 6 DSGVO) und dokumentierte *Vorüberlegungen zur Notwendigkeit und Verhältnismäßigkeit* der Verarbeitung (unter Beachtung der Datenschutzgrundsätze, Art. 5 DSGVO).

Rollen / Verantwortlichkeit:

*Verantwortliche** für die Verarbeitungstätigkeiten (i. S. d. Art. 4 Nr. 7 DSGVO), ggf. unterstützt durch *Auftragsverarbeiter* (vgl. Art. 28 Abs. 3 lit. f DSGVO), bei der Durchführung beratend begleitet durch die *Datenschutzbeauftragte* (Art. 35 Abs. 2 DSGVO).

Umsetzung:

Klärung, ob die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (vgl. Art. 35 Abs. 1 DSGVO). Dazu Prüfung der in Art. 35 Abs. 3 DSGVO genannten Fälle, Durchsicht der von den Aufsichtsbehörden erstellten Positivlisten („Muss-Listen") (vgl. Art. 35 Abs. 4 und Art. 68 DSGVO), den Kriterien der Artikel-29-Datenschutzgruppe, sowie ggf. eigenständige Prüfung der Höhe und Existenz von Risiken für Rechte und Freiheiten angesichts der Art, Umfang, Umstände und Zwecke der Verarbeitung.

Output:

2 Dokumentation der Schwellwertanalyse.

Ergebnis:

Wurde im Rahmen der Schwellwertanalyse festgestellt, dass durch eine Verarbeitung ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 35 Abs. 1 DSGVO besteht, so muss eine DSFA durchgeführt werden.

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

DSFA-Vorbereitungsphase

Ziel:

Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge (Art. 35 Abs. 7 lit. a DSGVO) und des konkreten Kontextes aus technischer, rechtlicher und organisatorischer Sicht sowie Planung der Durchführung (-sphase).

Input:

1 *Dokumentation* der neuen, geplanten oder geänderten *Verarbeitungsvorgänge* (mit den für das Verzeichnis der Verarbeitungstätigkeiten aufzunehmenden Angaben, gemäß Art. 30 Abs. 1 DSGVO), *Dokumentation der Sicherstellung der Rechtmäßigkeit* (i. S. d. Art. 6 DSGVO) und dokumentierte *Vorüberlegungen zur Notwendigkeit und Verhältnismäßigkeit* der Verarbeitung (unter Beachtung der Datenschutzgrundsätze, Art. 5 DSGVO).

2 Dokumentation der „positiven" Schwellwertanalyse aus Phase I.

Rollen / Verantwortlichkeiten:

Verantwortliche (i. S. d. Art. 4 Nr. 7 DSGVO) der Verarbeitung muss die DSFA vorab durchführen (Art. 35 Abs. 1 DSGVO), ggf. unterstützt durch Auftragsverarbeiter (vgl. Art. 28 Abs. 3 lit. f DSGVO). Umsetzung kann an Personen mit geeigneten Kompetenzen delegiert werden. Beratend begleitet die Datenschutzbeauftragte die Durchführung (Art. 35 Abs. 2 DSGVO).

Umsetzung:

a) Übersichtsartige Sammlung von Informationen (Art. 35 Abs. 7 lit. a DSGVO):
- Betroffene Personen, verarbeitete personenbezogene Daten, Datenflüsse, weitere Beteiligte, (geplante) Prozesse;
- Dokumentation der (geplanten) technischen Umsetzung, technische Infrastruktur, bereits bestehende technische und organisatorische Maßnahmen;
- Ggf. Betroffenenvertreter (z. B. Betriebsrat, Personalrat, Patientinnenrat), Organisation, Auftragsverarbeiter, Joint Controller (gemeinsam für die Verarbeitung Verantwortliche), Verträge etc.

b) Vorschlag eines DSFA-Teams für die Durchführungsphase und Planung von Workshops/Terminsetzung.

Output:

3 Übersichtsartige Sammlung von Informationen über die zu prüfende Verarbeitung.

4 Vorschlag DSFA-Team für die Durchführungsphase und Planung Workshops/Termine.

Ergebnis:

Abschluss der Vorbereitungsphase zur Durchführung der DSFA (Phase III).

DSFA-Durchführungsphase

Ziele:

Bewertung der Risiken der vorgesehenen Verarbeitung für die Rechte und Freiheiten betroffener (natürlicher) Personen (Art. 35 Abs. 7 lit. c DSGVO).

Auswahl von Abhilfemaßnahmen (Schutzmaßnahmen) zur Bewältigung der Risiken und Sicherstellung des Schutzes personenbezogener Daten (Art. 35 Abs. 7 lit. d DSGVO).

Bewertung der Notwendigkeit und Verhältnismäßigkeit der vorgesehenen Verarbeitungsvorgänge in Bezug auf den Zweck (Abs. 35 Abs. 7 lit. b DSGVO).

Input:

1 *Dokumentation* der neuen, geplanten oder geänderten *Verarbeitungsvorgänge* (mit den für das Verzeichnis der Verarbeitungstätigkeiten aufzunehmenden Angaben, gemäß Art. 30 Abs. 1 DSGVO), *Dokumentation der Sicherstellung der Rechtmäßigkeit* (i. S. d. Art. 6 DSGVO) und dokumentierte *Vorüberlegungen zur Notwendigkeit und Verhältnismäßigkeit* der Verarbeitung (unter Beachtung der Datenschutzgrundsätze, Art. 5 DSGVO).

2 Dokumentation der „positiven" Schwellwertanalyse aus Phase I.

3 Übersichtsartige Sammlung von Informationen zur Verarbeitung aus Phase II.

4 Vorschlag DSFA-Team für die Durchführungsphase und Planung Workshops/ Termine aus Phase II.

Rollen / Verantwortlichkeiten:

Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO ist für die Durchführung der DSFA verantwortlich. Umsetzung kann an Personen mit geeigneten Kompetenzen, hier als DSFA-Team bezeichnet, delegiert werden. Beim DSFA-Team handelt es sich i. d. R. nur teilweise um Personen mit ausgeprägten Vorkenntnissen im Datenschutz, da neben Expertise zu Datenschutz, auch andere Kompetenzen für die DSFA benötigt werden. Beratend begleitet die *Datenschutzbeauftragte* die Durchführung (Art. 35 Abs. 2 DSGVO). Unterstützend können *Auftragsverarbeiter* (vgl. Art. 28 Abs. 3 lit. f DSGVO) hinzugezogen werden.

Umsetzung:

a) Identifikation und Analyse von Schadensszenarien, um die Risiken für die Rechte und Freiheiten natürlicher Personen abzuschätzen. Zu jedem Schadensszenario sollten die folgenden Angaben ermittelt werden:
   - Beschreibung des Szenarios
   - Betroffene Personen

- Personenbezogene Daten
- Beteiligte Akteure
- Möglicher Schaden für die betroffene Person
- Auslösende Elemente für den Schadenseintritt

b) Bereits bestehende technische und organisatorische Maßnahmen (parallel sammeln);

c) Tangierte Gewährleistungsziele und ggf. Priorisierung der Gewährleistungsziele (Betrachtung, welche Gewährleistungsziele im Rahmen des untersuchten Szenarios besondere bzw. weniger Relevanz im Hinblick auf die verschiedenen betroffenen Personen haben);

d) Bewertung der Schwere des möglichen Schadens und der Eintrittswahrscheinlichkeit, als Ableitung: Bewertung des Risikos für die Rechte und Freiheiten (Art. 35 Abs. 7 lit c DSGVO);

Zwischenergebnis:
Risikobewertung, z. B. visualisiert durch Risikomatrix (mit den wesentlichen Angaben: Schwere des möglichen Schadens/Eintrittswahrscheinlichkeit, s. Ziffer d).

e) Auswahl neuer, zusätzlicher technischer und organisatorischer Abhilfemaßnahmen (Schutzmaßnahmen), Anpassung und Weiterentwicklung bestehender Maßnahmen, oder Anpassung der Verarbeitung (im Weiteren zusammengefasst als Abhilfemaßnahmen bezeichnet) um die Risiken für die Rechte und Freiheiten natürlicher Personen ausreichend einzudämmen und den Schutz personenbezogener Daten sicherzustellen (Art. 35 Abs. 7 lit. d DSGVO);

f) Bewertung der verbleibenden Restrisiken;

g) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (Art. 35 Abs. 7 lit. b DSGVO).

Output:
5 DSFA-Bericht (Art. 35 Abs. 7 DSGVO).

Ergebnis:
Beantwortung der Frage: *Können durch geeignete technische und organisatorische Maßnahmen die dokumentierten hohen Risiken ausreichend eingedämmt werden?*

Ja: *Verarbeitung kann umgesetzt werden, vorbehaltlich der erfolgreichen Umsetzung der Maßnahmen.*

Nein: *Konsultation der Aufsichtsbehörden (Art. 36 Abs. 1 DSGVO) durch die Verantwortliche oder Aufgabe der Verarbeitung.*

DSFA-Umsetzungsphase

Ziel:

Umsetzung der in Phase III. definierten und im DFSA-Bericht dokumentierten Abhilfemaßnahmen (Schutzmaßnahmen); auf dieser Grundlage Nachweis der Einhaltung der DSGVO und Freigabe der Verarbeitung.

Input:

5 DSFA-Bericht (Art. 35 Abs. 7 DSGVO) aus Phase III.

Rollen / Verantwortlichkeiten:

Verantwortlich (i. S. d. Art. 4 Nr. 7 DSGVO) für die DSFA ist weiterhin die Verantwortliche (Art. 35 DSGVO). Das *DSFA-Team* dient zur Unterstützung. Die konkrete Umsetzung geeigneter technischer und organisatorischer Maßnahmen kann an Personen mit geeigneten Kompetenzen delegiert werden. Beratend begleitet die *Datenschutzbeauftragte* die Durchführung der DSFA (Art. 35 Abs. 2 DSGVO), deren Durchführung überwacht (Art. 39 Abs. 1 lit. c DSGVO) wird.

Umsetzung:

a) Planung und Umsetzung der definierten Abhilfemaßnahmen

b) Planung und Umsetzung eines Testkonzepts, um die Wirksamkeit der Abhilfemaßnahmen zu testen und Risiken zu überwachen. Dabei sind Testergebnisse zu protokollieren.

c) Durchführung der definierten Tests und Dokumentation der Testergebnisse soweit vor Freigabe der Verarbeitung möglich.

d) Werden während dieses Prozesses weitere Risiken identifiziert, müssen diese auch behandelt werden.

Output:

5 DSFA-Bericht

6 Dokumentation der Abhilfemaßnahmen, des Testkonzepts und Protokollierung der Umsetzung der Tests zur Wirksamkeit der Abhilfemaßnahmen und zur Überwachung der Risiken.

7 Nachweis über die Einhaltung der DSGVO und Freigabe der Verarbeitung

Ergebnis:

Nachweis über die Einhaltung der DSGVO und Freigabe der geplanten Verarbeitung.

Nachhaltigkeitsphase

Nach Abschluss einer DSFA müssen geeignete Maßnahmen zur Nachhaltigkeit getroffen werden. Insbesondere gehören dazu die Überwachung der Risiken und eine regelmäßige Überprüfung und Anpassung der DSFA im Rahmen von Änderungen und generell wenn hinsichtlich der mit den Verarbeitungsvorgängen verbundenen Risiken Änderungen eingetreten sind (Art. 5 Abs. 2, Art. 35 Abs. 11, Art. 39 Abs. 1 lit. b DSGVO).

Ziel:

Fortlaufende Sicherstellung, dass die Risiken für die Rechte und Freiheiten natürlicher Personen ausreichend eingedämmt sind und die DSGVO eingehalten wird.

Input:

5 DSFA-Bericht

6 Dokumentation der Abhilfemaßnahmen, des Testkonzepts und Protokollierung der Umsetzung der Tests zur Wirksamkeit der Abhilfemaßnahmen und zur Überwachung der Risiken aus Phase IV.

Rollen / Verantwortlichkeiten:

Verantwortliche muss Überprüfung durchführen (Art. 35 Abs. 11 DSGVO), die *Datenschutzbeauftragte* muss Einhaltung der DSGVO überwachen (Art. 39 Abs. 1 lit. b DSGVO), ggf. weitere Zuständigkeiten der Überwachung nach nationalen Vorschriften (bspw. Betriebsrat gemäß Betriebsverfassungsgesetz (BVerfG).

Umsetzung:

Die Maßnahmen zur Nachhaltigkeit sollten möglichst in ein Datenschutz-Managementsystem eingebunden werden

a) Überprüfung der Wirksamkeit der Abhilfemaßnahmen und der Überwachung der Risiken auf Basis des Testkonzepts und der Protokollierung der Durchführung

b) Identifikation von Abweichungen bezogen auf die Wirksamkeit der Abhilfemaßnahmen und die Risiken

c) Dokumentation der Ergebnisse der Überprüfung

Im Falle von kleineren Abweichungen bzgl. der Wirksamkeit der Abhilfemaßnahmen oder Änderungen bzgl. der Verarbeitung:

d) Anpassungen der Risikobewertung, der Abhilfemaßnahmen und des zugehörigen Testkonzepts

e) Anpassung des DSFA-Berichts

Bei größeren Abweichungen bzgl. der Wirksamkeit der Abhilfemaßnahmen oder wesentlichen Änderungen bezüglich der Verarbeitung:

f) Erneuter Durchlauf der Phasen II. bis IV. der DSFA

Output:

5 DSFA-Bericht (ggf. angepasst).

6 Dokumentation der Abhilfemaßnahmen, des Testkonzepts und Protokollierung der Umsetzung der Tests zur Wirksamkeit der Abhilfemaßnahmen und zur Überwachung der Risiken.(ggf. angepasst)

Ergebnis:

Der durch die DSFA überprüfte Verarbeitungsvorgang erfüllt weiterhin die notwendigen Vorgaben, so dass kein hohes Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen besteht.

Übersicht Dokumente im Rahmen der DSFA

1 *Dokumentation* der neuen, geplanten oder geänderten *Verarbeitungsvorgänge* (mit den für das Verzeichnis der Verarbeitungstätigkeiten aufzunehmenden Angaben, gemäß Art. 30 Abs. 1 DSGVO), *Dokumentation der Sicherstellung der Rechtmäßigkeit* (i. S. d. Art. 6 DSGVO) und dokumentierte *Vorüberlegungen zur Notwendigkeit und Verhältnismäßigkeit* der Verarbeitung (unter Beachtung der Datenschutzgrundsätze, Art. 5 DSGVO).

2 Dokumentation der „positiven" Schwellwertanalyse

3 Übersichtsartige Sammlung von Informationen zu Art, Umfang, Umständen und Zwecken der Verarbeitung sowie sonstiger für die Prüfung relevanter Informationen.

4 Vorschlag DSFA-Team für die Durchführungsphase und Planung Workshops/Termine.

5 DSFA-Bericht

6 Dokumentation der Abhilfemaßnahmen, des Testkonzepts und Protokollierung der Umsetzung der Tests zur Wirksamkeit der Abhilfemaßnahmen und zur Überwachung der Risiken.

7 Nachweis über die Einhaltung der DSGVO und Freigabe der Verarbeitung

1 Einführung

Gemäß Artikel 35 der Datenschutz-Grundverordnung (DSGVO) müssen Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO unter bestimmten Umständen eine „Datenschutz-Folgenabschätzung" (DSFA) durchführen. Durch die DSFA sollen Risiken für die Rechte und Freiheiten betroffener (natürlicher) Personen, die sich aus einer Datenverarbeitung ergeben können, erkannt, bewertet und eingedämmt werden. Die Datenschutz-Grundverordnung definiert zwar Minimalanforderungen, die eine Datenschutz-Folgenabschätzung erfüllen muss, gibt aber keinen Prozess vor, nach dessen Kriterien die Umsetzung erfolgen muss.

Seit 2018 sind daher verschiedene Methoden, nach denen eine DSFA durchgeführt werden könnte, veröffentlicht worden. Dieses Handbuch operationalisiert eine dieser Methoden für die Praxisanwenderin in Unternehmen und Behörden. Die hier beschriebene Methode wurde vom BMBF-geförderten Forschungsprojekt Forum Privatheit entworfen, in zwölf Interviews bzw. Workshops mit Firmen und Behörden getestet und auf deren Grundlage fortlaufend für die Praxis weiterentwickelt.

1.1 Datenschutz

Der Begriff „Datenschutz" wird oft missverstanden. Entgegen seinem Wortlaut geht es nicht um den Schutz der Daten (begrifflich der Datensicherheit), sondern um den Schutz des Menschen (natürliche Person), auf den sich die Informationen beziehen (Datenschutz). Anders ausgedrückt, Datenschutz soll die Freiheit des Einzelnen schützen, selbst zu entscheiden, wie mit seinen Daten umgegangen wird und wer welche Informationen erhalten darf (Recht auf informationelle Selbstbestimmung), wobei dieses Recht nicht uneingeschränkt gilt. Vielmehr sind Umstände denkbar, in denen Personen ihre Daten weitergeben müssen, um beispielsweise Leistungen zu erhalten, mit anderen zu interagieren bzw. rechtsgeschäftlich tätig werden zu können. Doch gerade dann ist es wichtig, dass das jeweilige Individuum auch dann vor der Organisation geschützt wird (d. h. die beteiligen Unternehmen, öffentliche Stellen wie Ämter, Polizei oder Schulen, aber auch Vereine, Kirchen oder Nichtregierungsorganisationen). Denn diese Stellen (Organisationen), bei denen nicht selten ein Machtgefälle zwischen der Organisation und dem Individuum besteht, verfügen aufgrund ihrer Funktionen

zumeist über zahlreiche Informationen von Personen (bspw. ihren Beschäftigten, Leistungsempfängern, Schutzbefohlenen, Nutzern, Kunden etc.). Dabei lassen sich diese Informationen prinzipiell zu allen möglichen Zwecken einsetzen, oft mit schädlichen Konsequenzen für die betroffenen Personen. Denkbar sind hierbei neben materiellen und körperlichen Schäden, z. B. Arbeitsplatzverlust, Diskriminierung oder Gewaltverbrechen, auch immaterielle Schäden, wie beispielsweise Rufschädigung oder dem unspezifischen Gefühl, „ausgespäht" zu werden. Erwähnenswert ist in diesem Zusammenhang die Gefahr sogenannter Einschüchterungseffekte (chilling effects), also dass Menschen in eine Art Selbstzensur verfallen (aus Sorge vor der möglichen Sammlung von Informationen über sie) und ihre Äußerungen sowie Handlungen selbst beschränken.

Das Datenschutzrecht hilft unter anderem ein derartiges Machtgefälle zwischen Organisationen und Individuen zu verringern, um auf diese Weise nicht zuletzt auch die Handlungsautonomie von Menschen zu schützen. Ein Schritt dazu ist, dass die Verarbeitung personenbezogener Daten die Einhaltung bestimmter Prinzipien erfordert – zusammengefasst in den Datenschutzgrundsätzen des Art. 5 Abs. 1 DSGVO. Ein weiterer Schritt besteht darin, dass den betroffenen Personen bestimmte Rechte, bspw. auf Auskunft, Information, Berichtigung, Widerspruch, Löschung, Datenübertragbarkeit zugebilligt werden (vgl. Art. 12–22 DSGVO). Zusammen mit den übrigen Rechten und Pflichten des Datenschutzes dienen diese dazu, den Menschen, deren Daten direkt oder indirekt verarbeitet werden bzw. auf die sich die Daten direkt oder indirekt beziehen (den „betroffenen Personen") einen Grad an Kontrolle über die Verarbeitung ihrer persönlichen Informationen zu sichern, die einen Schutz vor Schäden gewährleistet und ihre Handlungsautonomie wahrt.

Das Schutzobjekt im Datenschutz ist also der Mensch, über den Rückschlüsse aus den verarbeiteten Daten gezogen werden könnten. Entsprechend fallen nur solche Daten in den Geltungsbereich des Datenschutzes, die Rückschlüsse auf natürliche Personen zulassen, also Personenbezug haben bzw. personenbeziehbar sind. Anders ausgedrückt: Informationen, mit denen sich Personen identifizieren lassen (vgl. Art. 4 Nr. 1 DSGVO). Daten, bei denen keine Rückschlüsse auf Personen möglich sind (z. B. Daten über Naturphänomene) unterliegen nicht dem Datenschutz (evtl. bestehen aber Anforderungen zur Datensicherheit). Zu beachten ist jedoch, dass aufgrund der wachsenden Möglichkeiten zur Verknüpfung und Auswertung von Daten durchaus auch Daten, denen scheinbar jeder Personenbezug fehlt, durch weitere Informationen einen Rückschluss auf Personen ermöglichen können (oftmals diskutiert unter Stichworten wie *Künstliche Intelligenz* und *Big Data*).

Eine wesentliche Risikoquelle im Datenschutz ist neben externen Angreifern vor allem die Organisation selbst. Es geht im Datenschutz auch darum, die betroffenen Personen vor Verarbeitungsvorgängen zu schützen, die die Organisation gemäß ihrer eigenen internen Regeln und Prozesse förmlich richtig und für ihre Ziele (Gewinn, Effizienz, etc.) zweckmäßig, (datenschutz-)rechtlich aber illegitim durchführt.

Datenschutz geht in diesem Sinne über die IT-Sicherheit hinaus, grenzt sich sogar von ihr ab. Risikoquellen sind – im Gegensatz zur IT-Sicherheit – nicht allein technische Ausfälle bzw. deren Fehlfunktionen oder die Handlungen unbefugter Insider und Outsider („Hacker"), sondern insbesondere auch die planmäßigen Aktivitäten der Organisation selbst. Während die IT-Sicherheit die Organisation als Schutzobjekt behandelt, sind im Datenschutz die betroffenen Personen das Schutzobjekt – und die Organisation selbst mit allen ihren Einheiten (Abteilungen, Beschäftigten, Auftragnehmern) neben Externen oftmals einer der wesentlichen und unbedingt zu berücksichtigenden „Angreifer".

1.2 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) im Sinne des Art. 35 DSGVO ist ein Instrument, um wesentliche Risiken für die Rechte und Freiheiten einer natürlichen Person, die aus einem Datenverarbeitungsvorgang hervorgehen können, zu identifizieren, zu bewerten und einzudämmen. Anders als die immer bei Verarbeitungstätigkeiten zu ergreifenden technischen und organisatorischen Sicherheitsmaßnahmen im Sinne des Art. 32 DSGVO, muss eine DSFA nach Art. 35 Abs. 1 DSGVO immer dann durchgeführt werden, wenn eine geplante Verarbeitung voraussichtlich ein „hohes Risiko" für Rechte und Freiheiten einer natürlichen Person zur Folge hat. Wie ein derartig „hohes Risiko" für die Rechte und Freiheiten einer natürlichen Person überhaupt festgestellt werden kann, um dann zu entscheiden, ob eine DSFA durchzuführen ist, wird in Kapitel 4 näher ausgeführt.

Die Datenschutz-Grundverordnung verpflichtet bei Vorliegen der Voraussetzung lediglich zur Durchführung der DSFA, ohne dabei die zu verwendende Methode näher festzulegen. Es werden jedoch vier Mindestanforderungen gestellt, die bei einer DSFA zu erfüllen sind.

Gemäß Art. 35 Abs. 7 DSGVO muss eine DSFA Folgendes enthalten:

- „a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der vom 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 [...];
- 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 [die DSGVO] eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird".

Zudem enthält Art. 35 Abs. 9 DSGVO als Teil der DSFA einen Hinweis darauf, dass Verantwortliche gegebenenfalls den Standpunkt betroffener Personen oder deren Vertreter einzuholen haben, wobei die Formulierung keinen konkreten Zwang hierzu enthält. Gleichwohl dürfte eine Konsultation bzw. zumindest eine Einbeziehung der betroffenen Personen oder deren Vertreter oftmals sinnvoll erscheinen. Auch dürfte die Einbeziehung Grundlage für die Feststellung sein, ob andere für die DSFA relevante Standpunkte bestehen könnten und auf diese Weise im Ergebnis auch den Aufsichtsbehörden bei eventuellen Prüfungen dazu dienen, zu erkennen, ob eine DSFA in der notwendigen Tiefe durchgeführt wurde.

Nach Abschluss dieser Prüfungsschritte und der Umsetzung der zur Eindämmung des Risikos erforderlichen technischen und organisatorischen Abhilfemaßnahmen, darf die geplante Verarbeitung durchgeführt werden – vorausgesetzt, die Risiken wurden ausreichend eingedämmt. Konnten die Risiken nicht ausreichend eingedämmt werden, darf die Verarbeitung nicht durchgeführt werden. In diesem Fall muss die Verantwortliche die geplante Verarbeitung entweder aufgeben oder die Aufsichtsbehörden gemäß Art. 36 DSGVO konsultieren.

Wird die Verarbeitung nach der Freigabe durchgeführt, so fordert Art. 35 Abs. 11 DSGVO, dass die Verantwortliche erforderlichenfalls überprüft, ob die Verarbeitung tatsächlich gemäß den Anforderungen der durch die DSFA festgestellten Abhilfemaßnahmen durchgeführt wird, d. h. ob alle Risiken weiterhin ausreichend eingedämmt sind. Eine solche Überprüfung ist gemäß Art. 35 Abs. 11 DSGVO zumindest immer dann durchzuführen, „wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind."

Art. 35 Abs. 11 DSGVO impliziert somit, dass die Verantwortliche die DSFA als „lebendes" Dokument betrachtet, dass während des Lebenszyklus der Verarbeitung weiterentwickelt wird, und für das durch die Verantwortliche ein adäquates Monitoringsystem möglichst im Rahmen eines Datenschutz-Managementsystems etabliert wird, um etwaige Änderungen der Risiken zu identifizieren und die Wirksamkeit der Abhilfemaßnahmen zu überprüfen. Die DSFA ist zu dokumentieren und den Aufsichtsbehörden auf Anfrage vorzulegen, muss allerdings nicht veröffentlicht werden.

1.3 Verantwortlichkeit für die DSFA

Art. 35 DSGVO weist die Verpflichtung zur Durchführung einer Datenschutz-Folgeabschätzung der Verantwortlichen zu. Dabei lässt die Datenschutz-Grundverordnung aber nicht außer Acht, dass auch andere Gruppen durchaus wichtige Funktionen bei den im Rahmen einer DSFA durchzuführenden Bewertungen haben können. So werden an verschiedener Stelle sowohl (etwaige) Auftragsverarbeiter und die Datenschutzbeauftragte als auch weitere Beteiligte mit verschiedenen Funktionen im

Rahmen der Datenschutz-Folgenabschätzung benannt. Auch die betroffenen Personen bzw. deren Vertreter sind ggf. in eine DSFA miteinzubeziehen.

Verantwortliche

Zur Durchführung einer DSFA ist nach dem Wortlaut des Art. 35 Abs. 1 DSGVO die Verantwortliche rechtlich verpflichtet. Verantwortliche im Sinne der Datenschutz-Grundverordnung ist gemäß Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, unabhängig davon, ob es sich um eine öffentliche oder nicht-öffentliche Stelle handelt. Abzustellen ist daher auf die datenverarbeitende rechtliche Einheit, wobei diese durch ihre Leitung vertreten wird, d. h. letztlich die Leitungsebene eines Unternehmens, einer Behörde, Einrichtung oder sonstigen Stelle (hiernach „Organisation") die Verantwortung zur Einhaltung datenschutzrechtlicher Vorgaben trägt.[6] Dabei muss eine Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO alleine oder gemeinsam mit anderen Entscheidungsgewalt über die Mittel und Zwecke der Verarbeitung haben, womit eine Abgrenzung zu Auftragsverarbeitern und eventuell anderen Beteiligten vorgenommen wird.

Demzufolge sind weder die Auftragsverarbeiter noch andere Beteiligte (bspw. Hersteller einzelner an dem Verarbeitungsvorgang beteiligter Komponenten, bspw. Hard- oder Software) von der Pflicht zur Durchführung einer DSFA erfasst.

Zur operativen Durchführung einer DSFA ist es der Verantwortlichen hingegen unbenommen, diese entweder an interne, fachlich vielleicht der Sache ohnehin näher stehende Personen (Beschäftigte, Abteilungsleitung) oder externe Dritte (Berater) zu delegieren.

Datenschutzbeauftragte

Eine besondere Rolle bei der DSFA kommt der Datenschutzbeauftragten zu. Eine solche ist zumindest in Deutschland bei Notwendigkeit einer DSFA ohnehin verpflichtend zu benennen. Art. 35 Abs. 2 DSGVO sowie Art. 39 Abs. 1 lit. c DSGVO sehen vor, dass die Verantwortliche bei der DSFA den Rat einer Datenschutzbeauftragten einholt, durch die deren Durchführung überdies „überwacht" wird. Zwar verbietet die Datenschutz-Grundverordnung nicht explizit, dass die Durchführung der DSFA an die Datenschutzbeauftragte delegiert wird, doch scheint eine solche Delegation kaum mit ihrem gesetzlich mandatierten Überwachungsauftrag vereinbar, da eine derartige Doppelrolle kaum gewollt sein kann.[7] Hintergrund ist, dass eine Datenschutzbeauftragte in einem derartigen Fall zum einen zu Rate gezogen werden soll, was eine Empfehlung einer anderen gegenüber voraussetzt, zum anderen aber die Aufgabe zur unabhängigen Überwachung der Durchführung einer DSFA inne hat. Es ist daher davon auszugehen, dass bei einer derartigen Doppelrolle die Aufsichtsbehörden einer etwaigen Delegierung an die Datenschutzbeauftrage ablehnend gegenüber stehen und deren Zulässigkeit angezweifelt werden muss.

Aufgrund ihres gesetzlich mandatierten Beratungsauftrags darf die Datenschutzbeauftragte dennoch eine umfangreiche Rolle bei der DSFA übernehmen. So empfiehlt die Artikel-29 Gruppe der europäischen Datenschutz-Aufsichtsbehörden, dass sie in alle wesentliche Fragen bei einer DSFA beratend eingebunden wird. Ihr Rat soll insbesondere zu folgenden Themen eingeholt werden:

- Ob eine DSFA durchzuführen ist;
- Anhand welcher Methode die DSFA durchgeführt werden sollte;
- Ob die Durchführung organisationsintern oder durch externe Dienstleister erfolgt;
- Welche Abhilfemaßnahmen (Schutzmaßnahmen) eingesetzt werden sollten, um die Risiken für die betroffenen Personen einzudämmen;
- Ob die DSFA korrekt durchgeführt wurde und die auf ihr basierenden Entscheidungen (Durchführung der geplanten Verarbeitung, Auswahl und Umsetzung von Abhilfemaßnahmen) im Einklang mit der Datenschutz-Grundverordnung stehen.[8]

Es steht der Verantwortlichen frei, dem Rat der Datenschutzbeauftragten nicht zu folgen; jedoch muss eine solche Entscheidung und deren Gründe in der DSFA-Dokumentation schriftlich begründet werden. Die finale Entscheidungsbefugnis über die DSFA und alle mit ihr zusammenhängenden Fragen liegen eben immer bei der Verantwortlichen und dürfen auch in dieser Frage nicht an die Datenschutzbeauftragte delegiert werden. Die Haftung für die ordnungsgemäße Anwendung der Datenschutz-Grundverordnung, einschließlich der DSFA liegt gemäß Art. 24 Abs. 1 DSGVO ebenfalls stets bei der Verantwortlichen selbst.

Produkthersteller, Auftragsverarbeiter und gemeinsam Verantwortliche

Produkthersteller, die selbst keine Datenverarbeitung vornehmen, sondern nur die zur Umsetzung einer Verarbeitung verwendeten Systeme und Komponenten liefern, trifft keine Pflicht aus Art. 35 DSGVO, für ihre Produkte eine entsprechende DSFA durchzuführen. Oft dürften aber gerade die Hersteller das beste Verständnis der sicherheits- und datenschutzrelevanten technischen Eigenschaften ihrer Produkte besitzen. Daher kann es schon aus wirtschaftlichem Eigeninteressen heraus Sinn ergeben, eine möglichst gute Dokumentation bereitzustellen, so dass die potentiellen Kunden bei der Nutzung der Komponenten deren Beschreibung möglichst leicht im Rahmen einer DSFA für den relevanten Verarbeitungsprozess integrieren können. Darüber hinaus besteht im Einzelfall die Möglichkeit, dass bei der Herstellung von einzelnen Komponenten einer Verarbeitung (bspw. Hard- oder Software), im Zusammenspiel mit weiteren Faktoren ein hohes Risiko im Sinne des Art. 35 Abs. 1 DSGVO ausgelöst wird. Im Einzelfall kann es daher durchaus sinnvoll – und für Hersteller von Vorteil – sein, sich im Rahmen des Datenschutzes by Design und by Default bereits frühzeitig Gedanken zu datenschutzfreundlichen Voreinstellungen und Beratung potentieller Kunden zu machen, um bereits im Vorfeld mögliche Risiken einzudämmen oder zumindest Alternativen aufzeigen zu können.

Auftragsverarbeiter sind natürliche oder juristische Personen, die personenbezogene Daten im Auftrag einer Verantwortlichen verarbeiten, selber aber keinen Entscheidungsspielraum über den Zweck und die Mittel der Verarbeitung haben (vgl. Art. 4 Nr. 7 und Nr. 8 DSGVO). Gemäß Art. 28 Abs. 3 lit. f DSGVO sind sie verpflichtet, die Verantwortliche bei der DSFA zu unterstützen. Im konkreten Fall dürfte es dabei regelmäßig vor allem darum gehen, der Verantwortlichen erforderliche Informationen bereitzustellen.

Gemeinsame Verantwortlichkeit liegt gemäß Art. 26 Abs. 1 DSGVO vor, wenn zwei oder mehrere Stellen gemeinsam über die Zwecke und Mittel der Verarbeitung entscheiden. Die Artikel-29-Datenschutzgruppe fordert in diesem Fall, dass die Verantwortlichen ihre jeweiligen Aufgaben genau festlegen und in der DSFA angeben, welche Verantwortliche für welche Abhilfemaßnahmen zuständig ist. Zudem müssen sie einander bei der DSFA unterstützen und „hilfreiche Informationen" für diese bereitstellen.[9]

Praxistipp **IT-Dienstleister**

Gerade bei IT-Dienstleistern, die einzelne Software- oder Hardware-Komponenten anbieten und auch Teile der Datenverarbeitung übernehmen, kann es schwierig sein zu entscheiden, ob im Einzelfall eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vorliegt. In jedem Fall dürfte die Anforderung an Dienstleister, bei der DSFA aktiv mitzuwirken und Verantwortung für die Identifikation und Analyse von Risiken und den Einsatz von Abhilfemaßnahmen zu übernehmen, zu dem Grad steigen, zudem sie eigene Entscheidungsspielräume über die Mittel und Zwecke der Verarbeitung genießen. Das gilt insbesondere je größer das Potenzial ist, dass sich negative Auswirkungen auf die betroffenen Personen aus den vom Dienstleister übernommenen Tätigkeiten ergeben. Umgekehrt kann es für solche Dienstleister nicht nur praktisch möglich, sondern auch wirtschaftlich interessant sein, „generische" Elemente einer DSFA für typische Einsatzszenarien, in denen ihre Dienste verwendet werden (z. B. Kommunikationsdienst im Gesundheitssektor), anzufertigen und sowohl bereits geprüfte Verarbeitungsvorgänge als Dokumentation vorzuhalten, als auch im Sinne des Datenschutzes by Design und by Default erleichterte Möglichkeiten für technische und organisatorische Maßnahmen zu entwickeln. Kunden (Verantwortliche) können die generische DSFA dann nutzen, um eine DSFA für die Verarbeitung in ihrem spezifischen Kontext zu erstellen bzw. entsprechende Abhilfemaßnahmen vorzunehmen.

2 Notwendige Vorarbeiten

Zur Durchführung einer DSFA müssen bestimmte Informationen vorab vorliegen. Diese sind das Verzeichnis der Verarbeitungstätigkeiten (nachfolgend „Verarbeitungsverzeichnis"), eine Dokumentation der Rechtsgrundlage der Verarbeitung und eine Bewertung der Notwendigkeit der geplanten Verarbeitung bezogen auf ihren Zweck. Fehlen diese, ist eine DSFA aufgrund der Komplexität der betrachteten Prozesse nur schwer durchführbar.

Nicht erforderlich aber dennoch sinnvoll ist es, bereits zu vor Beginn der DSFA eine – explizit provisorische und noch nicht abschließende – Vorab-Bewertung der Verhältnismäßigkeit der geplanten Verarbeitung zu erstellen, um frühzeitig auf ggf. vorhandene Unverhältnismäßigkeiten reagieren zu können.

2.1 Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO

Gemäß Art. 30 Abs. 1 DSGVO müssen Verantwortliche ein Verarbeitungsverzeichnis für alle ihrer Zuständigkeit unterliegenden Verarbeitungstätigkeiten führen, in dem eine Reihe von Informationen enthalten sein müssen. Zwar sind gemäß Art. 30 Abs. 5 DSGVO manche Kleinunternehmen von dieser Pflicht ausgenommen, doch sobald unter anderem die von ihnen vorgenommene Verarbeitung Risiken für die Rechte und Freiheiten der betroffenen Personen birgt oder es sich um die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO handelt, ist auch in diesen Fällen ein Verarbeitungsverzeichnis zu führen. Eine DSFA ohne diese grundlegenden Informationen wäre kaum durchführbar und sollten daher bereits zu Beginn der DSFA vorliegen.
Die nach Art. 30 Abs. 1 DSGVO ohnehin im Verarbeitungsverzeichnis vorzuhaltenden Informationen sind:

- Name und Kontaktdaten der Verantwortlichen, Vertreter und der Datenschutzbeauftragten (soweit vorhanden);
- Zwecke der Verarbeitung;
- Beschreibung der Kategorien der von der Verarbeitung betroffenen Personen;
- Beschreibung der Kategorien der verarbeiteten personenbezogenen Daten;
- Kategorien von Empfängern, gegenüber denen personenbezogenen Daten offengelegt werden oder werden sollen, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- Gegebenenfalls Übermittlungen von personenbezogenen Daten an Drittländer oder internationale Organisationen, einschließlich Angabe dieser Länder oder Organisationen sowie bei den in Art. 49 Abs. 1 UnterAbs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- Vorgesehene Löschfristen für die verschiedenen Datenkategorien (wenn möglich);

- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherung der Verarbeitung gemäß Art. 32 Abs. 1 DSGVO (wenn möglich).

Falls noch kein Verarbeitungsverzeichnis erstellt worden ist – weil sich die Verarbeitung beispielsweise noch im Planungsstadium befindet – sollten die genannten Informationen vorab soweit wie möglich zusammengetragen werden.

2.2 Beteiligte Stellen

Oft sind mehrere Bereiche innerhalb oder außerhalb eines Unternehmens bzw. einer Behörde an einer von dieser verantworteten Verarbeitung beteiligt (Abteilungen innerhalb der Organisation, Auftragsverarbeiter außerhalb der Organisation, ggf. gemeinsam Verantwortliche), indem sie z. B. Teile der Verarbeitung ausführen, Zugriff auf Daten erhalten oder Daten liefern, bzw. IT-Systeme und Dienste administrieren. Da Risiken für die betroffenen Personen prinzipiell von jeder dieser Beteiligten ausgehen könnte, sollten möglichst deren Vertreter in die DSFA einbezogen werden. Folglich ist es notwendig, diese vorab zu identifizieren.

2.3 Dokumentation der rechtlichen Grundlagen der Verarbeitung

Gemäß Art. 5 Abs. 1 lit. a DSGVO benötigt jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Eine Verarbeitung ohne wirksame Rechtsgrundlage stellt einen Verstoß gegen das Grundrecht auf Datenschutz gemäß Art. 8 GrCh dar. Es handelt sich somit um den Eintritt eines Risikos für Rechte und Freiheiten der betroffenen Personen und damit auch um einen Verstoß gegen die DSGVO. Um dies zu vermeiden, sollte bereits vorab dokumentiert werden, auf welche Rechtsgrundlage sich die geplante Verarbeitung stützt.

Art. 6 Abs. 1 lit. a–f DSGVO nennt sechs mögliche Rechtsgrundlagen, auf die sich die Verarbeitung personenbezogener Daten stützen kann. Werden besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO oder über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO verarbeitet, sind zudem die dort genannten Besonderheiten bei der Verarbeitung zu beachten.

Wenn mehrere juristisch eigenständige Stellen an einer Verarbeitung beteiligt sind, die darüber hinaus eventuell auch noch unterschiedliche personenbezogene Daten von (zum Teil) unterschiedlichen betroffenen Personen verarbeiten, kann es sein, dass sich unterschiedliche Verarbeitungsvorgänge auf separate Rechtsgrundlagen stützten müssen. Es ist daher sicherzustellen, dass jeder konkrete Verarbeitungsvorgang, und somit die Verarbeitung als Ganzes, von einer Rechtsgrundlage abgedeckt ist. Es

empfiehlt sich in derartigen Fällen, eine Skizze der beteiligten Stellen, betroffenen Personen, Verarbeitungsvorgänge und Rechtsbeziehungen anzufertigen (einschließlich vorhandener Datenflüsse).

2.4 Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung

Gemäß Art. 35 Abs. 7 lit. b DSGVO muss als Teil der DSFA eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck erstellt werden.

Die Frage der **Notwendigkeit** operationalisiert dabei den Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO). Es geht darum zu bewerten, ob die Verarbeitungsvorgänge einschließlich der für diese zu erhebenden Daten tatsächlich alle notwendig sind, um den Zweck der Verarbeitung zu erreichen, und ob der Zweck nicht auf anderen, alternativen, Wegen erreicht werden könnte, die weniger stark in die Rechte und Freiheiten der betroffenen Personen eingreifen. Es ist sinnvoll, diese Bewertung bereits vorab durchzuführen: Zum einen, weil jede Verarbeitung personenbezogener Daten – auch solche, die keine Pflicht zur DSFA auslösen – dem Grundsatz der Datenminimierung folgen müssen; zum anderen, weil ggf. nötige Anpassungen der Verarbeitungsvorgänge so frühzeitig vorgenommen werden können.

Die **Verhältnismäßigkeit** einer Datenverarbeitung ist nur dann gegeben, wenn die Nachteile der Verarbeitung für die betroffenen Personen – einschließlich des bei jeder Verarbeitung personenbezogener Daten gegebenen Eingriffs in das Grundrecht auf Datenschutz gemäß Art. 8 GrCh sowie mögliche Eingriffe in andere Rechte – in einem angemessenen Verhältnis zu den Vorteilen der Verarbeitung für die legitimen Interessen der Verantwortlichen stehen. Eine allgemeine Regel für die Bewertung der Verhältnismäßigkeit lässt sich schwer aufstellen, da die Rechte und Interessen, die gegeneinander abgewogen werden müssen, von Fall zu Fall variieren dürften. Um die Verhältnismäßigkeit der Verarbeitung abschließend bewerten zu können, muss die (in Kapitel 6 beschriebene) Bewertung der Risiken, die den betroffenen Personen durch die Verarbeitung entstehen, vorliegen. Schließlich kann nur dann beurteilt werden, ob die Vorteile für die Verantwortliche in einem angemessenen Verhältnis zu den Nachteilen (d. h. Risiken) für die betroffenen Personen stehen wenn klar ist, welche Risiken es überhaupt gibt und wie schwer diese wiegen.

Praxistipp **„Vorab-Bewertung“ der Verhältnismäßigkeit**

Es ist dennoch empfehlenswert, neben der Bewertung der Notwendigkeit zu Anfang auch schon eine Art provisorische „Vorab-Bewertung“ der Verhältnismäßigkeit vorzunehmen und sich die Frage zu stellen, ob der Eingriff in die Rechte und Freiheiten der betroffenen Personen, die die geplante Verarbeitung darstellt, überhaupt verhältnismäßig sein könnte. Wenn die Rechte und Interesse der betroffenen Personen offensichtlich die Interessen der Verantwortlichen überwiegen – aufgrund einer klare Rechtsprechung oder allgemein akzeptierter gesellschaftlichen Normen – dann sollte die Verarbeitung sogleich eingestellt oder so angepasst werden, dass sie nicht länger gegen Rechtsprechung oder Normen verstößt.

Diese „Vorab-Bewertung“ kann die Anforderung des Art. 35 Abs. 7 lit. b DSGVO nicht erfüllen. Wie oben dargelegt, ist eine vollständige Bewertung der Verhältnismäßigkeit nur auf Grundlage der im Rahmen der DSFA zu erstellenden Risikobewertung möglich. Die „Vorab-Bewertung“ dient vielmehr dem allgemeinen Zweck einer vorausschauenden und ethischen Technikgestaltung.

Die DSFA in der Praxis:
Eine Vorgehensweise

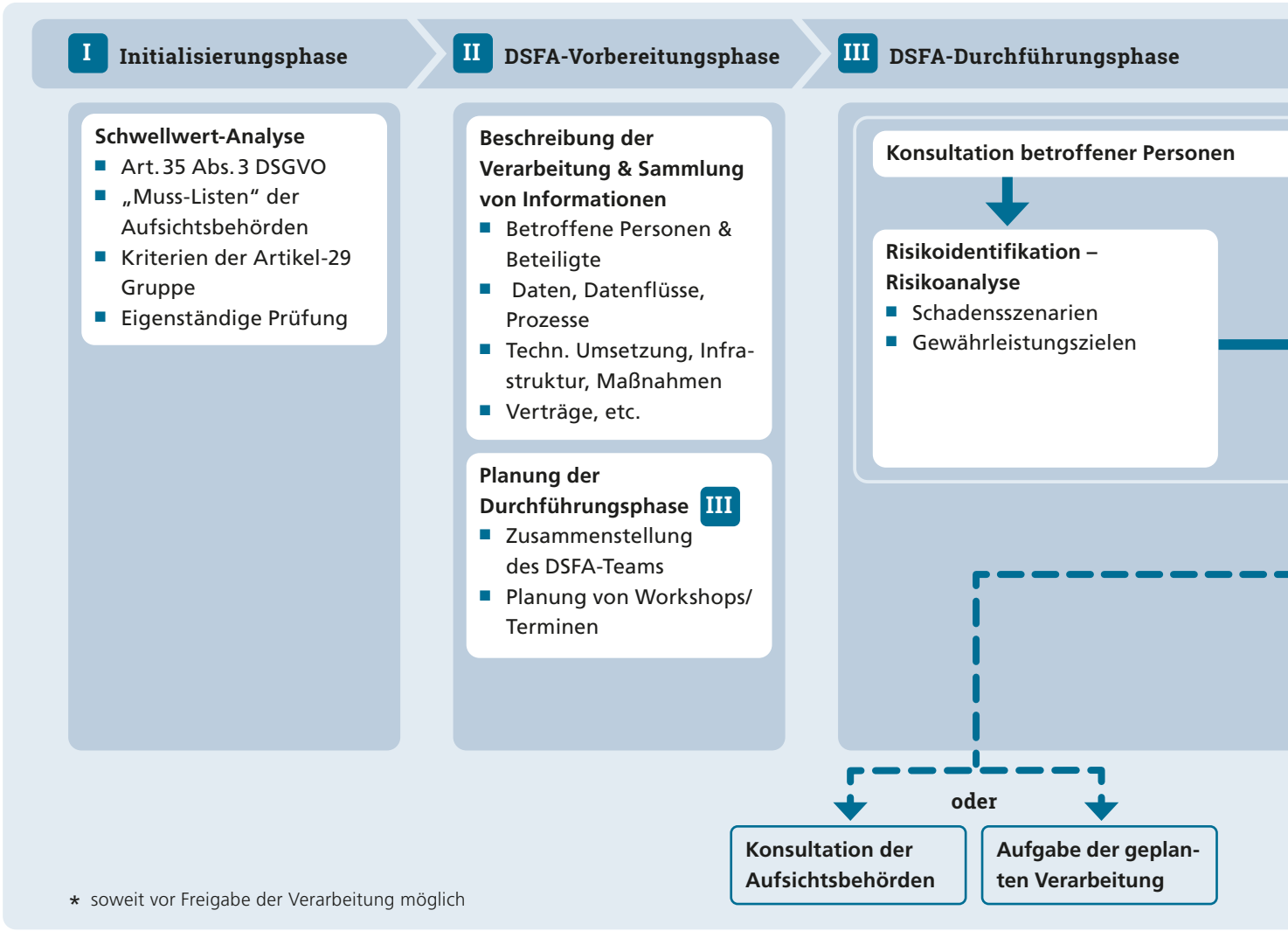
3 Phasen einer DSFA

Bei der Durchführung einer DSFA sollte nach Möglichkeit auf eine sehr strukturierte Vorgehensweise geachtet werden, um die notwendige Dokumentation im Nachhinein noch nachvollziehen zu können. Dabei ist es empfehlenswert jeden der vorgenommenen Schritte zumindest mit einem kurzen Protokoll zu begleiten und die anwesenden Personen zu benennen, um spätere Nachfragen zu ermöglichen Wegen des großen Umfangs einer DSFA ist es hilfreich, sie in verschiedene Phasen zu unterteilen, wobei sich die Untergliederung in fünf Phasen bewährt hat:

I **Initiierungsphase**, auch Schwellwertanalyse genannt, in der geprüft wird, ob eine DSFA erforderlich ist;

II **Vorbereitungsphase**, in der die für die Durchführung notwendigen Unterlagen und Informationen zur Verarbeitung, relevanten Datenflüsse und technischen Systemen, den betroffenen Personen sowie der Rechtsgrundlage gesammelt werden,

Abbildung 1:
Ablauf der fünf Phasen einer DSFA

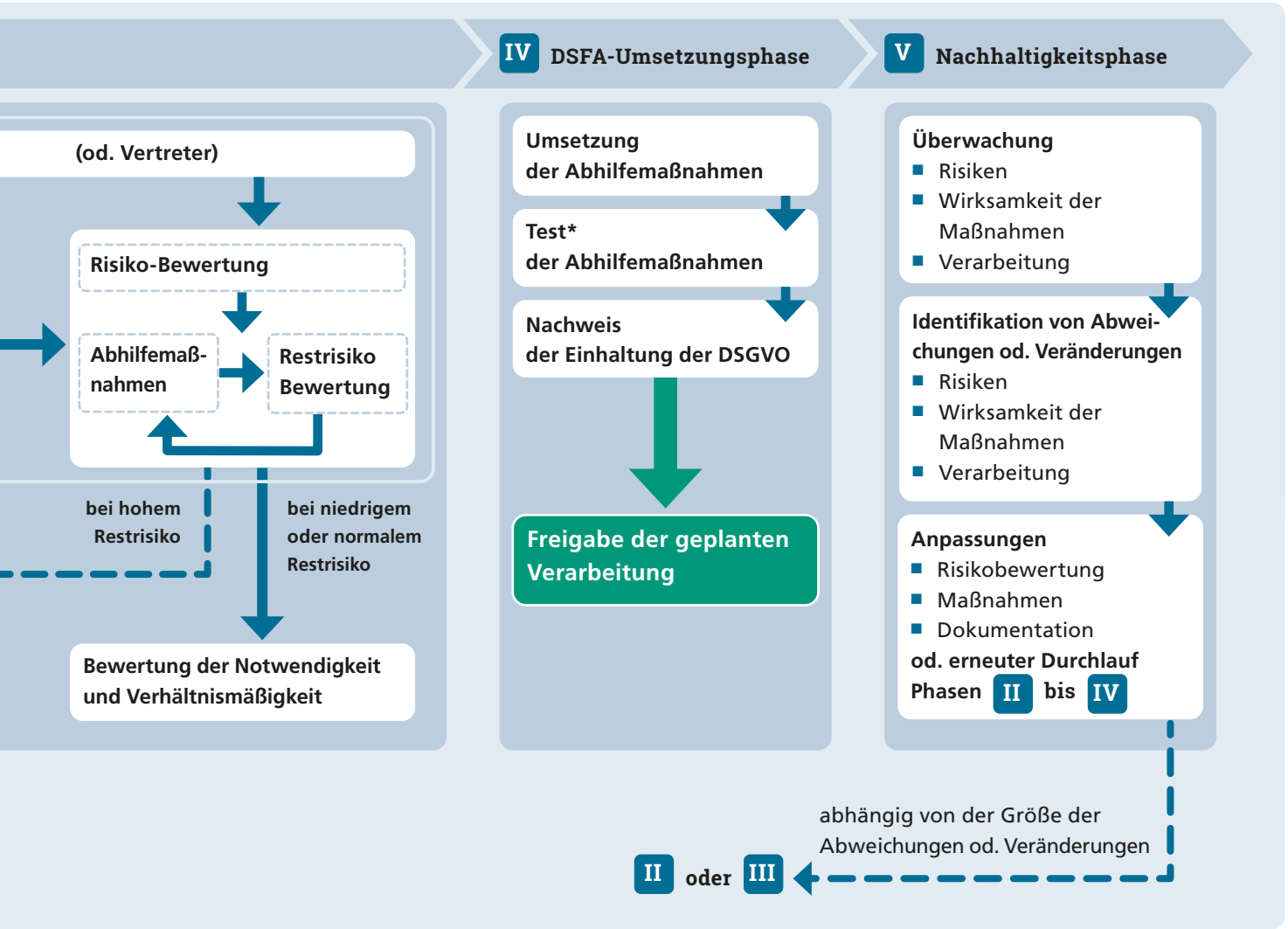


damit eine systematische Beschreibung der geplanten Verarbeitungsvorgänge erstellt, das DSFA-Team zusammengestellt und die DSFA geplant werden kann;

III Durchführungsphase, in der die in Phase II. erhobenen Informationen validiert, die Risikoidentifikation, -analyse und -bewertung (im Weiteren zusammengefasst als Risikobeurteilung bezeichnet) durchgeführt, passende Abhilfemaßnahmen ausgewählt und die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung bewertet werden;

VI Umsetzungsphase, in der die in Phase III. ausgewählten Abhilfemaßnahmen umgesetzt werden, der Nachweis der Einhaltung der DSGVO erbracht und die Verarbeitung freigegeben werden kann;

V Nachhaltigkeitsphase, in der eine fortlaufende Überprüfung und Anpassung während des Lebenszyklus der Verarbeitung stattfindet, um nachzuweisen, dass die Risiken für die betroffenen Personen, die sich aus der Verarbeitung ergeben, ausreichend eingedämmt sind.



4 Phase I: Initiierung der DSFA

4.1 Vorgehen

Gemäß Art. 35 Abs. 1 DSGVO muss eine DSFA durchgeführt werden, wenn eine Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" zur Folge hat. Um zu prüfen, ob ein solches hohes Risiko voraussichtlich besteht, sollten die folgenden drei Informationsquellen genutzt werden:

- Vorgaben des Art. 35 Abs. 3 DSGVO
- Positivlisten („Muss-Listen") der Aufsichtsbehörden
- Kriterien der Art.-29 Datenschutzgruppe

Daneben ist eine ergänzende eigenständige Prüfung der voraussichtlichen Höhe und Existenz von Risiken für Rechte und Freiheiten natürlicher Personen unabdingbar.

Diese Prüfungen können von der Verantwortlichen bzw. von ihr beauftragten Dritten durchgeführt werden, ggf. unterstützt durch Auftragsverarbeiter und die für die Verarbeitung zuständigen Fachabteilungen. Die Datenschutzbeauftragte sollte beratend eingebunden werden.

Es empfiehlt sich bei der Planung und Entwicklung neuer Verarbeitungen frühzeitig zu prüfen, ob eine DSFA nötig ist, da Gestaltungsspielräume in frühen Phasen meist noch relativ groß und Änderungen einfach und kostengünstig sind. Mittels einer diesen Prozess begleitenden DSFA kann ebenfalls die Umsetzung des Grundsatzes des Datenschutz by Design und by Default sichergestellt werden.

Unerlässlicher Input für die Schwellwert-Analyse sind, erstens, eine umfassende Dokumentation der zu prüfenden Verarbeitungstätigkeiten (zusätzlich zu den für das Verarbeitungsverzeichnis aufzunehmenden Angaben) und, zweitens, eine Dokumentation der Rechtsgrundlage der Verarbeitung.

Dabei kann auch eine Entwurfsfassung dieser Unterlagen ausreichen – etwa wenn die Verarbeitung sich in einem so frühen Planungsstadium befindet, dass noch keine endgültige Fassung vorliegen kann. Sollten in diesem Fall allerdings später Änderungen an der geplanten Verarbeitung oder ihrer Rechtsgrundlage vorgenommen werden, wird geprüft werden müssen, ob diese Änderungen Auswirkungen auf die Ergebnisse der Schwellwert-Analyse und die ggf. bereits vorgenommene DSFA haben. Ist das der Fall, werden beide wiederholt bzw. angepasst werden müssen.

Im Folgenden werden die Informationsquellen vorgestellt.

4.2 Prüfung der Vorgaben aus Artikel 35 Abs. 3 DSGVO

Art. 35 Abs. 3 lit. a–c DSGVO nennt drei Fälle, die eine DSFA in jedem Fall erforderlich machen:

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Art. 35 Abs. 3 lit. a).
- Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO (Art. 35 Abs. 3 lit. b);
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c).

Die Qualifizierung „umfangreich" (Englisch: „on a large scale") kann entsprechend des Beschluss der Artikel-29-Datenschutzgruppe ausgelegt werden (vgl. unten).

„Umfangreiche" Verarbeitungen

Die Artikel-29 Gruppe sieht davon ab, eine allgemeingültige quantitative Größe zu definieren, ab der eine Verarbeitung als „umfangreich" gilt; sie nennt stattdessen vier Kriterien und mehrere Beispiele anhand derer der Umfang von Verarbeitungen „insbesondere" eingestuft werden kann. Die Kriterien sind:

- Zahl der betroffenen Personen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe
- Verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Daten
- Dauer oder Dauerhaftigkeit der Datenverarbeitung
- Geographisches Ausmaß der Datenverarbeitung

Beispiele für „umfangreiche" Verarbeitungen im Sinne der Artikel-29-Datenschutzgruppe sind:

- Verarbeitungen von Daten von Patientinnen im gewöhnlichen Geschäftsbetrieb eines Krankenhauses
- Verarbeitung von Reisedaten natürlicher Personen aus dem kommunalen ÖPNV-System (z. B. Nachverfolgung über Netzkarten)
- Verarbeitung von Echtzeit-Geolokalisierungsdaten der Kundinnen einer internationalen Fast Food-Kette für statistische Zwecke durch einen spezialisierten Auftragsverarbeiter
- Verarbeitung von Daten von Kundinnen im gewöhnlichen Geschäftsbetrieb einer Versicherung oder Bank

- Verarbeitung personenbezogener Daten durch eine Suchmaschine zwecks verhaltensbasierter Werbung
- Verarbeitung von Daten (Inhalte, Datenverkehrsaufkommen, Standort) durch Telefon- und Internetdienstleister

Beispiele für Verarbeitungen, die nicht „umfangreich" sind, stellen dar:

- Verarbeitung von Daten von Patientinnen durch eine einzelne Ärztin
- Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durch eine einzelne Rechtsanwältin

Quelle: Artikel-29-Datenschutzgruppe, "Leitlinien für Datenschutzbeauftragte", S. 8–9

4.3 Positivlisten („Muss-Listen") der Datenschutz-Aufsichtsbehörden

Gemäß Art. 35 Abs. 4 DSGVO sind die Aufsichtsbehörden verpflichtet, eine Liste mit Verarbeitungsvorgängen zu veröffentlichen, für die eine DSFA durchzuführen ist. Diese Listen werden auch als „Positiv-" bzw. „Muss-Listen" bezeichnet. Ist die geplante Verarbeitung Bestandteil der Muss-Liste, muss eine DSFA durchgeführt werden.

Die Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder („Datenschutzkonferenz") hat für den nichtöffentlichen Bereich eine entsprechende Liste von 17 Verarbeitungen mit Beispielen und typischen Einsatzfeldern veröffentlicht, für die eine DSFA immer durchgeführt werden muss.[10] Diese Liste ist für den nichtöffentlichen Bereich in Deutschland maßgeblich. Für den öffentlichen Bereich haben die einzelnen Datenschutz-Aufsichtsbehörden des Bundes und der Länder entsprechend der jeweiligen Bundes-/Landesdatenschutzgesetze ebenfalls entsprechende Listen veröffentlicht.

Die Listen unterliegen dem Kohärenzverfahren des Europäischen Datenschutzausschusses. Er bezieht zu ihnen Stellung und empfiehlt ggf. Anpassungen. Ziel ist dabei nicht die Erstellung einer einheitliche EU-weiten Liste, sondern lediglich die Vermeidung „bedeutender Inkohärenzen". Die Aufsichtsbehörden genießen „Ermessensspielraum bezüglich des nationalen oder regionalen Kontextes".[11] Bei grenzüberschreitenden Verarbeitungen sind daher die Listen der jeweiligen Mitgliedsstaaten zu konsultieren.

Wichtig für die Arbeit mit den Muss-Listen ist, dass diese nicht abschließend sind, was die Aufsichtsbehörden auch betonen. Findet sich eine geplante Verarbeitung nicht in der Liste, heißt das nicht, dass ein hohes Risiko ausgeschlossen und auf eine DSFA verzichtet werden kann. Im Gegenteil sollte in diesem Fall die Schwellwertprüfung mit der Prüfung der Kriterien der Artikel-29-Datenschutzgruppe fortgesetzt werden.

4.4 Kriterien der Artikel-29 Datenschutzgruppe

Die Artikel-29 Datenschutzgruppe hat neun Kriterien ausgearbeitet, die auf ein hohes Risiko hindeuten können.[12]

Laut der Artikel-29 Datenschutzgruppe ist anzunehmen, dass ein „hohes Risiko" wahrscheinlich ist und eine DSFA durchgeführt werden muss, wenn zwei der Kriterien auf die geplante Verarbeitung zutreffen. Jedoch kann ein hohes Risiko auch gegeben sein (und eine DSFA-Pflicht), wenn nur eines – oder keines – der genannten Kriterien anschlägt. Schlagen zwei der Kriterien an, muss eine DSFA durchgeführt werden.

Schlägt nur ein Kriterium an, muss man eigenständig prüfen, ob die Verarbeitung voraussichtlich zu hohen Risiken für die Rechte und Freiheiten der betroffenen Personen führen könnte. In diesem Fall muss eine DSFA durchgeführt werden. Entscheidet man, dass trotz Anschlags eines Kriteriums kein hohes Risiko vorliegt und keine DSFA durchgeführt wird, sollte man die Gründe für diese Entscheidung dokumentieren, so dass man sie auf Anfrage den Aufsichtsbehörden vorlegen kann.

Wie die Muss-Liste sind auch die Kriterien der Artikel-29 Datenschutzgruppe nicht abschließend. Ergänzend sollte daher immer eine eigenständige Prüfung durchgeführt werden.

4.5 Eigenständige Prüfung

Neben der Nutzung der oben dargestellten Informationsquellen sollte die Verantwortliche zusätzlich generell prüfen, ob die Verarbeitung aufgrund ihrer Art, ihres Umfangs, Umstände oder Zwecke voraussichtlich zu einem hohen Risiko für die betroffenen Personen führen könnte. Besonders neue technologische Entwicklungen werden unter Umständen noch nicht in den Positivlisten der Datenschutz-Aufsichtsbehörden berücksichtigt sein. Um diese Prüfung vorzunehmen kann man sich an der in Kapitel 6 beschriebenen Risikoanalyse orientieren. Die Prüfung muss dabei – auch in Bezug auf Aufwand – keineswegs eine volle DSFA-Risikoanalyse replizieren. Vielmehr geht es darum, entsprechend der in Kapitel 6 beschriebenen Schritte, zu überlegen, was die geplante Verarbeitung tatsächlich macht (zu welchem Zweck sie wessen Daten wie erhebt und verarbeitet), wer die betroffenen Personen und beteiligte Stellen sind und ob plausible Szenarien denkbar sind, in denen die Verarbeitung zu signifikanten Risiken für die betroffen Personen führen könnte. Wenn ja, muss eine DSFA eingeleitet werden. Wenn nein, muss sie es nicht. Da eine DSFA allerdings ein gutes Instrument darstellt, um etwaigen Risiken vorzubeugen und die Einhaltung der DSGVO sicherzustellen, ist der Rechtsanwenderin geraten, im Zweifelsfall eine DSFA durchzuführen.

4.6 Dokumentation des Prüfergebnisses

Zwar schreibt die DSGVO nicht vor, die Ergebnisse der Schwellwertanalyse zu dokumentieren, doch ist dies im Sinne einer belastbaren Compliance in jedem Fall sinnvoll, so dass sie auf Anfrage den Datenschutzbehörden vorgelegt werden können. Dazu sollten Prüfergebnisse und die Begründung der Entscheidung dokumentiert werden. Sinnvoll wäre die Integration dieser Informationen in ein Datenschutz-Managementsystem.

5 Phase II: Vorbereitung der DSFA

5.1 Vorgehen

Ergibt die Schwellwertanalyse, dass eine DSFA durchgeführt werden muss, ist eine systematische Beschreibung der geplanten Verarbeitungsvorgänge (Art. 35 Abs. 7 lit. a DSGVO) und des konkreten Kontextes aus technischer, rechtlicher und organisatorischer Sicht zu erstellen. Diese wird für die Risikobeurteilung in der folgenden Durchführungsphase benötigt. In diesem Zusammenhang sind auch die betroffenen Personen und die Beteiligten zu identifizieren. Außerdem muss in dieser Phase das Team für die Durchführung der DSFA zusammengestellt und die folgende Durchführungsphase der DSFA geplant werden.

Die Zusammenstellung dieser Informationen kann wieder von der Verantwortlichen bzw. von ihr beauftragten Dritten durchgeführt werden, ggf. unterstützt durch Auftragsverarbeiter und die für die Verarbeitung zuständigen Fachabteilungen. Die Datenschutzbeauftragte sollte beratend eingebunden werden.

5.2 Sammlung von Informationen und Beschreibung der Verarbeitungsvorgänge und der Zwecke der Verarbeitung

Die Erstellung einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung erfüllt den ersten der vier in Art. 35 Abs. 7 lit. a-d DSGVO benannten inhaltlichen Anforderung an die DSFA, nämlich die Erstellung

> *eine[r] systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen (Art. 35 Abs. 7 lit. a)*

Der Zweck sollte bereits im Verarbeitungsverzeichnis vorgegeben sein. Zu beachten ist, dass während der Durchführung der DSFA mitunter weitere, bisher nicht in der Beschreibung des Verarbeitungsvorgang festgehaltene Zwecke „entdeckt“ werden, denen die geplante Verarbeitung ebenfalls dient. In diesem Fall ist die Zweckbeschreibung und das Verarbeitungsverzeichnis entsprechend zu ergänzen. Auch muss geprüft werden, ob diese „neuen“ Zwecke auch durch entsprechende Rechtsgrundlagen gedeckt sind.

Um die Verarbeitungsvorgänge (manchmal auch „Prüfgegenstand" genannt) sinnvoll beschreiben zu können, ist es i. d. R. zweckdienlich folgende Informationen zu erfassen:

- Betroffene Personen, verarbeitete personenbezogener Daten, Datenflüsse, weitere Beteiligte, (geplante) Prozesse;
- Dokumentation der (geplanten) technischen Umsetzung, technische Infrastruktur, bereits technische und organisatorische Maßnahmen;
- Ggf. Betroffenenvertreter (z. B. Betriebsrat, Personalrat, Patientinnenrat), Organisation, Auftragsverarbeiter, Joint Controller (gemeinsam für die Verarbeitung Verantwortliche), Verträge etc.

Um die Verarbeitungsvorgänge zu verdeutlichen und möglichst umfassend betroffene Personen, Kategorien personenbezogener Daten und weitere Beteiligte zu identifizieren, ist es oft hilfreich ein Datenflussdiagramm zu erstellen, in dem die gesamte Verarbeitung von der Erhebung, Speicherung, Nutzung, Weitergabe bis hin zur Löschung der Daten dokumentiert ist. Zu den dabei identifizierten Systemen, Netzwerken, technischen Infrastrukturen und Planungen zur Umsetzung der Verarbeitung sollten Dokumentationen zusammengestellt werden. Dabei sind insbesondere bereits geplante technisch-organisatorische Maßnahmen zu berücksichtigen. Auf Basis dieser Informationen soll das DSFA-Team in der folgenden Durchführungsphase in der Lage sein, mögliche Schadensszenarien für betroffene Personen im Rahmen der betrachteten Verarbeitung zu definieren und zu analysieren.

Praxistipp **Umgang mit Granularitätsgraden und Komplexität**

Eine Herausforderung bei der Beschreibung der Verarbeitung ist es, den richtigen Granularitätsgrad zu treffen – weder zu detailliert, noch zu oberflächlich. Allgemeine Regeln lassen sich hier schwer aufstellen. Eine Hilfsstellung, um einzuordnen, welche Informationen aufgenommen werden sollten, ist vom Ende her zu denken: letztlich soll die Beschreibung der Verarbeitungsvorgänge eine verlässliche Identifizierung, Analyse und Bewertung von Risiken und Auswahl von Abhilfemaßnahmen ermöglichen. Auch kann die Beschreibung iterativ angegangen werden: oft ist es zunächst am wichtigsten, einen belastbaren Überblick über die Bestandteile der Verarbeitung sowie der beteiligten Stellen zu bekommen, so dass mögliche Risiken identifiziert werden können. Zusätzliche Detailinformationen können, wenn nötig, anschließend noch erhoben werden.

Eine weitere mögliche Herausforderung ist, dass der Prüfgegenstand bei genauerer Betrachtung schnell sehr komplex werden kann, weil Verarbeitungen mittels umfangreicher technischer Infrastrukturen umgesetzt sind, häufig ernetzt mit anderen Systemen sind, mehrere Standorte und ggf. zusätzlich Auftragsverarbeiter und deren technische Systeme und Prozesse einbeziehen.

Für diese Herausforderung gibt es meist keine schnelle Lösung. Wenn anzunehmen ist, dass dabei identifizierte zusätzliche Verarbeitungen hohe Risiken für betroffene Personen darstellen, muss für sie ebenfalls eine DSFA durchgeführt werden. In solchen Situationen kann es sinnvoll sein, die verschiedenen Verarbeitungsvorgänge zunächst möglichst klar voneinander abzugrenzen (sowohl in Hinblick auf ihre Zwecke wie die verwendeten Daten, IT-Systeme, Verarbeitungsvorgänge und Beteiligten), um sie dann sukzessive mittels DSFA abzuarbeiten. Sofern die verschiedenen Verarbeitungen stark miteinander zusammenhängen, werden relativ viele Informationen und Dokumentationen zwischen den verschiedenen DSFA wiederverwertet werden können. Der Fokus sollte dann vor allem darauf liegen, wo die einzelnen Verarbeitungen tatsächlich (risikorelevante) Unterschiede aufweisen.

Eine verwandte Herausforderung ergibt sich, wenn grundsätzlich gleiche oder ähnliche Verarbeitungsvorgänge in verschiedenen Kontexten eingesetzt werden, etwa weil die gleiche Dienstleistung bzw. der Dienst bei mehreren Kunden zum Einsatz kommt. Wie in Kapitel 1.3.3 erwähnt, kann hier oft eine gemeinsame Verantwortlichkeit vorliegen. Da der Kontext und die Details der Implementierung bei jedem Kunden unterschiedlich sein werden, muss davon ausgegangen werden, dass auch die Risiken und gegebenenfalls notwendige Abhilfemaßnahmen von Kunde zu Kunde variieren werden. Daher wird wahrscheinlich jeder Kunden eine separate DSFA erstellt werden müssen. Um den Aufwand möglichst gering zu halten, kann es in dieser Situation empfehlenswert sein, zunächst eine oder mehrere „generische“ DSFA für „typische“ Implementierungen und Kontexte der fraglichen Dienstleistung zu erstellen, und diese dann als Template für DSFA für die übrigen Implementierungen zu nutzen. Hier wird es darum gehen, relevante Differenzen im Kontext und der Implementierung möglichst verlässlich zu erfassen, so dass jeweils kundenspezifische Risiken ermittelt und eingedämmt werden können.

5.3 Identifikation der betroffenen Personen

Betroffene Personen sind gemäß Art. 4 Nr. 1 DSGVO alle jene natürlichen Personen, die mittels der verarbeiteten Daten direkt oder indirekt identifiziert werden oder identifiziert werden könnten. Juristische Personen sind in diesem Sinne keine betroffenen Personen; sie fallen nicht unter das Datenschutzrecht (vgl. ErwGr 14 DSGVO).

Aufgrund heutiger Methoden zur Analyse von Daten und der Möglichkeit Datensätze zu verknüpfen, lässt sich häufig uch bei Daten, die nicht direkt einer natürlichen Person zugeordnet sind mit großer Wahrscheinlichkeit ein Personenbezug herstellen. So können GPS-Daten von Fahrzeugen oder Log-Daten von Maschinen oft einer Person zugeordnet werden. Auch wenn diese Daten erhoben wurden, um den Fuhrpark eines Unternehmens zu managen oder die Auslastung einer Maschine zu überwachen

und Hinweise zur Wartung zu erhalten, sind sie personenbeziehbar, so dass personenbezogene Daten betroffener Personen im Sinne der DSGVO verarbeitet werden.

Um die betroffenen Personen einer Verarbeitung verlässlich zu identifizieren, kann es hilfreich sein, drei Fragen zu beantworten:

1. Wessen Daten soll das System erfassen?
2. Wessen Daten werden zusätzlich noch erfasst, auch indirekt („Beifang")?
3. Auf wen sonst könnten Rückschlüsse auf Grundlage der erhobenen oder verarbeiteten Daten möglich sein?

Typische Kategorien betroffener Personen sind:

- **Beschäftigte** der Organisation sowie die **Belegschaft** ihrer Kunden, Zulieferer oder Dienstleister;
- **Kundinnen** und **Nutzerinnen** digitaler Dienste und digitalisierter, vormals „analoger" Produkte (z. B. smart car, smart TV) sowie **ihre Angehörigen, Freunde und weitere Personen**, die mit diesen Produkten „in Berührung" kommen (z. B. als Beifahrer, oder als anwesende Person in einem Raum mit Spracherkennungsgeräten);
- **Patientinnen, Pflegeheimbewohnerinnen, Schülerinnen** und **staatliche Leistungsempfängerinnen** sowie ihre Angehörigen, Freunde und weitere Personen;
- **Versicherungsnehmerinnen** und **Empfänger sonstiger Finanzdienstleistungen** sowie ihre Angehörigen;
- **Unbeteiligte Bürgerinnen** und **Passantinnen** (z. B. bei Videoüberwachung).

Praxistipp **Mitarbeiterinnen bei den betroffenen Personen mitdenken**

Beschäftigte sowie die Einzelne der Belegschaft Dritter finden sich ausgesprochen häufig nter den betroffenen Personen wieder – auch wenn die Auswertung ihrer Daten gar nicht Zweck der Verarbeitung ist. Der Grund hierfür ist, dass die meisten digitalen Arbeitsgeräte automatisch auch Daten aufzeichnen, die zur Überwachung und Leistungskontrolle von Mitarbeiterinnen eingesetzt werden könnten. Die Risiken, die eine Verarbeitung der Daten der Beschäftigten darstellen könnte, sollten daher immer mitbetrachtet und entsprechende Abhilfemaßnahmen gegebenenfalls getroffen werden.

5.4 Identifikation weiterer Beteiligter

Beteiligte sind alle organisationsinternen und externen natürlichen und juristischen Personen (Firmen, staatliche Institutionen, Nichtregierungsorganisationen, externe Angreifer, sonstige) sowie Organisationseinheiten ohne selbstständigen juristischen

Status (z. B. andere Firmenabteilungen), die bereits Zugriff auf die in der Verarbeitung verwendeten Daten, IT-Systeme und Verarbeitungsvorgänge haben oder plausibel Zugriff bzw. Einflussmöglichkeiten bekommen könnten.

Hier wurde bewusst der neutrale Begriff der Beteiligten gewählt. Beteiligte zu sein impliziert keinerlei illegitimes Verhalten oder „böse Absicht". Auch alle Personen und Institutionen, die völlig legitime Zugriffe genießen, sind Beteiligte. Dennoch bilden die Beteiligten oft die wichtigste Risikoquelle für die betroffenen Personen. Problematische Handlungen der Beteiligten müssen dabei keineswegs auf „böse Absicht" zurückgehen, sondern können im Gegenteil sogar (z. B. im Pflegekontext) vom Wunsch, der betroffenen Person zu helfen, motiviert sein. Es ist daher wichtig – wertungsfrei – alle aktuellen oder potentiellen, direkten und indirekten, internen und externen Beteiligten zu identifizieren.

Die Identifikation der Beteiligten sollte eine Analyse ihrer Motive, Interessen und Fähigkeiten einschließen, sich Zugriff zu bzw. Einfluss auf die Daten und Verarbeitungsvorgänge zu verschaffen. Diese Informationen sind für die spätere Risikoidentifikation und -analyse wichtig. Hierbei sollte auch auf mögliche Motive der legitim an der Verarbeitung Beteiligten geachtet werden, den Verarbeitungszweck zu überdehnen.

Schließlich ist zu beachten, dass ein Zugriff/eine Einflussnahme auch motivlos und sogar ungewollt erfolgen kann. Beschäftigte können z. B. ungewollt Zugriff auf Daten bekommen, weil Geschäftspartnerinnen sie ihnen ungebeten und nicht ordnungsgemäß zustellen. Ist ein solches Szenario denkbar, so gelten diese Beschäftigten als Beteiligte – auch wenn sie das gar nicht sein wollen!

Um alle Beteiligten zu identifizieren, kann es hilfreich sein, folgende Fragen zu beantworten:

1. Welche internen und externen Beteiligten – einschließlich Auftragsverarbeiter – sind aktiv an der Verarbeitung beteiligt?
2. Wer hat noch Zugriff auf die Daten und Verarbeitungsvorgänge (ohne bereits aktiv an der Verarbeitung beteiligt zu sein) oder könnte anderweitig den Verarbeitungsvorgang beeinflu sen oder ausnutzen?
3. Welche Interessen haben diese unter 1. und 2. identifizierten Beteiligten, die sie mittels der Daten oder sonstiger Einflussnahme auf die Verarbeitungsvorgänge verfolgen könnten, auch über den definierten Zweck der Verarbeitung hinaus?
4. Welche sonstigen internen oder externen Beteiligten, die noch nicht aktiv in die Verarbeitung involviert sind, könnten sich für die Daten und/oder Verarbeitungsvorgänge interessieren und motiviert und fähig sein, sich Zugang oder Einflussmöglichkeiten zu verschaffen?
5. Wer sonst könnte noch Zugriff oder Einflussmöglichkeit bekommen, möglicherweise ungewollt, und wenn ja wie?

Praxistipp **Typische Beteiligte**

Interne Beteiligte

- Mitarbeiterinnen (einschließlich ehemaliger Beschäftigten)
- Vorgesetzte
- „Datenintensive" Fachabteilungen wie Marketing, Personalwesen/HR, Produktentwicklung, IT
- Besucherinnen (geschäftlich und privat)

Externe Beteiligte

- Unternehmen, z. B.:
  - Anbieter von IT-Diensten, Systemen und Infrastrukturen
  - Zulieferer, Dienstleister und Kunden der Organisation allgemein
  - Banken, Versicherungen
  - Werbebranche
  - Auskunfteien, Adress- und Datenhändler, Marktforschung
  - „Datenintensive" Technologieentwickler
- Staatliche Stellen, z. B.:
  - Leistungsverwalter wie Job Center, Sozial- und Jugendämter, Rentenversicherungsträger
  - Sicherheitsbehörden
  - Statistische Ämter
- Gesundheitswesen, z. B.:
  - Krankenhäuser und Pflegeheime
  - Krankenversicherungen
- Forschung
  - Universitäten und außeruniversitäre Forschungseinrichtungen
- (Cyber-)Kriminelle /„Hackerinnen"

5.5 DSFA-Team

Eine DSFA wird meist von einem Team durchgeführt, da Einzelpersonen selten über alle relevanten Wissensbestände verfügen. Die genaue Team-Zusammensetzung wird von Organisation zu Organisation variieren. Es ist aber i. d. R. zweckmäßig, dass folgende Kompetenzen und Abteilungen vertreten sind:

- **Juristische Expertise**, insbesondere im **Datenschutzrecht**
- **Operativer Datenschutz** und die **Datenschutzbeauftragte**
- **IT-Expertise**
- (relevante) **Fachabteilungen** einschließlich ihrer **Mitarbeiterinnen**
- (ggf.) **Betriebsrat** und **Vertreter der betroffenen Personen**
- (ggf.) **Auftragsverarbeiter** und **externe IT-Dienstleister**

Wichtig bei der Einbindung der Datenschutzbeauftragten ins DSFA-Team ist, dass diese im Rahmen der DSFA nur beratende Aufgaben wahrnehmen, bzw. die Durchführung der DSFA überwachen, kann.

Die Einbindung der Fachabteilungen, die die geplante Verarbeitung durchführen bzw. ihre Ergebnisse nutzen sollen, einschließlich ihrer Mitarbeiterinnen ist sinnvoll, da diese oft das tiefste Verständnis der Verarbeitung, ihres Kontexts, der betroffenen Personen, sonstigen Beteiligten und der Risiken haben.

Die Einbindung des Betriebsrats (sofern vorhanden) ist empfehlenswert, da Beschäftigte – sowohl der Organisation selber wie ihrer Zulieferer, Dienstleister, Lieferanten, etc. – regelmäßig zu den betroffenen Personen zählen. Gleiches gilt für Repräsentanten anderer Gruppen von betroffenen Personen (z. B. Patientinnen- oder Angehörigenrat in einem Pflegeheim). Einzelne betroffene Personen (z. B. in der Form von Fokusgruppen) zur DSFA einzuladen ist im Einzelfall auch denkbar wobei hier der Grad der Repräsentativität der eingeladenen Personen zu berücksichtigen ist. Einerseits dürfte statistische Repräsentativität im Sinne eines Querschnitts der Betroffenengruppen meist kaum zu erzielen sein, und hätte in jedem Fall auch nur begrenzten Wert: keinesfalls zulässig wäre es, hohe Risiken zu ignorieren nur weil die eingeladenen betroffenen Personen sie übersehen haben. Gute Ideen zur Risikoeindämmung, ein tieferes Verständnis für mögliche Akzeptanzprobleme und für wesentliche Herausforderungen und Risiken, die sich den betroffenen Personen stellen, können auch ohne einen repräsentativen Querschnitt erreicht werden. Werden jedoch nur wenig repräsentative Einzelpersonen eingeladen, dürfte sich die Frage stellen, ob diese die Perspektiven unterschiedlicher Betroffenen-Gruppen adäquat wiedergeben können, oder ob sogar ein bestimmtes Ergebnis erzeugt werden soll.

Wenn wesentliche Verarbeitungsvorgänge extern erfolgen oder wichtige Teile der IT-Infrastruktur durch Externe bereitgestellt werden, kann es empfehlenswert sein – soweit möglich – Vertreter dieser Dienstleister zur DSFA hinzu zu ziehen. Wie in Kapitel 1.3.3 dargelegt, sind Auftragsverarbeiter in jedem Fall verpflichtet, die Verantwortliche bei der DSFA zu unterstützen.

6 Phase III: Durchführung der DSFA

6.1 Vorgehen

Die Durchführungsphase hat drei Ziele:

- Bewertung der Risiken der vorgesehenen Verarbeitung für die Rechte und Freiheiten betroffener (natürlicher) Personen (Art. 35 Abs. 7 lit. c DSGVO).
- Auswahl von Abhilfemaßnahmen (Schutzmaßnahmen) zur Bewältigung der Risiken und Sicherstellung des Schutzes personenbezogener Daten (Art. 35 Abs. 7 lit. d DSGVO).
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der vorgesehenen Verarbeitungsvorgänge in Bezug auf den Zweck (Abs. 35 Abs. 7 lit. b DSGVO). (Damit Abschluss der bereits vorab begonnen Umsetzung von Abs. 35 Abs. 7 lit. b DSGVO (vgl. Kapitel 2.4)).

Es ist meist zweckmäßig, die Risikobeurteilung im Rahmen eines oder mehrerer partizipativer Workshops durchzuführen, in denen das gesamte DSFA-Team einschließlich etwaiger Betroffenenvertreter zusammenkommt.

Die in den vorherigen Phasen I. und II. erstellten Materialien dienen als Informationsgrundlage für die Risikobeurteilung. Sie sollten den Workshop-Teilnehmerinnen im Voraus zur Verfügung gestellt werden. Es ist sinnvoll, diese Informationen am Anfang des Workshops zu validieren und gegebenenfalls zu ergänzen, so dass ein gemeinsames Verständnis aller Teilnehmerinnen vorausgesetzt werden kann. Insbesondere sollte außerdem zu Anfang geprüft werden, ob tatsächlich alle Kategorien von betroffenen Personen und Beteiligten identifiziert worden sind.

6.2 Was sind Risiken im Sinne der DSGVO?

Die DSGVO definiert den Begriff des Risikos nicht. Das Kurzpapier Nr. 18 der Datenschutzkonferenz leitet aus den Erwägungsgründen 75 und 94 der DSGVO die folgende Definition ab:

> *Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigungen von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.*
> *Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.*[13]

Diese Definition wirft drei Fragen auf: Was sind „Schäden" (einschließlich „ungerechtfertigte Beeinträchtigungen von Rechten und Freiheiten"), was sind „Ereignisse", und wie sind Schadensschwere und Eintrittswahrscheinlichkeiten zu beurteilen? Die ersten beiden Fragen werden in den nächsten beiden Kapiteln 6.2.1 und 6.2.2 behandelt; der Bewertung der Schadensschwere und Eintrittswahrscheinlichkeit wendet sich Kapitel 6.4 zu.

Schäden und die Beeinträchtigung von Rechten und Freiheiten

Im Europarecht umfasst der Begriff „Rechte und Freiheiten natürlicher Personen" alle Grundrechte und Grundfreiheiten, wie sie sich in der Grundrechtecharta der Europäischen Union und der Europäischen Menschenrechtskonvention wiederfinden.[14] Art. 35 DSGVO verlangt also eine Beurteilung der Risiken, dass die Verarbeitung zur Verletzung von Grundrechten führen bzw. diese selber verletzen könnte.

So abstrakt formuliert ist der Auftrag des Art. 35 DSGVO schwierig zu fassen. Glücklicherweise operationalisiert ErwGr. 75 DSGVO daher die Idee von Risiken für Rechte und Freiheiten über den konkreteren Begriffs des Schadens: Demnach ist ein Risiko für Rechte und Freiheiten dann zu vermuten, wenn die Verarbeitung zu Schäden für natürliche Personen führen könnte. Gemäß der oben zitierten Risikodefinition der Datenschutzkonferenz muss also primär nach Schäden geschaut werden, um die abstrakten Risiken für Rechte und Freiheiten identifizieren und eindämmen zu können. ErwG. 75 unterscheidet zwischen physischen, materiellen und immateriellen Schäden. Alle drei Kategorien müssen in der DSFA betrachtet werden.

Physische Schäden sind körperliche Schäden. Beispiele dafür, wie Datenschutzmängel zu körperlichen Schäden führen können, wären bspw. fehlerhafte Daten oder Verarbeitungen die zu falscher medizinischer Behandlung führen. Dies gilt gleichermaßen, wenn Verstöße gegen die Vertraulichkeit (z. B. von Adressdaten oder Daten über Religion, Gesundheit, politische Überzeugung, sexuelle Orientierung oder Strafvergehen) Gewaltverbrechen, einschließlich Stalking, Vorschub leisten. Auch psychologische Schäden können unter die physischen Schäden gefasst werden, z. B. Angstzustände, Depressionen und andere psychische Schäden aufgrund von Vertraulichkeitsverlusten oder ungerechtfertigter Überwachung.

Materielle Schäden sind primär wirtschaftliche Schäden. Eine Vielzahl wirtschaftlicher Schäden, die durch Datenschutzverstöße (einschließlich fehlerhafter Daten/Verarbeitung) ausgelöst werden können, sind denkbar. In Betracht kommen z. B. berufliche Nachteile (illegitime Leistungs- und Verhaltenskontrolle, entgangene Einstellung oder Beförderung, Abmahnung, Jobverlust, etc.), Beschneidung staatlicher Leistungen (z. B. Arbeitslosengeld, Wohngeld, Sozialhilfe), Diskriminierung (z. B. bei Versicherungsabschlüssen oder Wohnungssuche), Identitätsdiebstähle und -betrug, Erpressung auf Grundlage vertraulicher Daten, sonstige finanzielle Verluste, Verlust oder Verfälschung von Nachweisen und Beweismaterialien (z. B. in einem Gerichts-

prozess oder im Rahmen der Notwendigkeit des Nachweises, dass Leistungen im Arbeitskontext erbracht wurden), Verlust erworbener Vorteile und Leistungen (z. B. Bonusprogramme, eingekaufte Güter oder Dienste), ungerechtfertigte Gebühren oder Bußgelder, sowie durch Datenschutzverstößen entstandene zeitliche und monetäre Mehraufwände (z. B. um Account-Entsperrungen zu erwirken oder Bearbeitungsfehler aufzuklären, einschließlich Kosten für eventuellen Rechtsbeistand) u.v.a.m.

Immaterielle Schäden können sowohl gesellschaftlicher, persönlicher als auch juristischer Natur sein. Diese Kategorie ist recht divers. Es ist daher hilfreich, vier Unterkategorien zu bilden:

- **Gesellschaftliche und soziale Nachteile.** Hierunter fallen etwa Rufschädigungen, Ansehensverluste und Bloßstellungen unterschiedlichen Schweregrads (von Peinlichkeit über Gesichtsverlust bis hin zu schwerer öffentlicher Bloßstellung oder Verleumdung), Mobbing, gesellschaftliche Diskriminierung, Beschneidung gesellschaftlicher Teilhabe etwa durch (ungerechtfertigte) Account-Sperrung oder fehlerhafter Daten (z. B. Alter, Vermerke in Hausverbotslisten).
- **Schädigung der Privatsphäre** beschreibt primär die „unheimliche" Erfahrung fehlender Kontrolle über die eigenen Daten und das Gefühl „ausgespäht zu werden", etwa aufgrund von Videoüberwachung, biometrischer Erkennung, Profiling, Tracking über Webseiten, Endgeräte und Applikationen oder der Veröffentlichung, Erwähnung oder Bezugnahme (z. B. bei Werbung) auf intime Details, wie Adresse, Schwangerschaft, Gesundheitszustand, sexuelle oder politische Orientierung, Religion, etc.
- **Einschüchterungseffekte** (engl. chilling effects) beschreiben einen Zustand, in dem Menschen aufgrund von Angst vor negativen Folgen davon absehen, ihre Rechte (z. B. auf politische Meinungsäußerung) wahrzunehmen oder ihre (legitime) Persönlichkeitsentfaltung auszuleben (z. B. durch Besuch bestimmter Lokale). Einschüchterungseffekte drohen vor allem bei Datenverarbeitungen, die ungerechtfertigte Überwachung darstellen.
- **(Ungerechtfertigte) Beeinträchtigung von Rechten.** Jede Verarbeitung personenbezogener Daten stellt per se eine Beeinträchtigung des Grundrechts auf Schutz personenbezogener Daten dar. Sie benötigt daher eine Rechtsgrundlage. Verarbeitungen ohne ausreichende Rechtsgrundlage stellen somit einen unmittelbaren Schaden dar, selbst wenn sie zu keinen weiteren, „konkreteren" Schäden führen. Gleiches gilt für Verarbeitungen, die den Datenschutzprinzipien (Art. 5 DSGVO) zuwider laufen, die Betroffenenrechte (Art. 12–22 DSGVO) nicht oder unzureichend umsetzen, oder auf andere Weise mit der DSGVO nicht konform sind: Sie alle stellen eine Verletzung des Rechts auf informationelle Selbstbestimmung und somit einen Schaden dar. Datenverarbeitungsvorgänge können aber auch andere Grundrechte verletzen oder zu deren Verletzungen führen, z. B. der Grundrechte auf Nicht-Diskriminierung oder Meinungsfreiheit.

Wie diese Ausführungen verdeutlichen, gibt es eine Vielzahl möglicher Schäden, die heute aus Datenverarbeitungsvorgängen hervorgehen können. Angesichts der fortschreitenden Digitalisierung aller Lebensbereiche ist das kaum verwunderlich. Das erklärt zum einen die Länge und Vielfalt der Liste, verdeutlicht zum anderen aber auch, warum eine DSFA oft sinnvoll ist.

Praxistipp **Umfassende Betrachtung**

Wichtig ist es die eigene Datenverarbeitung gut zu durchdenken, um den möglichen Eintritt relevanter Schäden und Szenarien zu identifizieren. Dabei sollte ruhig eine umfassende Betrachtung zugelassen werden, ohne sich davon jedoch zu sehr einschüchtern zu lassen bzw. den im ersten Augenblick vielleicht sehr groß wirkenden Arbeitsaufwand zu scheuen. Wichtig ist es, die für den eigenen zu prüfenden Datenverarbeitungsvorgang potentiellen Schäden zu identifizieren.

Ereignisse

Das „Ereignis" sind die Ursachen, die den Eintritt eines Schadens auslösen (d. h., zur „Verwirklichung des Risikos" führen). Diese dürften regelmäßig in der Nichteinhaltung der Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO), der Nichtgewährung der Betroffenenrechte (Art. 12–22 DSGVO) oder anderer Verstöße gegen die DSGVO liegen (z. B. ungerechtfertigte Datentransfers in Ausland). Typische Ereignisse sind:[15]

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Für die Betroffenen intransparente Verarbeitung
- Unbefugte Offenlegung von und Zugang zu Daten
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
- Verweigerung der Betroffenenrechte
- Verwendung der Daten durch die Verantwortliche zu inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener Daten
- Verarbeitung nicht richtiger Daten
- Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler)
- Verarbeitung über die Speicherfrist hinaus
- Die Verarbeitung selber, wenn der Schaden in der Durchführung der Verarbeitung liegt (z. B. weil diese illegitim ist/einer Rechtsgrundlage entbehrt)

6.3 Risikoidentifikation und Risikoanalyse

Das Standard-Datenschutzmodell (SDM) verdichtet und systematisiert sämtliche Anforderungen der DSGVO in Form von sieben Gewährleistungszielen. Diese werden im Anhang eingehend beschrieben und hier zunächst nur benannt:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

Im Katalog der Referenzmaßnahmen des SDM werden jedem Gewährleistungsziel spezifische technische und organisatorische Abhilfemaßnahmen zugeordnet, mittels derer das Ziel und die dahinter stehenden Anforderungen der DSGVO gewährleistet und der Eintritt von Schadensereignissen verhindert werden kann.

Um zu identifizieren, wie, durch wen oder was, und unter welchen Umständen, Schäden für die betroffenen Personen ausgelöst und die Einhaltung der Gewährleistungsziele gefährdet werden könnte, ist es hilfreich, in zwei Schritten vorzugehen. Im ersten Schritt werden auf Grundlage der identifizierten betroffenen Personen und Beteiligten, der Beschreibung der Verarbeitungsvorgänge und sonstigen Informationen zu Art, Umfang, Umständen und Zwecken der Verarbeitung, konkrete Schadensszenarien entwickelt und analysiert. Um systematisch vorzugehen, sollte für jede identifizierte Gruppe betroffener Personen gefragt werden, inwiefern Handlungen der Beteiligten oder sonstige Ereignisse (z. B. technische Fehlfunktionen, höhere Gewalt) zum Eintritt eines physischen, materiellen oder immateriellen Schadens führen könnten. Für jedes Szenario gilt es auch zu identifizieren, welche Gewährleistungsziele tangiert werden. Kapitel 6.3.1 beschreibt eine Methode zur Entwicklung und Analyse von Schadensszenarien.

Im zweiten Schritt wird von den Gewährleistungszielen ausgegangen. Es wird für jedes Ziel abgefragt, inwiefern Handlungen der Beteiligten oder sonstige Ereignisse zur Verletzung seiner Gewährleistung führen könnten und welche Schäden für betroffene Personen (neben der Datenschutzverletzung selbst, die einen Schaden an sich darstellt) dabei eintreten könnten.

Praxistipp **Risikoanalyse**

Dieses augenscheinlich redundante zweistufi e Vorgehen hat drei Vorteile: Zum einen vereinfacht es die Einbindung von Menschen ohne vertiefte Kenntnisse im Datenschutz (bspw. Mitarbeiterinnen von Fachabteilungen, betroffene Personen und ihre Vertreter). Wo genau in einer Verarbeitung das Risiko schadensauslösender Ereignisse liegt, hängt von den Details der jeweiligen Art und Umstände der Verarbeitung ab. Gerade die Mitarbeiterinnen von Fachabteilungen, die mit der Planung oder täglichen Ausführung der Verarbeitung betraut sind, haben hier oft den besten Einblick. Für Personen ohne datenschutzrechtliche Ausbildung ist es allerdings oft intuitiver, Risiken anhand konkreter Schadensszenarien zu ermitteln, als direkt Verletzungen der Gewährleistungsziele zu identifizieren..
Umgekehrt lässt sich die Einhaltung der DSGVO durch eine Analyse aus dem Blickwinkel der Gewährleistungsziele verlässlicher sichern, da diese die Anforderungen der DSGVO systematisch operationalisieren. Gleichzeitig profitiert die Gewährleistungsziel-Analyse vom Detailwissen um die Verarbeitung und ihrer genauen Umstände, welches bei der Entwicklung konkreter Szenarien zutage gefördert und verdichtet wird.
Schließlich hat die Risikoidentifikation und -analyse immer ein gewisses kreatives Element. Daher ist es nützlich, sie aus verschiedenen Blickwinkeln anzugehen.

Erstellung von Schadensszenarien

Um Schadensszenarien zu bilden, ist es hilfreich drei übergeordnete Fragen zu beantworten:[16]

1. Welche Schäden können für die identifizierten betroffenen Personen auf Grundlage der geplanten Verarbeitung oder der zu verarbeitenden Daten auftreten?
2. Durch welche Handlungen und Umstände kann es zum Eintritt der jeweiligen Schadensereignisse kommen? Welche Beteiligten sind wie involviert? Sind nichtmenschliche Risikoquellen relevant, z. B. technische Fehlfunktionen?
3. Welche Abhilfemaßnahmen sind bereits implementiert bzw. geplant?

Um ein systematisches Vorgehen zu gewährleisten, sollten die verschiedenen Schadenskategorien und Unterkategorien (physisch, materiell, immateriell, etc.) für jede identifizierte Betroffenen- und Beteiligten-Gruppe durchgearbeitet werden. Es gilt zu fragen, inwiefern solche Schäden für die betroffenen Personen auf Grundlage der Daten und ihrer Verarbeitung ausgelöst werden könnten, und welche Beteiligten daran wie involviert wären.

Es ist dabei hilfreich zu fragen, welche Informationen über die betroffenen Personen aus den erhobenen Daten herausgelesen werden und welche Beteiligten an diesen Informationen ein Interesse haben könnten. Ebenfalls sollte gefragt werden, ob Ver-

arbeitungsfehler (falsche Daten oder Auswertung), technische Fehlfunktionen oder höhere Gewalt Schäden auslösen könnten. In jedem Fall sollte das spezifische auslösende Element (der Faktor, der zum Eintritt des Ereignisses führt) identifiziert werden, damit dieses anschließend über Maßnahmen behandelt werden kann. Es sollte dabei auch erfasst werden, welche(s) Gewährleistungsziel(e) im jeweiligen Szenario tangiert werden.

Sowohl bei geplanten als auch laufenden Verarbeitungen werden fast immer bereits einige Abhilfemaßnahmen implementiert oder geplant sein. Diese Maßnahmen sollten bei der Bildung der Schadensszenarien miterfasst werden. Dabei ist es wichtig, klar zwischen bereits implementierten und nur geplanten Maßnahmen zu unterscheiden.

Zu jedem Schadensszenario sollten also die folgenden Angaben ermittelt werden:

- Beschreibung des Szenarios
- Betroffene Personen
- Personenbezogene Daten
- Beteiligte Akteure
- Möglicher Schaden für die betroffenen Personen
- Auslösende Elemente für den Schadenseintritt
- Tangierte Gewährleistungsziele
- Etwaige bereits bestehende technische und organisatorische Maßnahmen

Die gebildeten Szenarien sollten schriftlich festgehalten werden, z. B. in einer Szenario-Tabelle, wie der in Abbildung 2 gezeigten. Die in den weiteren Beurteilungsschritten erfolgende Risikobewertung sowie die ausgewählten Abhilfemaßnahmen können ebenfalls in der Tabelle festgehalten werden. Der Wert der Tabelle liegt dabei darin, dass sie die Szenarien in ihre wesentlichen Elemente aufschlüsselt und eine Übersicht verschafft.

Analyse an Hand der Gewährleistungsziele

Im nächsten Schritt wird die Identifikation und Analyse der Risiken mittels der Gewährleistungsziele vervollständigt.

Abbildung 2:
Szenario-Tabelle

Szenario-Nr.	Beschreibung des Szenarios	Betroffene Personen	Personenbezogene Daten	Beteiligte Akteure (Beteiligte)	Möglicher Schaden für die betroffene Person	Auslösende Elemente für den Schadenseintritt
1						
2						

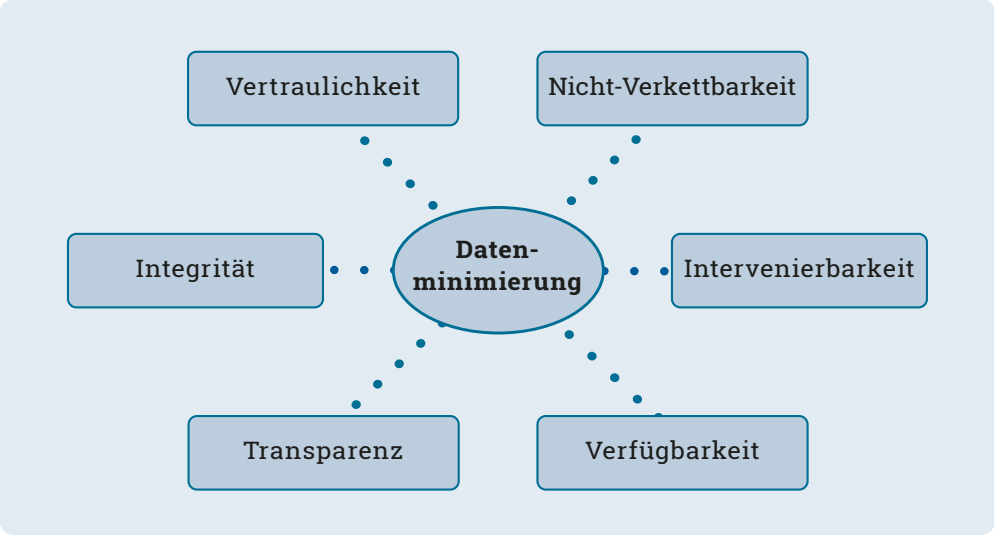


Abbildung 3:
Die Gewährleistungsziele

Für jedes Gewährleistungsziel sollten in Bezug auf jede Kategorie betroffener Personen folgende Fragen beantwortet werden:

1. Ist die Einhaltung des jeweiligen Gewährleistungsziels bei der gegenwärtig angedachten Gestaltung der Verarbeitung gewährleistet?
2. Unter welchen Umständen ist eine Verletzung des Gewährleistungsziels realistisch möglich? Auf welche Beteiligten oder nicht-menschliche Gefahrenquellen wäre die Verletzung zurückzuführen – was wären die auslösenden Elemente?
3. Welche zusätzlichen Schäden – über die Verletzung der im Gewährleistungsziel abgebildeten Datenschutzanforderungen hinaus – würden welche betroffenen Personen dabei erleiden?

Bei der Analyse der Gewährleistungsziele – sowie der späteren Auswahl von Maßnahmen – ist zu beachten, dass die Ziele z. T. strukturell in Spannung zueinander stehen. Je nach Systemgestaltung und Kontext kann bspw. ein „Mehr" an Intervenierbarkeit ein „Weniger" an Integritätsgewährleistung bedeuten, eine bessere Verfügbarkeit eine schwächere Vertraulichkeit, oder eine höhere Transparenz eine geringere Nichtverkettung, und umgekehrt. Diese Spannung ist in der sternförmigen Darstellung der Gewährleistungsziele (Abbildung 3) angedeutet. Wenn in einem

Bereits bestehende technische & organisatorische Abhilfemaßnahmen	Tangierte Gewährleistungsziele	Schwere der Schäden	Eintrittswahrscheinlichkeit	Risiko-Bewertung	Mögliche zusätzliche Abhilfemaßnahmen bzw. mögliche Weiterentwicklung bestehender Maßnahmen

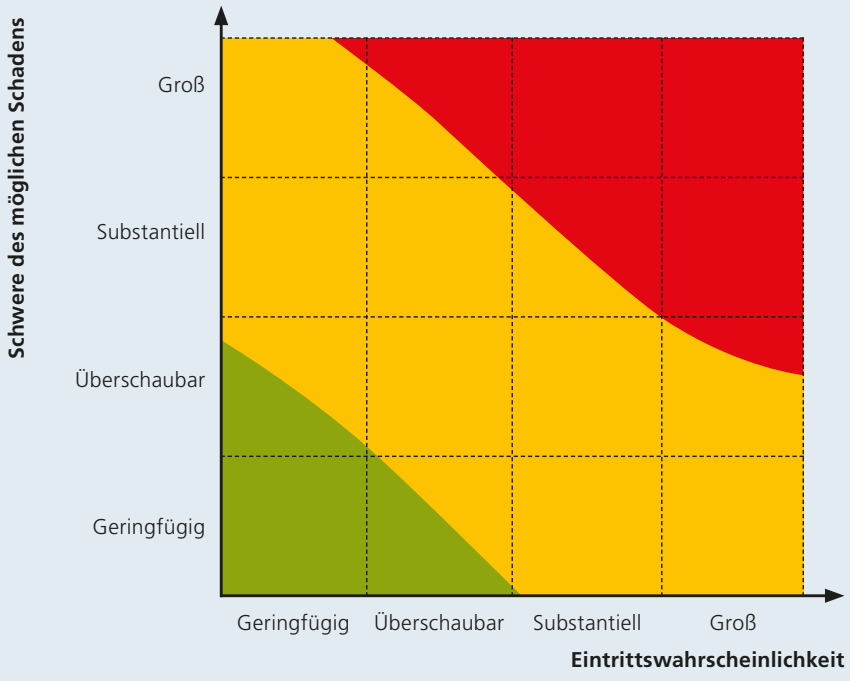
Schadensszenario mehrere Gewährleistungsziele tangiert werden und zwischen diesen Spannungen bestehen, ist es daher wichtig zu analysieren, welches der Ziele aus Sicht der betroffenen Personen prioritär zu gewährleisten ist. Dies ist wichtig, um später jeweils die für den Schutz der Rechte und Interessen der betroffenen Personen zweckmäßigsten Abhilfemaßnahmen auswählen zu können.

6.4 Risikobewertung

Nachdem die Risiken über die Betrachtung der Schadensszenarien und der Gewährleistungsziele erfasst und analysiert worden sind, gilt es diese zu bewerten. Risiken werden typischerweise in drei Stufen klassifiziert: **geringes Risiko**, **normales Risiko** und **hohes Risiko**.

Die Risikostufe ergibt sich wiederum aus der **Schadensschwere** und der **Eintrittswahrscheinlichkeit** der Ereignisse, die den Schaden auslösen bzw. diesen selber darstellen. Zur Einstufung von Schadensschwere und Eintrittswahrscheinlichkeit

Risikobewertung



Risikobereiche nach DSGVO

Geringes Risiko | Normales Risiko | Hohes Risiko

Quelle: Nach DSK Kurzpapier Nr. 18

Abbildung 4:
Risiko-Matrix

schlägt die Datenschutzkonferenz jeweils eine vierstufi e Skala vor: **geringfügig**, **überschaubar**, **substantiell** und **groß**. Die in Abbildung 4 dargestellte Risikomatrix verdeutlicht diese Zusammenhänge.

Weder die Schadensschwere noch die Eintrittswahrscheinlichkeit ist i. d. R. seriös quantifizierbar. Es sollte eine nachvollziehbare Argumentation anhand möglichst objektiver Kriterien dokumentiert werden, warum den Eintrittswahrscheinlichkeiten und Schadensschweren der verschiedenen Risiken ihre jeweiligen Skalenwerte zugeordnet wurden.

Die Schadensschwere ergibt sich dabei aus den physischen, materiellen oder immateriellen Auswirkungen auf die betroffene Person. Hier ist auch die Reversibilität des Schadens in Betracht zu ziehen (je schwieriger oder aufwendiger Reversibilität ist, desto schwerer der Schaden), und die Schwierigkeit für die betroffene Person, sich der Verarbeitung zu entziehen (auch aufgrund fehlender Kenntnis der Verarbeitung) oder diese selber oder gerichtlich prüfen zu lassen. Je mehr die Person der Verarbeitung „ausgeliefert" ist, desto schwerer wiegen etwaige mit der Verarbeitung verbundene Schäden.

Um die Eintrittswahrscheinlichkeit zu bewerten, ist es sinnvoll, die Motive und Fähigkeiten der Beteiligten in Betracht zu ziehen sowie den zur Auslösung des Ereignis nötigen Aufwand und die Belastbarkeit bestehender Abhilfemaßnahmen.

6.5 Auswahl von Abhilfemaßnahmen

Nachdem die Risiken analysiert und bewertet worden sind, gilt es, sie geeignet zu adressieren, d. h. nach Möglichkeit abzumildern oder ganz zu eliminieren. Dies erfolgt in den meisten Fällen über die Auswahl und Implementation von technischen und organisatorischen Maßnahmen. Alternativ kann die Verarbeitung auch angepasst oder ganz aufgegeben werden.

Art. 35 Abs. 7 lit. d DSGVO fordert, dass die Risiken „bewältigt" werden müssen und der Nachweis erbracht werden muss, dass die Verarbeitung die DSGVO einhält. „Bewältigung" wird gemeinhin als „Reduktion" bzw. „Eindämmung" verstanden. Zumindest müssen alle als „hoch" bewerteten Risiken mindestens insoweit reduziert werden, dass sie nur noch als „normal" zu bewerten sind, wobei sich bei „normalen" Risiken stets die Frage stellt, warum sie nicht auf ein „geringes" Niveau reduziert werden, sofern passende Maßnahmen verfügbar wären. Dies sollte im Einzelfall begründet werden.

Während der Risiko-Beurteilung muss für jedes identifizierte Risiko festgehalten werden, was genau zu seiner Verwirklichung führen könnte (bzw. was die auslösenden

Elemente sind) und welche Gewährleistungsziele genau dadurch tangiert werden. Auf dieser Grundlage können nun geeignete Maßnahmen ausgewählt werden. Diese können sowohl technischer als auch organisatorischer Art sein. Dabei müssen nicht zwangsläufig mmer zusätzliche Maßnahmen implementiert werden – es kann unter Umständen sinnvoller sein, bestehende Maßnahmen zu stärken.

Maßnahmen können entsprechend der Schwere der Risiken priorisiert werden. Nicht zulässig ist es, Maßnahmen allein unter Kostengesichtspunkten zu bewerten und hohe Risiken einfach in Kauf zu nehmen, weil die notwendigen Abhilfemaßnahmen für zu teuer befunden werden. Unzulässig ist es ebenfalls, hohe Risiken zu akzeptieren weil die Anzahl der betroffenen Personen als klein erachtet wird.

Hilfe bei der Auswahl passender Maßnahmen bieten die im Standard-Datenschutzmodell (SDM) aufgeführten Listen typischer Abhilfemaßnahmen, sowie der – sich noch in Arbeit befindliche – Maßnahmen-Katalog des Standard-Datenschutzmodells. Der Maßnahmen-Katalog ist in Bausteine gegliedert, die jeweils generische Maßnahmen für unterschiedliche datenschutzrechtliche Anforderungen beschreiben (z. B. Protokollierung, Trennung, Löschen und Vernichten, etc.). Für jeden Baustein wird angegeben, welche Gewährleistungsziele sich mittels der im Baustein beschriebenen Maßnahmen adressieren lassen. Das SDM enthält selber eine nach Gewährleistungszielen strukturierte Liste mit generischen Maßnahmen. Zusätzliche Orientierung bieten auch das „Knowledge Bases"-Dokument der französischen Datenschutz-Aufsichtsbehörde CNIL sowie die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Standards für den IT-Grundschutz.

Praxistipp **Listen typischer Abhilfemaßnahmen**

Standard-Datenschutzmodell V.2, Teil D
https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V2.0a.pdf

Maßnahmen-Katalog des Standard-Datenschutzmodell mit Bausteinen
https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

IT-Grundschutz-Kompendium des BSI
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

CNIL Privacy Impact Assessment: Knowledge Base:
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

6.6 Bewertung der verbleibenden Risiken und Entscheidung über weitere Schritte

In diesem Schritt ist zu bewerten, ob die ausgewählten Maßnahmen die identifizierten Risiken tatsächlich auf ein vertretbares Maß eindämmen. Verbleiben trotz der ausgewählten Maßnahmen noch hohe Risiken, so müssen entweder weitere, zusätzliche Abhilfemaßnahmen ausgewählt werden, bis die fraglichen Risiken ausreichend eingedämmt sind, oder die Datenschutz-Aufsichtsbehörde muss gemäß Art. 36 DSGVO (vgl. Kapitel 6.10) konsultiert werden, oder die Verarbeitung wird aufgegeben. Diese grundsätzliche Entscheidung muss die Verantwortliche treffen.

In jedem Fall darf die Verarbeitung nicht freigegeben werden, solange hohe Restrisiken verbleiben.

6.7 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Auf Grundlage der (Rest-)Risikobewertung sowie den in den vorherigen Phasen erarbeiteten Materialien kann die gemäß Art. 35 Abs. 7 lit. b DSGVO geforderte Bewertung der Notwendigkeit und der Verhältnismäßigkeit in Bezug auf den Zweck abgeschlossen werden. Dabei ist zu berücksichtigen, dass ausreichende Gründe, die gerade diese Art der Datenverarbeitung erfordern, dokumentiert wurden. Folgende Kriterien müssen dabei erfüllt werden:

1. Die Rechtmäßigkeit i. S. d. Art. 6 Abs. 1 DSGVO ist sichergestellt.
2. Die Datenschutzgrundsätze des Art. 5 Abs. 1 DSGVO wurden beachtet.
3. Sämtliche weiteren Anforderung der DSGVO (bspw. die Einhaltung der Betroffenenrechte) sind erfüllt und der Schutz der personenbezogenen Daten ist sichergestellt.
4. Alle Risiken sind ausreichend eingedämmt und es besteht kein hohes Risiko für die betroffenen Personen mehr.

6.8 Empfohlene Methodik: Partizipatives Workshop-basiertes Vorgehen

Unter Beachtung der in Kapitel 1.2 beschriebenen Verpflichtungen, steht es der Verantwortlichen frei zu entscheiden, wie die DSFA ausgeführt wird. Insbesondere für die Phase III. (Durchführungsphase), die den eigentlichen Kern der DSFA bildet, empfiehlt die in diesem Handbuch beschriebene DSFA-Methode eine partizipative Workshop-basierte Methodik. Der Grund hierfür ist, dass viele der für die DSFA benötigten Informationen zur geplanten Verarbeitung, den IT-Systemen und Geschäftsprozessen sowie den betroffenen Personen und weiteren Beteiligten sich zwar bereits in der Organisation finden, oftmals aber nicht in dokumentierter Form, sondern allenfalls als

intuitives Verständnis des Verarbeitungskontextes in den Köpfen der Mitarbeiterinnen. Für die DSFA müssen diese, in der Organisation oft verstreut vorliegenden Informationen, systematisch aufgearbeitet werden. Das lässt sich häufig m besten mittels Interviews und einem oder mehreren partizipativen Workshops umsetzen, in dem das DSFA-Team mit Vertretern der relevanten Organisationseinheiten und – falls möglich – betroffenen Personen bzw. ihren Vertretern gemeinsam Informationen sammelt, Risiken identifiziert, analysiert sowie bewertet und adäquate Abhilfemaßnahmen diskutiert.

Der genaue Ablauf der DSFA kann dann beispielsweise wie folgt aussehen: Die Schwellwertanalyse in Phase I. und die Zusammenstellung der Unterlagen und Informationen in Phase II. können von einzelnen Expertinnen oder einem kleinen Kernteam vorgenommen werden, möglicherweise auf Grundlage von Interviews mit Beschäftigten der jeweiligen Fachabteilungen. In Phase III. kommt dann das gesamte DSFA-Team – einschließlich möglicher Betroffenenvertreter – in einem oder mehreren Workshops zusammen, um die in Phase II. erstellten Informationen zu validieren und in einem partizipativen, dialogorientierten Prozess die Risikoidentifikation, -analyse und -bewertung vorzunehmen. Eine Konsultation der betroffenen Personen sollte in den Workshop integriert werden, sofern möglich.

Konkrete Vorschläge zu Abhilfemaßnahmen und insbesondere Anpassungen der geplanten Verarbeitung (z. B. Einsatz von kryptographischen Verfahren, Rollen- und Rechte -modellen, Reduktion bzgl. der Verarbeitung personenbezogener Daten im Sinne einer Datenminimierung) werden i. d. R. von Expertinnen erarbeitet werden müssen. Es ist allerdings sinnvoll, die in Frage kommenden Maßnahmen ebenfalls im Workshop zu diskutieren, da ihre praktische Anwendbarkeit und Effektivität auch vom Kontext der jeweiligen Geschäftsprozesse und Arbeitsabläufe, in denen sie greifen sollen, beeinflusst wird. Hier können Beschäftigte der betroffenen Fachabteilungen (in einem Pflegekontext z. B. das Pflegepersonal) wichtigen Input liefern.

6.9 DSFA-Bericht

Die Erstellung eines DSFA-Berichts schließt die Durchführungsphase der DSFA ab. Die Erstellung eines solchen Berichts ist Teil der allgemeinen Rechenschaftspflichten der Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO. Gemäß Art. 58 Abs. 1 lit. a DSGVO muss der Bericht auf Nachfrage der Datenschutz-Aufsichtsbehörde vorgezeigt werden. Die Entscheidung über eine weitergehende Veröffentlichung (z. B. auf der Unternehmenswebseite) ist der Verantwortlichen überlassen. Da die Veröffentlichung allerdings Transparenz und damit das Vertrauen in Verarbeitung (und letztlich die Organisation insgesamt) stärken kann, sollte sie in jedem Fall in Betracht gezogen werden, und wird auch von der Artikel-29 Datenschutzgruppe empfohlen.[17] Etwaige Geschäftsgeheimnisse oder Informationen, die als Angriffsvorlage missbraucht

werden könnten, können selbstverständlich aus einer veröffentlichen Fassung des Berichts entfernt werden. Was jedoch nicht geschehen sollte, ist das problematische Tatsachenverhältnisse in der veröffentlichten Fassung verschwiegen werden, so dass diese ein verzerrtes oder unwahres Bild der Verarbeitung und ihrer Risiken zeichnet. Der Bericht ist auch notwendig, um die folgenden Phasen IV. und V. der DSFA (Umsetzung und Nachhaltigkeit) verlässlich ausführen zu können.

Der Bericht sollte einer klaren Struktur folgen und die folgenden Informationen enthalten:

1. Beschreibung des Verarbeitungsvorgangs gemäß Art. 30 DSGVO
2. Weitere Informationen und Dokumentation der Verarbeitungsvorgänge sowie deren Zusammenhänge
3. Dokumentation der Rechtsgrundlage i. S. v. Art. 6 Abs. 1 DSGVO
4. Ergebnisse der Risikobeurteilung (Identifi ation, Analyse, Bewertung der Risiken)
5. Zur Eindämmung der Risiken ausgewählte Abhilfemaßnahmen
6. Angaben über etwaige Restrisiken einschließlich deren Rechtfertigung

6.10 Vorherige Konsultation der Aufsichtsbehörde

Ergibt die Bewertung des Restrisikos, dass hohe Risiken verbleiben, die die Verantwortliche nicht über weitere Maßnahmen eindämmen kann, so muss sie die Verarbeitung entweder aufgeben oder die zuständige Aufsichtsbehörde konsultieren. Diese Pflicht wird in Artikel 36 DSGVO geregelt. Gemäß Art. 36 Abs. 3 DSGVO muss die Verantwortliche der Aufsichtsbehörde dabei folgende Informationen zur Verfügung stellen:

- (Ggf.) Angaben zu den Zuständigkeiten der Verantwortlichen und etwaiger gemeinsamer Verantwortlicher oder Auftragsverarbeiter (Art. 36 Abs. 3 lit. a DSGVO);
- Zwecke und Mittel der beabsichtigten Verarbeitung (Art. 36 Abs. 3 lit. b DSGVO);
- (Informationen zu) den vorgesehenen Abhilfemaßnahmen und Garantien (Art. 36 Abs. 3 lit. c DSGVO);
- (Ggf.) Kontaktdaten der Datenschutzbeauftragten (Art. 36 Abs. 3 lit. d DSGVO);
- Bericht und etwaige sonstige Dokumentationen zur DSFA (Art. 36 Abs. 3 lit. e DSGVO)
- Alle sonstigen von der Aufsichtsbehörde angeforderten Informationen (Art. 36 Abs. 3 lit. f DSGVO)

Die Aufsichtsbehörde hat der Verantwortlichen innerhalb von 8 Wochen nach Erhalt des Konsultationsersuchens entsprechende schriftliche Empfehlungen (z. B. über mögliche zusätzliche Maßnahmen) zu geben. Bei komplexen Verarbeitungsvorgängen kann die Aufsichtsbehörde die Antwortfrist um weitere sechs Wochen verlängern.

7 Phase IV: Umsetzung der DSFA

7.1 Implementierung und Test der Abhilfemaßnahmen

Sofern die ausgewählten Abhilfemaßnahmen die Risiken ausreichend eindämmen können und die Verarbeitung weiter verfolgt werden soll, müssen diese Maßnahmen in einem weiteren Schritt umgesetzt werden.

Die Wirksamkeit der Maßnahmen ist zu testen soweit vor Freigabe der Verarbeitung möglich, und die Testergebnisse sind zu protokollieren. Die Tests sollten auf Basis eines zu erstellenden Testkonzepts nach Freigabe der Verarbeitung regelmäßig durchgeführt und die Ergebnisse protokolliert werden. Sollten in diesem Prozess neue Risiken identifiziert werden, müssen diese entsprechend der in Kapitel 6 beschriebenen Vorgehensweise behandelt werden.

7.2 Nachweis der Einhaltung der DSGVO und Freigabe der Verarbeitung

Nach der erfolgreichen Implementierung der Abhilfemaßnahmen kann gemäß Art. 35 Abs. 7 lit. d DSGVO dargelegt werden, dass die Verarbeitung die Anforderungen der DSGVO insgesamt erfüllt.

Mit dem Nachweis der Einhaltung der DSGVO insgesamt kann die Verarbeitung durch die Verantwortliche schließlich freigegeben werden.

8 Phase V: Fortlaufende Überprüfung der DSFA

Nach Abschluss eines DSFA-Zyklus müssen geeignete Maßnahmen zur Nachhaltigkeit getroffen werden. Hierzu gehört die Überwachung der Risiken und eine regelmäßige Überprüfung und Anpassung der DSFA im Rahmen von Änderungen, wenn sich hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen ergeben haben (Art. 5 Abs. 2, Art. 35 Abs. 11, Art. 39 Abs. 1 lit. b DSGVO).

Als Grundlage für ein solches Monitoring dient der DSFA-Bericht, insbesondere die in ihm enthaltene Dokumentation zu den Risiken, Abhilfemaßnahmen und dazugehörigem Testkonzept und Test-Protokollierungen. Dabei sollen bei den festgestellten Risiken ggf. eingetretene Änderungen verlässlich identifiziert und die Wirksamkeit der Abhilfemaßnahmen regelmäßig geprüft werden. Bei größeren Abweichungen bzgl. der Wirksamkeit der Abhilfemaßnahmen oder wesentlichen Änderungen der Verarbeitung sollten die vorhergegangenen Phasen II. bis IV. der DSFA erneut durchlaufen werden.

Etwaige Anpassungen im Rahmen der Risikobewertung, Abhilfemaßnahmen und des Testkonzepts sowie der Verarbeitung selber sind im DSFA-Bericht entsprechend zu dokumentieren.

Um ein verlässliches Monitoring der DSFA zu gewährleisten, ist es sinnvoll dieses in ein allgemeines Datenschutz-Management System, wie es etwa im Standard-Datenschutzmodell Teil D beschrieben wird, zu integrieren bzw. ein solches aufzubauen. Die Gewährleistung der Nachhaltigkeit und Durchführung der fortlaufenden Prüfung ist Aufgabe der Verantwortlichen bzw. von ihr beauftragter Dritter, ggf. unterstützt durch Mitglieder des DSFA-Teams und (in beratender Funktion) der Datenschutzbeauftragten.

ANHANG

A Beschreibung der Gewährleistungsziele

Gewährleistungsziele (früher Schutzziele) sind im Bereich der IT-Sicherheit schon seit vielen Jahren ein verbreiteter und bewährter Operationalisierungsansatz. Aus diesem Grund ist es empfehlenswert diesen Ansatz auch für die DSFA zu nutzen. In den vergangenen Jahren wurden die drei klassischen IT-Sicherheitsschutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) um drei spezifische Datenschutz-Gewährleistungsziele ergänzt, die die bekannten Datenschutzprinzipien operationalisieren: Transparenz als Voraussetzung für Nachvollziehbarkeit und damit für die Steuerung von Datenverarbeitungsprozessen, Nichtverkettbarkeit als Operationalisierung von Zweckbindung und Erforderlichkeit sowie Intervenierbarkeit als Operationalisierung von Betroffenenrechten. Die sechs Schutzziele decken die Datenschutzprinzipien des Art. 5 DSGVO vollständig ab (vgl. Tabelle 1) und sind mittlerweile Bestandteil des von der Konferenz der unabhängigen Datenschutzbehörden erarbeiteten Standard-Datenschutz-Modells. Zur weiteren Konkretisierung sind die Gewährleistungsziele mit Maßnahmen zu deren Erreichen auf unterschiedlichen Ebenen (Daten, Systeme, Prozesse) hinterlegt. Für die Praxis bedeutet die Nutzung von Gewährleistungszielen, dass die abstrakten normativen Vorgaben von Art. 5 DSGVO in konkrete funktionale Anforderungen übersetzt werden, die von den Ausführenden einer DSFA sehr viel besser verstanden werden, da sie es erlauben unmittelbare Verbindung zur Funktionalität und Implementierung des zu bewertenden Verfahrens herzustellen. Die folgenden Erläuterungen sind eine gekürzte Fassung des Textes im SDM-Handbuch (S. 24–33).

A.1 Datenminimierung

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken. Die Umsetzung dieses Minimierungsgebots hat einen durchgreifenden Einfluss auf Umfang und Intensität des durch die anderen Gewährleistungsziele bestimmten Schutzprogramms. Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grundsatz der Notwendigkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu verarbeiten, als für

Gewährleistungsziel	Anforderungen der DSGVO
Datenminimierung	Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)
	Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)
	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Verfügbarkeit	Verfügbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
	Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
	Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b, lit. c DSGVO)
	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DSGVO)
Integrität	Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)
	Integrität (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. b, DSGVO) I
	Fehler- und Diskriminierungsfreiheit beim Profiling (Art. 22 Abs. 3, 4 i. V. m. ErwGr. 71)
	Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DSGVO)
	Angemessene Überwachung der Verarbeitung (Art. 32, 33, 34 DSGVO)
Vertraulichkeit	Vertraulichkeit (Art. 5 Abs. 1 lit. f, Art. 28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 1 lit. b, Art. 32 Abs. 4, Art. 38 Abs. 5 DSGVO)
	Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DSGVO)
Intervenierbarkeit	Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DSGVO)
	Identifizierung und Authentifizierung (Art. 12 Abs. 6 DSGVO)
	Berichtigungsmöglichkeit von Daten (Art. 5 lit. d, Art. 16 DSGVO)
	Löschbarkeit von Daten (Art. 17 Abs. 1 DSGVO)
	Einschränkbarkeit der Verarbeitung von Daten (Art. 18 DSGVO)
	Datenübertragbarkeit (Art. 20 Abs. 1 DSGVO)
	Eingriffsmöglichkeit in Prozesse automatisierter Entscheidungen (Art. 22 Abs. 3 DSGVO)
	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
	Behebung und Abmilderung von Datenschutzverletzungen (Art. 33 Abs. 3 lit. d, 34 Abs. 2 DSGVO)
	Einwilligungsmanagement (Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO)
	Umsetzung aufsichtsbehördlicher Anordnungen (Art. 58 Abs. 2 lit. f und lit. j)

Tabelle 1:
Systematisierung der rechtlichen Anforderungen mit Hilfe der Gewährleistungsziele (Quelle: SDM 2.0a (2019), S. 28–29)

Nichtverkettbarkeit	Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)
Transparenz	Transparenz für Betroffene (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DSGVO)
	Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DSGVO)
Evaluierbarkeit (Art. 32 Abs. 1 lit. d DSGVO) ist als Prozess umzusetzen, der alle Anforderungen umfasst.	

das Erreichen des Verarbeitungszwecks benötigt werden. Das Minimierungsgebot erstreckt sich dabei nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Insbesondere muss sichergestellt werden, dass personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für den Zweck der Verarbeitung erforderlich ist. Datenminimierung reicht vom Design der Informationstechnik durch den Hersteller über ihre Konfiguration und Anpassung an die Betriebsbedingungen bis zu ihrem Einsatz in den Kernprozessen der Verarbeitung wie auch in den unterstützenden Prozessen zum Beispiel bei der Wartung der verwendeten Systeme.

Das Gewährleistungsziel Datenminimierung kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Festlegung von Voreinstellungen für betroffene Personen, die die Verarbeitung ihrer Daten auf das für den Verarbeitungszweck erforderliche Maß beschränken
- Bevorzugung von automatisierten Verarbeitungsprozessen
- Implementierung von Datenmasken, die Datenfelder unterdrücken, sowie automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
- Festlegung und Umsetzung eines Löschkonzepts
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten

A.2 Verfügbarkeit

Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass der Zugriff auf personenbezogene Daten und ihre Verarbeitung unverzüglich möglich ist und sie ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können. Die Verfügbarkeit umfasst die

konkrete Auffindbarkeit von Daten z. B. durch Datenmanagement-Systeme, strukturierte Datenbanken und Suchfunktionen und die Fähigkeit der verwendeten technischen Systeme, Daten auch für Menschen angemessen darzustellen. Darüber hinaus müssen zur Umsetzung der Verfügbarkeit Maßnahmen ergriffen werden, die sicherstellen, dass personenbezogene Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. Es müssen auch Maßnahmen umgesetzt werden, die die Verfügbarkeit der personenbezogenen Daten und der Systeme und Dienste, die diese verarbeiten, garantieren, wenn diese unter einer der Verarbeitung angemessenen zu erwartenden Last stehen und im Falle unerwartet hoher Last sicherstellen, dass der Schutz der personenbezogenen Daten nicht gefährdet ist. Sollte in Ausnahmefällen der Schutz personenbezogener Daten bezüglich der Verfügbarkeit dennoch verletzt werden, so ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der Verletzung getroffen werden.

Typische Maßnahmen zur Gewährleistung der Verfügbarkeit sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Dokumentation der Syntax der Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Erstellung eines Notfallkonzepts zur Wiederherstellung einer Verarbeitungstätigkeit
- Vertretungsregelungen für abwesende Mitarbeitende

A.3 Integrität

Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit sie berücksichtigt und korrigiert werden können. Dies gilt auch dann, wenn die zugrundeliegenden Systeme und Dienste unerwartet hoher Last unterliegen. Neben dem Aspekt der Fehlerfreiheit muss gerade bei automatisierten Bewertungs- und Entscheidungsprozessen der Aspekt der Diskriminierungsfreiheit gewahrt werden. Die Faktoren und Eigenschaften eines Bewertungs- oder Entscheidungsprozesses, die potenziell diskriminierende Wirkungen entfalten können, sind a priori im Rahmen der rechtlichen Prüfung festzustellen, bei der Umsetzung zu berücksichtigen und im Betrieb zu überwachen. Dieser Aspekt schlägt sich zum Beispiel durch Maßnahmen zur Bereinigung von Trainingsdaten und der Validierung von Ergebnissen bei der Anwendung von KI-Verfahren nieder.

Typische Maßnahmen zur Gewährleistung der Integrität oder zur Feststellung von Integritätsverletzungen sind:

- Einschränkung von Schreib- und Änderungsrechten
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts
- dokumentierte Zuweisung von Berechtigungen und Rollen
- Löschen oder Berichtigen falscher Daten
- Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen
- Prozesse zur Aufrechterhaltung der Aktualität von Daten
- Prozesse zur Identifizierung und Authentifizierung von Personen und Gerätschaften
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

A.4 Vertraulichkeit

Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der jeweiligen betroffenen Person haben. Die Vertraulichkeit personenbezogener Daten ist auch dann sicherzustellen, wenn die unterliegenden Systeme und Dienste unerwartet hoher Last unterliegen. Sollte in Ausnahmefällen die Vertraulichkeit dennoch verletzt werden, so ist sicherzustellen, dass Maßnahmen zur Behebung und Abmilderung der einhergehenden Verletzung des Schutzes personenbezogener Daten getroffen werden.

Typische Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

- Festlegung eines Berechtigungs- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
- Implementierung eines sicheren Authentifizierungsverfahrens
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle und spezifizierte, für die Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume)

- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen usw.)
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen
- Schutz vor äußeren Einflüssen (Spionage, Hacking)

A.5 Nichtverkettbarkeit

Das Gewährleistungsziel Nichtverkettbarkeit bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden. Je größer und aussagekräftiger Datenbestände sind, umso größer können die Begehrlichkeiten sein, die Daten über die ursprüngliche Rechtsgrundlage hinaus zu nutzen. Rechtlich zulässig sind derartige Weiterverarbeitungen nur unter eng definierten Umständen. Die Nichtverkettbarkeit soll durch technische und organisatorische Maßnahmen sichergestellt werden. Neben der Pseudonymisierung sind hierfür auch Maßnahmen geeignet, mit denen die Weiterverarbeitung organisations- bzw. systemseitig getrennt von der Ursprungsverarbeitung geschieht. Der Datenbestand kann bspw. durch Berechtigungssysteme und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

Typische Maßnahmen zur Gewährleistung der Nichtverkettbarkeit sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- Programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten
- Regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Trennung nach Organisations-/Abteilungsgrenzen
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
- Geregelte Zweckänderungsverfahren

A.6 Transparenz

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt. Transparenz ist für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich und eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in diese, soweit erforderlich, von betroffenen Personen informiert eingewilligt werden kann. Transparenz der gesamten Datenverarbeitung und der beteiligten Instanzen kann dazu beitragen, dass insbesondere betroffene Personen und Kontrollinstanzen Mängel erkennen und ggf. entsprechende Änderungen an der Verarbeitung einfordern können.

Typische Maßnahmen zur Gewährleistung der Transparenz sind:

- Dokumentation im Sinne einer Inventarisierung aller Verarbeitungstätigkeiten gemäß Art. 30 DSGVO
- Dokumentation der Bestandteile von Verarbeitungstätigkeiten insbesondere der Geschäftsprozesse, Datenbestände, Datenflüsse und Netzpläne, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten
- Dokumentation von Tests, der Freigabe und ggf. der Datenschutz-Folgenabschätzung von neuen oder geänderten Verarbeitungstätigkeiten
- Dokumentation der Faktoren, die für eine Profilbildung, zum Scoring oder für teilautomatisierte Entscheidungen genutzt werden
- Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
- Dokumentation von Einwilligungen, deren Widerruf sowie Widersprüche
- Protokollierung von Zugriffen und Änderungen
- Versionierung
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
- Dokumentation der Quellen von Daten, bspw. des Umsetzens der Informationspflichten gegenüber Betroffenen, wo deren Daten erhoben wurden sowie des Umgangs mit Datenpannen
- Benachrichtigung von Betroffenen bei Datenpannen oder bei Weiterverarbeitungen zu einem anderen Zweck
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte

- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept
- Bereitstellung von Informationen über die Verarbeitung von personenbezogenen Daten an Betroffene

A.7 Intervenierbarkeit

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Soweit der Verantwortliche über Informationen verfügt, die es ihm erlauben, die betroffenen Personen zu identifizieren, muss er auch Maßnahmen zur Identifizierung und Authentifizierung der betroffenen Personen, die ihre Rechte wahrnehmen möchten, treffen. Zur Umsetzung der Betroffenenrechte und aufsichtsbehördlicher Anordnungen sowie der Behebung und Abmilderung von Datenschutzverletzungen müssen die für die Verarbeitungsprozesse Verantwortlichen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen. Sollte sich die Verarbeitung personenbezogener Daten auf die Einwilligung der betroffenen Person stützen, müssen Maßnahmen ergriffen werden, die sicherstellen, dass die personenbezogenen Daten nur verarbeitet werden, wenn eine Einwilligung der betroffenen Person vorliegt und diese nicht widerrufen wurde.

Für informationstechnische Verarbeitungen, auf die betroffene Personen selbst Zugriff haben (z. B. Anwendungen auf dem Smartphone) und für die unterschiedliche Datenschutzeinstellungen vorgesehen sind, sind durch den Verantwortlichen datenschutzfreundliche Voreinstellungen (Data Protection by Default) festzulegen und weitere Maßnahmen zu treffen. Diese weiteren Maßnahmen müssen die Betroffenen in die Lage versetzen, Konfigurationen differenziert nach den jeweiligen Verarbeitungszwecken selbst vorzunehmen und zu entscheiden, welche Verarbeitungen sie gestatten wollen, die über das erforderliche Minimum hinausgehen.

Typische Maßnahmen zur Gewährleistung der Intervenierbarkeit sind:

- Maßnahmen für differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen an Verarbeitungstätigkeiten sowie an den technischen und organisatorischen Maßnahmen

- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
- Betreiben einer Schnittstelle für strukturierte, maschinenlesbare Daten zum Abruf durch Betroffene
- Identifizierung und Authentifizierung der Personen, die Betroffenenrechte wahrnehmen möchten
- Einrichtung eines Single Point of Contact für Betroffene
- Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- Bereitstellen von Optionen für Betroffene, um Programme datenschutzgerecht einstellen zu können

B Weiterführende Literatur

Artikel-29-Datenschutzgruppe, „Leitlinien in Bezug auf Datenschutzbeauftragte (‚DSB')", 16/DE, WP 243 rev. 01, Brüssel, 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

––, „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'", 17/DE, WP 248 rev. 01, Brüssel, 2017. http:// ec.europa.eu/newsroom/document.cfm?doc_id=44137

CNIL (Commission Nationale de l'Informatique et des Libertés), „Privacy Risk Assessment: Knowledge Bases", Paris, 2018. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

––, „Privacy Risk Assessment: Templates", Paris, 2018. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

––, „Privacy Risk Assessment: Methodology", Paris, 2018. https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

De, Sourya Joyee, and Daniel Le Métayer, Privacy Risks Analysis, Morgan & Claypool, San Rafael, 2016.

ISO/IEC 29134:2017, „Information technology - Security techniques - Guidelines for privacy impact assessment", Internationale Organisation für Normung (ISO), Genf, 2017.

Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK), „Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (Version 2.0a)", 2019. https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V2.0a.pdf

––, „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO", Kurzpapier 5, 2017. https://www.datenschutzkonferenz-online.de/kurzpapiere.html

––, „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist", Version 1.1, 2018. https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

––, „Risiko für die Rechte und Freiheiten natürlicher Personen", Kurzpapier 18, 2018. https://www.datenschutzkonferenz-online.de/kurzpapiere.html

Mester, Britta, Nicholas Martin, Ina Schiering, Michael Friedewald und Dara Hallinan, Schwerpunktheft „Datenschutz-Folgenabschätzung", Datenschutz und Datensicherheit (DuD), 3/2020.

Wright, David und Paul De Hert (Hrsg.), Privacy Impact Assessment, Springer, Dordrecht, Heidelberg, London, New York, 2012.

C Abkürzungen

BDSG Bundesdatenschutzgesetz

BMBF Bundesministerium für Bildung und Forschung

BSI Bundesamt für Sicherheit in der Informationstechnik

CNIL Commission Nationale de l'Informatique et des Libertés

DSFA Datenschutz-Folgenabschätzung

DSGVO Datenschutz-Grundverordnung

DSK Datenschutzkonferenz (kurz für: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder)

ENISA European Union Agency for Cybersecurity (früher: European Network and Information Security Agency)

ErwGr Erwägungsgrund

GPS Globales Positionsbestimmungssystem

GrCh Charta der Grundrechte der Europäischen Union (kurz: Grundrechte-Charta)

HR Human Resource (engl. für Personalwesen)

IT Informationstechnik

lit. Littera (lateinisch für: Buchstaben)

NGO Non-governmental organization (engl. für Nichtregierungsorganisation)

ÖPNV Öffentlicher Personennahverkehr

Rn. Randnotiz

SDM Standard-Datenschutzmodell

D Anmerkungen

1. Friedewald, M.; Bieker, F.; Obersteller, H. et al. (2017): Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz. Dritte, überarbeitete Auflage. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt).
2. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) (2017): Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Kurzpapier 5;
   DSK (2018): Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18.
3. Gonscherowski, S.; Herber, T.; Robrahn, R. et al. (2017). Durchführung einer Datenschutz-Folgenabschätzung gemäß 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)
4. DSK (2019). Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (Version 2.0a).
5. Im Zweifel wurden auch weitere Sprachversionen herangezogen, um sprachliche Unterschiede zu erkennen, ohne dabei eine detaillierte Auswertung der hinzugezogenen Sprachversionen vorzunehmen.
6. Hierzu im Einzelnen bei Arning/Rothkegel, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG Kommentar, Art. 4 Rn. 164 ff., womit aber je nach vertretener Meinung auch ein Betriebs- oder Personalrat in der Pflicht stehen kann.
7. Ebenso bspw. Reibach, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG Kommentar, Art. 35 Rn. 9.
8. Artikel-29 Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte, WP 243 rev. 01, 5.4.2017, S. 16–17
9. Artikel-29 Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt",
   WP 248 rev. 01, 4.10.2017, S. 8
10. DSK (2018): „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist", https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.

11. Europäischer Datenschutzausschuss (EDS), Stellungnahme 5/2018 zu der von den zuständigen Aufsichtsbehörden Deutschlands entworfenen Liste der Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Artikel 35 Absatz 4 DSGVO), 25.09.2018. Verfügbar unter: https://edpb.europa.eu/sites/edpb/fi es/fi es/fi e1/2018-09-25-opinion_2018_art_64_de_sas_dpia_list_de_0.pdf Zuletzt aufgerufen am 16.01.2020.

12. Artikel-29 Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung, S. 10–13

13. DSK (2018): Risiko für die Rechte und Freiheiten natürlicher Personen, S. 1.

14. Bieker, F. und Bremert, B. (2020) Identifizierung von Risiken für die Grundrechte von Individuen. Auslegung und Anwendung des Risikobegriffs der DS-GVO, in: Zeitschrift für Datenschutz (ZD) 10(1), S. 7–14.

15. Basierend auf: DSK (2018): Risiko für die Rechte und Freiheiten natürlicher Personen, S. 3

16. Basierend auf: DSK (2018): Risiko für die Rechte und Freiheiten natürlicher Personen, S. 2

17. Artikel-29 Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung, S. 22

E Über die Autoren

Dr. Nicholas Martin

Wissenschaftlicher Mitarbeiter und Projektleiter im Competence Center Neue Technologien am Fraunhofer-Institut für System und Innovationsforschung in Karlsruhe

Dr. Michael Friedewald

Leiter des Geschäftsfeldes Informations- und Kommunikationstechnik am Fraunhofer-Institut für System und Innovationsforschung in Karlsruhe; Koordinator des vom BMBF geförderten „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“

Prof. Dr. Ina Schiering

Institut für Information Engineering der Ostfalia Hochschule für angewandte Wissenschaften; forscht zu Privacy by Design in Internet of Things Anwendungen; Sprecherin des vom Niedersächsischen Ministeriums für Wissenschaft und Kultur geförderten Forschungsschwerpunkt SecuRIn.

Dr. Britta Alexandra Mester

RAin, Justiziarin und Leiterin Akademie bei der datenschutz nord GmbH, Lehrbeauftragte C3L Universität Oldenburg, Herausgeberin DuD - Datenschutz und Datensicherheit, Lehrende BBS Wechloy

Dr. Dara Hallinan

Wissenschaftlicher Mitarbeiter im Bereich Immaterialgüterrechte in verteilten Informationsinfrastrukturen am FIZ Karlsruhe - Leibniz-Institut für Informationsinfrastrukturen

Prof. Dr. Meiko Jensen

Professor für IT-Sicherheit und Datenschutz am Institut für Angewandte Informatik, Fachhochschule Kiel; Adjunct Associate Professor für Cybersecurity an der Syddansk Universitet, Dänemark.

Wer personenbezogene Daten verarbeitet und dadurch die Rechte von Personen gefährden könnte, muss seit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) eine Datenschutz-Folgenabschätzung durchführen. Dabei handelt es sich um eine systematische Risikoanalyse, die bereits vor Inbetriebnahme einer Datenverarbeitung zu erstellen ist und zum Ziel hat, etwaige Gefahren zu erkennen, diese in ihrer Tragweite zu bewerten und geeignete Abhilfemaßnahmen zu ergreifen.

Dieses Praxishandbuch gibt eine knappe Einführung in die Vorgaben der DSGVO an die Datenschutz-Folgenabschätzung und die damit verbundenen Ziele. Es erläutert die Voraussetzungen für die erfolgreiche Durchführung und erläutert Schritt für Schritt, wie eine Datenschutz-Folgenabschätzung in fünf Phasen praktisch umgesetzt werden kann.

Der Inhalt:

- Datenschutz-Folgenabschätzung in der DSGVO
- Phasen einer Datenschutz-Folgenabschätzung
- Risiken in Sinne der DSGVO
- Identifi ation und Bewertung von Datenschutz-Risiken

Die Zielgruppen:

- Datenschutzbeauftrage
- Verantwortliche in Unternehmen und Verwaltung

ISBN 978-3-8396-1594-2

ISBN 978-3-8396-1594-2
9 783839 615942

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung