

Durchführung & Chancen einer Datenschutz- Folgenabschätzung

Nutzen der DSFA bei der Entwicklung
und zur Verbesserung innovativer
Geschäftsmodelle

SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE



DIGITALES BUSINESS · TECHNOLOGIE · MEDIEN

Inhaltsverzeichnis

1	Einleitung.....	1
1.1	Intention des Whitepapers und Ausgangslage.....	1
1.2	Schwerpunkte des Whitepapers	2
1.3	Anwendung des Whitepapers in der Praxis	2
2	Vorbereitungsphase	4
2.1	Ablauf der Vorbereitungsphase (Musterbeispiel).....	4
2.2	Festlegung der Verarbeitungstätigkeit (Scope).....	5
2.3	Notwendigkeit der DSFA (Schwellwertanalyse)	6
2.4	Planung, Interviews und Absprachen	8
2.5	Ermittlung beteiligter Akteure.....	9
2.6	Informationsbeschaffung	10
3	Durchführungsphase I	11
3.1	Aufbau des DSFA-Berichts (Musterbeispiel).....	11
3.2	Geltungsbereich der DSFA (Abgrenzung des Prüfungsgegenstands).....	12
3.3	Beschreibung der Verarbeitungstätigkeit.....	12
3.4	Zwecke der Verarbeitung	13
3.5	Rechtsgrundlagen	14
3.6	Zugriffs- und Berechtigungskonzept.....	17
3.7	Löschkonzept	18
3.8	Weitergabe an Dritte	19
3.9	Informationspflichten und Wahrung der Betroffenenrechte	21
3.10	Notwendigkeit und Verhältnismäßigkeit.....	22
4	Durchführungsphase II: Risikoanalyse.....	26
4.1	Aufbau der Risikoanalyse (Musterbeispiel).....	26
4.2	Gewährleistungsziele definieren	27
4.3	Risiken erfassen und beschreiben	28
4.4	Risiken bewerten – Eintrittswahrscheinlichkeit und Schadenshöhe bestimmen	31
4.5	Risiken bewerten – Risikomatrix erstellen und Risikoklasse bestimmen	32
4.6	Risiken behandeln – Technische und organisatorische Maßnahmen prüfen	32

4.7	Neubewertung unter Einbeziehung getroffener Maßnahmen	33
5	Finalisierungs- und Überprüfungsphase.....	34
5.1	Umsetzung der Maßnahmen.....	34
5.2	Abschließende Beurteilung.....	34
5.3	Konsultation der Aufsichtsbehörde.....	34
5.4	Freigabe, Überprüfung und Wiedervorlage	35
6	Empfehlungen aus der Praxis	37
6.1	Wichtigkeit guter Vorbereitung, Planung und Dokumentation	37
6.2	Lösungsorientierte Herangehensweise	37
6.3	Einholung von Fachexpertise.....	37
7	Anhang: DSFA-Modelle.....	38
7.1	Standard-Datenschutzmodell der DSK	38
7.2	PIA der CNIL	39
8	Literaturverzeichnis	40



1. Einleitung

Eine Datenschutz-Folgenabschätzung („DSFA“) ist in Art. 35 der Datenschutz-Grundverordnung („DSGVO“) zur Prüfung riskanter Datenverarbeitungen vorgeschrieben. Sie stellt mehr als nur eine bloße Datenschutzanforderung dar und bietet Unternehmen zudem Vorteile. Wenn die DSFA von Anfang an systematisch in die Entwicklung neuartiger und innovativer datenbasierter Produkte und Dienstleistungen integriert wird, hilft sie nicht nur bei der Identifikation und Behandlung von unerkannten oder unterschätzten Datenschutzrisiken, sondern auch bei der allgemeinen Optimierung der Geschäftsprozesse, des Datenschutz-Managements und der Compliance. Dieses Whitepaper gibt einen praxisorientierten Überblick über die zentralen Fragen, die sich bei der Planung, Durchführung, Dokumentation und Überprüfung einer DSFA stellen. Es zeigt, welche entscheidende Bedeutung die Risikoanalyse im Rahmen der DSFA hat und wie sie Grundlage zur Anpassung von Prozessen und Vorgängen sein kann. Ergänzt wird das Whitepaper durch zahlreiche Beispiele zu bekannten Tools und Anwendungsfällen.

1.1 Intention des Whitepapers und Ausgangslage

Die deutschen Aufsichtsbehörden für den Datenschutz haben zwar mit dem Standard-Datenschutzmodell („SDM“) ein umfassendes Referenzwerk zu Fragen der Gewährleistungsziele und Abhilfemaßnahmen im Rahmen der Risikobetrachtung geschaffen, jedoch eignet sich dieses nur bedingt als praktische Handlungsanleitung. Gleiches gilt für die Leitlinien der Artikel-29-Datenschutzgruppe¹ zur DSFA, die schwerpunktmäßig die sog. Schwellwertanalyse und die Frage des Vorhandenseins eines hohen Risikos in den Blick nehmen. Auch das Kurzpapier Nr. 5 der Datenschutzkonferenz² („DSK“) bildet nur eine grobe Modellierung der Vorgehensweise ab und reicht nicht für eine umfassende Abwägung. Mit dem sogenannten „Planspiel“ haben Beschäftigte von deutschen Aufsichtsbehörden anhand eines fiktiven Musterbeispiels zwar den möglichen Ablauf und die Dokumentation einer DSFA nach dem SDM in praktischer Hinsicht erläutert. Es lässt es sich jedoch nicht ohne Weiteres auf den unternehmerischen Alltag übertragen, da ein Vorgehen wie im Planspiel oftmals zu einem unverhältnismäßigen organisatorischen und dokumentarischen Aufwand führen würde. Zudem ist die Anwendung des SDM nicht für alle Verarbeitungsvorhaben sachgerecht.

Aktuell fehlt es an einer praxisnahen und gut anwendbaren Handlungsanleitung von den Aufsichtsbehörden – obwohl die DSFA nach Art. 35 eines der wichtigsten Instrumente der

¹ Die Artikel-29-Datenschutzgruppe ist der Vorgänger des heutigen Europäischen Datenschutzausschusses („EDSA“), ein unabhängiges Gremium der Europäischen Union, welches die EU-weite einheitliche Anwendung der DSGVO sicherstellen soll (Art. 68, 70 DSGVO). Dazu veröffentlicht der EDSA Leitlinien zur Auslegung einzelner Regelungen der DSGVO, an denen sich die nationalen Datenschutzbehörden orientieren. Der EDSA hat die Leitlinien der Artikel-29-Datenschutzgruppe zur DSFA in seiner ersten Plenarsitzung bestätigt.

² Die Datenschutzkonferenz ist ein gemeinsames Gremium der deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie tagt regelmäßig und gibt insbesondere Entschlüsse, Beschlüsse, Orientierungshilfen und Stellungnahmen zum Datenschutz ab, um die einheitliche Anwendung des Datenschutzrechts zu erreichen.

DSGVO darstellt. Um dieser Unsicherheit entgegenzuwirken, soll dieses Whitepaper mit einem verständlichen und strukturierten Ansatz die Vorgehensweise bei einer DSFA praxisnah aufzeigen und diese mit Schemata zum Ablauf schnell erfassbar machen. Zum besseren Verständnis werden die Prüfungsschritte zudem beispielhaft anhand der Einführung einer neuen Software im Unternehmen erläutert.

1.2 Schwerpunkte des Whitepapers

Zunächst sollte ein Schwerpunkt auf die Vorbereitungsphase der DSFA gelegt werden. Die Maßnahmen im Vorfeld, insbesondere die Informationssammlung, die Ermittlung wesentlicher Aspekte der Verarbeitung und die Absprachen im Unternehmen, sind essenziell für eine erfolgreiche Durchführung der DSFA. Nicht zuletzt hängt die Frage, ob eine DSFA durchgeführt werden muss, maßgeblich davon ab, ob den bearbeitenden Personen alle relevanten Informationen zur Verfügung stehen, um eine belastbare Einschätzung des Datenschutzrisikos vornehmen zu können. Deshalb sollte in diesem Zusammenhang auch die Schwellwertanalyse nicht unterschätzt werden.

Hauptschwerpunkt wird nach der Vorbereitungsphase aber die Durchführung einer DSFA und ihre Dokumentation in Form eines DSFA-Berichts sein. Je nachdem, welches Vorgehensmodell gewählt wird, müssen hierfür zunächst die möglichen Rechtsgrundlagen, ihre Grenzen und Anforderungen geklärt werden, insbesondere vor dem Hintergrund spezialgesetzlicher Regelungen, wie etwa aus dem Gesundheitsbereich. Daneben liegt auch ein besonderes Augenmerk auf der Prüfung der Verhältnismäßigkeit einer Verarbeitungstätigkeit. Darüber hinaus sind auch die Anforderungen an die Wahrung der Betroffenenrechte ein wichtiger Ausgangspunkt für die Compliance.

Wichtigster Punkt bei der Durchführung der DSFA ist jedoch die Risikoanalyse. Die Erfassung und Bewertung von Risiken sowie die Umsetzung organisatorischer und technischer Maßnahmen ist dabei nicht nur als bloße Anforderung aus der DSGVO zu sehen, sondern kann auch unternehmensintern risikohafte Prozesse aufdecken und Gegenmaßnahmen ermöglichen – insbesondere noch bevor es zu einem Datenschutzvorfall kommt oder die Aufsichtsbehörde auf die Verarbeitungstätigkeit aufmerksam wird.

Ohne IT und Software ist die heutige Unternehmens- und Arbeitswelt kaum mehr vorstellbar. Darum wird dieses Whitepaper auch an vielen Stellen konkrete Bezüge zu weit verbreiteter Software und repräsentativen Anwendungsfällen nehmen, wie Microsoft 365, Videoüberwachung, 360-Grad-Feedback, dem Einsatz künstlicher Intelligenz und automatisierter Prozesse.

1.3 Anwendung des Whitepapers in der Praxis

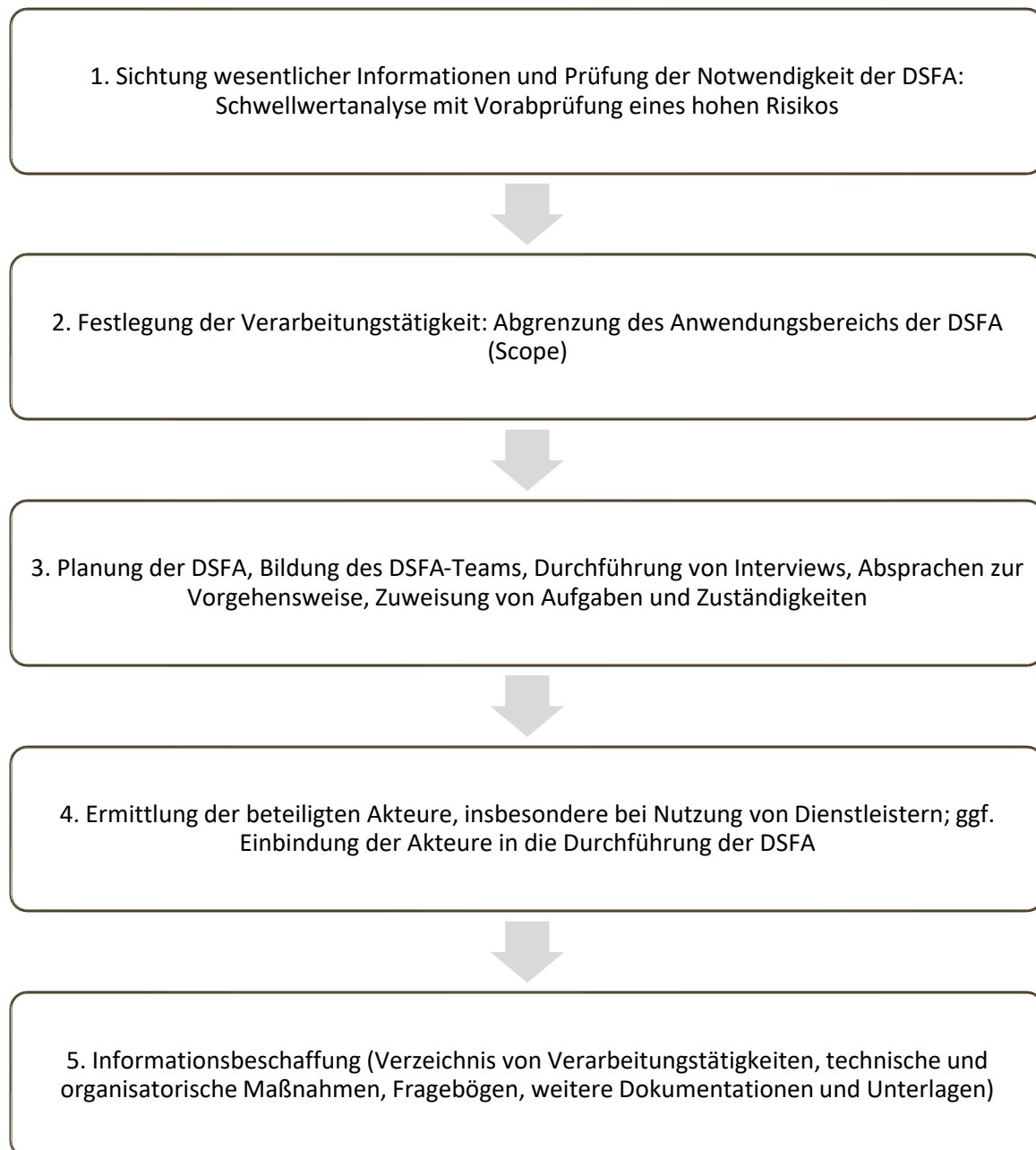
Um sowohl den Einstieg in die Struktur und Vorgehensweise als auch die Vertiefung und Ergänzung des vorhandenen Wissens durch dieses Whitepaper zu gewährleisten, werden zu Beginn jedes Kapitels beispielhaft einfach zugängliche und übersichtliche Ablaufschemata präsentiert, die der praktischen Anwendung im Unternehmen dienen und die wesentlichen Vorgänge zeigen. Anschließend erfolgt die tiefere Erläuterung der einzelnen Schritte. Dabei werden diese in gold umrandeten Kästen auf die Einführung einer Software angewendet und in den goldenen Kästen praktische Beispiele und bekannte Anwendungsfälle

erläutert. Sie können auch ohne Probleme übersprungen bzw. losgelöst vom Fließtext betrachtet werden, denn der Fließtext setzt nahtlos am zuvor Geschriebenen an.



2. Vorbereitungsphase

2.1 Ablauf der Vorbereitungsphase (Musterbeispiel)



2.2 Festlegung der Verarbeitungstätigkeit (Scope)

Die Datenschutz-Folgenabschätzung bezieht sich auf die Prüfung von einer oder mehreren Verarbeitungstätigkeiten, die einer Risikoanalyse unterzogen werden sollen (Art. 35 Abs. 1 DSGVO). Dabei können ähnliche Verarbeitungstätigkeiten (hinsichtlich Art, Umfang und Zweck) mit **ähnlichen Risiken** in einer *einzig*en DSFA untersucht werden (auch sog. thematische DSFA).³ Wie aus Erwägungsgrund 92 DSGVO hervorgeht, dürfen hierbei auch **ökonomische Gesichtspunkte** eine Rolle spielen. So könne eine DSFA etwa für eine gemeinsame Anwendung von mehreren Beteiligten vorgenommen werden. Da bei einer DSFA neue Situationen untersucht werden sollen, brauchen bereits geprüfte Verarbeitungen nicht erneut abgebildet werden.⁴ Allerdings ist die DSFA ein fortlaufender Prozess, weshalb eine regelmäßige Wiederholung nötig ist.

Zu mehreren Verarbeitungstätigkeiten im Zusammenhang mit Videoüberwachung: Ein Unternehmen hat mehrere Standorte, an denen es beispielsweise die Einführung einer ähnlich ablaufenden **Videoüberwachung** plant. In diesem Fall muss nicht für jeden Standort eine eigene DSFA vorgenommen werden, sondern es ist die Zusammenfassung der Videoüberwachung in einer DSFA möglich.

Praxisbeispiel 2-1

*Der Begriff „**Verarbeitungsvorgang**“ (aus Art. 35 DSGVO) überschneidet sich regelmäßig mit dem der „**Verarbeitungstätigkeit**“ (aus Art. 30 DSGVO) und kann der Einfachheit halber nachfolgend synonym betrachtet werden.*

Auch wenn die Festlegung der Verarbeitungstätigkeit zunächst selbstverständlich wirkt, kann sie im Detail durchaus Schwierigkeiten mit sich bringen. Zudem ist die Festlegung maßgeblich für die spätere Abgrenzung des **Geltungsbereichs**. Deshalb sollten bereits bei diesem ersten Schritt die Art und der Umfang der Verarbeitungstätigkeit eindeutig bestimmt werden.

Zur Bestimmung der Verarbeitungstätigkeit am Beispiel von Microsoft 365: Eine Datenschutz-Folgenabschätzung für die „*Microsoft Cloud*“ durchzuführen dürfte nicht konkret genug sein. Microsoft bietet eine Vielzahl von Diensten und Anwendungen an, die innerhalb der Cloud laufen und kaum mittels einer einzigen DSFA in Gänze abgedeckt werden könnten. Bei solch großen Technologieanbietern ist daher eine Abgrenzung der Verarbeitung auf bestimmbar Bereiche notwendig. Werden etwa nur bestimmte Produkte von Microsoft 365 eingesetzt, könnte die Verarbeitungstätigkeit beispielsweise „*Nutzung von Teams, OneDrive, SharePoint und Azure Active Directory innerhalb von Microsoft 365 am Standort X*“ lauten. Durch diese Konkretisierung kann die DSFA auch klar zu anderen genutzten Diensten und Produkten sowie Anwendungszusammenhängen abgegrenzt sowie der Umfang der Informationsbeschaffung präzisiert werden.

Praxisbeispiel 2-2

³ Art. 35 Abs. 1 S. 2 DSGVO sowie DSK: Kurzpapier Nr. 5, S. 1.

⁴ Art.-29-DS-Gruppe: WP 248, S. 8.

Wird dabei festgestellt, dass die betrachteten Verarbeitungsvorgänge doch erheblich voneinander abweichen, sollten diese in verschiedene DSFA aufgeteilt werden.

Anwendungsbeispiel Software-Einführung: Nachfolgend wird die Einführung einer neuen Cloud-Software eines Drittanbieters als Anwendungsbeispiel bei verschiedenen Prüfungspunkten einer DSFA herangezogen. Dabei wird angenommen, dass die Software für die Erfüllung von Dienstleistungen im Rahmen von Kundenverträgen genutzt wird, wobei auch eine KI-Unterstützung zur Vorbereitung und Beschleunigung der ablaufenden Prozesse geplant ist.

2.3 Notwendigkeit der DSFA (Schwellwertanalyse)

Eine DSFA muss durchgeführt werden, wenn die Verarbeitung „**voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge**“ hat (Art. 35 Abs. 1 DSGVO). Diese Prüfung wird Schwellwertanalyse genannt und in den nachfolgenden Schritten abgestuft durchgeführt.⁵

Die DSFA ist **zwingend notwendig**, sobald sie gesetzlich oder von den Behörden für die Verarbeitungstätigkeit vorgeschrieben ist:

- 1) Ist die Verarbeitungstätigkeit in den drei aufgeführten Fällen des **Art. 35 Abs. 3 DSGVO** umfasst (**Regelbeispiele**)?
- 2) **Im öffentlichen Bereich:** Steht die Verarbeitungstätigkeit auf der nicht abschließenden **Positivliste** gemäß Art. 35 Abs. 4 DSGVO der für das Unternehmen **zuständigen Aufsichtsbehörde des Bundeslands**, in welchem es seinen Sitz hat?
- 3) **Im nicht-öffentlichen Bereich:** Steht die Verarbeitungstätigkeit auf der nicht abschließenden **Positivliste** (17 Fallgruppen) gemäß Art. 35 Abs. 4 DSGVO der **Datenschutzkonferenz**?⁶

⁵ Vgl. DSK: SDM, S. 50 f.

⁶ DSK: Positivliste, S. 1-4.

Zur zwingenden Notwendigkeit einer DSFA im Zusammenhang mit Videoüberwachung:

Plant ein Unternehmen, die Geschäftsbereiche mit Kundenverkehr dauerhaft mit Videoüberwachungsanlagen zu beobachten und aufzunehmen, liegt eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereich“ nach Art. 35 Abs. 3 DSGVO vor und für die Verarbeitungstätigkeit ist eine DSFA erforderlich.

Erfolgt hingegen beispielsweise eine Überwachung der Beschäftigten im Logistikbereich, die auch zur Bewertung der Arbeitstätigkeit eingesetzt werden könnte, ist Nr. 8 der Positivliste der DSK einschlägig.

Anders wäre es, wenn ein Unternehmen lediglich eine Videoüberwachungsanlage mit einem Beobachtungswinkel installiert, der einzig und allein auf die Tür des Serverraums gerichtet ist, um das unbefugte Betreten desselben festzustellen. Diese Verarbeitung wäre weder von Art. 35 Abs. 3 DSGVO noch von den Positivlisten der Behörden aufgeführt. Nichtsdestotrotz könnte eine DSFA für eine solche Verarbeitungstätigkeit aufgrund der nachfolgenden Prüfungspunkte notwendig sein.

Praxisbeispiel 2-3

Sofern die Verarbeitungstätigkeit weder gesetzlich noch von den Behörden in ihren Listen vorgeschrieben ist, wird die Prüfung wie folgt weitergeführt:

- 4) Erfüllt die Verarbeitungstätigkeit mindestens **zwei** der neun **Kriterien der Artikel-29-Datenschutzgruppe**?⁷
- 5) Liegt aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitungstätigkeit voraussichtlich ein **hohes Risiko** in Hinblick auf die Eintrittswahrscheinlichkeit und die potentiellen Auswirkungen („Schadenshöhe“) für die Rechte und Freiheiten natürlicher Personen vor? (Vorab-**Risikoanalyse**)

Die „**Rechte und Freiheiten natürlicher Personen**“ umfassen dabei insbesondere die Rechte der Europäischen Grundrechtecharta. Dazu zählen der Schutz personenbezogener Daten (Art. 7), die Achtung des Privat- und Familienlebens (Art. 8), die Gedanken-, Gewissens- und Religionsfreiheit (Art. 10), die Meinungs- und Informationsfreiheit (Art. 11) und die Nichtdiskriminierung (Art. 21). Aus der DSGVO sind vor allem die Grundsätze nach Art. 5, die Rechte betroffener Personen nach den Art. 12 ff. und die Gewährleistungsziele nach Art. 32 relevant.⁸ Die DSK empfiehlt, an dieser Stelle **Praxiserfahrung** und **konkretisierende Gerichtsurteile** zur Vorabprüfung eines hohen Risikos einzubeziehen.⁹ Insbesondere bei der Verarbeitung vieler oder **sensiblerer Daten** (wie z.B. Zahlungsdaten, Gesundheitsdaten) erscheint ein höheres Risiko naheliegender. Wichtig ist zu betonen, dass die Schwellwertanalyse **nicht die Risikoanalyse des Hauptteils der DSFA vorwegnehmen** oder diese ersetzen soll. Es ist vielmehr eine Vorabprüfung, die in ihrem Umfang deutlich begrenzter ist.

⁷ Art.-29-DS-Gruppe: WP 248, S. 10-12.

⁸ Vgl. DSK: Kurzpapier Nr. 18, S. 1.

⁹ DSK: SDM, S. 52.

Anwendungsbeispiel Software-Einführung: Die oben erwähnte Software erfüllt keines der Regelbeispiele des Art. 35 Abs. 3 DSGVO. Die geplante KI-Unterstützung könnte jedoch Nr. 11 der Positivliste der DSK berühren, wonach eine DSFA notwendig ist beim „Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person“. Zwar soll die KI die Prozesse vorbereiten und beschleunigen, jedoch nicht die Interaktion mit den betroffenen Personen steuern. Auch die Beispiele der DSK mit einer automatisierten Auswertung der Stimmungslage eines Anrufenden oder der Konversation mit einem KI-Bot passen eher nicht zur Software. Deshalb ist für die Einführung dieser Software eine DSFA zunächst nicht zwingend notwendig.

Folglich wird geprüft, ob mindestens zwei Kriterien der Art.-29-Datenschutzgruppe einschlägig sind. Dort findet sich zwar Kriterium Nr. 2 mit der automatisierten Entscheidungsfindung, jedoch soll die KI gerade nur unterstützend wirken und keine Entscheidungen eines Menschen abnehmen. Zutreffend erscheint jedoch Nr. 5, die Datenverarbeitung in großem Umfang – bei allen Kunden des Unternehmens –, sowie Nr. 8, die Anwendung neuer technologischer Lösungen – die KI-Unterstützung. Somit liegen mindestens zwei der Kriterien vor, wonach mit einem hohen Risiko bei der Verarbeitungstätigkeit zu rechnen und eine DSFA deshalb notwendig ist.

Sollte am Ende unklar sein, ob eine DSFA erforderlich ist, wird empfohlen, sie im Zweifel durchzuführen.¹⁰ Während die Punkte 1 bis 3 eine DSFA in jedem Fall notwendig machen, besteht bei den Punkten 4 bis 5 ein **Abwägungsspielraum**. Unter Berücksichtigung der Umstände des Einzelfalls kann dort auch zu dem Ergebnis gelangt werden, dass voraussichtlich kein hohes Risiko zu erwarten ist. Die Schwellwertanalyse ist immer zu **dokumentieren** und insbesondere im Falle einer abgelehnten Notwendigkeit ausführlich zu **begründen**.

2.4 Planung, Interviews und Absprachen

Wenn eine DSFA notwendig ist, kann die eigentliche Planung zur Durchführung der DSFA beginnen. Hierzu muss zunächst festgestellt werden, welche Personen:¹¹

- für die Verarbeitung **datenschutzrechtlich** sowie **technisch verantwortlich** sind;
- **juristische** (datenschutzrechtliche) sowie **IT-Fachexpertise** einbringen können;
- die **Prozesse, Richtlinien** und weitere relevante **Dokumente** entwickelt haben;
- die **Kontaktpersonen** bei Erstellung der DSFA sind (Einbindung der **Fachabteilungen**);
- den **DSFA-Bericht** zusammenstellen und schreiben;
- in kritischen oder unklaren Situationen **Entscheidungen** treffen;
- darüber hinaus ggf. gemäß Art. 35 Abs. 9 DSGVO zur Einholung ihres Standpunktes **eingebunden** werden sollen.

Ziel ist es, ein **interdisziplinäres DSFA-Team** zu bilden, welches für die Durchführung der DSFA und insbesondere für die Risikoanalyse inhaltlich und fachlich die Zusammenstellung, Einordnung und Bewertung von Informationen, Prozessen und Risiken vornehmen kann.

¹⁰ Art.-29-DS-Gruppe: WP 248, S. 9.

¹¹ Vgl. auch Fraunhofer ISI: DSFA-Handbuch, S. 36.

Hierfür sollten dem DSFA-Team alle erforderlichen Informationen zur Verfügung gestellt sowie eine effektive Koordination und schnelle Auskunft durch Verweis auf die jeweils zuständigen Personen ermöglicht werden. Zudem sollten auch die benötigten Dokumente, Zuständigkeiten und Aufgaben – etwa in Form eines **Projektplans** – festgelegt und dokumentiert werden. Darüber hinaus sollte der zeitliche Rahmen abgesteckt und nach Bedarf Interviews und erforderliche Ab- und Rücksprachen geplant werden.

Gegebenenfalls soll der **Standpunkt** der betroffenen Personen oder ihrer Vertretung gemäß Art. 35 Abs. 9 DSGVO eingeholt werden. Dies gewinnt insbesondere beim Einsatz neuer Technologien an Bedeutung, die weitreichend Daten sammeln und damit Konfliktpotential bergen könnten.¹² Der Standpunkt kann beispielsweise mithilfe von Studien oder Umfragen direkt bei den betroffenen Personen, mittels Konsultation von Verbraucherschutzverbänden oder durch Einbeziehung des Betriebsrats eingeholt werden.¹³ Dabei erfährt die datenverarbeitende Stelle insbesondere die für die Prüfung der Verhältnismäßigkeit relevanten **Erwartungen** der betroffenen Personen.

Zur Einbindung des Betriebsrats: Der Betriebsrat muss insbesondere nach **§ 87 Abs. 1 Nr. 6 BetrVG** eingebunden werden, wenn das Unternehmen die Einführung und Anwendung technischer Einrichtungen plant, die dazu bestimmt sind, das **Verhalten oder die Leistung der Beschäftigten zu überwachen**. Nach der Rechtsprechung genügt dafür schon die bloße Eignung der Einrichtung zur Überwachung. Hierzu kann bereits die Videoüberwachung gehören. Aber auch Software kann aufgrund der automatischen Verarbeitung von Nutzungsdaten diese Voraussetzung erfüllen.

Praxisbeispiel 2-4

Je nach Komplexität der Verarbeitungstätigkeit kann die Durchführung einer DSFA **wenige Tage bis hin zu mehreren Wochen oder sogar Monate** dauern.

Verantwortliche müssen während des gesamten Prozesses den Rat des/der **Datenschutzbeauftragten** einholen (Art. 35 Abs. 2 DSGVO), sofern diese/r benannt wurde. Allerdings sollte der/die Datenschutzbeauftragte wegen seiner/ihrer Stellung als weisungsunabhängige Person sowie den übertragenen Aufgaben (vgl. Art. 38, 39 DSGVO), zu denen vor allem die Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften gehören, grundsätzlich nicht selbst die DSFA durchführen, insbesondere vor dem Hintergrund möglicher Interessenkonflikte (vgl. Art. 38 Abs. 6 S. 2 DSGVO). Gleichwohl kann der/die Datenschutzbeauftragte zur **Beratung** und **Überwachung** im Zusammenhang mit der Durchführung der DSFA herangezogen werden (Art. 39 Abs. 1 lit. c DSGVO).

2.5 Ermittlung beteiligter Akteure

In der Regel sind bei modernen Datenverarbeitungen weitere Akteure außer dem Unternehmen selbst beteiligt, z.B.:

- **Weitere datenschutzrechtlich Verantwortliche**, etwa Tochterunternehmen oder Unternehmen in gemeinsamer Verantwortlichkeit, oder

¹² Vgl. Forum Privatheit: DSFA-Whitepaper, S. 25 f.

¹³ Vgl. Art.-29-DS-Gruppe: WP 248, S. 18, sowie weiterführend Forum Privatheit: DSFA-Whitepaper, S. 25 f.

- **Auftragsverarbeiter/innen**, etwa Dienstleister/innen für bestimmte Software-Produkte.

Diese müssen dann in der DSFA berücksichtigt und bei Bedarf in die Informationsbeschaffung eingebunden werden. Bei gemeinsam Verantwortlichen, die etwa einen Dienst kooperativ betreiben, kann eine DSFA auch gemeinsam durchgeführt werden.¹⁴ Dabei sollte jedoch darauf geachtet werden, die jeweiligen **Aufgaben und Zuständigkeiten** für Maßnahmen genau festzulegen. Dies kann insbesondere im Rahmen des Vertrags nach Art. 26 DSGVO geschehen, denen gemeinsam Verantwortliche abzuschließen haben.

Anwendungsbeispiel Software-Einführung: Die Software wird von einem internationalen Dienstleister aus Kanada mit einem deutschen Tochterunternehmen bereitgestellt, das einen Desktop- und einen Web-Client für die Bearbeitung und Nutzung in der Cloud anbietet. Dabei werden die Daten grundsätzlich in einem deutschen Rechenzentrum gespeichert und verarbeitet. Mit dem deutschen Tochterunternehmen wurde ein Auftragsverarbeitungsvertrag abgeschlossen, in dem die von ihm verarbeiteten Daten und die getroffenen technischen und organisatorischen Maßnahmen beschrieben sind. Dieser Vertrag und die Datenübermittlung an den Dienstleister und die Rechenzentren müssen bei der Erstellung der DSFA und der Informationsbeschaffung berücksichtigt werden.

2.6 Informationsbeschaffung

Die Informationsbeschaffung erfolgt durch gezielte Nachfrage bei den jeweils zuständigen Personen, insbesondere durch Fragebögen. Regelmäßig werden dabei, sofern vorhanden, insbesondere folgende Unterlagen benötigt werden:

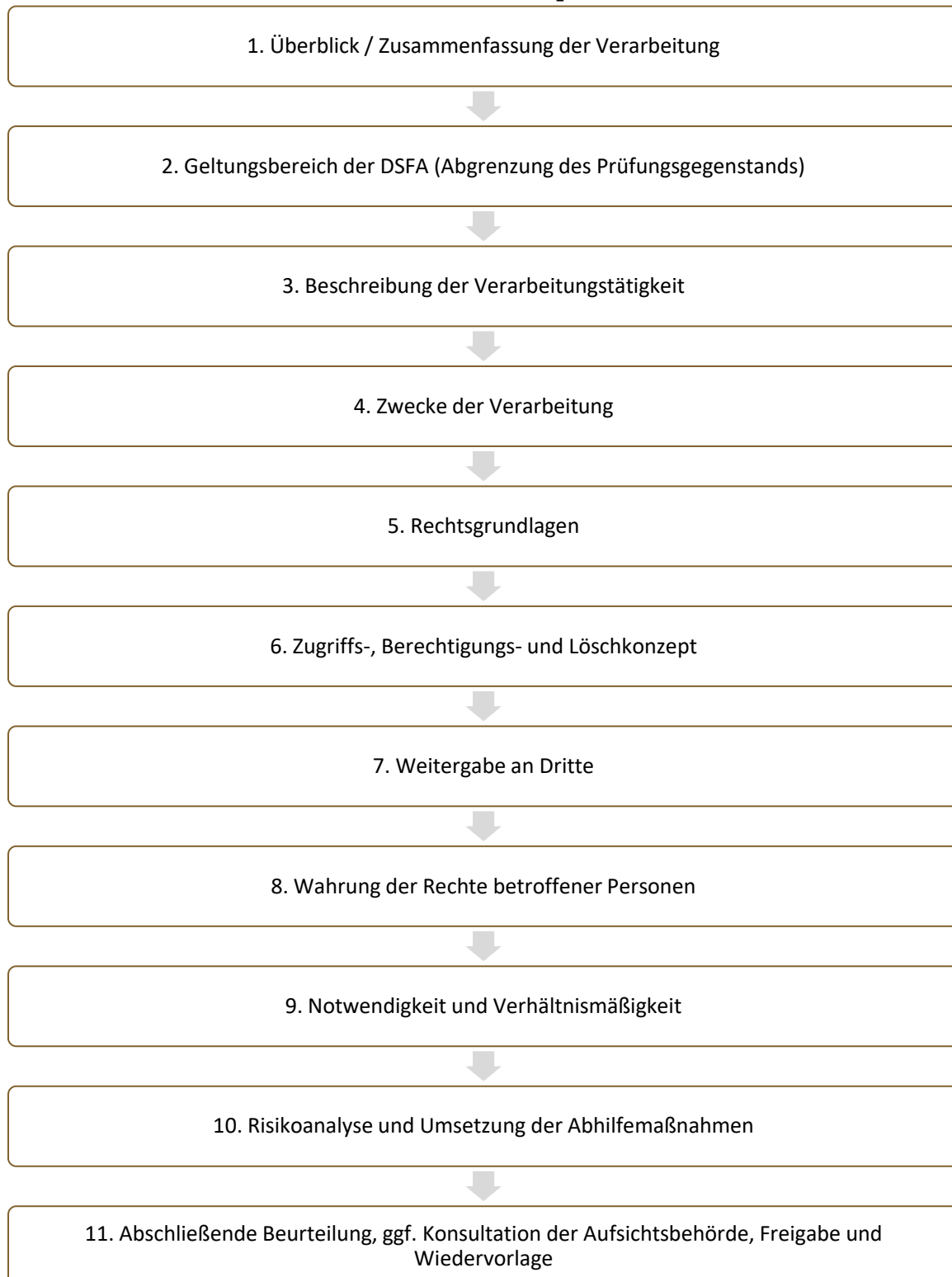
- **Verzeichnis der Verarbeitungstätigkeit** („VVT“) nach Art. 30 DSGVO;
- **Technische und organisatorische Maßnahmen** („TOMs“) nach Art. 32 DSGVO;
- **Datenschutzkonzept** für die Verarbeitungstätigkeit;
- **Richtlinien/Prozess zum Umgang mit Anfragen betroffener Personen**;
- **Prozessbeschreibungen** für die Verarbeitungstätigkeit;
- **Datenflussdiagramme und Netzpläne**;
- **Zugriffs- und Berechtigungskonzept**;
- **Löschkonzept**;
- **Verträge mit gemeinsam Verantwortlichen** sowie **Auftragsverarbeitungsverträge** („AVV“).

Das DSFA-Team muss sich anhand der bereitgestellten Unterlagen ein genaues Bild von der Verarbeitungstätigkeit machen können. Sollten während der Durchführung der DSFA weitere Fragen auftauchen, sind diese zeitnah zu klären. Auf die Dokumente kann im DSFA-Bericht auch als **Anhänge** verwiesen werden. Dann können die jeweiligen Ausführungen kürzer und zusammengefasst ausfallen, sofern im verwiesenen Dokument die Details erläutert werden.

¹⁴ Art.-29-DS-Gruppe: WP 248, S. 8.

3. Durchführungsphase I

3.1 Aufbau des DSFA-Berichts (Musterbeispiel)



3.2 Geltungsbereich der DSFA (Abgrenzung des Prüfungsgegenstands)

Auf Grundlage der festgelegten Verarbeitungstätigkeit (siehe 2.2) wird nach einem kurzen Überblick über diese zunächst der Geltungsbereich der DSFA erläutert. Dabei wird die Verarbeitungstätigkeit von anderen Prozessen abgegrenzt:¹⁵

- **Vorgelagerte** Prozesse;
- **Gleichgelagerte**, aber nicht betrachtete, Prozesse;
- **Nachgelagerte** Prozesse.

Hierzu wird beschrieben, wann die betrachtete Verarbeitungstätigkeit beginnt und wann sie endet. Sofern die abzugrenzenden Prozesse bereits in einer anderen DSFA untersucht wurden, kann auf diese verwiesen werden. Insbesondere bei komplexen Verfahren oder umfassender Software kann die Abgrenzung des Prüfungsgegenstands durchaus umfangreicher werden.

Anwendungsbeispiel Software-Einführung: Die Software soll die Erfüllung von Dienstleistungen im Rahmen der bereits abgeschlossenen Kundenverträge ermöglichen. Hierfür verwendet sie die beim Vertragsabschluss erhaltenen Kundendaten, der jedoch selbst nicht zum Geltungsbereich der DSFA gehört, sondern diesem vorgelagert ist. Auch wird die Software nicht für den Kundensupport eingesetzt, einem gleichgelagerten, aber hier nicht betrachteten Prozess außerhalb des Geltungsbereichs. Schließlich gehört auch die Kündigung des Kundenvertrags nicht zum Geltungsbereich, sondern ist der betrachteten Verarbeitungstätigkeit nachgelagert und wird durch den Kundendienst händisch vorgenommen.

3.3 Beschreibung der Verarbeitungstätigkeit

Im Rahmen einer DSFA soll eine „*systematische Beschreibung*“ der Verarbeitungstätigkeit erfolgen (Art. 35 Abs. 7 lit. a DSGVO), bei der auch auf die Ausführungen im VVT zurückgegriffen werden kann. Darunter ist vor allem eine **funktionale Darstellung** zu verstehen, welche **die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung** ausführlich und strukturiert einschließlich etwaig getroffener technischer und organisatorischer Maßnahmen beschreibt. Hierzu gehören insbesondere:¹⁶

- **Prozessschritte** („*Verarbeitungsphasen*“);
- eingesetzte **IT-Systeme, Produkte, Datenflüsse, Datenformate** und **Schnittstellen**;
- **Auswahl** und **Anzahl** der **involvierten Parteien** (insb. Verantwortliche und Auftragsverarbeiter/innen) und der (auch nur mittelbar) **betroffenen Personen(-gruppen)**;
- **Quantität** und **Qualität** der **Verarbeitung** und **verarbeiteten Daten(-kategorien)**;
- **zugriffsberechtigte Personen** und die **Weitergabe** der Daten an Dritte;
- **Speicherdauer** der Daten.

Ziel ist es, den gesamten **Lebenszyklus der Daten** – von der Erhebung, über die Speicherung, Nutzung und Weitergabe bis zur Löschung – **nachverfolgen** zu können.¹⁷ Dabei können auch

¹⁵ DSK: Kurzpapier Nr. 5, S. 2.

¹⁶ Vgl. Forum Privatheit: DSFA-Whitepaper, S. 24 ff.; DSK: SDM, S. 41 f.

¹⁷ Bitkom: DSFA-Leitfaden, S. 40.

Tabellen für eine strukturiertere Ansicht oder **Datenflussdiagramme** zur graphischen Darstellung ergänzend zur verbalen Beschreibung verwendet werden.¹⁸ Die Beschreibung der Verarbeitungstätigkeit kann dabei auch – wie in diesem Whitepaper – auf weitere **Unterpunkte** aufgeteilt werden. Dies kann helfen, insbesondere die Aspekte der Verarbeitungszwecke, der Zugriffsberechtigung, der Speicherdauer und der Weitergabe an Dritte genauer und übersichtlicher zu beschreiben. Die Datenschutzkonferenz stellte als Modell zur Strukturierung, Aufbereitung und Erfassung der Verarbeitungstätigkeit den sogenannten **SDM-Würfel** vor, der die Lebenszyklus-Phasen der Datenverarbeitung in Bezug zu wesentlichen Einflussgrößen der Verarbeitung setzt, die auf unterschiedlichen Ebenen (Fachverfahren, Fachapplikation und Infrastruktur) und vor dem Hintergrund der Gewährleistungsziele darstellt werden.¹⁹

3.4 Zwecke der Verarbeitung

Neben der vor allem technischen Beschreibung der Verarbeitungstätigkeit erfolgt zudem die systematische Beschreibung der Zwecke (Art. 35 Abs. 7 lit. a DSGVO), wofür auch auf das VVT zurückgegriffen werden kann. Damit sind alle **legitimen Interessen des Unternehmens** im datenschutzrechtlichen Sinne gemeint, die mit der Verarbeitungstätigkeit verfolgt werden. In dem Zusammenhang sollten auch die mit der Verarbeitung ggf. verfolgten berechtigten Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO erläutert werden.

Die Beschreibung der Zwecke wird oftmals eher nebensächlich behandelt, hat jedoch entscheidenden Einfluss auch auf die spätere Beurteilung der Notwendigkeit und Verhältnismäßigkeit und schließlich auch der Risikoanalyse selbst. Daher sollten die Zwecke **ausführlich, konkret** und **vollständig** aufgeführt werden. Abstrakte oder zu allgemeine Ziele sind im datenschutzrechtlichen Sinne unzureichend, was nicht zuletzt aus dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO hervorgeht.²⁰

Zur genauen Benennung der Zwecke im Zusammenhang mit Videoüberwachung:

Insbesondere im Bereich der Videoüberwachung ist eine konkrete Bezeichnung der Zwecke erforderlich. Sind die formulierten Zwecke zu allgemein oder abstrakt, werden sie von den Aufsichtsbehörden nicht anerkannt. In der von der Datenschutzkonferenz vorgelegten Orientierungshilfe Videoüberwachung etwa führt sie aus, dass diese nicht aus „Sicherheitsgründen“ oder unter Berufung auf das „Hausrecht“ durchgeführt werden dürfe. Vielmehr seien präzise Zwecke zu nennen, wie der Schutz vor Einbrüchen, Diebstählen, Vandalismus oder Übergriffen, die Beweissicherung, die Durchsetzung von Rechtsansprüchen, die Verhinderung von Betrug, Leistungsmisbrauch oder Geldwäsche.

Praxisbeispiel 3-1

Dabei kann es auch hilfreich sein, die Zwecke von anderen, ggf. verwandten, aber nicht verfolgten **Zwecken abzugrenzen**.²¹ Idealerweise können die mit der Verarbeitungstätigkeit verbundenen Zwecke den einzelnen Verarbeitungsphasen zugeordnet werden.

¹⁸ Fraunhofer ISI: DSFA-Handbuch, S. 32.

¹⁹ Vgl. DSK: SDM, S. 46.

²⁰ Vgl. auch DSK: Orientierungshilfe Videoüberwachung, S. 7 ff.

²¹ Vgl. DSK: SDM, S. 41.

Anwendungsbeispiel Software-Einführung: Die Software soll insbesondere folgende Zwecke verfolgen:

- Erhöhung der Effizienz bei der Bearbeitung von Vertragsangelegenheiten / Erfüllung von Dienstleistungen;
- Vereinheitlichung des Ablaufs bei Erfüllung von Verträgen;
- Beschleunigung des Arbeitsablaufes;
- Optimierung der Zusammenarbeit der Beschäftigten bei der Bearbeitung von Vertrags- und Kundendaten;
- Sicherstellung einer hohen Verfügbarkeit und Erreichbarkeit der Kundendaten.

3.5 Rechtsgrundlagen

Die Benennung und Klärung der Rechtsgrundlagen ist – obgleich sie nicht unter Art. 35 Abs. 7 DSGVO aufgezählt ist – im Rahmen der DSFA von elementarer Bedeutung und baut auf die festgelegten Zwecke der Verarbeitung auf. Sie dient nicht nur der Überprüfung, ob für die Verarbeitung in den einzelnen Prozessschritten tatsächlich eine Legitimation vorliegt, sondern bildet zugleich die Basis für Fragen zur Wahrung der Betroffenenrechte.

Eine Rechtsgrundlage sollte für jede von der Verarbeitungstätigkeit betroffene Personen-Gruppe vorliegen. Werden beispielsweise Geschäftspartnerinnen und -partner, Kunden und Beschäftigte von einer Verarbeitung betroffen, etwa weil ihre Daten alle in derselben Anwendung verarbeitet werden, sind für diese jeweils Rechtsgrundlagen festzulegen. Dabei ist es wichtig, auch nur mittelbar betroffene Personen der Verarbeitungstätigkeit, wie Familienmitglieder, Angehörige oder andere Dritte, die etwa in Dokumenten auftauchen können, zu berücksichtigen. Auch an dieser Stelle kann auf das VVT zurückgegriffen werden.

Aufgrund der Stellung der DSGVO als unmittelbar anzuwendende Verordnung kommen als Rechtsgrundlagen zunächst die aus **Art. 6 Abs. 1 S. 1 DSGVO** in Betracht:

- a) **Einwilligung;**
- b) Erforderlichkeit zur Erfüllung eines **Vertrags** oder zur Durchführung vorvertraglicher Maßnahmen;
- c) Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung;
- d) Erforderlichkeit zum Schutz lebenswichtiger Interessen;
- e) Erforderlichkeit zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt;
- f) Erforderlichkeit zur Wahrung der **berechtigten Interessen** (relevant insbesondere bei nur mittelbar betroffenen Personen).

Bei letzterer Rechtsgrundlage muss eine **dokumentierte Interessenabwägung** erfolgen, bei der die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person gegen die berechtigten Interessen der datenverarbeitenden Stelle abgewogen werden. Überwiegen bei dieser Abwägung die Interessen der betroffenen Person, dürfen die Daten nicht auf dieser Rechtsgrundlage verarbeitet werden. Wichtig ist dabei zu erwähnen, dass nicht leichtfertig ohne eingehende Prüfung eine Verarbeitung auf dieser Rechtsgrundlage erfolgen sollte.

Kommt es zur Verarbeitung **besonderer personenbezogener Daten** nach Art. 9 Abs. 1 DSGVO, wie etwa Gesundheitsdaten, muss auch eine Rechtsgrundlage nach **Art. 9 Abs. 2 DSGVO** existieren. Sowohl Art. 6 Abs. 1 S. 1 lit. c, e DSGVO als auch manche Rechtsgrundlagen unter Art. 9 Abs. 2 DSGVO setzen zudem eine **Rechtsgrundlage im Unionsrecht oder im nationalen Recht** voraus. Letztere können sowohl im deutschen Bundes- (z.B. BDSG) als auch im Landesrecht zu finden sein.

Zur Anwendung nationaler Regelungen bei der Verarbeitung von Gesundheitsdaten:

Werden Gesundheitsdaten verarbeitet, kommt neben der Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO im Behandlungskontext auch Art. 9 Abs. 2 lit. h DSGVO zusammen mit § 22 Abs. 1 Nr. 1 lit. b BDSG in Betracht, wenn etwa die Verarbeitung zur Durchführung der Behandlung bzw. des Behandlungsvertrags erforderlich ist. Dabei gelten zusätzliche Voraussetzungen nach Art. 9 Abs. 3 DSGVO, um die Geheimhaltungspflicht sicherzustellen. Dabei werden insbesondere das Berufsgeheimnis aus § 203 StGB und das Sozialgeheimnis aus § 35 SGB I relevant. Daneben müssen zudem spezialgesetzliche Regelungen wie Landeskrankenhausgesetze berücksichtigt werden.

Praxisbeispiel 3-2

Daneben können nationale Regelungen auch aufgrund der sogenannten **Öffnungsklauseln** aus **Art. 85, 88 und 89 DSGVO** in Betracht kommen, die im Rahmen der Meinungsfreiheit und Informationsfreiheit, im Beschäftigungskontext sowie zu im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken gelten. Für den **Beschäftigungskontext** wird hier vor allem **§ 26 BDSG** relevant.

Zur Anwendung von § 26 BDSG im Beschäftigungskontext: § 26 Abs. 1 S. 1 BDSG ist die naheliegendste Rechtsgrundlage, wenn die Daten von Beschäftigten zur Begründung, zur Durchführung oder zur Beendigung des Beschäftigungsverhältnisses verarbeitet werden. Hierzu gehört beispielsweise die Verarbeitung der Daten von Bewerberinnen und Bewerbern und die Verarbeitung der Beschäftigtendaten für das Management, die Planung und Organisation der Arbeit.

§ 26 Abs. 1 S. 2 BDSG ermöglicht demgegenüber die Verarbeitung zur Aufdeckung von Straftaten im Beschäftigungsverhältnis, wenn tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen. Diese Rechtsgrundlage ist eng zu sehen und darf nur herangezogen werden, wenn einem konkreten Verdacht nachgegangen werden soll. Für Videoüberwachung im Allgemeinen ist hingegen Art. 6 Abs. 1 S. 1 lit. f DSGVO einschlägig, auch wenn Beschäftigte aufgenommen werden.

Praxisbeispiel 3-3

Darüber hinaus muss beachtet werden, dass manche Regelungen im nationalen Recht **zusätzliche Anforderungen** an bestimmte Verarbeitungstätigkeiten stellen. Diese sind zwar nicht unmittelbar datenschutzrechtlicher Natur, müssen aber bei der Entscheidung für eine Rechtsgrundlage berücksichtigt werden.

Für das **Recht am gesprochenen Wort** sieht etwa § 201 StGB vor, dass das Gesprochene nur befugt (i.d.R. mit Zustimmung) aufgenommen werden darf. Beim **Recht am eigenen Bild**

sollten, etwa für Zwecke der Werbung und des Marketings, die Erwägungen der §§ 22, 23 KUG im Zuge einer Interessenabwägung berücksichtigt werden.²² Im Ergebnis führen beide Regelungen dazu, dass man aus datenschutzrechtlicher Sicht bei der **Interessenabwägung** wohl häufig keine überwiegenden berechtigten Interessen für solche Verarbeitungen annehmen kann, es sei denn, in den jeweiligen Regelungen selbst sind entsprechende Ausnahmen vorgesehen, wie etwa in § 23 KUG.

Zu Ton- und Videoaufnahmen im Rahmen von Microsoft Teams: Zwar kann man die Nutzung von Microsoft Teams im Unternehmen für die Kommunikation mit Geschäftspartnerinnen und -partnern grundsätzlich auf Art. 6 Abs. 1 S. 1 lit. b DSGVO und im Beschäftigungskontext auf Art. 6 Abs. 1 S. 1 lit. b DSGVO i.V.m. § 26 Abs. 1 BDSG stützen. Sofern jedoch Meetings aufgenommen werden sollen, bei denen die Teilnehmerinnen und Teilnehmer entweder mit ihrem Bild zu sehen oder ihrer Stimme zu hören sind, wird ihre Zustimmung aufgrund von § 201 StGB und den Erwägungen der §§ 22, 23 KUG nötig.

In datenschutzrechtlicher Hinsicht könnte für solche Fälle eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO eingeholt werden, sofern sie allen Anforderungen nach Art. 7 DSGVO entspricht. Dies käme beispielsweise bei externen Teilnehmenden in Betracht. Im Beschäftigungskontext sind jedoch aufgrund von § 26 Abs. 2 BDSG zusätzliche Anforderungen, insbesondere an die Freiwilligkeit, zu beachten. Dabei sind alle Umstände der Einwilligungserteilung und die Eingriffsintensität zu berücksichtigen. Hierzu gehört insbesondere, ob auf die Beschäftigten Druck ausgeübt wird oder diese Nachteile erleiden würden, wenn sie ihre Einwilligung nicht erteilen. Deshalb könnte es im Rahmen einer Abwägung dazu kommen, dass eine Einwilligung von Beschäftigten für nicht freiwillig erachtet wird.

Statt einer Einwilligung kann jedoch in eng begrenzten Anwendungsfällen der Arbeitsvertrag nach Art. 6 Abs. 1 S. 1 lit. b DSGVO, Art. 88 DSGVO i.V.m. § 26 Abs. 1 S. 1 BDSG als mögliche Rechtsgrundlage in Betracht kommen, etwa um referierende Personen eines Workshops im Einzelfall aufzunehmen, um diesen für abwesende Personen nachträglich zur Verfügung zu stellen. Hierbei sind jedoch enge Anforderungen, insbesondere an die Transparenz, die Zugriffsberechtigungen und die Speicherdauer, zu stellen. In jedem Fall ist eine umfangreiche Interessenabwägung durchzuführen.

Praxisbeispiel 3-4

Ist die Verarbeitung zur Erfüllung der Zwecke nicht mehr erforderlich oder fällt der Zweck weg, kann diese nicht mehr auf Grundlage der ausgewählten Rechtsgrundlage erfolgen (Art. 5 Abs. 1 lit. e DSGVO). Danach können jedoch gesetzliche **Aufbewahrungspflichten** zusammen mit **Art. 6 Abs. 1 S. 1 lit. c DSGVO** eine darüber hinausgehende Speicherung ermöglichen, ohne während dieser Zeit jedoch die Daten anderweitig nutzen zu dürfen.

²² Werden Fotos zu journalistischen Zwecken angefertigt oder veröffentlicht, gelten die §§ 22, 23 KUG als Spezialregelungen, die wegen der Öffnungsklausel in Art. 85 Abs. 2 DSGVO den Rechtsgrundlagen in Art. 6 DSGVO vorgehen.

Die Festlegung der Rechtsgrundlagen sollte **präzise** erfolgen. Alle mit der Verarbeitungstätigkeit verfolgten Zwecke müssen mit einer Rechtsgrundlage abgedeckt werden. An dieser Stelle kann die DSFA auch dazu dienen, das bisher existierende VVT hinsichtlich der verfolgten Zwecke und Rechtsgrundlagen zu überprüfen und bei Bedarf zu überarbeiten.

Anwendungsbeispiel Software-Einführung: Die Verarbeitung der Kundendaten in der Software erfolgt auf Grundlage des abgeschlossenen Kundenvertrags gemäß Art. 6 Abs. 1 S. 1 lit. b DSGVO. Darüber hinaus werden die Daten der Beschäftigten bei der Anmeldung verarbeitet, insbesondere die E-Mail-Adresse. Dies erfolgt auf Grundlage des Arbeitsvertrages nach Art. 6 Abs. 1 S. 1 lit. b DSGVO i.V.m. § 26 Abs. 1 S. 1 BDSG.

Sofern die zur Unterstützung herangezogene KI weiter trainiert werden soll, erfolgt die Verarbeitung auf Grundlage berechtigter Interessen an der Verbesserung der Software zur Optimierung der anfallenden Aufgaben nach Art. 6 Abs. 1 S. 1 lit. f DSGVO. Auch die Daten nur mittelbar betroffener Personen, wie Angehörige der Kunden, werden auf Grundlage berechtigter Interessen verarbeitet. Dabei wurden beide Interessenabwägungen dokumentiert.

3.6 Zugriffs- und Berechtigungskonzept

Die Beschreibung des Zugriffs- und Berechtigungskonzepts umfasst:

- die Vergabe, die Änderung und den Entzug (Widerruf) von Rollen und Berechtigungen („**Autorisierung**“) sowie
- die Gewährleistung eines sicheren Zugriffs auf die Daten und der Verhinderung eines unbefugten Zugriffs („**Authentifizierung**“).

Ausgangspunkt hierfür sind das **Need-to-Know-** sowie das **Least-Privilege-**Prinzip: Zugriffsberechtigungen (z.B. Lesen / Bearbeiten / Vollzugriff) bzw. Rollen (z.B. Standard / Erweitert / Administration) dürfen nur so weit vergeben werden, wie dies für die Personen zur Erfüllung ihrer Aufgaben notwendig ist. Dabei sollte die Autorisierung nach einem **standardisierten und dokumentierten Verfahren** ablaufen. Die verschiedenen Rollen und ihre Berechtigungen sollten nachvollziehbar beschrieben und begründet werden. Für den analogen Bereich gilt dies für die Ausgabe von Schlüsseln für gesicherte Räume und Schränke entsprechend.

Um unbefugten Zugriff zu verhindern, müssen klare Regeln für die Authentifizierung definiert werden. Dies umfasst im technischen Bereich insbesondere eine **Passwort-Richtlinie** zur Erstellung, den Mindestanforderungen und der Nutzung von Passwörtern. Außerdem gehören dazu Regelungen zum Umgang mit technischen Geräten, zur (automatischen) Sperrung der Geräte bei Abwesenheit, zur Verwendung von Mehr-Faktor-Authentifizierung oder zur Verwendung verschlüsselter Datenträger und Verbindungen – etwa im Rahmen einer **IT-Nutzungs-Richtlinie**. Im analogen Bereich würde der Zugriff auf verschlossene Akten oder der Zugang zu gesicherten Räumen entsprechend geregelt werden.

Anwendungsbeispiel Software-Einführung: Die verwendete Software beinhaltet ein Zugriffs- und Rollensystem, mit dem der Zugriff auf das unbedingt erforderliche Maß reduziert wird. So erhalten grundsätzlich nur die persönlichen Bearbeiter/innen Zugriff auf die Vertragsunterlagen des jeweiligen Kunden und sind zur Bearbeitung dieser berechtigt. Sofern Beschäftigte ausfallen, kann nur die Personalabteilung anderen Beschäftigten für diese Zeit kurzfristig Zugriff auf die Vertragsunterlagen einräumen, um die bis dahin aufkommenden Aufgaben zu erledigen. Bei einem Personalwechsel wird der vorherige Zugriff durch die Personalabteilung gesperrt und ein neuer eingerichtet. Der administrative Support erfolgt durch eigens dafür geschultes eigenes Personal. Dieses hat keinen Zugriff auf die Vertragsunterlagen, kann jedoch dabei helfen, Passwörter zurückzusetzen oder weitere im Zusammenhang mit der Nutzung der Software anfallende Probleme zu lösen.

Bei der Vergabe der Passwörter werden strenge Mindestanforderungen durch die Software vorgegeben (min. 8 Zeichen, min. ein Großbuchstabe, ein Kleinbuchstabe, eine Zahl und ein Sonderzeichen). Es erfolgt ein automatischer Logout nach fünf Minuten Inaktivität, nach dem das Passwort erneut eingegeben werden muss. In einer eigenen Nutzungsrichtlinie wird zudem intern für die Beschäftigten geregelt, wie sie die Software am Arbeitsplatz und im Homeoffice sicher einsetzen können. Bevor Beschäftigte die Software nutzen dürfen und die entsprechenden Berechtigungen erhalten, müssen sie eine Schulung absolvieren, deren Teilnahme dokumentiert wird.

Die Beschränkung von Zugriffen und Berechtigungen ist auch eine Anforderung aus Art. 5 Abs. 1 lit. c sowie Art. 25 DSGVO. Sofern bereits ein Konzept separat dokumentiert wurde, kann deren Beschreibung innerhalb des DSFA-Berichts kürzer erfolgen und das Konzept als **Anhang** aufgenommen werden.

3.7 Löschkonzept

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies zur Erfüllung der Verarbeitungszwecke erforderlich ist (Art. 5 Abs. 1 lit. e DSGVO). Das bedeutet, dass die Daten – auch ohne Antrag der betroffenen Person nach Art. 17 Abs. 1 DSGVO – gelöscht werden müssen, sofern der Zweck entfällt sowie keine Zweckänderung (Art. 6 Abs. 4 DSGVO) oder alternative Rechtsgrundlage in Betracht kommen. Ausnahmsweise dürfen die Daten jedoch länger verwendet bzw. gespeichert werden:

- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche und historische Forschungszwecke oder statistische Zwecke gemäß **Art. 5 Abs. 1 lit. e 2. Hs., Art. 89 Abs. 1 DSGVO**; oder
- wenn gesetzliche Aufbewahrungspflichten, etwa nach **§ 147 AO, § 257 HGB** oder **§§ 195, 199 BGB**, bestehen.

Eine darüber hinausgehende Nutzung der personenbezogenen Daten ist dabei nicht zulässig.

Zur Aufbewahrungspflicht bei Kundendaten: Werden beispielsweise Kundendaten auf Grundlage von Art. 6 Abs. 1 S. 1 lit. b DSGVO verarbeitet, kann diese Rechtsgrundlage wegfallen, wenn der Kundenvertrag gekündigt wird. Dann stellt sich die Frage, ob die Daten weiter aufbewahrt oder wegen des Grundsatzes der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO gelöscht werden müssen. Viele Dokumente im Zusammenhang mit dem Kundenvertrag, wie etwa Bestellunterlagen, Aufträge, Unterlagen für einen Dauerauftrag, Mietverträge, Mahnbescheide und vertragsrelevanter Schriftverkehr, zählen als Handelsbriefe und müssen gemäß § 147 Abs. 1 Nr. 2, 3 AO bzw. § 257 Abs. 1 Nr. 2, 3 HGB **sechs Jahre**, Buchungsbelege nach § 147 Abs. 1 Nr. 4 AO bzw. § 257 Abs. 1 Nr. 4 HGB sogar **zehn Jahre** aufbewahrt werden.

Zur Aufbewahrungspflicht bei Bewerbungsdaten: Die Bewerbungsunterlagen abgelehnter Bewerberinnen und Bewerber sollten aufgrund der § 15 Abs. 4, § 61b Abs. 1 ArbGG für **sechs Monate** aufbewahrt werden. Für die Unterlagen eines eingestellten Beschäftigten gilt hingegen eine Aufbewahrungsdauer von **drei Jahren** gemäß § 109 GewO i.V.m. §§ 195, 199 BGB.

Praxisbeispiel 3-5

Idealerweise erfolgt die Löschung der Daten im technischen Bereich **automatisiert**, nachdem die Aufbewahrungsfrist erreicht ist. Werden mehrere IT-Systeme parallel mit denselben Daten betrieben, muss sichergestellt werden, dass die Löschung **synchron** in allen Systemen erfolgt. Analoge Dokumente müssen nach Ablauf der Aufbewahrungsdauer sicher vernichtet werden.

Anwendungsbeispiel Software-Einführung: In der Software wird der aktuelle Vertragsstatus einschließlich der Vertragsdauer dokumentiert. Ausgehend davon erhalten dort bearbeitete und gespeicherte Vertragsunterlagen die Markierung „Löschung 6 Jahre nach Vertragsende“ sowie Rechnungen und Buchungsbelege die Markierung „Löschung 10 Jahre nach Vertragsende“. Nach Ablauf dieser Frist werden die Unterlagen auf den Servern unwiederbringlich vernichtet.

Sofern die Daten nach Wegfall des ursprünglichen Zwecks **anonymisiert** werden sollen, ist hierfür auch eine Rechtsgrundlage notwendig. Allerdings fallen die erfolgreich anonymisierten Daten, wenn also keine Re-Identifizierung mehr möglich ist, nicht mehr in den Anwendungsbereich der DSGVO und sie dürfen unbeschränkt verwendet werden.

Der **Prozess** von der Erhebung, über die Verwendung, bis zur Aufbewahrung und letztendlich der Löschung sollte am besten in einem **Löschkonzept** dokumentiert werden, auf welches im DSFA-Bericht verwiesen werden kann.

3.8 Weitergabe an Dritte

Ausgehend von den ermittelten beteiligten Akteuren (siehe 2.5) muss im Rahmen der DSFA die Weitergabe an Dritte beschrieben werden. Dabei kommt es insbesondere darauf an, wer konkret welchen Zugriff auf die bei Dritten gespeicherten Daten hat. Dies hat auch vor dem Hintergrund des Urteils „**Schrems II**“ vom 16.07.2020 (Az.: C-311/18) des Europäischen Gerichtshofs („**EuGH**“) zu erfolgen. Insbesondere bei der Einbindung von Software und **Cloud-**

Technologien, bei denen Daten auf Drittanbieter-Servern gespeichert werden, stellt sich die Frage, ob eine Übermittlung von Daten in Drittländer im Sinne des Art. 44 DSGVO vorliegt. Dies kommt in Betracht, wenn Dienstleister/innen – einschließlich ihrer Tochterunternehmen – aus Drittländern wie den USA eingesetzt, Zugriff aus diesen Drittländern auf die Daten besteht oder Daten direkt dorthin übermittelt werden. In diesem Fall muss die Übermittlung:

- durch einen **Angemessenheitsbeschluss** gerechtfertigt sein (Art. 45 DSGVO), wie beispielsweise für die Schweiz, Kanada, Israel, Japan, Südkorea oder Neuseeland;²³
- mit geeigneten Garantien wie **Standardvertragsklauseln**²⁴ oder verbindlichen internen Datenschutzvorschriften erfolgen (Art. 46 DSGVO), wobei der EuGH auch – jedenfalls vor dem Hintergrund der damals gültigen Standardvertragsklauseln (Durchführungsbeschluss 2010/87/EU) – **zusätzliche Maßnahmen** zum Schutze der Daten verlangte, um ein **angemessenes Datenschutzniveau** zu gewährleisten; oder
- im Übrigen auf Grundlage einer Ausnahme nach Art. 49 DSGVO legitimiert sein, insbesondere durch **ausdrückliche Einwilligung** oder – bei „gelegentlichen Übermittlungen“ – wegen der Erforderlichkeit zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen.

Seit dem „*Schrems II*“-Urteil hat dieser Teil einer DSFA enorm an Bedeutung gewonnen und sollte ausführlich – auch unter Einbindung juristischen und technischen Fachpersonals – geprüft und betrachtet werden. Das im Rahmen der Nutzung von Standardvertragsklauseln verpflichtende *Transfer Impact Assessment*²⁵ sowie die umgesetzten **technischen und organisatorischen Maßnahmen** können dabei auch in der Risikoanalyse eingehender betrachtet und erläutert werden.

In dem Zusammenhang geht es besonders um technische Maßnahmen der Verschlüsselung von Daten und Verbindungen, der Schlüsselverwaltung und der Pseudonymisierung, um den konkreten Speicherorts der Daten und die Zugriffsmöglichkeiten durch Dritte. Aber auch organisatorische Maßnahmen, wie der Abschluss von Individualverträgen, eine risikobasierte Betrachtung der konkret verarbeiteten Daten oder Transparenzberichte etwa über den Zugriff durch Geheimdienstbehörden, spielen eine Rolle.

²³ Siehe alle Angemessenheitsbeschlüsse unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

²⁴ Aktuelle Standardvertragsklauseln (Durchführungsbeschluss 2021/914/EU) abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0914>.

²⁵ Das sogenannte Transfer Impact Assessment ist eine Anforderung der Standardvertragsklauseln, Klausel 14.

Anwendungsbeispiel Software-Einführung: Auch wenn der Software-Vertrag mit dem deutschen Tochterunternehmen abgeschlossen und die Daten vorrangig auf deutschen Servern gespeichert werden, kann ein Zugriff durch die Muttergesellschaft aus Kanada nicht vollständig ausgeschlossen werden. Denn es erfolgen Backups für den Fall, dass die deutschen Serverstandorte ausfallen, auf Servern der Muttergesellschaft in Kanada. Auch kann in Ausnahmefällen ein Support durch kanadische Beschäftigte aus Kanada erfolgen.

Aus diesem Grund wird an dieser Stelle die Übermittlung der Daten an den deutschen Vertragspartner und an die kanadische Muttergesellschaft geprüft. Der Support-Zugriff durch Beschäftigte erfolgt auf Grundlage des Auftragsverarbeitungsvertrags, der den Zugriff durch Beschäftigte aus der EU und Kanada umfasst. Auch wird in diesem Vertrag der Backupvorgang beschrieben, um eine hohe Verfügbarkeit und Wiederherstellbarkeit der Dienste sicherzustellen. Kanada ist zwar ein Drittland im Sinne des Art. 44 DSGVO, jedoch liegt für die Datenübermittlung für kommerzielle Unternehmen ein Angemessenheitsbeschluss nach Art. 45 DSGVO vor. Aus diesem Grund kann die Software trotz der teilweisen Übermittlung von Daten nach Kanada eingesetzt werden.

Aufgrund der Komplexität der mit dem Urteil verbundenen Rechtsfragen und der immer nötigen konkreten Betrachtung des jeweiligen Einzelfalls wird an dieser Stelle nicht weiter auf den Einsatz von Standardvertragsklauseln, das Transfer Impact Assessment, die EuGH-Rechtsprechung und die Drittlandübermittlung eingegangen.

3.9 Informationspflichten und Wahrung der Betroffenenrechte

Die Umsetzung von Informationspflichten (Art. 13, 14 DSGVO) und die Wahrung der Rechte betroffener Personen (Art. 15 bis 21 DSGVO) ist ein wichtiger Bestandteil der DSFA und hat Einfluss auf die Bewertung der Risiken im Rahmen der Risikoanalyse.

Es muss sichergestellt werden, dass die von der Verarbeitungstätigkeit betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Das kann bei Beschäftigten etwa über unternehmensinterne **Datenschutzhinweise** erfolgen oder bei Kunden über die **Datenschutzerklärung** bei Abschluss eines Vertrags. Auf diese sollte im Rahmen der DSFA verwiesen werden. Sofern noch keine solchen Dokumente existieren, sind sie zeitnah anzulegen, denn ein Fehlen von Informationen über die Datenverarbeitung ist ein weitreichender Verstoß gegen die DSGVO.

Für die Wahrung der **Betroffenenrechte** ist es wichtig, einen **Prozess** zu etablieren, der den Empfang einer Datenschutzanfrage über deren Bearbeitung bis hin zum Abschluss durch Antwort an die betroffene Person umfasst. Dies kann auch im Rahmen des Datenschutz-Managements erfolgen. Entweder wird an dieser Stelle auf den allgemeinen Prozess im Unternehmen verwiesen oder es erfolgt eine Erläuterung, wie die einzelnen Rechte umgesetzt werden.

Anwendungsbeispiel Software-Einführung: Die Beschäftigten des die Software nutzenden Unternehmens werden im Rahmen der Schulung und durch Datenschutzhinweise im Intranet über die Datenverarbeitung informiert. Kunden erhalten bei Vertragsschluss eine Datenschutzerklärung. Die Anfragen aller betroffenen Personen werden nach der im Unternehmen vorhandenen Richtlinie bearbeitet.

Sofern durch die erhobenen Daten keine eindeutige **Identifikation** der betroffenen Person möglich ist und auch mit zusätzlichen Informationen keine solche erfolgen kann, sind die Rechte aus Art. 15 – 20 DSGVO ausnahmsweise nicht einschlägig (Art. 11 Abs. 2 DSGVO). Dies kann etwa der Fall sein, wenn die Daten nur für einen sehr kurzen Zeitraum gespeichert oder unmittelbar nach der Erhebung anonymisiert werden. Dann könnte darauf hingewiesen werden, dass die Geltendmachung der Rechte in der Regel aus den oben genannten Gründen nicht erfolgreich sein wird.

Auf Grundlage der hier erläuterten Dokumente und Prozesse erfolgt später in der Risikoanalyse die Prüfung, ob diese zur Sicherstellung der Transparenz und Intervenierbarkeit ausreichen.

3.10 Notwendigkeit und Verhältnismäßigkeit

Die Prüfung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungstätigkeit in Bezug auf den Zweck wird für die DSFA explizit gefordert (Art. 35 Abs. 7 lit. b DSGVO). Dabei kann jedoch eine starre Trennung von Notwendigkeit und Verhältnismäßigkeit entfallen, da die Notwendigkeit regelmäßig in der Prüfung der Verhältnismäßigkeit aufgeht, für welche die nachfolgenden Schritte empfehlenswert sind:²⁶

1. **Legitimer Zweck:** Dient die Verarbeitungstätigkeit legitimen Zwecken?
2. **Geeignetheit:** Werden die verfolgten Zwecke damit erreicht oder zumindest gefördert?
3. **Erforderlichkeit (Notwendigkeit):** Gibt es keine gleich geeigneten, mildereren Mittel, um diese Zwecke zu erreichen?
4. **Angemessenheit:** Ist die Verarbeitungstätigkeit insgesamt im Rahmen einer Interessenabwägung zwischen den Interessen der betroffenen Personen mit denen der datenverarbeitenden Stelle angemessen, greift also zur Erreichung des Zwecks nicht zu stark in die Rechte der betroffenen Personen ein?

Bei der Beschreibung der legitimen Zwecke kann in der Regel auf vorherige Ausführungen zurückgegriffen oder verwiesen werden kann (siehe 3.4). Für die Geeignetheit wird auf die Funktionalität/Möglichkeiten der Verarbeitungstätigkeit Bezug genommen und wie diese die verfolgten Zwecke erreichen können. Hierfür kann auch auf die Beschreibung der Verarbeitungstätigkeit zurückgegriffen werden (siehe 3.3).

Ein Schwerpunkt der Prüfung der Verhältnismäßigkeit stellt die Erörterung zur Erforderlichkeit (Notwendigkeit) dar. Dort müssen **alternative Mittel** zur Erreichung der verfolgten Zwecke aufgezeigt werden. Stellt sich an dieser Stelle heraus, dass es deutlich mildere Mittel gibt, die

²⁶ Vgl. auch DSK: Kurzpapier Nr. 5, S. 3; Forum Privatheit: DSFA-Whitepaper, S. 24.

sogar gleich geeignet sind, müsste man feststellen, dass die Verarbeitungstätigkeit nicht verhältnismäßig ist. Oftmals wird es sich hier jedoch vielmehr so darstellen, dass es zwar Alternativen gibt, diese jedoch für die geforderten Zwecke und aufgrund der benötigten Funktionalität nicht gleich geeignet sind. Hier muss dann eine ausführliche Begründung erfolgen, die im Detail auf die Unterschiede eingeht und aufzeigt, wieso eine bestimmte Funktionalität zur Erfüllung der Zwecke unabdingbar ist.

Zur Prüfung der Erforderlichkeit am Beispiel von Microsoft 365: Für die einzelnen Dienste von Microsoft 365 existieren Alternativen, etwa On-premise-Lösungen wie Collabora Online / Office in Verbindung mit LibreOffice statt Office-Anwendungen wie Word und Excel, Videokonferenzen-Lösungen wie Blizz von TeamViewer oder BigBlueButton und Messenger-Alternativen wie Threema oder Wire statt Teams sowie Cloud-Lösungen wie die Open Telekom Cloud statt OneDrive oder SharePoint.

Gegenüber den jeweiligen Diensten von Microsoft 365 sind diese Alternativen für sich genommen zwar meist geeignet, ermöglichen jedoch nicht gleichermaßen ein effizientes, schnelles und einfaches Zusammenwirken der einzelnen Dienste. Somit sind die alternativen Dienste gegenüber der Nutzung von Microsoft 365 als Gesamtpaket nicht gleich geeignet, insbesondere hinsichtlich des kollaborativen Arbeitens.

Eine vergleichbar umfassende SaaS-Lösung wie Microsoft 365 wäre etwa der Google Workspace. Jedoch erscheint diese Alternative hinsichtlich der datenschutzrechtlichen Grundsätze wie Datenminimierung und Zweckbindung problematischer als Microsoft 365 und ist deshalb weder gleich geeignet noch milder. Insgesamt könnte man so zu dem Ergebnis kommen, dass es damit im Rahmen der Erforderlichkeitsprüfung an gleich geeigneten, milderer Mitteln zur Erfüllung der mit der Nutzung von Microsoft 365 verfolgten Zwecke fehlt.

Praxisbeispiel 3-6

Ein weiterer Schwerpunkt vor der abschließenden Bewertung der Verhältnismäßigkeit ist die Prüfung der Angemessenheit. Bei dieser geht es um eine **umfassende Interessenabwägung**, bei der die durch die Verarbeitungstätigkeit entstehenden **Vor- und Nachteile** für die betroffenen Personen (hinsichtlich ihres Persönlichkeitsrechts und des Eingriffs in ihre Rechte und Freiheiten) und für die datenverarbeitende Stelle (hinsichtlich ihrer unternehmerischen Freiheit) gegeneinander abgewogen werden. Hierbei sollte auf die konkret verarbeiteten Daten und betroffenen Personen Bezug genommen werden. Eine pauschale Angemessenheitsprüfung, die sich nicht auf den konkreten Prüfungsgegenstand bezieht, ist unzulässig.

Zur Prüfung der Angemessenheit beim 360-Grad-Feedback: Beim 360-Grad-Feedback im Unternehmen spielt der Beschäftigtendatenschutz, der Grundsatz der Datenminimierung sowie das Verbot einer Verhaltens- und Leistungskontrolle eine entscheidende Bedeutung. Es darf nicht zu einem Überwachungs- und Leistungsdruck kommen, der die Beschäftigten belastet. Auch müssen negative Folgen für die Personal- und Lohnentscheidungen (z.B. Kündigung, Abmahnung) und die kollegiale Zusammenarbeit (z.B. Diskriminierung) berücksichtigt werden. Das 360-Grad-Feedback ist insgesamt ein sehr komplexes Thema, welches im Rahmen einer DSFA ausführlich und konkret auf den jeweiligen Einzelfall und die genaue Ausgestaltung geprüft werden sollte. Pauschal lässt sich die Zulässigkeit nicht feststellen.

Praxisbeispiel 3-7

Zudem müssen auch die **Erwartungen** der betroffenen Personen (vgl. Erwägungsgrund 47 DSGVO) sowie die bereits getroffenen **Datenschutzeinstellungen** oder Maßnahmen zur Sicherstellung der Privatsphäre berücksichtigt werden.

Zur Prüfung der Angemessenheit am Beispiel von Microsoft 365: Auf Seiten der datenverarbeitenden Stelle stehen die umfassenden Vorteile durch den Einsatz von Microsoft 365, insbesondere hinsichtlich der schnellen, sicheren, effektiven und kollaborativen Zusammenarbeit im Unternehmen, auch hinsichtlich der hohen Verfügbarkeit und Zuverlässigkeit der Cloud-Systeme.

Betroffene Personen wie Beschäftigte eines Unternehmens erwarten, dass ihnen eine einfach zu bedienende Anwendung zur Verfügung gestellt wird, mit der sie effizient und mit kurzer Einarbeitungszeit ihre Aufgaben erfüllen können. Die meisten Beschäftigten haben bereits Erfahrung mit Anwendungen wie Word und Excel oder mit der Nutzung der Cloud bei Teams und OneDrive. Für sie hätte die Umstellung auf eine andere Software – erst recht, wenn es für jeden Dienst eine andere wäre – Nachteile durch die erhöhte Einarbeitungszeit und die fehlende schnelle kollaborative Zusammenarbeit.

Durch den Einsatz von Microsoft 365 werden zwar auch Beschäftigtendaten verarbeitet, insbesondere die bei der Verwendung automatisch anfallenden Nutzungsdaten. Um deren Umfang zu reduzieren und die weitergehende Verarbeitung von Nutzungsdaten zu verhindern, bietet Microsoft jedoch vielfältige Einstellungsmöglichkeiten zum Datenschutz sowie abschaltbare Funktionen (z.B. Deaktivierung von Diagnosedaten, verbundenen Erfahrungen, Microsoft-365-Berichten, Viva Insights) an, wodurch das Aufkommen von Nutzungsdaten auf das erforderliche Minimum reduziert werden kann. Dadurch wird dem Grundsatz der Datenminimierung Rechnung getragen. Zusammen mit der Schulung der Beschäftigten, einem funktionierenden Zugriffs- und Löschkonzept sowie der Gewährleistung der Betroffenenrechte könnte so im Einzelfall die Angemessenheit der Nutzung von Microsoft 365 angenommen werden.

Praxisbeispiel 3-8

Gleichwohl handelt es sich bei der Prüfung der Angemessenheit um **keine Vorwegnahme der Risikoanalyse**. Sollte sich jedoch bereits an dieser Stelle herausstellen, dass die Verarbeitungstätigkeit nicht verhältnismäßig ist, bedarf es schon dann einer umfassenden Anpassung der

Verarbeitungstätigkeit zur Erhöhung des Datenschutzes.²⁷ Denn ein Mangel bereits in dieser Phase der Prüfung stellt ein hohes Risiko dar. Demzufolge sind technische und organisatorische Maßnahmen vorzunehmen oder zu planen, um die Verhältnismäßigkeit der Verarbeitungstätigkeit sicherzustellen.

Die Prüfung aller Risiken im Detail mit der umfassenden Erörterung der erforderlichen technischen und organisatorischen Maßnahmen erfolgt jedoch grundsätzlich in der Risikoanalyse selbst, die im folgenden Kapitel behandelt wird.

Anwendungsbeispiel Software-Einführung: Da das die Software einführende Unternehmen nur eine zweistellige Zahl an Beschäftigten hat, wäre der Aufbau einer lokalen On-premise-Lösung kaum realisierbar und würde auch nicht die Vorteile durch ständige Verfügbarkeit und Zuverlässigkeit in der Cloud durch Backups und Ausfallserver besitzen. Die Software verarbeitet bereits in den Standardeinstellungen nur die unbedingt notwendigen Nutzungsdaten, zu denen die Verarbeitung der Zugangsdaten und die Protokollierung der Zugriffe gehören, um die sichere Anmeldung und Authentifizierung zu gewährleisten und im Zweifel Cyberangriffe und unbefugte Zugriffe nachvollziehen zu können. Eine Nutzungsanalyse findet standardmäßig nicht statt und es ist auch nicht beabsichtigt, sie zu aktivieren. Aus dem Auftragsvertragsvertrag geht hervor, dass der Dienstleister jede über die Auftragsbefreiung hinausgehende Verarbeitung der Daten, insbesondere zu eigenen Zwecken, vollständig ausschließt. Alle Daten werden während der Übermittlung transportverschlüsselt und auf allen Serverstandorten inhaltsverschlüsselt gespeichert. Insgesamt ist die Nutzung der Software damit erforderlich, angemessen und insgesamt verhältnismäßig.

²⁷ Vgl. auch Fraunhofer ISI: DSFA-Handbuch, S. 22 f.

4. Durchführungsphase II: Risikoanalyse

4.1 Aufbau der Risikoanalyse (Musterbeispiel)



4.2 Gewährleistungsziele definieren

Die Risikoanalyse ist eine explizite gesetzliche Voraussetzung im Rahmen der DSFA (Art. 35 Abs. 7 lit. c DSGVO). Sie erfordert ein **strukturiertes und nachvollziehbares Vorgehen**. Hierfür bietet sich das Konzept der Gewährleistungsziele an. Dabei handelt es sich um Orientierungswerte, mit denen die rechtlichen Anforderungen der DSGVO so praxisnah dargestellt werden, dass ihnen konkrete technische und organisatorische Maßnahmen zugeordnet werden können. Überprüft man die Risiken anhand von Gewährleistungszielen, lässt sich übersichtlich darstellen, ob Risikoszenarien vollumfänglich analysiert wurden. Listet man stattdessen Risikoszenarien der Reihe nach auf, wird eine vollständige Analyse schwerer.

Gewährleistungsziele als Konzept ist keine neue Erfindung des Datenschutzrechts. Es hat **Ähnlichkeiten mit Schutzzielen der Informationssicherheit** und ist daher gut geeignet, um zwischen rechtlichen Vorgaben und technischen Anforderungen zu „übersetzen“. Das SDM greift dieses Konzept auf, um die Anforderungen der DSGVO zu systematisieren.²⁸ Aus Praktikabilitätsgründen bietet es sich an, diesem Konzept zu folgen.²⁹ Für eine Risikoanalyse ist es jedoch nicht verpflichtend, sich an den Gewährleistungszielen des SDM zu orientieren. Es sind auch andere Einteilungen denkbar, insbesondere wegen der Überschneidungen zwischen den Gewährleistungszielen.

Das SDM fasst die **Gewährleistungsziele** wie folgt zusammen:³⁰

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

Datenminimierung bedeutet, dass nicht mehr personenbezogene Daten erhoben und gespeichert werden dürfen, als für die Verarbeitungstätigkeit notwendig sind.³¹ Entsprechend erfordert dieses Gewährleistungsziel Maßnahmen in allen Stadien des Verarbeitungsvorgangs, um die Verarbeitung auf das unbedingt notwendige Maß zu beschränken.

Das Gewährleistungsziel **Verfügbarkeit** beschreibt das Erfordernis, dass berechnigte/befugte Personen während des Verarbeitungsvorganges auf ihre Daten zugreifen können müssen, also die konkrete Auffindbarkeit der Daten.³² Dazu gehören auch die Ziele der Belastbarkeit und Wiederherstellbarkeit.

Integrität beschreibt die Unversehrtheit, Vollständigkeit und Richtigkeit der personenbezogenen Daten.³³ Weder der Verarbeitungsvorgang selbst noch ein Zugriff durch unbefugte Personen soll die Datensätze kompromittieren können. Zur Integrität gehören auch die

²⁸ DSK: SDM, S. 9 ff.

²⁹ So auch Fraunhofer ISI: DSFA-Handbuch, S. 42.

³⁰ DSK: SDM, S: 25 ff., dort auch im Detail erklärt.

³¹ DSK: SDM, S. 25.

³² DSK: SDM, S. 25 f.

³³ DSK: SDM, S. 26.

Funktionsstüchtigkeit und Belastbarkeit informationstechnischer Systeme. Beeinträchtigungen müssen zumindest registriert werden können, um Veränderungen zu korrigieren.

Vertraulichkeit ist die Anforderung, dass keine unbefugten Personen Zugriff auf die personenbezogenen Daten erhalten oder ihnen diese offengelegt werden. Sollte dies doch einmal passieren, muss ein Mechanismus zur Schadensminimierung greifen.³⁴

Nichtverkettung bedeutet, dass die verarbeiteten Daten nicht außerhalb ihres Verarbeitungszwecks zusammengeführt werden dürfen, um etwa im Rahmen des Profilings neue Erkenntnisse zu gewinnen.

Unter **Transparenz** versteht man das Erfordernis, dass für alle Beteiligten am Verarbeitungsvorgang zu jedem Zeitpunkt (im jeweils angemessenen Maß) erkennbar ist, wo, wie, zu welchem Zweck und von wem die Daten berechtigterweise verarbeitet werden. Dies dient der Kontrolle und der Sichtbarkeit von Mängeln.³⁵

Intervenierbarkeit ist die Voraussetzung, dass die betroffenen Personen ihre Rechte jederzeit wahrnehmen und wirksam geltend machen können müssen.

4.3 Risiken erfassen und beschreiben

Den zuvor definierten Gewährleistungszielen werden nun **Risikoszenarien** für die Rechte und Freiheiten natürlicher Personen (vgl. 2.3) zugeordnet. Aufgrund der Überschneidungen unter den Gewährleistungszielen können Risikoszenarien **mehrfach zugeordnet** werden. Dabei tritt dann jeweils ein anderer Aspekt in den Vordergrund, unter dem das Risiko zu analysieren ist.

Die DSGVO selbst definiert nicht direkt, was in ihrem Kontext unter „**Risiko**“ zu verstehen ist. Es handelt sich also um einen auslegungsbedürftigen Begriff, bei dessen Auslegung der europarechtliche Hintergrund zu berücksichtigen ist. Ausgehend von den Erwägungsgründen 75 und 94 der DSGVO ist ein Risiko deshalb zu verstehen als eine **Möglichkeit des Eintritts eines Ereignisses**, das selbst einen **Schaden** darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.³⁶

Unter „**Schaden**“ sind dabei alle möglichen **physischen** (d.h. körperlichen), **materiellen** (d.h. wirtschaftlichen) und **immateriellen** (d.h. gesellschaftlichen, persönlichen oder juristischen) **Beeinträchtigungen** zu verstehen (vgl. Erwägungsgrund 75 DSGVO).³⁷

³⁴ DSK: SDM, S. 26.

³⁵ DSK: SDM, S. 27.

³⁶ Vgl. DSK: Kurzpapier Nr. 18, S. 1.

³⁷ Vgl. DSK: Kurzpapier Nr. 18, S. 1, 2; vgl. Fraunhofer ISI: DSFA-Handbuch, S. 39 f., dort auch mit einigen Beispielen für physische, materielle und immaterielle Schäden.

Beispiele für mögliche Schäden: Im Kurzpapier Nr. 18 nennt die DSK folgende Beispiele für Schäden: Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile, Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen, Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten, Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte, körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten.

Praxisbeispiel 4-1

Sie können durch verschiedene **Risikoereignisse** hervorgerufen/ausgelöst werden, die sich etwa aus der Verarbeitungstätigkeit selbst (z.B. aufgrund ungeeigneter Prozesse) oder aus einer eigenverantwortlichen (z.B. durch Beschäftigte) oder fremdverursachten (z.B. durch unbefugte Dritte) Abweichung von der geplanten Verarbeitung ergeben.³⁸

Beispiele für Risikoereignisse: Die DSK nennt im Kurzpapier Nr. 18 folgende Ereignisse, die zur Verwirklichung von Schäden führen können: unbefugte oder unrechtmäßige Verarbeitung, Verarbeitung wider Treu und Glauben, intransparente Verarbeitung, unbefugte Offenlegung von und Zugang zu Daten, unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten, Verweigerung der Betroffenenrechte, Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken, Verarbeitung nicht vorhergesehener Daten, Verarbeitung nicht richtiger Daten, Verarbeitung über die Speicherfrist hinaus.

Praxisbeispiel 4-2

Die Schadensereignisse sind sodann einer **Risikoquelle** zuzuordnen, also etwa einer Person (z.B. Beschäftigte, Auftragsverarbeiter/innen oder unbefugte Dritte) oder einer Sache bzw. einem äußeren Einfluss (z.B. fehlerhafte Hardware, Stromausfall).³⁹ Dies kann interne, externe und sonstige Quellen umfassen.⁴⁰

Es ist dabei nicht notwendig, alle *nur irgendwie denkbaren* Risikoszenarien aufzuführen. Bei der Erfassung von Risiken für die Rechte und Freiheiten natürlicher Personen werden vielmehr all solche Risikoszenarien ermittelt, beschrieben und den Gewährleistungszielen zugeordnet, **deren Eintritt nicht ausgeschlossen und deren Auswirkungen nicht komplett unerheblich sind**. Dabei sollten typische Risiken ebenso wie für die Verarbeitung spezifische Risiken (etwa bei der Verarbeitung von Gesundheitsdaten) auf jeden Fall enthalten sein. Die Betrachtung erfolgt hierbei (zunächst) ohne Berücksichtigung der bereits getroffenen Maßnahmen. Unterstützend kann bei der Ermittlung der Risiken auch das umfangreiche **IT-Grundschutz-Kompodium** herangezogen werden.⁴¹

³⁸ DSK: Kurzpapier Nr. 18, S. 2

³⁹ Vgl. DSK: Kurzpapier Nr. 18, S. 4.

⁴⁰ Vgl. Bitkom: DSFA-Leitfaden, S. 26.

⁴¹ Siehe BSI: IT-Grundschutz-Kompodium, in der jeweils aktuellen Version unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html.

Zu Risiken im Zusammenhang mit Videoüberwachung: Bei der Videoüberwachung entstehen vor allem Risiken für die Gewährleistungsziele Vertraulichkeit, Datenminimierung, Transparenz und Intervenierbarkeit. Werden Aufnahmen der Personen gemacht und so deren Bewegungsabläufe und Aufenthalte gespeichert, besteht das Risiko, dass auf die Aufnahmen der Kamera von unbefugten Personen zugegriffen werden kann. Auch besteht das Risiko, dass die Aufnahmen länger als erforderlich gespeichert werden. Zudem existiert die Gefahr, dass die aufgenommenen Personen nicht über die Videoüberwachung informiert werden und so keine Möglichkeit haben, sich dieser zu entziehen oder Rechte gegen diese geltend zu machen. Auch besteht das Risiko, dass keine Prozesse eingerichtet sind, wie auf Anfragen betroffener Personen hinsichtlich der Videoüberwachung reagiert und mit diesen umgegangen wird.

Praxisbeispiel 4-3

Es bietet sich an, eine **tabellarische Auflistung** der Risiken nach den Gewährleistungszielen vorzunehmen, die folgende Spalten enthält:⁴²

- **Beschreibung** des **Risikos** einschließlich des **Ereignisses**, der **Quelle** und des möglichen **Schadens** (ggf. auch als separate Spalten);
- Betrachtetes **Gewährleistungsziel**;
- **Eintrittswahrscheinlichkeit** (Grad und Begründung);
- **Schadenshöhe** (Grad und Begründung);
- **Risikoklasse**.

Näheres zur Einstufung und Begründung der Eintrittswahrscheinlichkeit, der Schadenshöhe und der Risikoklasse wird in den nächsten Abschnitten erläutert.

Anwendungsbeispiel Software-Einführung: Bei der Verwendung der Software bestehen vor allem Risiken für die Vertraulichkeit der Daten. Ohne hinreichendes Zugriffs- und Berechtigungskonzept könnten unbefugte Beschäftigte oder Dritte auf die Daten in der Software zugreifen. Ohne ausreichende Sicherheit während des Transports und bei der Speicherung könnten die Daten abgefangen oder ausgespäht werden. Dies könnte dazu führen, dass unbefugte Personen Zugriff auf Namen, Adressen, Kennnummern und Vertragsdetails der Kunden erhalten – und diese insbesondere für Identitätsdiebstahl missbrauchen könnten.

Darüber hinaus bestehen insbesondere Risiken für die Datenminimierung, wenn die befugten Beschäftigten mehr Daten in die Software eintragen als nötig. Auch besteht ein Risiko bei der Transparenz der Verarbeitung, wenn die betroffenen Kunden nicht über die Datenverarbeitung in der Software informiert werden. Ein Risiko für die Intervenierbarkeit besteht, wenn die betroffenen Personen nicht über ihre Rechte aufgeklärt werden und so ihre Kontrolle nicht ausüben können. Schließlich existiert auch ein Risiko für die Verfügbarkeit der Daten, wenn diese auf Servern eines Drittanbieters gespeichert werden.

⁴² Vgl. auch Fraunhofer ISI: DSFA-Handbuch, S. 44 f., welche jedoch mehr Spalten empfiehlt.

4.4 Risiken bewerten – Eintrittswahrscheinlichkeit und Schadenshöhe bestimmen

Nachdem die Risiken erfasst und beschrieben wurden, erfolgt die Bewertung der Risiken anhand einer **Abschätzung** der Eintrittswahrscheinlichkeit und der Schadenshöhe aus der **Perspektive der betroffenen Person**.⁴³ Teilt man beiden Komponenten **Zahlenwerte** zu, lassen sich die Risiken in einem Koordinatensystem einordnen. Dies ermöglicht eine **quantitative Bewertung** der Verletzungsmöglichkeit in Bezug auf ein bestimmtes Gewährleistungsziel, welche nach **objektiven Maßstäben** erfolgen sollte (vgl. Erwägungsgrund 76 DSGVO). Entscheidend ist bei dieser (ersten) Bewertung, dass technische und organisatorische Maßnahmen zunächst außer Acht gelassen werden. Die Auswirkungen dieser Abhilfemaßnahmen werden erst in einer zweiten Risikobewertung (der sog. „*Neubewertung*“) berücksichtigt.

Die Einstufung der **Eintrittswahrscheinlichkeit** sollte durch geeignetes Fachpersonal auf Basis des aktuellen Kenntnisstandes erfolgen. Dabei sollte insbesondere berücksichtigt werden:⁴⁴

- wie viele Risikoquellen die Schäden hervorrufen können,
- welche Erfahrungen das Unternehmen bisher gemacht hat,
- mit welcher Wahrscheinlichkeit es zu Folgeschäden kommt,
- ob Statistiken zur Wahrscheinlichkeit eines Schadenseintritts vorliegen und
- ob bekannte oder mögliche Schwachstellen in IT-Systemen existieren.

Die Einstufung der **Schadenshöhe** sollte unter qualitativen und quantitativen Erwägungen erfolgen und insbesondere berücksichtigen:⁴⁵

- ob besonders schützenswerte Daten nach Art. 9 DSGVO (z.B. Gesundheitsdaten oder genetische Daten),
- Daten schützenswerter Personengruppen (z.B. Kinder und Beschäftigte) oder
- eindeutig identifizierbare Daten (z.B. Personalausweisnummer oder IBAN) verarbeitet werden,
- ob ein Schaden kaum oder komplett unumkehrbar ist,
- ob sich die betroffenen Personen der Verarbeitung entziehen können sowie
- wie viele Personen oder Daten betroffen sind.

In seiner einfachsten Form könnte die Einordnung dreistufig erfolgen: niedrige, mittlere und hohe Eintrittswahrscheinlichkeit oder Schadenshöhe.⁴⁶ Hierbei handelt es sich um das Minimum an Differenziertheit, weil weniger Bewertungsstufen kaum noch brauchbare Risikobewertungen zulassen. Deshalb sind **mindestens vier Stufen** für Eintrittswahrscheinlichkeit und Schadenshöhe zu empfehlen:⁴⁷

- **geringfügig** (Grad 1);
- **überschaubar** (Grad 2);

⁴³ DSK: SDM, S. 10.

⁴⁴ Vgl. DSK: Kurzpapier Nr. 18, S. 4 f.; vgl. Bitkom: DSFA-Leitfaden, S. 30.

⁴⁵ Vgl. DSK: Kurzpapier Nr. 18, S. 5; vgl. Fraunhofer ISI: DSFA-Handbuch, S. 47.

⁴⁶ Vgl. Forum Privatheit: DSFA-Handbuch, S. 31.

⁴⁷ Vgl. DSK: Kurzpapier Nr. 18, S. 4; ähnlich auch Bitkom: DSFA-Leitfaden, S. 29, 31, sowie Fraunhofer ISI: DSFA-Handbuch, S. 47.

- **gravierend** (Grad 3);
- **groß** (Grad 4).

Dabei sollte eine **nachvollziehbare Beschreibung** der Kategorien erfolgen, wodurch die Einstufung auch über mehrere DSFA hinweg innerhalb des Unternehmens einheitlich und verständlich bleibt.⁴⁸ Dafür kann eine **Einstufungstabelle** genutzt werden.⁴⁹ Die Einordnung der einzelnen Risiken in diese Kategorien sollte zudem jeweils **begründet** werden.⁵⁰

4.5 Risiken bewerten – Risikomatrix erstellen und Risikoklasse bestimmen

Die konkrete Bewertung der Risiken durch Einteilung in Risikoklassen erfolgt mithilfe einer graphisch darstellbaren **Risikomatrix** (siehe rechte Abbildung).⁵¹ Dazu werden die ermittelten Werte für Eintrittswahrscheinlichkeit und Schadenshöhe miteinander **multipliziert**.⁵² Die Einfärbung stellt einen Bewertungsvorschlag für die zu ermittelnde **Risikoklasse** dar. Wegen der Systematik der DSGVO erscheint dabei folgende Abstufung angebracht:⁵³

S4	4	8	12	16
S3	3	6	9	12
S2	2	4	6	8
S1	1	2	3	4
	E1	E2	E3	E4

- **„geringes Risiko“** (grün, 1-2);
- **„mittleres Risiko“** (gelb, 3-9);
- **„hohes Risiko“** (rot, 12-16).

Eine dreistufige Einteilung der Risikoklassen dürfte die Minimalanforderung sein. Denn weniger Risikoeinteilungen lassen kaum noch eine differenzierte Bewertung zu. Weitere Risikoklassen einzusetzen ist möglich und erfordert dann oftmals eine entsprechende Anpassung der Skalen für Eintrittswahrscheinlichkeit und Schadenshöhe.

4.6 Risiken behandeln – Technische und organisatorische Maßnahmen prüfen

Nach der Feststellung der bestehenden Risiken für die Rechte und Freiheiten natürlicher Personen müssen die **Möglichkeiten zur Behandlung dieser Risiken** geprüft und dokumentiert werden (Art. 35 Abs. 7 lit. d DSGVO). Dies können in erster Linie technische oder organisatorische Maßnahmen sein, die geeignet sind, die Eintrittswahrscheinlichkeit oder die Schadenshöhe der betrachteten Risiken zu reduzieren (**Risikominimierung durch Abhilfemaßnahmen**).⁵⁴ Ziel der Risikobehandlung ist es, dass unter Berücksichtigung der Abhilfemaßnahmen keine hohen Risiken mehr für die betroffenen Personen vorliegen und dadurch die Verarbeitungstätigkeit insgesamt **sicherer** und **datenschutzfreundlicher** wird.

⁴⁸ Vgl. Fraunhofer ISI: DSFA-Handbuch, S. 47; vgl. Bitkom: DSFA-Leitfaden, S. 29.

⁴⁹ Siehe Beispiele bei Bitkom: DSFA-Whitepaper, S. 50 ff.

⁵⁰ DSK: Kurzpapier Nr. 18, S. 4.

⁵¹ So auch DSK: Kurzpapier Nr. 18, S. 5; Bitkom: DSFA-Leitfaden, S. 32; Fraunhofer ISI: DSFA-Handbuch, S. 46.

⁵² Anders hingegen Forum Privatheit: DSFA-Whitepaper, S. 33, wonach eine solche Multiplikation beim Datenschutz nicht praktikabel sei.

⁵³ Vgl. DSK: Kurzpapier Nr. 18, S. 2; so auch Bitkom: DSFA-Leitfaden, S. 31. Anders hingegen wohl Forum Privatheit: DSFA-Whitepaper, S. 31, wo die Berechnung des Risikos abgelehnt und sich stattdessen bei der Feststellung eines hohen Risikos und der Bestimmung der Abhilfemaßnahmen an der Eingriffsintensität und dem Schutzbedarf orientiert wird.

⁵⁴ Vgl. DSK: Kurzpapier Nr. 18, S. 6.

Anwendungsbeispiel Software-Einführung: Insbesondere folgende Abhilfemaßnahmen zur Risikominimierung werden bei der Software eingesetzt:

- Deaktivierung zusätzlicher Funktionen;
- Regelmäßige Backups und Rückgriff auf alternative Server bei Serverausfall;
- Transportverschlüsselung und Inhaltsverschlüsselung der Daten auf dem Server;
- Zugriffs- und Rollensystem, restriktive Zuordnung der Berechtigungen, Einbindung der Personalabteilung, Support durch eigenes Personal;
- Automatische Löschung auf Grundlage der festgelegten Aufbewahrungsfristen;
- Schulung zur Nutzung der Software;
- Datenschutzhinweise für Beschäftigte und Kunden;
- Nutzungsrichtlinie für die Software, hohe Mindestanforderungen an Passwörter, automatischer Logout.

Neben der Risikominimierung kann Risiken grundsätzlich auch mit **Risikovermeidung** oder **Risikoakzeptanz** begegnet werden, wobei letzteres bei hohen Risiken nicht infrage kommt und im Übrigen besonderer Begründung bedarf, wieso keine Reduzierung auf ein niedrigeres Risiko vorgenommen wird.⁵⁵

Viele **praktische Beispiele** für Abhilfemaßnahmen zur Risikominimierung bieten das **SDM** der DSK, gruppiert nach Gewährleistungszielen,⁵⁶ sowie die **Knowledges Bases** der CNiL (PIA-3).⁵⁷ Auch kann das bereits erwähnte **IT-Grundschutz-Kompendium** herangezogen werden. Im Übrigen ist es aber unerlässlich, an dieser Stelle **Fachleute mit Expertise und Erfahrung** aus der IT, der IT-Sicherheit und des Datenschutzes hinzuzuziehen, die kooperativ zusammenarbeiten, um die erforderlichen technischen und organisatorischen Maßnahmen (TOM) zu erörtern.

Die **Dokumentation** zur Risikominimierung sollte mindestens Folgendes umfassen:⁵⁸

- Abhilfemaßnahmen;
- Verantwortliche Personen zur Umsetzung der Maßnahmen;
- Frist zur Umsetzung der Maßnahmen (sofern diese nicht bereits umgesetzt sind).

4.7 Neubewertung unter Einbeziehung getroffener Maßnahmen

Nach der Prüfung der Maßnahmen erfolgt die Neubewertung unter Berücksichtigung der getroffenen Maßnahmen. Dabei wird der Grad der Eintrittswahrscheinlichkeit und der Schadenshöhe sowie die daraus resultierende Risikoklasse (siehe 4.4 und 4.5) überprüft und ggf. neu festgelegt. Anschließend wird das **Gesamtrisiko** der Verarbeitungstätigkeit (auch „**Restrisiko**“) festgestellt, welches sich an der höchsten ermittelten Risikoklasse der einzelnen Risikoszenarien orientiert und Basis für die abschließende Beurteilung der DSFA ist.⁵⁹

⁵⁵ Vgl. Bitkom: DSFA-Leitfaden, S. 33; vgl. Fraunhofer ISI: DSFA-Handbuch, S. 47; anders Forum Privatheit: DSFA-Whitepaper, S. 33, 34, wo die Risikoakzeptanz nicht als Risikobehandlung anerkannt wird.

⁵⁶ DSK: SDM, S. 30 ff.

⁵⁷ CNiL: PIA-Knowledge Bases, S. 14 ff.

⁵⁸ Vgl. Bitkom: DSFA-Leitfaden, S. 34.

⁵⁹ Vgl. DSK: Kurzpapier Nr. 18, S. 5.

5. Finanzierungs- und Überprüfungsphase

5.1 Umsetzung der Maßnahmen

Die im Rahmen der Risikoanalyse ermittelten technischen und organisatorischen Maßnahmen werden spätestens nach der Risikoanalyse und grundsätzlich vor dem Einsatz der Verarbeitungstätigkeit umgesetzt.⁶⁰ Dabei muss auch die **Wirksamkeit der Maßnahmen** in Tests **überprüft** und **protokolliert** werden.⁶¹ Sollte sich dabei herausstellen, dass die Maßnahmen nicht die gewünschte Wirkung entfalten, müssten sie angepasst und ergänzt werden. Die Risikoanalyse sollte in diesem Fall mit den neu gewonnenen Erkenntnissen überprüft und erweitert werden. Im Übrigen sollten für den Test der Wirksamkeit der Maßnahmen nach Möglichkeit **keine Echtdate**n verwendet werden.⁶² Ist dies unausweichlich, so sollte der Umfang auf ein Minimum reduziert werden.

5.2 Abschließende Beurteilung

Nach der Umsetzung der Maßnahmen folgt die abschließende Beurteilung der Verarbeitungstätigkeit, insbesondere hinsichtlich der Verhältnismäßigkeit, der ermittelten Risiken, der umgesetzten oder geplanten Abhilfemaßnahmen sowie des **Restrisikos** der Verarbeitung. Diese kann auch von einer/einem unabhängigen Dritten oder der/dem **Datenschutzbeauftragten** erfolgen.⁶³ Das Ergebnis dieser abschließenden Beurteilung, welche auch die Notwendigkeit zur Konsultation der Aufsichtsbehörde einschließt, kann sodann der verantwortlichen Stelle zur Freigabe vorgelegt werden.

5.3 Konsultation der Aufsichtsbehörde

Die Konsultation der zuständigen Aufsichtsbehörde kann in zwei Fällen erforderlich sein:

- die abschließende Beurteilung ergibt, dass trotz der umgesetzten Maßnahmen (weiterhin) ein **hohes Restrisiko** für die Rechte und Freiheiten natürlicher Personen besteht – Art. 36 Abs. 1 DSGVO; oder
- die verantwortliche Stelle wird für Verarbeitungstätigkeiten zur **Erfüllung einer im öffentlichen Interesse liegenden Aufgabe durch nationales Recht verpflichtet**, die vorherige Genehmigung einzuholen, etwa für Verarbeitungen zum Zwecke der sozialen Sicherheit und der öffentlichen Gesundheit – Art. 36 Abs. 5 DSGVO.

Ein **hohes Restrisiko** liegt etwa vor, wenn:⁶⁴

- erhebliche oder gar unumkehrbare und nicht zu bewältigende Folgen für die betroffenen Personen existieren, die beispielsweise ihr Leben, ihre Arbeitsstelle oder finanzielle Situation bedrohen, oder

⁶⁰ Vgl. DSK: Kurzpapier Nr. 5, S. 4.

⁶¹ DSK: Kurzpapier Nr. 5, S. 4; DSK: Kurzpapier Nr. 18, S. 6.

⁶² Vgl. Forum Privatheit, DSFA-Whitepaper, S. 36.

⁶³ DSK: Kurzpapier Nr. 5, S. 4.

⁶⁴ Siehe Art.-29-DS-Gruppe: WP 248, S. 23.

- der Eintritt des Risikos unausweichlich erscheint, beispielsweise weil es keine Möglichkeit gibt, den Datenzugriff zu verhindern oder Sicherheitsmängel nicht geschlossen werden können.

Im Falle der Konsultation sind der Aufsichtsbehörde alle erforderlichen Informationen nach Art. 36 Abs. 3 DSGVO, insbesondere der DSFA-Bericht selbst, zur Verfügung zu stellen. Die Aufsichtsbehörde prüft daraufhin die Verarbeitungstätigkeit und die in der DSFA vorgenommene Risikoanalyse. Sofern sie der Auffassung ist, dass die Verarbeitungstätigkeit nicht im Einklang mit der DSGVO steht, kann sie **Empfehlungen** (etwa für zusätzliche Maßnahmen) geben oder von ihren Befugnissen aus Art. 58 DSGVO (insbesondere Warnung, Anweisung oder **Untersagung** der Verarbeitungstätigkeit) Gebrauch machen.⁶⁵ Sofern sich die Aufsichtsbehörde auch nach der gesetzlichen Beantwortungsfrist von bis zu **14 Wochen** nicht auf das Konsultationsschreiben zurückmeldet, könnte zwar zunächst von der Zulässigkeit der Verarbeitungstätigkeit ausgegangen werden.⁶⁶ Allerdings steht es der Aufsichtsbehörde auch danach noch frei, von ihren Befugnissen aus Art. 58 DSGVO Gebrauch zu machen (vgl. Erwägungsgrund 94 DSGVO).

Eine Untersagung würde dazu führen, dass das geprüfte Verfahren nicht zur Anwendung kommen darf. Deshalb ist es wichtig, die Risikoanalyse so ausführlich und umfassend wie für den Prüfungsgegenstand erforderlich durchzuführen. Dann ergeben sich bereits auf Seiten der verantwortlichen Stelle die zu treffenden technischen und organisatorischen Maßnahmen. Und falls im Ergebnis doch noch ein hohes Restrisiko verbleibt, erhöht eine umfassend vorgenommene Risikoanalyse die Chance, dass die Aufsichtsbehörde auf deren Grundlage nur Empfehlungen ausspricht und von einer Untersagung absieht. Die Empfehlungen sind entsprechend umzusetzen und eine Neubewertung vorzunehmen.

5.4 Freigabe, Überprüfung und Wiedervorlage

Schließlich kann die Verarbeitungstätigkeit, wenn **kein hohes Restrisiko** (mehr) besteht, von der verantwortlichen Stelle formal freigegeben werden.⁶⁷ Doch damit endet der Prozess einer DSFA nicht; dieser umfasst vielmehr (vgl. Art. 35 Abs. 11 1. Hs. DSGVO):

- die **fortlaufende Überwachung** der Verarbeitungstätigkeit,
- die Prüfung der **Notwendigkeit weiterer Abhilfemaßnahmen** zur Risikoreduktion,
- die **Sicherstellung der Wirksamkeit der Maßnahmen** und
- die **regelmäßige Überprüfung** in Form einer Wiedervorlage der DSFA.

Je nach Kritikalität des Prüfungsgegenstands bieten sich hier beispielsweise **Wiedervorlagen** alle sechs Monate bis hin zu drei Jahren an. Die Überwachung im Rahmen der DSFA kann auch in ein **Datenschutz-Management** eingebunden werden. Sofern sich jedoch **Rahmenbedingungen der Verarbeitungstätigkeit ändern**, welche zu einem höheren Risiko führen, muss sie **sofort** im Rahmen der DSFA wieder überprüft werden (vgl. Art. 35 Abs. 11 2. Hs DSGVO).⁶⁸

⁶⁵ Vgl. DSK: Kurzpapier Nr. 5, S. 5.

⁶⁶ Vgl. Bitkom: DSFA-Leitfaden, S. 49.

⁶⁷ DSK: Kurzpapier Nr. 5, S. 4.

⁶⁸ Vgl. Art.-29-DS-Gruppe: WP 248, S. 25; DSK: Kurzpapier Nr. 5, S. 5.

Eine **frühere Wiedervorlage**, etwa nach drei oder sechs Monaten, kann jedoch auch notwendig sein, wenn bisher noch nicht alle Maßnahmen umgesetzt sind oder die Wirksamkeit bestimmter Maßnahmen erneut überprüft werden soll.



6. Empfehlung aus der Praxis

6.1 Wichtigkeit guter Vorbereitung, Planung und Dokumentation

In der Beratungspraxis erleben wir, dass eine gute Vorbereitung, klare Absprachen und die Übermittlung aller relevanten Dokumente wichtig sind, um eine gelungene DSFA durchzuführen. Fällt während des Schreibens des DSFA-Berichts auf, dass an bestimmten Punkten **Informationen fehlen** oder **Unklarheit** herrscht, können diese zwar nachgefragt werden. Dadurch verzögert sich aber die Durchführung der DSFA, insbesondere durch häufige Unterbrechungen, die eine erneute Einarbeitung erfordern. Auch entstehen Schwierigkeiten, wenn sich im Laufe der DSFA herausstellt, dass der **Prüfungsgegenstand** anfangs nicht klar genug umrissen wurde und sich doch als **umfangreicher** herausstellt. Dann ist die komplette Überarbeitung des DSFA-Berichts aufgrund der neuen Rahmenbedingungen erforderlich, die auch wieder zeitaufwändig ist. All das sind **vermeidbare Situationen**, die durch eine **von Anfang an strukturierte und gut geplante Vorgehensweise** verhindert werden können.

6.2 Lösungsorientierte Herangehensweise

Als Anwältinnen und Anwälte orientieren wir uns an einer lösungsorientierten Herangehensweise bei der Durchführung der DSFA. Ziel der DSFA ist es, insbesondere mittels der Risikoanalyse bestehende Risiken aufzudecken und mit Abhilfemaßnahmen zu minimieren, um die **gewünschten Geschäftsprozesse datenschutzkonform ablaufen** lassen zu können. Die DSFA hilft also, die eigenen Prozesse zu verbessern und zu optimieren – nicht nur für die betrachtete Verarbeitungstätigkeit allein, sondern auch nachhaltig für weitere Prozesse, die im Unternehmen stattfinden. In den allermeisten Fällen kann so den in der Erstbewertung festgestellten hohen Risiken durch technische und organisatorische Maßnahmen abgeholfen werden. Und sollten auch bei der Neubewertung noch hohe Risiken existieren, dient die DSFA auch als **Selbstschutz für das Unternehmen**: es kann von einer riskanten Verarbeitungstätigkeit absehen und so im Zweifel Konflikte mit der Aufsichtsbehörde vermeiden – oder die Verarbeitungstätigkeit ist so wichtig, dass die Konsultation mit der Behörde gesucht werden muss. In beiden Fällen bietet die DSFA dem Unternehmen enorme Vorteile beim Aufbau und der Realisierung datenschutzkonformer Geschäftsprozesse.

6.3 Einholung von Fachexpertise

Die Durchführung einer DSFA erfordert ein **interdisziplinäres Team**, insbesondere mit juristischer Fachexpertise im Bereich des Datenschutzes. Vor allem bei umfangreicheren technischen Anwendungen, beim Einsatz von KI, bei der Verarbeitung von Gesundheitsdaten oder bei automatisierten Entscheidungen sind ausführliche datenschutzrechtliche Prüfungen und Erörterungen notwendig. Anwalt:innen mit **Erfahrung und Wissen** sollten insbesondere bei diesen Bereichen herangezogen werden. Denn es existieren in den unterschiedlichen Bereichen und Branchen **zusätzliche Anforderungen und Problemstellungen**, bei denen die **Kenntnisse aus der Praxis** unerlässlich sind. Daher möchten wir nachdrücklich empfehlen, datenschutzrechtliche Fachexpertise einzuholen, um Fehler bei der Durchführung einer DSFA zu vermeiden, die womöglich negative Auswirkungen auf das Unternehmen haben.

7. Anhang: DSFA-Modelle

7.1 Standard-Datenschutzmodell der DSK

Das Standard-Datenschutzmodell („SDM“) in der Version 3.0 der Datenschutzkonferenz („DSK“) zeigt die **zentralen datenschutzrechtlichen Anforderungen** aus der DSGVO auf (Teil B), systematisiert sie und fasst sie als **Gewährleistungsziele** zusammen (Teil C).⁶⁹

- **Datenminimierung:** Beschränkung der Verarbeitung auf das unbedingt notwendige Maß;
- **Verfügbarkeit:** Zugriffsmöglichkeit auf personenbezogene Daten und ihre Wiederherstellbarkeit;
- **Integrität:** Funktionstüchtigkeit und Belastbarkeit informationstechnischer Prozesse und Systeme;
- **Vertraulichkeit:** Keine unbefugte Kenntnisnahme bzw. kein unbefugter Zugriff auf personenbezogene Daten;
- **Nichtverkettung:** Keine Zusammenführung von Daten unter Missachtung der Zweckbindung;
- **Transparenz:** Erfüllung der Informations- und Nachweispflichten;
- **Intervenierbarkeit:** Wirksame Geltendmachung der Rechte betroffener Personen.

Darüber hinaus zeigt das SDM auch beispielhaft viele verschiedene **technische und organisatorische Maßnahmen** zur Erfüllung der Gewährleistungsziele auf (Teil D1). Auch beschreibt das SDM die mögliche Strukturierung, Aufbereitung und Erfassung von Verarbeitungstätigkeiten (Teil D2), dabei insbesondere deren Einordnung in Lebenszyklus-Phasen der Datenverarbeitung und in Verarbeitungsebenen (Fachverfahren, Fachapplikation und Infrastruktur), die im Modell des sogenannten „SDM-Würfel“ schematisch dargestellt werden. Außerdem enthält das SDM Erwägungen zur Erfassung und Bewertung von **Risiken** und zur Klassifizierung der Risikohöhe mit Zuordnung zum Schutzbedarf (Teil D3), wobei diesbezüglich auch auf das Kurzpapier Nr. 18 der DSK verwiesen wird. Zudem werden die Grundlagen zur Umsetzung eines **Datenschutz-Managements** erläutert (Teil D4).

Im Ergebnis ist das SDM damit zwar keine Handlungsanleitung zur Durchführung einer DSFA, bietet jedoch einen guten Überblick über die Gewährleistungsziele und die Abhilfemaßnahmen im Rahmen einer Risikoanalyse, die auch in diesem Whitepaper berücksichtigt wurden.

⁶⁹ Vgl. DSK: SDM, S. 25 - 29. Das SDM ermittelte die Gewährleistungsziele insbesondere aus den Artikeln 5, 6, 7, 9, 12 - 22, 24, 25, 28, 32 - 35, 38, 58 der DSGVO.

7.2 PIA der CNIL

Die französische Aufsichtsbehörde CNIL hat bereits 2015 eine **Methodik** zur Durchführung und zum Aufbau einer DSFA veröffentlicht (PIA-1: *Methodology*), die zuletzt 2018 überarbeitet wurde und die DSFA als Kreislauf beschreibt:⁷⁰

- **„Context“**: Festlegung und Beschreibung der Verarbeitungstätigkeit, insbesondere der Verarbeitungszwecke und der beteiligten und betroffenen Personen;
- **„Fundamental principles“**: Ermittlung der existierenden oder geplanten Maßnahmen zur Erfüllung wesentlicher datenschutzrechtlicher Prinzipien, insbesondere die Datenschutzgrundsätze aus Art. 5 DSGVO, die Rechte betroffener Personen nach Art. 12 – 22 DSGVO, die Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO und zum Drittlandtransfer nach Art. 44 ff. DSGVO;
- **„Risks“**:
 - Ermittlung der existierenden oder geplanten technischen und organisatorischen Maßnahmen;
 - Ermittlung der Risikoquellen, der Auswirkungen/Schadenshöhe von befürchteten Bedrohungen auf die betroffenen Personen und deren Eintrittswahrscheinlichkeit;
- **„Validation“**: Bewertung der Risiken und Entscheidung zur Freigabe (unter Bedingungen) oder zur Wiederholung der vorherigen Schritte (Umsetzung zusätzlicher Maßnahmen).

Gegenüber der in Deutschland verbreiteten Vorgehensweise, zuerst die Risiken zu ermitteln und dann die Abhilfemaßnahmen zu erörtern, geht die PIA der CNIL den umgekehrten Weg und führt zunächst die vorhandenen oder geplanten Maßnahmen auf, um anschließend zu prüfen, ob diese für die bestehenden Risiken ausreichen. Beide Methoden führen jedoch letztendlich zum selben Ziel, die Risiken für die betroffenen Personen bei einer Verarbeitungstätigkeit zu bewerten und zu minimieren.

Ergänzt wird die Methodik mit **Vorlagen** und **Mustern** zur Umsetzung der DSFA (PIA-2: *Templates*) sowie einem umfangreichen **Nachschlagewerk** zur Erläuterung von Begriffen und verschiedenen technischen und organisatorischen Maßnahmen (PIA-3: *Knowledge Bases*). Schließlich stellt die CNIL auch eine **Software** zur Durchführung der DSFA auf Grundlage ihrer Methodik bereit.⁷¹

Die von der CNIL vorgelegten Dokumente und die Software stellen im Gegensatz zum SDM tatsächlich ein zur Durchführung der DSFA direkt anwendbares Instrument dar. Zugleich existieren teils erhebliche Unterschiede im Aufbau und der Methodik zu der in diesem Whitepaper vorgeschlagenen Vorgehensweise. Insgesamt würden wir die PIA der CNIL eher für einfachere Verarbeitungstätigkeiten oder Vorprüfungen empfehlen, da sich individuellere oder komplexere Verarbeitungen in PIA meist nicht vollständig abbilden lassen.

⁷⁰ Vgl. CNIL: PIA-Methodology, S. 3 f.

⁷¹ Siehe: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>.

8. Literaturverzeichnis

Autor	Titel	Datum	Zitiert als
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom)	Risk Assessment & Datenschutz-Folgenabschätzung – Leitfaden Link	2017	Bitkom: DSFA-Leitfaden, [S.]
Commission Nationale de l'Informatique et des Libertés	Privacy Impact Assessment (PIA) – Knowledge Bases Link	Februar 2018	CNiL: PIA-Knowledge Bases, [S.]
Commission Nationale de l'Informatique et des Libertés	Privacy Impact Assessment (PIA) – Methodology Link	Februar 2018	CNiL: PIA-Methodology, [S.]
Datenschutzgruppe nach Artikel 29	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 Link	04.10.2017	Art.-29-DS-Gruppe: WP 248, [S.]
Datenschutzkonferenz	Das Standard-Datenschutzmodell, Version 3.0 Link	24.11.2022	DSK: SDM, [S.]
Datenschutzkonferenz	Kurzpapier Nr. 5 – Datenschutz-Folgenabschätzung nach Art. 35 DSGVO Link	17.12.2018	DSK: Kurzpapier Nr. 5, [S.]
Datenschutzkonferenz	Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 Link	17.10.2018	DSK: Positivliste, [S.]

Datenschutz-konferenz	Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen Link	17.07.2020	DSK: Orientierungshilfe Videoüberwachung, [S.]
Datenschutz-konferenz	Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen Link	26.04.2018	DSK: Kurzpapier Nr. 18, [S.]
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt	White Paper: Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, 3. Auflage Link	November 2017	Forum Privatheit: DSFA-Whitepaper, [S.]
Fraunhofer-Institut für System- und Innovationsforschung ISI	Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis Link	2020	Fraunhofer ISI: DSFA-Handbuch, [S.]
S. Gonscherowski, T. Herber, R. Robrahn1, M. Rost, R. Weichelt	Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens (V 0.10) Link	06.11.2017	SDM-Planspiel, [S.]

Unsere Experten



Simone Rosenthal

Rechtsanwältin und Partnerin
SCHÜRMAN ROSENTHAL DREYER Rechtsanwälte

Beratungsschwerpunkte

IT- und Datenschutzrecht,
Wettbewerb, Marketing & Vertrieb, Vertragsrecht



Roman von der Heide

Rechtsanwalt, Associated Partner
Fachanwalt für Informationstechnologierecht bei
SCHÜRMAN ROSENTHAL DREYER Rechtsanwälte

Beratungsschwerpunkte

Datenschutzrecht, IT-Recht & Digitales Business



Ilan Leonard Selz, LL.M. (Minnesota)

Rechtsanwalt, Senior Associate
SCHÜRMAN ROSENTHAL DREYER Rechtsanwälte

Beratungsschwerpunkte

IT- und Datenschutzrecht,
Wettbewerb, Marketing & Vertrieb



SCHÜRMANN ROSENTHAL DREYER Rechtsanwälte

SCHÜRMANN ROSENTHAL DREYER Rechtsanwälte ist eine hochspezialisierte Anwalts-Boutique mit dem Schwerpunkt Digitales & Recht. Die Kanzlei unterstützt Ihre Mandanten von der Planung bis zur Umsetzung ihrer IT- und Digitalisierungsprojekte. SCHÜRMANN ROSENTHAL DREYER stehen für eine enge, vertrauensvolle, agile Zusammenarbeit und eine zukunftsorientierte Beratung.

Mehr Informationen finden Sie auf der Webseite www.srd-rechtsanwaelte.de

**SCHÜRMANN
ROSENTHAL
DREYER**
RECHTSANWÄLTE

SCHÜRMANN ROSENTHAL DREYER Rechtsanwälte
Am Hamburger Bahnhof 4 10557 Berlin

office@srd-rechtsanwaelte.de
www.srd-rechtsanwaelte.de

BUJ - Bundesverband der Unternehmensjuristen e. V.

Der Bundesverband der Unternehmensjuristen e.V. (BUJ) ist die älteste Interessenvertretung für Juristinnen und Juristen in Rechtsabteilungen von Unternehmen sowie Institutionen, Verbänden und Körperschaften und bietet seinen Mitgliedern ein Forum für den gewinnbringenden Meinungs- und Erfahrungsaustausch unter Kolleg:innen.

Mehr Informationen finden Sie auf der Webseite www.buj-verband.de

BUJ
Bundesverband
der Unternehmensjuristen

Bundesverband der Unternehmensjuristen e. V.
Friedrichstraße 94 10117 Berlin

kontakt@buj-verband.de
www.buj-verband.de