

Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.



Deutsche Gesellschaft für Medizinische Informatik, Biometrie und
Epidemiologie e. V.



Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Deutsche Krankenhausgesellschaft e. V.



Autoren

Ina Haag	Deutsche Krankenhausgesellschaft e.V.
Andrea Hauser	Deutsche Krankenhausgesellschaft e.V.
Christoph Isele	Cerner Deutschland GmbH
Lukas Mempel	Sana Kliniken AG
Christoph Nahrstedt	Nuance Communications
Jan Neuhaus	Deutsche Krankenhausgesellschaft e.V.
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Ratajczak und Partner mbB Rechtsanwälte
Stefan Wunschel	Sana Kliniken AG

Stand: 10.04 2018

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:



- Teilen: Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: Das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

<https://creativecommons.org/licenses/by-sa/4.0/deed.de>

bzw. für den vollständigen Lizenztext

<https://creativecommons.org/licenses/by-sa/4.0/legalcode>

Inhaltsverzeichnis

Zusammenfassung	4
1 Einführung	5
2 Intention des europäischen Gesetzgebers bzgl. der DSFA und Anwendung auf laufende Verarbeitungsvorgänge	6
3 Erläuterungen zum rechtlichen Hintergrund	7
3.1 Art 35 und seine tatbestandlichen Voraussetzungen	7
3.1.1 Rechtmäßigkeit der Datenverarbeitung	7
3.1.2 Rechte und Freiheiten natürlicher Personen	9
3.1.3 Risiko der Verarbeitung	9
3.1.4 „Neue Technologien“	11
3.1.5 Art und Umfang der Verarbeitung, Art. 35 Abs. 1 S. 1 DS-GVO	11
3.1.6 Zwecke der Verarbeitung, Art. 35 Abs. 1 S. 1 DS-GVO	12
3.1.7 Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, Art. 35 Abs. 3 lit. a DS-GVO	15
3.1.8 Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten, Art. 35 Abs. 3 lit. b DS-GVO	16
3.1.9 Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche, Art. 35 Abs. 3 lit. c DS-GVO	16
3.2 „Befreiung“ von der Datenschutz-Folgenabschätzung	17
3.3 Inhalt einer Datenschutzfolgenabschätzung, Art. 35 Abs. 7 DS-GVO	18
3.4 Weitergehende Anforderungen	18
3.4.1 Einbindung des Datenschutzbeauftragten, Art. 35 Abs. 2 DS-GVO	18
3.4.2 Standpunkt der Betroffenen, Art. 35 Abs. 9 DS-GVO	18
3.4.3 Überprüfung durch den Verantwortlichen, Art. 35 Abs. 11 DS-GVO	20
3.4.4 Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO	20
3.5 Verantwortlichkeiten, Art. 35 Abs. 1, Art. 4 Nr. 7 DS-GVO	20
3.6 Kumulierte Folgenabschätzung, Art. 35 Abs. 1 S. 2 DS-GVO	21
3.7 Folgen/Vorherige Konsultation der Aufsichtsbehörde, ErwGr. 84, Art. 36 Abs. 1 DS-GVO	21
3.8 Bedeutung für das deutsche Gesundheitswesen	22
3.9 Sanktionierung	22
4 Vorgaben durch die Aufsichtsbehörden	24
4.1 Listen von Verarbeitungsvorgängen	24
4.2 Aufsichtsbehörden: eine DSFA ist erforderlich ...	25
4.2.1 Beispiel „hospital information system“	26
4.3 Aufsichtsbehörden: eine DSFA ist nicht erforderlich ...	27
4.4 Aufsichtsbehörden: Vorgehen bei einer DSFA	27

5	Vorgehensweise bei der Erstellung einer Datenschutz-Folgenabschätzung	29
5.1	Feststellen, ob eine DSFA notwendig ist oder nicht	29
5.1.1	Keine Datenschutz-Folgenabschätzung erforderlich?	31
5.1.2	Fälle, in denen eine Datenschutz-Folgenabschätzung durchgeführt werden muss	31
5.2	Vorbereitung	31
5.2.1	DSFA-Team	32
5.2.2	Einbeziehung der Stakeholder	32
5.3	Durchführung	33
5.3.1	Analyse der Auswirkungen der Verarbeitungsprozesse	33
5.3.2	Abschätzung des datenschutzrechtlichen Risikos	34
5.3.3	Umgang mit den datenschutzrechtlichen Risiken	37
5.4	Bericht	37
6	Vorschlag für die strukturierte Dokumentation einer Datenschutz-Folgenabschätzung (DSFA-Bericht)	39
6.1	Beschreibung des Verarbeitungsverfahrens	39
6.1.1	Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien	39
6.2	Welche Daten werden verarbeitet?	40
6.2.1	Welche Datenarten werden verarbeitet?	40
6.2.2	Wo werden die Daten erhoben?	40
6.2.3	Darstellung der potenziellen Risiken	41
6.3	Zwecke und Mittel der Verarbeitung	41
6.3.1	Begründung, warum die Informationen verarbeitet werden müssen	41
6.3.2	Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung	41
6.3.3	Darstellung der Erlaubnistatbestände	41
6.3.4	Darstellung der Speicherdauer	41
6.3.5	Darstellung der potenziellen Risiken	41
6.4	Weitergabe der Daten	42
6.4.1	Mit wem werden die Daten geteilt?	42
6.4.2	Darstellung der potenziellen Risiken	42
6.5	Wahrung der Betroffenenrechte	42
6.5.1	Information des Betroffenen	42
6.5.2	Auskunftsrecht	42
6.5.3	Widerspruchsrecht	43
6.5.4	Recht auf Berichtigung und Vervollständigung	43
6.5.5	Recht auf Löschen („Vergessenwerden“)	43
6.5.6	Recht auf Einschränkung der Verarbeitung („Sperrung“)	43
6.5.7	Recht auf Datenübertragbarkeit	43
6.6	Gewährleistung der Sicherheit der Daten	43
6.6.1	Darstellung der Erbringung der Anforderungen aus Art. 32 DS-GVO „Sicherheit der Verarbeitung“	44
6.7	Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung	46

6.8	Fazit	47
6.8.1	Abschließende Bewertung	47
6.8.2	Entscheidung bzgl. Information Aufsichtsbehörde	47
7	Beispiele	48
7.1	Beispiele für die Darstellung der Datenarten	48
7.2	Beispiele für Verarbeitungszwecke	49
7.3	Erlaubnistatbestände	50
7.4	Beispiele für Risiken und Ursachen aus der DS-GVO	52
7.5	Beispiele für Risiken aus dem IT-Einsatz	53
8	Checkliste	55
9	Abkürzungen	56
10	Begriffserklärungen	57
11	Literatur	59
11.1	Fachzeitschriften	59
11.2	Standardisierungsorganisationen	59
11.3	Internet	59
11.3.1	Ausarbeitungen	59
11.3.2	Aufsichtsbehörden	60
11.3.3	Behörden/öffentliche Einrichtungen	61
Anlage 1:	Gesetzeswortlaut von Art. 35 DS-GVO	63

Zusammenfassung

Eine Datenschutz-Folgenabschätzung (abgekürzt DSFA) soll in den Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, helfen, die Risiken zu minimieren und durch Darstellung der Maßnahmen zur Reduzierung der Risiken auch für Dritte nachvollziehbar aufzeigen, wie Verantwortliche für die Datenverarbeitung mit diesen Risiken umgehen.

Dabei beschreibt Art. 35 DS-GVO verschiedene Fälle, in denen eine DSFA erfolgen muss. Unabhängig davon steht es jedem Verantwortlichen selbstverständlich frei, auch in anderen Fällen eine DSFA durchzuführen, beispielsweise zur Darstellung der Einhaltung der Vorgaben der DS-GVO hinsichtlich der Sicherheit der Verarbeitung.

Art. 35 DS-GVO definiert die Mindestanforderungen an die Inhalte einer DSFA.

Demzufolge sind diese Mindestinhalte

- a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge;
- b) eine systematische Beschreibung der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- c) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- d) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DS-GVO;
- e) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Anforderungen der DS-GVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

In dieser Praxishilfe wird auf Hinweise der Artikel-29-Datenschutzgruppe ebenso wie auf international bestehende Erfahrungen zur DSFA zurückgegriffen und dargestellt, wie mit dieser Thematik umgegangen werden kann.

1 Einführung

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die EU Datenschutz-Grundverordnung (DS-GVO) unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass diese Risiken durch geeignete Abhilfemaßnahme (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) eingedämmt werden. Das Instrument einer „Datenschutz-Folgenabschätzung“ (DSFA, engl. „Data protection impact assessment“) kann hierfür systematisch eingesetzt werden.¹ Die DSFA stellt ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten dar.² Sie ist in Art. 35 DS-GVO geregelt und bestimmt die Voraussetzungen, unter denen eine DSFA erfolgen muss. Grund dafür ist gemäß ErwGr. 84 die Gewährleistung der Einhaltung der DS-GVO insbesondere in Fällen, in denen eine Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

Die bald für ganz Europa vorgeschriebene DSFA ist im anglo-amerikanischen Raum wesentlicher Bestandteil zur Gewährleistung von „Privacy“ und ist dort in mehr oder weniger abgewandelter Form als „Privacy Impact Assessment“ (PIA) bekannt. Sowohl bei der DSFA als auch bei der PIA wird das gleiche Ziel verfolgt. Denn in beiden Verfahren gilt es, die Auswirkungen eines Verarbeitungsverfahrens personenbezogener Daten auf die Gewährleistung des Rechts auf informationelle Selbstbestimmung des Betroffenen zu untersuchen, darzustellen und zu bewerten.

Bei der Verarbeitung personenbezogener Daten im Gesundheitswesen werden i.d.R. besondere Kategorien personenbezogener Daten verarbeitet, dazu fallen in Einrichtungen wie Krankenhäusern, Forschungseinrichtungen oder Institutionen, die Patientenakten anbieten, zugleich größere Datenmengen an, so dass die Wahrscheinlichkeit, dass hier eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung greift, sehr hoch ist.

Zielgruppe dieser Ausarbeitung sind Verarbeiter von personenbezogenen Daten im Gesundheitswesen. Insbesondere versorgende Einrichtungen/Institutionen und medizinische Forscher sollen in dieser Ausarbeitung eine Unterstützung beim Umgang mit der DSFA finden.

Ferner sei bemerkt, dass diese Ausarbeitung die wesentlichen Inhalte sowie Fragen zum Thema „DSFA“ abhandelt, aber keinen Anspruch auf Vollständigkeit erhebt. Es bleibt vorbehalten, die Ausführungen / Darstellungen den spezifischen Anforderungen des konkreten Anwenders / Nutzers anzupassen.

¹ Datenschutzkonferenz: Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“. Seite 1 Abs. 1, S. 1-3. Online, zitiert am 2017-12-17; Verfügbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_DatenschutzFolgeabschaetzung.pdf;jsessionid=2191F877FFE87422A2F6646332B70D91.2_cid354?_blob=publicationFile&v=2

² Datenschutzkonferenz: Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“. Seite 1 Abs. 2, S. 2. Online, zitiert am 2017-12-17; Verfügbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Kurzpapier_DatenschutzFolgeabschaetzung.pdf;jsessionid=2191F877FFE87422A2F6646332B70D91.2_cid354?_blob=publicationFile&v=2

2 Intention des europäischen Gesetzgebers bzgl. der DSFA und Anwendung auf laufende Verarbeitungsvorgänge

Entsprechend ErwGr. 84 DS-GVO soll „in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen“, eine DSFA durchgeführt werden. Bei der DSFA handelt es sich also um eine Präventionsmaßnahme des europäischen Gesetzgebers, was sich auch im Wortlaut von Art. 35 Abs. 1 DS-GVO wiederfindet, wenn auf „voraussichtliche Risiken“ verwiesen wird. ErwGr. 89 DS-GVO bzw. Art. 35 Abs. 1 DS-GVO weisen darauf hin, dass der europäische Gesetzgeber diesbezüglich insbesondere neue Technologien als Auslöser einer DSFA im Blick hatte.

In diesem Zusammenhang stellt sich die Frage, ab welchem Zeitpunkt, die Pflicht zur Durchführung einer DSFA konkret greift, bzw. auf welche Verarbeitungen diese in zeitlicher Hinsicht abstellt. ErwGr. 171 DS-GVO sieht vor, dass „Verarbeitungen, die zum Zeitpunkt der Anwendung (25. Mai 2016) dieser Verordnung bereits begonnen haben, innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden sollten“. Im Umkehrschluss bedeutet dies, dass Verfahren, die bis zum 24. Mai 2018 beendet sind, von dieser Regelung nicht betroffen sind.

Allerdings ist es fraglich, ob zum Zeitpunkt des Inkrafttretens der DS-GVO etablierte Verfahren, die ohne Beanstandung seit Jahren betrieben werden und deren Verarbeitung auch nach der DS-GVO rechtmäßig erfolgen, eine DSFA benötigen³. Dagegen spricht, dass schon Art. 17 Abs. 1 S.2 RL 95/46 eine Risikobetrachtung forderte („ein Schutzniveau [zu] gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist“) und dementsprechend alle bereits nach heutigem Stand rechtskonform erfolgenden Verarbeitungen einem risikobasierten Ansatz folgen. Hinzu kommt der Präventionsgedanke des Ordnungsgebers, dass eine DSFA „vorab“ (Art. 35 Abs. 1 S. 1 DS-GVO) durchzuführen ist und nicht hinsichtlich etablierter Verfahren.

In diesem Sinne dürfte einiges dafür sprechen, dass eine DSFA für etablierte und entsprechend den Vorgaben der RL 95/46 langjährig durchgeführte und unbeanstandete sowie legitim eingesetzte Verarbeitungsverfahren nicht erforderlich sein dürfte.

Jedoch kann bei Anpassung/Änderung des Verfahrens nach Geltungseintritt der DS-GVO eine DSFA erforderlich werden, da die regelmäßige Pflicht zur Überprüfung auch für bereits laufende Verfahren gilt.

³ Gleiche Meinung vertritt die Gesellschaft für Datenschutz und Datensicherheit e.V. in ihrer GDD-Praxishilfe DS-GVO X „Voraussetzungen der Datenschutz-Folgenabschätzung“, Abschnitt 2.4 Altverfahren. Online, zitiert am 2017-11-21; Verfügbar unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf

3 Erläuterungen zum rechtlichen Hintergrund

Art. 35 enthält eine Vielzahl an Voraussetzungen und unbestimmten Rechtsbegriffen. Da sich deren objektiver Inhalt häufig nicht eindeutig erschließt, da diese Begriffe z. B. vage sind oder mehrere Bedeutungen haben können, bedürfen diese somit einer näheren Betrachtung. Einige dieser Begrifflichkeiten sind für das Verständnis der DSFA essenziell, weshalb die wichtigsten und klärungsbedürftigsten Begrifflichkeiten im Nachfolgenden kurz vorgestellt werden. Ferner werden dabei Hinweise / Vorschläge zur Definition und zur Interpretation gegeben.

3.1 Art 35 und seine tatbestandlichen Voraussetzungen

Nach Art. 35 Abs. 1 DS-GVO muss eine DSFA erfolgen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat.

Darüber hinaus ist gemäß Art. 35 Abs. 3 DS-GVO eine DSFA insbesondere in den folgenden Fällen erforderlich:

- a) bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf eine automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen können oder
- b) bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder
- c) bei der umfangreichen Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO oder
- d) bei der systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche.

Diese Voraussetzungen werden nachfolgend im Einzelnen näher erläutert.

3.1.1 Rechtmäßigkeit der Datenverarbeitung

Art. 35 DS-GVO enthält zwar nicht ausdrücklich die Forderung, dass in einer DSFA die Rechtmäßigkeit des geplanten Verarbeitungsverfahrens betrachtet wird, jedoch besteht das Ziel einer DSFA gerade darin, eine risikoreiche Verarbeitung in Einklang mit den Anforderungen der DS-GVO zu bringen. Dazu ist auch die Betrachtung der Rechtmäßigkeit der Datenverarbeitung erforderlich. Jegliche Verarbeitung personenbezogener Daten stellt eine Durchbrechung des Verbots mit Erlaubnisvorbehalt (Art. 6 Abs. 1, Art. 9 Abs. 1 DS-GVO) dar⁴, weshalb die Erlaubnistatbestände in der Untersuchung dargelegt und überprüft werden müssen, ob diese die Verarbeitung legitimieren. Eine Verarbeitung erfolgt immer dann legitim, wenn entweder ein rechtlicher Erlaubnistatbestand oder eine Einwilligung der betroffenen Person vorliegt.

3.1.1.1 Einwilligung

Hinsichtlich der Erlaubnistatbestände behandelt Art. 6 DS-GVO personenbezogene Daten, besonderen Kategorien von Daten, insbesondere auch Gesundheitsdaten, werden in Art. 9 DS-GVO geregelt.

⁴ Martini M. Art. 35 Rn. 22 in Paal/Pauly (Hrsg.) GVO Datenschutz-Grundverordnung. C.H.Beck Verlag 2017. ISBN 978-3-406-69570-4

Art. 6 Abs. 1 lit. a DS-GVO gestattet die Verarbeitung personenbezogener Daten, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung gegeben hat. Art. 9 Abs. 2 lit a DS-GVO gestattet eine Verarbeitung besonderer Kategorien personenbezogener Daten, wenn

- a) die betroffene Person einwilligt und
- b) Unionsrecht oder das Recht von Mitgliedstaaten die Verarbeitung nicht verbieten.

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden.

3.1.1.2 Verarbeitung ohne Einwilligung des Betroffenen

Zusätzlich zur Einwilligung sieht die DS-GVO eine Reihe von Erlaubnistatbeständen hinsichtlich der Verarbeitung besonderer Kategorien von personenbezogenen Daten vor, z.B.:

- Die eigentliche Patientenbehandlung findet eine Legitimierung in Art. 9 Abs. 2 lit. h DS-GVO i.V.m. § 630a ff. BGB, jedoch ist zwingend erforderlich, dass die Verarbeitung entsprechend Art. 9 Abs. 3 DS-GVO
 - a. durch Fachpersonal oder unter dessen Verantwortung erfolgt,
 - b. dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt
 - c. oder, wenn die Verarbeitung durch eine andere Personen erfolgt, dass diese Personen ebenfalls einer entsprechenden Geheimhaltungspflicht unterliegt.Dieser Anforderung bzgl. Verschwiegenheitspflicht der datenverarbeitenden Personen wird insbesondere durch § 203 StGB genügt.
- Zur Abrechnung von einem Patienten gegenüber erbrachten Leistungen müssen naturgemäß auch dessen personenbezogene Daten verarbeitet werden. Art. 9 Abs. 2 lit. f, h DS-GVO, beispielsweise i. V. m. § 301 SGB V als nationaler Erlaubnistatbestand, gestattet dies.
- Arbeitsmedizinische Untersuchungen können einerseits durch Art. 9 Abs. 2 lit. b DS-GVO gestattet sein, andererseits werden diese auch von Art. 9 Abs. 2 lit. h DS-GVO adressiert.
- Die gesetzliche Qualitätssicherung (z. B. §§ 137, 137a SGB V; § 136 SGB V i. V. m. § 299 SGB V bzw. den Richtlinien des G-BA) wie auch die Regelungen zur öffentlichen Gesundheitsvorsorge (Gesundheitsämter, Impfungen in Schule usw. durch Ämter) können einen Legitimationstatbestand in Art. 9. Abs. 2 lit. i DS-GVO finden.

Hierbei muss beachtet werden, Art. 9 Abs. 2 lit. b, g, h, i, j DS-GVO vorsehen, dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erfolgt, welches der DS-GVO genügende Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

Grundsätzlich muss die Legitimation der Verarbeitung im jeweiligen Einzelfall genauestens geprüft werden.

3.1.1.3 Verarbeitung nach Treu und Glauben

Des Weiteren muss die Verarbeitung der Daten legitim erfolgen, d. h. die Verarbeitung der Daten erfolgt auf Grund eines Erlaubnistatbestandes nach Treu und Glauben⁵. Was genau der Verordnungsgeber unter der Regelung einer „Verarbeitung nach Treu und Glauben“ versteht, wird an

⁵ Treu und Glauben ist ein unbestimmter Rechtsbegriff und bezeichnet das Verhalten eines redlich und anständig handelnden Menschen. In Art. 5 Abs. a lit. a DS-GVO wird verlangt, dass die Verarbeitung personenbezogener Daten auf eine rechtmäßige und in einer für die betroffene Person nachvollziehbaren Weise erfolgt. Dies beinhaltet also eine Forderung nach einer Rechtmäßigkeit und Transparenz der Verarbeitung, geht also über den allgemeinen „Treu und Glauben“ Begriff hinaus.

keiner Stelle in der DS-GVO präzisiert. Jegliche Vergleiche zu entsprechenden Regelungen in anderen Richtlinien oder zu nationalen Regelungen (z. B. zu § 242 BGB) überzeugen nicht, weshalb eine klare Definition noch nicht feststeht.

In ErwGr. 38 RL 95/46 findet sich hierzu Folgendes: „Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.“ D. h. die Verarbeitung muss „fair“ erfolgen.

3.1.2 Rechte und Freiheiten natürlicher Personen

Da auch bei einer rechtmäßigen Verarbeitung ein hohes Risiko für die betroffenen Personen bestehen kann, bedarf es zunächst einer Darstellung, welche „Betroffenenrechte“ existieren, um eine Aussage treffen zu können, ob diesbezüglich Risiken zu vermuten oder Schäden zu erwarten sind. Dabei ist als Ausgangspunkt zu beachten, dass der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ein Grundrecht darstellt. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten (siehe ErwGr. 1 DS-GVO). Eine besondere Ausprägung dieses Schutzes findet sich in Kapitel III DS-GVO „Rechte der betroffenen Person“ (Artt. 12 - 22). Dort werden die Rechte der betroffenen Person geregelt, die sich im Überblick wie folgt darstellen:

- Transparente Verarbeitung ihrer Daten, Art. 12 DS-GVO
- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten, unterschieden nach:
 - o Erhebung bei der betroffenen Person („Direkterhebung“), Art. 13 DS-GVO
 - o Erhebung nicht bei der betroffenen Person („Dritterhebung“), Art. 14 DS-GVO
- Auskunftsrecht, Art. 15 DS-GVO
- Recht auf Berichtigung, Art. 16 DS-GVO
- Recht auf Löschung, Art. 17 DS-GVO
- Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung, Art. 19 DS-GVO
- Recht auf Datenübertragbarkeit, Art. 20 DS-GVO
- Widerspruchsrecht, Art. 21 DS-GVO
- Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall, Art. 22 DS-GVO..

Diese Rechte sind nicht absolut, sondern werden sowohl durch den europäischen als auch nationalen Gesetzgeber beschränkt, z. B. um die Rechte und Freiheiten anderer zu schützen oder die nationale Sicherheit zu gewährleisten.

3.1.3 Risiko der Verarbeitung

Die DS-GVO definiert nicht den Begriff „Risiko“. ErwGr. 75 führt aus, dass „aus einer Verarbeitung personenbezogener Daten“ Risiken für die Rechte und Freiheiten natürlicher Personen „mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere“ resultieren können, „die zu einem physischen, materiellen oder immateriellen Schaden führen“ können. Daraus folgt, dass die Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne des Art. 35 DS-GVO somit in Abhängigkeit von „Eintrittswahrscheinlichkeit“ und „Schadensschwere“ darzustellen ist⁶.

⁶ Martini M. Art. 35 Rn. 15 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4

Nach ErwGr. 76 sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person „in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung“ bestimmt werden. Das Risiko soll anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein normales (im Sinne des „Lebensrisikos“⁷) oder ein hohes Risiko in sich birgt.

3.1.3.1 Bewertung eines voraussichtlichen Risikos, Art. 35 Abs. 1 S. 1 DS-GVO

Art. 35 Abs. 1 DS-GVO setzt lediglich voraus, dass ein Risiko „voraussichtlich“ eintritt. D. h., es wird eine objektive (ErwGr. 76) Bewertung bzgl. der Unsicherheit verlangt. Die Richtigkeit der Bewertung muss ggf. gerichtlich überprüfbar sein, d. h. kann von unabhängigen Stellen ebenfalls bewertet werden. Somit muss sich der Verarbeiter bewusst sein, dass die DS-GVO den Spielraum bzgl. der Bewertung des Risikos nicht bei ihm sieht. Vielmehr ist eine nachvollziehbare Bewertung des Risikos aufgrund der Berücksichtigung der relevanten und überprüfbaren Risikofaktoren aus objektiver Sicht der betroffenen Personen erforderlich.

Später eintretende Tatsachen oder nicht vorhersehbare Entwicklungen verändern jedoch die Richtigkeit der Bewertung nicht rückwirkend. Für die Beurteilung bzgl. der Bewertung ist einzig und allein relevant, dass zum Zeitpunkt der Erstellung eine Analyse der zu diesem Zeitpunkt vorhandenen Informationen erfolgte. Dies heißt jedoch nicht, dass eine DSFA nach einmaliger Durchführung abgeschlossen ist. Vielmehr muss bei geänderter Informationslage die Datenschutz-Folgenabschätzung angepasst oder auch neu durchgeführt werden.

Entsprechend ErwGr. 83 ist es unerheblich, ob die Risiken aus einer beabsichtigten, einer unbeabsichtigten oder auch einer unrechtmäßigen Handlung resultieren. D. h. der Verantwortliche muss im Rahmen einer DSFA grundsätzlich auch unrechtmäßige Handlungen berücksichtigen.

3.1.3.2 Hohes Risiko für die Rechte und Freiheiten natürlicher Personen, Art. 35 Abs. 1 S. 1 DS-GVO

Die DS-GVO beschreibt nicht, wann das Risiko einer Verarbeitung „hoch“ ist. Ein Risiko ist zumindest dann als „hoch“ einzustufen, wenn mit „hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten natürlicher Personen“ anzunehmen ist.⁸ Ein hohes Risiko kann sowohl aus einer hohen Eintrittswahrscheinlichkeit (des Schadens) als auch aus einem hohen Schaden resultieren. Daneben ergibt sich aus ErwGr. 91, dass insbesondere die Sensibilität der Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt.

ErwGr. 75 führt weiter aus, dass von entsprechenden Risiken für die Rechte und Freiheiten natürlicher Personen insbesondere dann auszugehen ist, wenn die Verarbeitung zu

- einer Diskriminierung,
- einem Identitätsdiebstahl oder -betrug,
- einem finanziellen Verlust,
- einer Rufschädigung,
- einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,

⁷ Bzgl. Lebensrisiko siehe auch: BGH Urt. V. 1993-05-04, AZ VI ZR 283/92. Online, zitiert am 2017-11-21; Verfügbar unter <https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=04.05.1993&Aktenzeichen=VI%20ZR%20283/92>

⁸ Martini M. Art. 35 Rn. 25 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. ottoschmidt Verlag 2016. ISBN 978-3-504-56074-4

- der unbefugten Aufhebung der Pseudonymisierung

oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann. Desgleichen, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren. Insbesondere wenn personenbezogene Daten verarbeitet werden, die zu den besonderen Kategorien von Daten gemäß Art. 9 DS-GVO gehören, muss von hohen Risiken ausgegangen werden.

3.1.4 „Neue Technologien“

Der in Art. 35 Abs. 1 S. 1 DS-GVO genannte Begriff „Verwendung neuer Technologien“ wird im Rahmen der DS-GVO nicht definiert, jedoch in ErwGr. 89 aufgegriffen. Gemeint sind insbesondere Verarbeitungsvorgänge, bei denen „neue Technologien eingesetzt werden oder die neuartig sind“ und die bisher noch nicht Gegenstand einer DSFA waren bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine DSFA notwendig geworden ist. Dabei ist der Begriff „Technologie“ die Übersetzung des englischen Wortes „technologies“, der in der englischsprachigen Bedeutung umfassender ist als sein korrespondierender deutscher Begriff⁹. Unter „technologies“ sind Techniken, Fähigkeiten, Methoden und Prozesse zu verstehen. Dementsprechend weit ist auch der Begriff im Sinne des Art. 35 DS-GVO auszulegen.

3.1.5 Art und Umfang der Verarbeitung, Art. 35 Abs. 1 S. 1 DS-GVO

Um Art und Umfang einer Verarbeitung näher beschreiben zu können, ist zunächst zu klären, was alles unter den Begriff „Verarbeitung“ zu subsumieren ist. Der Begriff der Verarbeitung ist in der DS-GVO weiter gefasst als im bisherigen deutschen Datenschutzrecht. Art. 4 Ziff. 2 DS-GVO nennt als Arten der Verarbeitung insbesondere:

- Erheben,
- Erfassen,
- Organisation,
- Ordnen,
- Speicherung,
- Anpassung oder Veränderung,
- Auslesen,
- Abfragen,
- Verwendung,
- Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- Abgleich oder die Verknüpfung,
- Einschränkung,
- Löschen oder Vernichtung.

Art. 35 folgend müssen die vorstehenden Verarbeitungstätigkeiten „umfangreich“ sein. Aus den korrespondierenden ErwGr. 75 bzw. 91 wird ersichtlich, dass im Bereich des „Umfangs der Datenverarbeitung“ zwei Einflussgrößen zu berücksichtigen sind: Zum einen die Anzahl der Personen, zum anderen die Menge der verarbeiteten Daten.

⁹ siehe z. B. Begriffserklärung in der Wikipedia: Technology. Online, zitiert am 2017-06-04; Verfügbar unter <https://en.wikipedia.org/wiki/Technology>

Daraus folgt zum einen, dass je mehr Daten zu einer Person vorhanden sind, desto weitreichendere Aussagen sind über eine bestimmte Person möglich, wodurch sich das Risiko für diese Person erhöht. Zum anderen folgt daraus, dass je höher die Anzahl der betroffenen Personen ist, deren Daten verarbeitet werden, desto bessere/genauere Aussagen sind möglich z. B. über etwaige Verbindungen zwischen diesen Personen. Aus diesen Verbindungen lassen sich wiederum weitere Schlüsse über die betroffene Person ziehen, sodass sich daraus wiederum höhere Risiken hinsichtlich der informationellen Selbstbestimmung für die betroffenen Personen ergeben. Zugleich erhöht sich mit einem größeren Verarbeitungsumfang auch die Eintrittswahrscheinlichkeit etwaiger Risiken¹⁰.

In der Fassung der DS-GVO vom europäischen Parlament war in den ErwGr. 63 und 75 und auch im Art. 32a („Risk analysis“) von der Verarbeitung der Daten von 5000 betroffenen Personen innerhalb von 12 Monaten die Rede¹¹. Auch wenn dieser Ansatz nicht in der finalen Version des DS-GVO Einzug fand, bietet dieser Wortlaut einen Hinweis, was sich der europäische Gesetzgeber unter einer großen Anzahl von betroffenen Personen vorstellte.

Diesen Erwägungen folgend, sollten sich medizinische Einrichtungen mit um die 5000 Behandlungsfälle in einem Jahr gut überlegen, ob sie auf eine DSFA - aus welchen Gründen auch immer - für ihre Daten verarbeitenden Systeme verzichten wollen.

3.1.6 Zwecke der Verarbeitung, Art. 35 Abs. 1 S. 1 DS-GVO

Art. 35 Abs. 1 S. 1 DS-GVO nennt außerdem als Grund für die Durchführung einer DSFA, wenn Umstände und Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.

3.1.6.1 Systematische Beschreibung der Zwecke der Verarbeitung

Art. 35 Abs. 7 lit. a DS-GVO fordert daher bei der Durchführung der DSFA in einem ersten Schritt eine systematische Beschreibung des geplanten Verarbeitungsvorgangs und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen.

Die systematische Beschreibung des geplanten Verarbeitungsvorgangs erfordert in diesem Zusammenhang eine Erläuterung

- des Datenverarbeitungsprozesses,
- der hierfür eingesetzten Technik sowie
- Art, Umfang und Umstände der Datenverarbeitung.¹²

Die Beschreibung der Zwecke der Datenverarbeitung erfordert eine Erläuterung des konkreten Einsatzgebietes der verarbeiteten Daten bzw. des Zweckes ihrer Verarbeitung¹³. Dem Wortlaut nach

¹⁰ Martini M. Art. 24 Rn. 33 in Plath (Hrsg.) BDSG/DSGVO: Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG. otto schmidt Verlag 2016. ISBN 978-3-504-56074-4

¹¹ European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). Online, zitiert am 2017-04-27; Verfügbar unter <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212#BKMD-6>

¹² Jandt, in: Kühling/Buchner, Kommentar zur Datenschutz-Grundverordnung, Art. 35 DS-GVO, Rn. 35

¹³ Hinweis: Die Norm DIN CEN ISO/TS 14265 (Stand 2014-03) „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“ legt eine Reihe von Kategorien höchster Ebene für die Zwecke fest, für die persönliche Gesundheitsinformationen verarbeitet werden. Die Norm ist in Deutschland über den

fakultativ sind bei der Beschreibung des Prüfgegenstandes der DSFA die von dem Verantwortlichen verfolgten berechtigten Interessen zu erläutern.¹⁴ Art. 5 Abs. 1 lit. b DS-GVO gibt vor, dass personenbezogene Daten nur zu festgelegten, eindeutigen und legitimen Zwecken verarbeitet werden dürfen. Andere Sprachfassungen der DS-GVO machen deutlich, dass mit dem Begriff „eindeutig“ eher „explizit“ oder „konkret“ gemeint sein dürfte. Es geht also darum, die Verarbeitungszwecke nicht zu breit anzugeben.¹⁵ Der Verarbeitungszweck sollte klar umschrieben werden. Vermieden werden sollte darüber hinaus eine vage Zweckfestlegung, die eine Erhebung und Speicherung zu vielen unterschiedlichen Zwecken ermöglicht und im Ergebnis keine wirkliche Festlegung darstellen würde.¹⁶

3.1.6.2 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Gemäß Art. 35 Abs. 7 lit. b DS-GVO sind bei der Durchführung der DSFA sodann in einem zweiten Schritt die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck der Verarbeitung zu bewerten. Der Verantwortliche hat in diesem Zusammenhang auch zu prüfen, ob es alternative und datenschutzrechtlich weniger eingreifende Verarbeitungsformen gibt, durch die der Zweck der Datenverarbeitung in gleichem Maße erreicht werden kann.¹⁷ Die Datenverarbeitung ist in Bezug auf den Zweck grundsätzlich als notwendig anzusehen, wenn der verfolgte Zweck sonst nicht, nicht vollständig oder nicht in rechtmäßiger Weise erreicht werden kann.¹⁸ Im Rahmen der Verhältnismäßigkeitsprüfung sind der Datenverarbeitungsprozess und der mit ihm durch den Verantwortlichen verfolgte Zweck zueinander ins Verhältnis zu setzen und gegeneinander abzuwägen. Je umfassender und intensiver die Datenverarbeitung ist, desto höherrangiger muss der Zweck einzuordnen sein.¹⁹

3.1.6.2.1 Erforderlichkeit, Notwendigkeit²⁰

Die Begrifflichkeiten „Erforderlichkeit“ und „Notwendigkeit“ werden oftmals synonym verwendet. Im juristischen Schrifttum besagt der Grundsatz der Verhältnismäßigkeit, dass kollidierende Interessen, Freiheiten oder Rechtsprinzipien nur dann in einem angemessenen Verhältnis zueinander stehen, wenn das zu wahrende Interesse, Freiheitsrecht oder Rechtsprinzip schwerer wiegt als das zu seinen Gunsten geopfert. Auch im Sinne dieses Grundsatzes können die Begrifflichkeiten „Erforderlichkeit“ und „Notwendigkeit“ synonym verwendet werden.

In der DS-GVO selbst wird der Begriff der „Erforderlichkeit“ bzw. „Notwendigkeit“ nicht definiert. Allerdings finden sich in den Erwägungsgründen Kriterien, welche die Beurteilung der Erforderlichkeit erleichtern. Die Verarbeitung von Daten ist insbesondere dann erforderlich bzw. notwendig, wenn

- der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder

Beuth-Verlag erhältlich. Online, zitiert am 2018-01-16; Verfügbar unter <https://www.beuth.de/de/technische-regel/din-cen-iso-ts-14265/149023541>

¹⁴ Jandt, a.a.O., Rn. 36

¹⁵ Pötters, in: Gola, Kommentar zur DS-GVO, Art. 5 DS-GVO, Rn. 14

¹⁶ Vgl. Pötters, a.a.O., Rn.14

¹⁷ Jandt, a.a.O., Rn. 39

¹⁸ Jandt, a.a.O., Rn. 40

¹⁹ Jandt, a.a.O., Rn. 41

²⁰ Entnommen Kap. 4.7 der Ausarbeitung „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, erarbeitet von Mitgliedern aus den Verbänden GDD und GMDS. Online, zitiert am 2017-12-17; Verfügbar unter <http://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php>

- der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112).

D. h. damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht. Um die Erforderlichkeit / Notwendigkeit beurteilen zu können, müssen daher drei Fragen beantwortet werden:

- Gibt es ein anderes Mittel?
- Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
- Ist dieses Mittel ein milderes, also die Rechte der betroffenen Person weniger belastendes Mittel?

3.1.6.2.2 Verhältnismäßigkeit / Interessenabwägung²¹

Der BGH konkretisierte die erforderliche Abwägung, die bei einer Verarbeitung personenbezogener Daten vorgenommen werden muss, in seinem Urteil vom 17.12.1985 (Az. VI ZR 244/84) . Demzufolge ist eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für den oder die Betroffenen hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgte, erforderlich. „Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen ihre Speicherung dient“²².

Diese Abwägung ist für jede Art der Datenverarbeitung (Erhebung, Speicherung, Übermittlung, ...) getrennt, den entsprechenden rechtlichen Regelungen nach zu prüfen. Dabei kann es vorkommen, dass eine Abwägung zum Ergebnis führt, dass die Erhebung und Speicherung von personenbezogenen Daten statthaft ist, eine Übermittlung der Daten an andere Empfänger jedoch nicht legitimiert werden kann.

Grundsätzlich kommen als schutzwürdige Interessen der Betroffenen „alle menschlichen Ziele in Betracht, wie etwa das Streben nach Geld, Anerkennung, nach Privatheit wie nach Kommunikation“, ebenso „das Streben nach Glück“²³. Dabei gilt, dass die Interessen der Betroffenen als umso schutzwürdiger anzusehen sind,

- je sensibler die Daten sind und
- je größer die Zahl der die Daten verarbeitenden Personen bzw., bei Übermittlungen, der Abrufberechtigten ist²³.

Bei der Darstellung der Betroffeneninteressen kann die Sphärentheorie^{24,25}, und ihre Einteilung in die drei Sphären Intim-, Privat- und Sozialsphäre helfen:

- ein Eingriff in die Intimsphäre muss vermieden werden, da hier der Kern der Menschenwürde betroffen ist

²¹ Entnommen Kap. 4.8 der Ausarbeitung „Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung (DS-GVO)“, erarbeitet von Mitgliedern aus den Verbänden GDD und GMDS. Online, zitiert am 2017-12-17; Verfügbar unter <http://ds-gvo.gesundheitsdatenschutz.org/html/forschung.php>

²² Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84, Rn. 13 Online, zitiert am 2016-12-03; Verfügbar unter <https://www.jurion.de/>

²³ BeckOK DatenSR/von Lewinski BDSG § 10 Rn. 23-29

²⁴ BeckOK DatenSR/Wolff BDSG § 28 Rn. 64-70

²⁵ BVerfG Urteil vom 31.01.1973, AZ.: 2 BvR 454/71 Online, zitiert am 2016-12-04; Verfügbar unter <http://dejure.org/> Az.: IV ZR 129/09 Online, zitiert am 2016-12-04; Verfügbar unter <https://dejure.org/>

- Privat- und Sozialsphäre: hier gilt, je stärker der Eingriff, desto gewichtiger muss das verfolgte Gemeinwohlinteresse (= Verarbeitungszweck) sein.

3.1.6.3 Beispiel: Zugriff auf im Krankenhaus vorhandene Vorbehandlungsdaten

Danach könnte im Krankenhaus beispielsweise als Datenverarbeitungsprozess der Zugriff auf im Krankenhaus vorhandene Vorbehandlungsdaten in Betracht kommen. Im ersten Schritt wären demnach neben der Nennung dieses Datenverarbeitungsprozesses die hierfür erforderliche Technik und der Umfang der Datenverarbeitung zu erläutern. Um den Zweck der Verarbeitung möglichst konkret zu beschreiben, könnte beispielsweise neben der Nennung der „Behandlung des Patienten“ als Verarbeitungszweck ergänzend erläutert werden, dass der Zugriff auf Vorbehandlungsdaten erfolgt, um eine optimale Behandlung des Patienten sicherzustellen. Durch den Zugriff auf Vorbehandlungsdaten sollen insbesondere Wechselwirkungen der aktuellen Behandlung mit vorangegangenen Behandlungen des Patienten überprüft und negative Auswirkungen auf die aktuelle Behandlung, deren Ursache in vorangegangenen Behandlungen des Patienten liegen können, ausgeschlossen werden.

Darüber hinaus folgt aus der im zweiten Schritt vorzunehmenden Bewertung der Notwendigkeit und Verhältnismäßigkeit, dass ein Zugriff auf Vorbehandlungsdaten nicht generell, sondern nur zulässig ist, wenn dies zur Erreichung des Verarbeitungszweckes erforderlich und verhältnismäßig ist. Insofern wäre beispielsweise zu erläutern, dass ein Zugriff auf Vorbehandlungsdaten nur erforderlich und verhältnismäßig ist, wenn Anhaltspunkte für mögliche Wechselwirkungen bzw. Auswirkungen auf die aktuelle Behandlung durch vorangegangene Behandlungen des Patienten ersichtlich sind. Darüber hinaus darf bei einem Vorliegen derartiger Anhaltspunkte nur im erforderlichen Umfang auf die für die aktuelle Behandlung notwendigen Vorbehandlungsdaten zugegriffen werden. Kann hingegen ein Zusammenhang zwischen aktueller und vorheriger Behandlung des Patienten mit hinreichender Sicherheit ausgeschlossen werden, besteht keine Notwendigkeit für einen Zugriff auf im Krankenhaus vorhandene Vorbehandlungsdaten.

3.1.7 Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, Art. 35 Abs. 3 lit. a DS-GVO

Art. 35 Abs. 3 lit. a DS-GVO bestimmt des Weiteren, dass eine DSFA insbesondere im Falle einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen erforderlich ist, ohne die genauen Anforderungen weiter zu umschreiben. Der ErwGr. 91 führt hierzu ergänzend aus, dass eine DSFA auch durchgeführt werden sollte, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßnahmen verarbeitet werden.

ErwGr. 24 stellt dar, dass eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen dient bzw. beinhaltet, wenn ihre Aktivitäten nachvollziehbar werden. Das LDI

NRW leitet daraus ab, dass eine systematische Beobachtung dann vorliegt, wenn die Beobachtung methodisch nach einem bestimmten, vorgegebenen System oder einer Strategie erfolgt²⁶.

3.1.8 Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten, Art. 35 Abs. 3 lit. b DS-GVO

Gemäß Art. 35 Abs. 3 lit. b DS-GVO ist eine DSFA des Weiteren insbesondere im Falle einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO erforderlich.

Bzgl. der Einordnung der Begrifflichkeit „umfangreiche Verarbeitung“ wird auf Abschnitt 3.1.5 verwiesen.

Zu den besonderen Kategorien von personenbezogenen Daten entsprechend Art. 9 DS-GVO gehören:

- Rassistische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetischen Daten
- Biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung.

Im Gesundheitswesen sind insbesondere die Kategorien „Gesundheitsdaten“ und „genetische Daten“ von Relevanz, da eine dieser Kategorien nahezu immer betroffen sein dürfte. D. h., hier ist die Entscheidung bzgl. der Notwendigkeit der Durchführung einer DSFA ausschließlich vom Umfang der Datenverarbeitung abhängig.

ErwGr. 91 führt aus, dass die Verarbeitung personenbezogener Daten nicht als umfangreich gilt, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. D. h., dass eine Arztpraxis mit einem Arzt und dessen Personal nicht allein aus den hier genannten Gründen eine DSFA durchführen muss. Hierbei ist zu beachten, dass der ErwGr. von *einem* Arzt und dessen Personal ausgeht; ob der ErwGr. daher für eine Praxis mit zwei Ärzten gilt, kann man nur im Einzelfall betrachten. Sicherlich stellt dieser ErwGr. jedoch keine Ausnahme für Krankenhäuser dar.

3.1.9 Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche, Art. 35 Abs. 3 lit. c DS-GVO

Art. 35 Abs. 3 lit. c DS-GVO verlangt eine DSFA, wenn öffentlich zugängliche Bereiche systematisch und umfangreich überwacht werden. ErwGr. 91 benennt hier insbesondere optoelektronische

²⁶ Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Wann liegt eine „regelmäßige und systematische Überwachung“ gemäß Artikel 37 Absatz 1 Buchstabe b) DS-GVO vor? Online, zitiert am 2017-06-04; Verfügbar unter https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Datenschutzbeauftragte_nach_der_DS-GVO_und_der_JI-RL/Inhalt/I_Benennung_eines_Datenschutzbeauftragten__Artikel_37_DS-GVO_Artikel_32_JI-Richtlinie/Wann_liegt_eine_regelm_ige_und_systematische_berwachung_gem_Artikel_37_Absatz_1_Buchstabe_b_DS-GVO_vor_.php

Vorrichtungen zur Überwachung, also Videoüberwachungen. Eine Videoüberwachung erfolgt stets systematisch, jedoch ist nicht jede Videoüberwachung gleichzeitig als „umfangreich“ anzusehen. Somit muss nicht für jede Videoüberwachung eine DSFA erfolgen, sondern nur dort, wo diese in einem besonderen Umfang (siehe Abschnitt 3.1.5) erfolgt.

Bei der Bewertung der Videoüberwachung ist neben dem Umfang auch die Intensität (z. B. hinsichtlich der Möglichkeit des Hineinzoomens in Gesichtsabschnitte) zu berücksichtigen. Evtl. ist in diesen Fällen eine DSFA aus anderen Gründen erforderlich, z. B. weil aus dieser Datenverarbeitung besonders hohe Risiken für die betroffene Person erwachsen. Ein Beispiel hierfür könnte sein, wenn eine Videokamera eine Kasse überwacht und mit der Zoomfunktion die Eingabe der Geheimnummer von Kreditkarten eingesehen werden kann.

Art. 35 Abs. 3 lit. c DS-GVO beschränkt den Tatbestand nicht nur auf die Überwachung des öffentlichen Raumes. Vielmehr werden von dieser Regelung alle Räumlichkeiten erfasst, welche der Öffentlichkeit zugänglich gemacht werden. Damit wird grundsätzlich auch Privatgelände adressiert, wenn dieses der Öffentlichkeit zugänglich ist.

3.2 „Befreiung“ von der Datenschutz-Folgenabschätzung

Gemäß Art. 35 Abs. 10 DS-GVO kann trotz eines hohen Risikos eine Datenschutz-Folgenabschätzung entfallen, falls es sich bei der Verarbeitung um einen der folgenden Erlaubnistatbestände handelt:

- Verarbeitung gemäß Art. 6 Abs. 1 lit. c DS-GVO, d. h. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, welcher der Verantwortliche unterliegt
- Verarbeitung gemäß Art. 6 Abs. 1 lit. e DS-GVO, d. h. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Allerdings müssen zusätzlich alle nachfolgend dargestellten Voraussetzungen erfüllt sein, damit keine Datenschutz-Folgenabschätzung erforderlich ist.

- Die Verarbeitung erfolgt auf einer gesetzlichen Rechtsgrundlage, welcher der Verantwortliche unterliegt.
- Die Rechtsgrundlage regelt den konkreten Verarbeitungsvorgang.
- Eine allgemeine Datenschutz-Folgenabschätzung erfolgte im Gesetzgebungsverfahren.
- Der zuständige Mitgliedsstaat verlangt für den Vorgang nicht explizit eine Datenschutz-Folgenabschätzung.

Daraus können sich beispielsweise für den Krankenhausbereich Ausnahmen für die Verpflichtung zur Durchführung von DSFA ergeben.

Dabei ist die am schwierigsten zu überprüfende Voraussetzung die im dritten Spiegelstrich der Aufzählung dargestellte Frage, ob bei dem Erlass der spezifischen mitgliedstaatlichen Rechtsgrundlage vom Gesetzgeber eine DSFA durchgeführt worden ist. Nach einer Auffassung in der Literatur²⁷ können Anhaltspunkte hierfür z. B. den jeweiligen Gesetzesbegründungen entnommen werden, sofern dort entsprechende Ausführungen gemacht wurden. Des Weiteren können der Rechtsgrundlage selbst Hinweise entnommen werden, dass sie als Ergebnis einer DSFA abgefasst worden ist. Dies ist z. B. anzunehmen, wenn auf der Tatbestandsebene spezifische und riskante Datenverarbeitungen beschrieben werden, die nur bei Einhaltung besonderer Voraussetzungen und konkreter risikominimierender technischer und organisatorischer Anforderungen zulässig sind. Maßgeblich ist, ob die Rechtsgrundlage aufgrund ihrer spezifischen Anforderungen zur Minimierung

von Datensicherheitsrisiken beiträgt und trotz der Einstufung als riskante Datenverarbeitung im Ergebnis zu einem angemessenen Datenschutzniveau für den Betroffenen führt.²⁷ Nach einer anderen Auffassung in der Literatur enthält die DS-GVO keine konkreten Anforderungen an die allgemeine Folgenabschätzung durch den Gesetzgeber, so dass es genügt, wenn eine allgemeine aber systematische Erfassung und Analyse der intendierten und unbeabsichtigten Folgen der Rechtsnormen stattgefunden hat.²⁸ Hiervon zu unterscheiden sind Datenverarbeitungen auf der Grundlage von Einwilligungen von Patienten.

3.3 Inhalt einer Datenschutzfolgenabschätzung, Art. 35 Abs. 7 DS-GVO

Entsprechend Art. 35 Abs. 7 DS-GVO enthält eine Datenschutz-Folgenabschätzung mindestens

- a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge;
- b) eine systematische Beschreibung der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- c) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- d) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DS-GVO;
- e) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Anforderungen der DS-GVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

3.4 Weitergehende Anforderungen

3.4.1 Einbindung des Datenschutzbeauftragten, Art. 35 Abs. 2 DS-GVO

Entsprechend Art. 35 Abs. 2 DS-GVO holt der Verantwortliche bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein. Gemäß Art. 39 Abs. 1 lit. c DS-GVO gehört zu den Aufgaben des Datenschutzbeauftragten auch die Überwachung der Durchführung einer DSFA. Somit ist der Datenschutzbeauftragte nicht derjenige, der eine DSFA durchführt, denn die Durchführung einer DSFA durch den Datenschutzbeauftragten würde zu einem Interessenkonflikt führen, da sich der Datenschutzbeauftragte dann selbst überwachen müsste.

3.4.2 Standpunkt der Betroffenen, Art. 35 Abs. 9 DS-GVO

Der Verantwortliche holt gemäß Art. 35 Abs. 9 DS-GVO gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein. Durch den Zusatz „gegebenenfalls“ ist unklar, unter welchen Umständen der Standpunkt der Betroffenen einzuholen ist und in welchen Fällen darauf verzichtet werden kann²⁹. Um die Frage der Notwendigkeit der Einbeziehung der Betroffenen zu klären, wird sich der Verantwortliche im Rahmen der DSFA damit auseinandersetzen haben, ob eine Einbeziehung der betroffenen Personen sinnvoll erscheint. Sofern eine Einbeziehung nicht praktikabel oder mit einem hohen wirtschaftlichen Aufwand

²⁷ Jandt S. Art 35 Rn. 27 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129.

²⁸ Sassenberg/Schwendemann in Sydow, Europäische Datenschutzgrund-Verordnung, Handkommentar 2017, Art. 35 Rn. 19, Nomos Kommentar, ISBN978-3-8487-1782-8.

²⁹ Vgl. zu Vorstehendem: Jandt S. Art. 35 Rn. 56 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129.

verbunden ist, dürfte im Regelfall keine Verpflichtung bestehen³⁰. Z. B. bei DSFA bzgl. der Verarbeitung von Arbeitnehmerdaten dürfte eine Beteiligung der betroffenen Personen in der Regel ohne großen Aufwand, z. B. über das Intranet, möglich sein. In derartigen Fällen müsste somit eine Beteiligung erfolgen bzw. es wäre in der DSFA zu dokumentieren, aus welchen Gründen dennoch von der Einbeziehung abgesehen wurde.³¹ Ferner sollte die Einbeziehung der Betroffenen grundsätzlich nur dann in Betracht kommen, wenn eine solche Einbeziehung geeignet ist, d. h. zu einem Mehrwert bzw. zusätzlichen Erkenntnissen für den Verantwortlichen führt.³²

Fraglich ist, wie die Entscheidung zu treffen ist, sofern es um die Verarbeitung von Patientendaten geht. Der Betroffenenkreis „Patienten“ kann zwar grob benannt werden, je nach DSFA ist allerdings fraglich, welche Patienten dies betrifft und wie deren Einbeziehung erfolgen könnte. Denkbar ist die Einbeziehung von Betroffenengruppen wie z. B. krankheitsbezogenen Selbsthilfegruppen als Vertreter im Sinne des Art. 35 Abs. 9 DS-GVO³³. Sollte keine entsprechende Interessensgruppierung bekannt sein, könnte sich die Kontaktaufnahme zu der Bundesarbeitsgemeinschaft der PatientInnenstellen und -Initiativen anbieten, um zu versuchen, über deren Kontakte eine entsprechende Beteiligung von Patientenvertretern zu realisieren.³⁴

In denjenigen Fällen, in denen die Angemessenheitsprüfung ergibt, dass der Standpunkt der Betroffenen einzuholen ist, ist des Weiteren fraglich, ob die Regelung auch eine Informationspflicht der Betroffenen vorsieht. Davon ist auszugehen, da Betroffene ihren Standpunkt nur einbringen können, wenn ihnen alle benötigten Informationen zur Verfügung gestellt werden. Die Regelung kann auch einzelne Personen adressieren³⁵.

³⁰ Bisher als Einzelmeinung in der Literatur zu finden: Nolte N, Werkmeister C. Art. 35 Rn. 59, 60 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

³¹ Vgl. zu Vorstehendem: Nolte N, Werkmeister C. Art. 35 Rn. 59, 60 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8.

³² Sassenberg/Schwendemann in Sydow, Europäische Datenschutzgrund-Verordnung, Handkommentar 2017, Art. 35 Rn. 32, Nomos Kommentar, ISBN978-3-8487-1782-8.

³³ Vertreter im Sinne des Art. 35 Abs. 9 DS-GVO können einerseits gesetzliche Vertreter (z. B. Personensorgeberechtigte bei Kindern) sein, sowie andererseits Interessenvereinigungen von betroffenen Personen. S. hierzu z. B.

- Bausewein C, Steinhaus J. Art. 35 Rn. 45 in Wybitul (Hrsg.) EU-Datenschutz-Grundverordnung. Fachmedien Recht und Wirtschaft. ISBN 978-3-8005-1623-0
- Jandt S. Art. 35 Rn. 55 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129

³⁴ Die „Verordnung zur Beteiligung von Patientinnen und Patienten in der Gesetzlichen Krankenversicherung“ (Patientenbeteiligungsverordnung - PatBeteiligungsV), die aufgrund von § 140g SGB V in Verbindung mit § 140f Abs. 2 S. 3 SGB V erlassen worden ist, konkretisiert die Patientenbeteiligung im Gesundheitswesen hinsichtlich der maßgeblichen Organisationen und kann insofern eine Hilfestellung bei der Findung von Ansprechpartnern zur Patientenbeteiligung darstellen. Entsprechend § 2 Abs. 1 PatBeteiligungsV sind die maßgeblichen Organisationen der Deutsche Behindertenrat, die Bundesarbeitsgemeinschaft der PatientInnenstellen, die Deutsche Arbeitsgemeinschaft Selbsthilfegruppen e. V. und der Verbraucherzentrale Bundesverband e. V. Gerade im Bereich der medizinischen Versorgung können somit Selbsthilfegruppen, die häufig bzgl. einer bestimmten Erkrankung ausgerichtet sind, geeignete Ansprechpartner darstellen.

³⁵ Siehe hierzu z. B.

- Jandt S. Art. 35 Rn. 55 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129
- Martini M. Art. 35 Rn. 60 in Paal/Pauly (Hrsg.) GVO Datenschutz-Grundverordnung. C.H.Beck Verlag 2017. ISBN 978-3-406-69570-4

Informationen, die einem besonderen Geheimhaltungsschutz unterworfen sind, sind hiervon entsprechend Art. 35 Abs. 9 DS-GVO nicht betroffen. Denn die Einholung des Standpunktes erfolgt „unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge“. Insbesondere sind somit Informationen, deren Bekanntwerden für öffentliche Interessen oder der Sicherheit der Verarbeitung Nachteile beinhalten, nicht von dieser Informationspflicht betroffen.

In Fällen einer automatisierten Verarbeitung, „die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen“ ist ggf. unabhängig vom Umfang der Verarbeitung eine DSFA durchzuführen.

Auch wenn die DS-GVO lediglich vorschreibt, dass der Standpunkt einzuholen ist, dürfte davon auszugehen sein, dass sich der Verantwortliche mit dem dargelegten Standpunkt bzw. den Standpunkten auch auseinandersetzen und in der Datenschutz-Folgenabschätzung darauf eingehen muss, da die Regelung ansonsten ins Leere liefe.

3.4.3 Überprüfung durch den Verantwortlichen, Art. 35 Abs. 11 DS-GVO

Gemäß Art. 35 Abs. 11 DS-GVO hat der Verantwortliche erforderlichenfalls zu überprüfen, ob die im Rahmen der DSFA festgelegten Prozesse und Standards bei der Datenverarbeitung umgesetzt werden. Erforderlich ist eine Überprüfung zumindest dann, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

3.4.4 Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO

Auch für die Datenschutzfolgenabschätzung gilt die in Art. 5 Abs. 2 DS-GVO definierte „Rechenschaftspflicht“. Nach dieser Pflicht muss der Verantwortliche nachweisen können, dass die Datenverarbeitung (zu jeder Zeit) rechtskonform erfolgt(e). Diese gesetzliche Anforderung hat mithin zur Konsequenz, dass bei einer Änderung von Verfahren, die eine erneute DSFA erfordern, eine Historie vorhanden ist, um damit die Einhaltung der Vorgaben der DS-GVO auch für den zurückliegenden Zeitraum nachweisen zu können.

3.5 Verantwortlichkeiten, Art. 35 Abs. 1, Art. 4 Nr. 7 DS-GVO

Verantwortlich für die Durchführung einer DSFA ist „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, also der „Verantwortliche“ im Sinne des Art. 4 Nr. 7 DS-GVO. Der Verantwortliche muss gewährleisten, dass sowohl die Erforderlichkeit einer DSFA bei entsprechenden Verarbeitungsverfahren geprüft wird als auch die Durchführung der DSFA, sofern die Prüfung dies ergibt.

In der Praxis dürfte deshalb diese Verantwortlichkeit der mit der Führung des Unternehmens / Organisation betrauten Person(en) obliegen, z. B. Geschäftsführer, Vorstand, etc. In einzelnen Ausnahmefällen kann jedoch auch eine einzelne natürliche Person wie beispielsweise die ein bestimmtes Forschungsprojekt durchführende ärztliche Person - ggf. gemeinsam mit der Geschäftsführung – als „Verantwortlicher“ anzusehen sein oder sogar als alleiniger Verantwortlicher.

Die Verantwortlichkeit sollte nicht beim betrieblichen Datenschutzbeauftragten liegen vgl. Abschnitt 3.4.1.

3.6 Kumulierte Folgenabschätzung, Art. 35 Abs. 1 S. 2 DS-GVO

Oftmals ist es sinnvoll, die Betrachtung des „Verfahrens“ bzw. der Verarbeitung umfassender zu verstehen und eine DSFA nicht lediglich auf ein bestimmtes Projekt zu beziehen. So nennt etwa ErwGr. 92 nachfolgende Beispiele, die auch im Gesundheitsbereich Relevanz haben:

- Gemeinsame Anwendungen oder Verarbeitungsplattformen
- Verarbeitungsumgebung für einen gesamten Wirtschaftssektor
- Verarbeitungsumgebung für ein bestimmtes Marktsegment.

Dem Wortlaut dieses Erwägungsgrundes folgend, kann eine DSFA deshalb auch für ein entsprechendes Geschäftsmodell erfolgen. Für mehrere ähnliche/thematisch zusammenpassende Verarbeitungsvorgänge mit ähnlich hohem Risiko erlaubt Art. 35 Abs. 1 S. 2 DS-GVO daher eine gemeinsame DSFA. Dies ist im Sinne einer Klarstellung/Erleichterung zu verstehen, dass eine Verarbeitung aus mehreren einzelnen Verarbeitungsvorgängen bestehen kann³⁶.

Neben der Betrachtung des Gesamtrisikos adressiert die Möglichkeit einer gemeinsamen DSFA entsprechend ErwGr. 92 insbesondere auch „ökonomische“ sowie „vernünftige“ Gesichtspunkte. D. h. eine gemeinsame DSFA soll auch den ökonomischen und pragmatischen Zielen des Verarbeiters entsprechen.

Dabei sollte entsprechend ErwGr. 92 gerade bei Geschäftsmodellen nach Ansicht der Verfasser zweistufig vorgegangen werden. Auf der ersten Stufe sollten zunächst die abstrakten Risiken bewertet werden, die mit einem solchen Geschäftsmodell einhergehen können. In einem zweiten Schritt gilt es dann, die konkreten Risiken, die bei der Umsetzung in der Praxis bestehen können, zu bewerten.

So könnte beispielsweise eine (abstrakte) Datenschutz-Folgenabschätzung für einrichtungsübergreifende Gesundheitsaktensysteme erfolgen, die beispielsweise von einer wissenschaftlichen Fachgesellschaft durchgeführt wird. Im Rahmen der Umsetzung einer konkreten Schlaganfallakte würden dann durch deren Betreiber (= Verantwortlicher im Sinne der DS-GVO) diese abstrakte DSFA als Vorlage genutzt und für ihre konkrete, real existierende Anwendung erweitert werden. Hierbei werden die speziell in dieser Anwendung existierenden konkreten Risiken benannt und betrachtet.

3.7 Folgen/Vorherige Konsultation der Aufsichtsbehörde, ErwGr. 84, Art. 36 Abs. 1 DS-GVO

Die Ergebnisse der DSFA sind entsprechend ErwGr. 84 zu berücksichtigen, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen,

- a) damit die Verarbeitung der personenbezogenen Daten den Anforderungen der DS-GVO genügt und
- b) um dies nachweisen zu können.

Geht aus einer DSFA hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen und der Verantwortliche dieses Risiko nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten hinreichend eindämmen kann, so muss die Aufsichtsbehörde gemäß Art. 36 Abs. 1 DS-GVO vor der Verarbeitung konsultiert werden.

³⁶ Jandt S. Art. 35 Rn. 11 in Kühling/Buchner (Hrsg.) DS-GVO Datenschutz-Grundverordnung Kommentar. C.H.Beck Verlag 2017. ISBN 978-3-406-702129

3.8 Bedeutung für das deutsche Gesundheitswesen

Kennzeichnend für das Gesundheitswesen ist die Verwendung von Gesundheitsdaten, ggf. auch von genetischen Daten. Daher werden im Bereich des Gesundheitswesens immer Daten der besonderen Kategorien entsprechend Art. 9 DS-GVO verarbeitet. Zudem hat die Verarbeitung von personenbezogenen Daten im Bereich der Gesundheitsversorgung nahezu immer erheblichen Einfluss auf die betroffene Person. Ob eine Datenschutz-Folgenabschätzung erforderlich ist, entscheidet sich - unter der Maßgabe (siehe Kapitel 3.2), dass keine gesetzliche Grundlage eine Befreiung der Pflicht zur Datenschutz-Folgenabschätzung beinhaltet - dementsprechend an folgenden Fragestellungen:

- a) Erfolgt eine „umfangreiche Verarbeitung“?
- b) Erfolgt eine systematische und umfassende Bewertung basierend auf einer Verarbeitung unter Einsatz von IT und dient diese Bewertung als Grundlage für Entscheidungen, welche eine „Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen“ kann. Im Rahmen der Gesundheitsversorgung ist hier ggf. also auch ein Einfluss auf die Gesundheit der betroffenen Person zu beachten.

Ist eine dieser Fragen mit „ja“ zu beantworten, so ist eine DSFA für die Verarbeitung unumgänglich. Ist der Verantwortliche der Meinung, dass eine DSFA nicht erforderlich ist, ist die Einholung einer Zweitmeinung anzuraten. Denn kommt die Aufsichtsbehörde oder schlimmstenfalls ein Gericht zu der Auffassung, dass eine DSFA für die Verarbeitung der Gesundheitsdaten/genetischen Daten erforderlich gewesen wäre, so könnte die Verarbeitung ggf. auch einen Verstoß gegen die Vorgaben von Art. 5 DS-GVO darstellen, welcher mit einer höheren Geldbuße sanktioniert würde als ein Verstoß gegen Art. 35 bzw. 36 DS-GVO.

D. h., in allen Fällen, in denen man die Notwendigkeit einer DSFA nicht sicher ausschließen kann, sollte dies vorab ausreichend geklärt werden. Insbesondere unter Berücksichtigung der Tatsache, dass eine DSFA ein Mittel zur Erfüllung der Rechenschaftspflicht im Sinne von Art. 5 DS-GVO darstellt, ist im Zweifelsfall die Durchführung einer DSFA anzuraten.

3.9 Sanktionierung

Wird eine Datenschutz-Folgenabschätzung nicht oder nicht richtig durchgeführt oder eine erforderliche Meldung an die Aufsichtsbehörde unterlassen, so erfüllen diese Handlungen bzw. die Unterlassung dieser Handlungen den Tatbestand des Art. 83 Abs. 4 lit. a DS-GVO. Eine Aufsichtsbehörde kann diesbezüglich ein Bußgeld von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (je nachdem, welcher der Beträge höher ist) verhängen.

Bei der Verhängung des Bußgeldes sind auch die Vorgaben von Art. 83 Abs. 2 zu berücksichtigen, insbesondere sind zu beachten:

Art, Schwere und Dauer des Verstoßes (Art. 83 Abs. 2 lit. a)	Hierzu ist z. B. zu betrachten: <ul style="list-style-type: none">- Liegt ein genereller Verstoß vor, d. h. kann man generell der gesetzlichen Pflicht nicht genügen?- Sind es nur die konkreten Umstände des Einzelfalles, die eine Erfüllung der gesetzlichen Pflicht verhindern?<ul style="list-style-type: none">- Wie groß ist der potenzielle Schaden für jeden einzelnen Betroffenen? Wie groß ist der Schaden insgesamt?
Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes	Hierzu ist z. B. zu betrachten: <ul style="list-style-type: none">- Wurde die gesetzliche Pflicht vom Verantwortlichen im

(Art. 83 Abs. 2 lit. b)	<p>Ablauf seiner Prozesse ignoriert?</p> <ul style="list-style-type: none"> - Wurden ausreichend die Betroffenenrechte bei der Verarbeitung berücksichtigt?
Maßnahmen zur Minderung des Schadens für betroffene Personen (Art. 83 Abs. 2 lit. c)	<ul style="list-style-type: none"> - Aktionen gegenüber dem Schädiger (z. B. Unterlassungsklage) - Betroffenen wird vom Verantwortlichen Rechtsbeistand zur Wahrnehmung seiner Rechte gegenüber dem Schädiger zur Verfügung gestellt - Betroffenen wird angemessener Schadensersatz geleistet
Grad der Verantwortung Verantwortlicher/ Auftragsverarbeiter (Art. 83 Abs. 2 lit. d)	<p>Hierzu ist z. B. zu betrachten:</p> <ul style="list-style-type: none"> - Bemühen des Verantwortlichen bzw. Auftragsverarbeiters, potenzielle (materiellen oder auch immateriellen) Schäden für betroffene Personen zu vermeiden oder möglichst gering zu halten
Etwaige einschlägige frühere Verstöße (Art. 83 Abs. 2 lit. e)	Handelt es sich um einen Wiederholungstatbestand?
Umfang der Zusammenarbeit mit der Aufsichtsbehörde (Art. 83 Abs. 2 lit. f)	<p>Hierzu ist z. B. zu betrachten:</p> <ul style="list-style-type: none"> - Wurden der Aufsichtsbehörde unverzüglich alle benötigten Informationen gegeben? - Wurden Anstrengungen unternommen, um nachteilige Auswirkungen zu mildern? - Wurden Anstrengungen unternommen, damit künftig Verstöße dieser Art nicht mehr vorkommen?
Kategorien personenbezogener Daten (Art. 83 Abs. 2 lit. g)	Im Kontext der Gesundheitsversorgung/-forschung handelt es sich immer um besondere Kategorien von Daten, sodass ein Verstoß schwerer wiegt.
Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde (Art. 83 Abs. 2 lit. h)	<p>Hierzu ist z. B. zu betrachten:</p> <ul style="list-style-type: none"> - Meldete der Verantwortliche bzw. der Auftragsverarbeiter selbst das Vergehen an die Aufsichtsbehörde? - Erfuhr die Aufsichtsbehörde vom Betroffenen davon? Ggfs. aufgrund der Tatsache, dass der Verantwortliche den Betroffenen auf diese Möglichkeit hinwies? - Wurde die Aufsichtsbehörde erst über Dritte (z. B. Presse) informiert?
Einhaltung früherer Vorgaben der Aufsichtsbehörden bzgl. aktuell beanstandeter Verarbeitung (Art. 83 Abs. 2 lit. i)	
Einhaltung genehmigter Verhaltensregeln (Art. 83 Abs. 2 lit. j)	
Einhaltung genehmigter Zertifizierungsverfahren (Art. 83 Abs. 2 lit. j)	
Jegliche anderen erschwerenden oder mildernden Umstände (Art. 83 Abs. 2 lit. k)	

4 Vorgaben durch die Aufsichtsbehörden

Da eine einheitliche Anwendung der Regelungen der DS-GVO in der gesamten EU schwierig umzusetzen ist, werden den Aufsichtsbehörden – neben der Verpflichtung zu ihrer Zusammenarbeit – zahlreiche Aufgaben übertragen, um zu einer einheitlichen Anwendung beizutragen. Beispielhaft seien hier im Allgemeinen die Überwachung sowie Durchsetzung der Anwendung der DS-GVO, die Beratung von Betroffenen, die Sensibilisierung von Verantwortlichen und Auftragsverarbeitern hinsichtlich der ihnen aus der DS-GVO entstehenden Pflichten und viele mehr genannt.

Um zu einer einheitlichen Anwendung beizutragen, ist des Weiteren ein Europäischer Datenschutzausschuss gemäß Art. 68 DS-GVO einzurichten. Dieser setzt sich gemäß Art. 68 Abs. 3 DS-GVO aus den Leitern der Datenschutzbehörden der EU-Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten zusammen. Entsprechend Art. 70 Abs. 1 lit. e DS-GVO gehört es zu den Aufgaben des Datenschutzausschusses, Leitlinien, Empfehlungen und bewährte Verfahren bereitzustellen, welche eine einheitliche Anwendung der DS-GVO in Europa gewährleisten. Insofern bestimmt letztlich der Datenschutzausschuss, wie die Regelungen der DS-GVO in Europa zu interpretieren sind. Die entsprechenden Ausarbeitungen liegen noch nicht vor und bleiben abzuwarten. Allerdings gilt es zu bedenken, dass der Datenschutzausschuss die bisher bekannte Artikel-29-Datenschutzgruppe ersetzt, deren personellen Zusammensetzungen sich jedoch decken. Daher kommt den Ausarbeitungen / Empfehlungen der Artikel-29-Datenschutzgruppe – unter Berücksichtigung neuer Entwicklungen – bei der Interpretation der DS-GVO eine besondere Bedeutung zu.

Ergänzend muss klargestellt werden, dass die endgültige Entscheidungshoheit nicht bei den Aufsichtsbehörden liegt, sondern bei den zuständigen Gerichten, d. h. den nationalen Gerichten, aber insbesondere auch dem Europäischen Gerichtshof (EuGH). Dies wird aus Art. 78 DS-GVO deutlich, welcher das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde beinhaltet.

4.1 Listen von Verarbeitungsvorgängen

Gemäß Art. 35 Abs. 4 DS-GVO *muss* die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellen und veröffentlichen, für die eine DSFA zwingend erforderlich ist. Diese Liste muss dem europäischen Datenschutz-Ausschuss übermittelt werden (sog. „Positivliste“).

Weiterhin *kann* die Aufsichtsbehörde eine Liste von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung durchzuführen ist, Art. 35 Abs. 5 DS-GVO. Auch diese Liste muss dem europäischen Datenschutz-Ausschuss übermittelt werden (sog. „Negativliste“).

In Deutschland besteht diesbezüglich die Besonderheit, dass 17 verschiedene Aufsichtsbehörden existieren, die entsprechende Listen erstellen müssen/können. Um einheitliche Rahmenbedingungen in Deutschland zu gewährleisten, wird insofern die Forderung unterstützt, dass der nationale Gesetzgeber die verschiedenen Aufsichtsbehörden zur Koordination beim Erlass der entsprechenden Listen im Sinne von Art. 35 Abs. 4 sowie 5 DS-GVO verpflichtet.³⁷

³⁷ Vgl. zu Vorstehendem: Nolte N, Werkmeister C. Art. 35 Rn. 29 in Gola (Hrsg.) DSGVO: Datenschutz-Grundverordnung V= (EU) 2016/679 Kommentar. C. H. Beck Verlag 2017. ISBN 978-3-406-69543-8

4.2 Aufsichtsbehörden: eine DSFA ist erforderlich ...

Am 4. April 2017 veröffentlichte die Artikel-29-Datenschutzgruppe eine Orientierungshilfe (Arbeitspapier 248), in welcher sie aus ihrer Sicht darstellte, wann eine DSFA zu erfolgen hat³⁸.

Grundsätzlich muss eine DSFA nach Ansicht der Artikel-29-Datenschutzgruppe immer dann erfolgen, wenn eine Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen mit sich bringt. Wenn seitens des Verantwortlichen nicht eindeutig zu bestimmen ist, ob eine DSFA notwendig ist oder nicht, empfiehlt die Artikel-29-Datenschutzgruppe die Durchführung einer DSFA.

Weiterhin führt die Artikel-29-Datenschutzgruppe aus, dass es sich bei der Aufzählung in Art. 35 Abs. 3 DS-GVO nicht um eine abschließende Aufzählung handelt, sondern lediglich Beispiele von Verarbeitungen aufgezeigt werden, die in einem hohen Risiko münden. Die Artikel-29-Datenschutzgruppe erstellte 10 Kriterien, an Hand derer Verantwortliche Verarbeitungen identifizieren können, denen ein hohes Risiko innewohnt:

1. Bewertung/Scoring (inklusive Profiling) von sie betreffenden persönlichen Aspekten, insbesondere „zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person“ (ErwGr. 71, 91)
2. Automatisierte Entscheidungsfindung, welche als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
3. Systematische Überwachung: Verarbeitung, die genutzt wird, um natürliche Personen zu beobachten, überwachen oder zu kontrollieren
4. Verarbeitung sensibler Daten, dazu gehört insbesondere die Verarbeitung von Daten, welche zu den besonderen Kategorien gemäß Art. 9 oder zu den in Art. 10 genannten Daten bzgl. strafrechtliche Verurteilungen und Straftaten gehören
5. Verarbeitung großer Mengen an Daten: die DS-GVO definiert nicht, was eine „große Menge“ ist, die Artikel-29-Datenschutzgruppe geht von der Erfüllung der Anforderung aus, wenn
 - die Anzahl der betroffenen Personen hoch ist, sei es numerischer Natur oder prozentual bzgl. einer bestimmten Population
 - oder
 - die Datenmenge groß ist oder die Heterogenität der Daten hoch ist
 - oder
 - die Verarbeitungsdauer oder die Speicherdauer sehr lang ist
 - oder
 - die geografische Ausdehnung der Verarbeitungsaktivität hoch ist
6. Datenbestände, die entweder aufeinander abgestimmt („been matched“) oder zusammengeführt wurden
7. Verarbeitung von Daten schutzbedürftiger Personen (i. S. v. ErwGr. 71): Hier kann eine DSFA z. B. auf Grund eines bestehenden Ungleichgewichts, wie es, z. B. zwischen Arbeitgeber und

³⁸ Article 29 Working Party: Working Paper 248 „Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.“ Online, zitiert am 2017-04-27; Verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Arbeitnehmer existiert, erforderlich sein, ebenso besitzen Kinder einen hohen Schutzbedarf, da diese die Folgen der Verarbeitung ggf. nicht abschätzen können

8. Innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen:
Einerseits kann die Anwendung neuer Technologie eine DSFA erforderlich machen (Art. 35 Abs. 1 DS-GVO bzw. ErwGr. 89, 91), andererseits können eingesetzte Lösungen, wie z. B. die Kombination von Fingerabdruckscannern mit Gesichtserkennung zur Zugangskontrolle für sensible Bereiche, ein hohes Risiko für die betroffenen Personen beinhalten
9. Datentransfer außerhalb der EU (ErwGr. 116)
10. Wenn die Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren (Art. 22 DS-GVO, ErwGr. 91)

Je mehr der oben genannten Kriterien auf das Verarbeitungsvorhaben zutreffen, desto höher ist nach Meinung der Artikel-29-Datenschutzgruppe die Wahrscheinlichkeit, dass das Verarbeitungsvorhaben ein hohes Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen Personen beinhaltet. In einigen Fällen wird nach Ansicht der Artikel-29-Datenschutzgruppe aber auch schon die Erfüllung eines Kriteriums ausreichen, um eine DSFA erforderlich zu machen.

4.2.1 Beispiel „hospital information system“

Die Artikel-29-Datenschutzgruppe führt in ihrem Arbeitspapier 248 weiter aus, dass eine DSFA für „a general hospital keeping patients’ medical records“ erforderlich ist. Beispielhaft führt sie in dem Arbeitspapier aus, dass für ein „hospital information system“ eine DSFA grundsätzlich erforderlich ist.

So wie bei sämtlichen anderen Datenschutzbeauftragten ist auch bei den Mitgliedern der Artikel-29-Datenschutzgruppe – und auch beim späteren Datenschutz-Ausschuss – das gesetzlich geforderte Fachwissen vorhanden. Bei der Interpretation der an das Fachpublikum gerichteten Informationen muss somit das jeweils aktuelle rechtliche, betriebswirtschaftliche, informationstechnische und branchenspezifische Fachwissen herangezogen werden. Im Gesundheitswesen beinhaltet das „branchenspezifische Fachwissen“ sowohl das entsprechende medizinische Fachwissen bzgl. Aufbau und Organisation der verantwortlichen Stelle sowie deren Ablaufstrukturen im medizinischen Bereich, als auch spezielle Kenntnisse in medizinischer Informatik. Diese Bereiche müssen daher zur Interpretation der Arbeitspapiere der Artikel-29-Datenschutzgruppe herangezogen werden. Nur so können branchenspezifische Fachbegriffe, wie z. B. „hospital information system“³⁹, in den Papieren der Artikel-29-Datenschutzgruppe richtig interpretiert werden.

Insofern liegt dem Verständnis eines HIS ein anderes Verständnis zugrunde als der Beschreibung eines KIS in der Orientierungshilfe Krankenhausinformationssysteme der deutschen Aufsichtsbehörden. Unabhängig von begrifflichen Feinzeleinerungen – die OH KIS definiert zusätzlich auch noch den Begriff eines PAS (Patientenaktensystems) - sollte der Fokus der Praxis eher auf die konkreten Verarbeitungsvorgänge gerichtet werden. Wenn ein konkreter Verarbeitungsvorgang aus

³⁹ Der Begriff „hospital information system“ (HIS) wurde 1956 von Zworkyn eingeführt . Heute ist der Begriff etabliert, in der pubmed Datenbank, welche in ihrer Suche 5633 Fachzeitschriften aus den Gebieten Medizin, Zahnmedizin, Veterinärmedizin, öffentliches Gesundheitswesen, Psychologie, Biologie, Genetik, Biochemie, Zellbiologie, Biotechnologie, Biomedizin berücksichtigt, finden sich über 67.000 Fachartikel , welche den Terminus „hospital information system“ nutzen.

In der englischsprachigen Wikipedia findet man „A hospital information system (HIS) is an element of health informatics that focuses mainly on the administrative needs of hospitals“ , Gartner schreibt dazu: „The IT applications used to manage hospital operations (e.g., patient financials, registration, scheduling, general financials, back-office systems and order communications)“.

materiell rechtlichen Gründen eine DSFA erfordert, ist die Unterscheidung eher akademisch, ob dieser in einem HIS, KIS oder PAS erfolgt.

4.3 Aufsichtsbehörden: eine DSFA ist nicht erforderlich ...

Entsprechend des o.g. Arbeitspapiers 248 der Artikel-29-Datenschutzgruppe ist eine DSFA insbesondere dann nicht erforderlich⁴⁰, wenn

- die Verarbeitung „wahrscheinlich [kein] hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“ (Art. 35 Abs. 1 DS-GVO)
- oder
- sich die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung von denen einer anderen Verarbeitung, für die bereits eine DSFA durchgeführt wurde, nur in geringem Maße unterscheiden (Art. 35 Abs. 1 DS-GVO)
- oder
- die Verarbeitungsvorgänge vor Mai 2018 von einer Aufsichtsbehörde unter bestimmten Bedingungen geprüft worden sind, die sich nicht geändert haben
- oder
- ein Verarbeitungsvorgang gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten beruht und diese Rechtsvorschrift den konkreten Verarbeitungsvorgang regelt und falls bereits im Rahmen der Schaffung dieser Rechtsgrundlage eine DSFA erfolgte (Art. 35 Abs. 10 DS-GVO), es sei denn, ein Mitgliedstaat erklärt, dass es notwendig ist, vor den fraglichen Verarbeitungstätigkeiten eine DSFA durchzuführen
- oder
- der Verarbeitungsvorgang auf einer (von der Aufsichtsbehörde erstellten) optionalen Liste der Verarbeitungsvorgänge aufgeführt ist, für die keine DSFA erforderlich ist (Art. 35 Abs. 5).

4.4 Aufsichtsbehörden: Vorgehen bei einer DSFA

Es gibt verschiedene Methoden, eine DSFA anzulegen. Welche der Verantwortliche nimmt, bleibt ihm überlassen. Im Anhang 1 des Arbeitspapiers 248 zählt die Artikel-29-Datenschutzgruppe einige Möglichkeiten auf, ohne einzelnen hierbei einen Vorzug einzuräumen.

Eine DSFA muss mindestens den Anforderungen von Art. 35 Abs. 7 DS-GVO in Verbindung mit ErwGr. 84 und 90 genügen. Der Prozess der Erstellung einer DSFA wird von der Artikel-29-Datenschutzgruppe als PDCA-Zyklus⁴¹ angesehen und sollte mindestens alle 3 Jahre erneuert werden, je nach Art der Verarbeitung und der Anzahl der Änderungen im Verarbeitungsprozess auch früher. Auch wenn die Verordnung selbst keine Pflicht zu einer turnusmäßigen Erneuerung / Kontrolle vorschreibt, sollte dieser Empfehlung gefolgt werden. Indirekt ergibt sich die

⁴⁰ DATENSCHUTZGRUPPE NACH ARTIKEL 29: WP 248 rev.01 „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“. Stand 2017-10-04. S. 152, 13: „Nach Ansicht der WP29 ist in folgenden Fällen keine DSFA erforderlich [...]“. Online, zitiert am 2017-09-02; Verfügbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48464

⁴¹ Demingkreis oder PDCA-Zyklus (PDCA steht für das englische Plan-Do-Check-Act): ein iterativer Prozess für Lernen und Verbesserung eines Prozesses: der Prozess wird geplant („plan“, dann umgesetzt („do“), anschließend Prozessablauf und Ergebnisse überprüft („check“) und basierend auf den Ergebnissen der Prüfung der Vorgang bei Bedarf angepasst („act“)

Notwendigkeit entsprechender Kontrollen nämlich daraus, dass es regelmäßiger Prüfungen bedarf, ob eine Veränderung des Risikos eingetreten ist.

Eine Veröffentlichung der DSFA ist gesetzlich nicht gefordert, wird aber von der Artikel-29-Datenschutzgruppe im Sinne des Transparenzgedankens empfohlen. Dabei muss nicht zwangsläufig die vollständige DSFA veröffentlicht werden, insbesondere nicht die Teile einer DSFA, welche ggf. Sicherheitsrisiken oder Firmengeheimnisse des Verarbeiters enthüllen würde.

5 Vorgehensweise bei der Erstellung einer Datenschutz-Folgenabschätzung

Das grundsätzliche Vorgehen bzgl. einer DSFA ist wie folgt⁴²:

- 1) Feststellen, ob eine DSFA notwendig ist oder nicht
- 2) Vorbereitung
 - a. Zusammenstellung des DSFA-Teams
 - b. Erstellen eines DSFA-Plans
 - c. Beschreibung des Untersuchungsgegenstandes
 - i. Was wird betrachtet?
 - ii. Wer ist betroffen?
 - iii. Identifikation der relevanten Rechtsgrundlagen
 - d. Einbeziehung der Stakeholder
 - i. Identifizierung der Stakeholder
 - ii. Erstellung eines Umsetzungsplans
 - iii. Befragung der Stakeholder
- 3) Durchführung
 - a. Identifizierung der betroffenen Daten sowie des Informationsflusses der Daten
 - b. Analyse der Auswirkungen der use cases
 - c. Festlegung der dazugehörigen Sicherheitsmaßnahmen
 - i. Identifikation von Schutzzielen
 - d. Abschätzung des datenschutzrechtlichen Risikos
 - i. Identifikation der Risiken
 - ii. Analyse der Risiken
 - iii. Bewertung der Risiken
 - e. Erarbeiten der Behandlung der datenschutzrechtlichen Risiken
 - i. Darstellung der Möglichkeiten bzgl. der Verringerung des Risikos, Identifikation passender Schutzmaßnahmen
 - ii. Festlegung der Kontrolle bzgl. des Risikos, Identifikation von Bewertungskriterien und -maßstäben
 - iii. Erstellen des Behandlungsplans bzgl. der Risiken
- 4) Bericht

Auf ausgewählte Aspekte der vorstehend genannten Schritte gehen wir im Folgenden ein, andere sind bereits aus anderen Aspekten der Tätigkeit im Datenschutzzumfeld bekannt (z.B. die Identifizierung des Informationsflusses) und bedürfen keiner weiteren Erläuterung.

5.1 Feststellen, ob eine DSFA notwendig ist oder nicht

Die Feststellung, ob eine DSFA erforderlich ist (bzw. die Aktualisierung einer bestehenden DSFA) liegt beim Verantwortlichen, also der Leitung des Unternehmens. Diese muss diese Entscheidung treffen. Bei der Entscheidung ist sie nicht frei, sondern die DS-GVO gibt hier einen Rahmen vor, wann eine DSFA erforderlich ist (siehe auch Kapitel 2). Unabhängig von der gesetzlichen Vorgabe steht es dem Unternehmen natürlich jederzeit frei, auch ohne gesetzlichen Zwang eine DSFA durchzuführen. Eine Übersicht bietet Abbildung 1, im Folgenden wird dargestellt, wann auf eine DSFA verzichtet werden kann und wann sie erforderlich ist.

⁴² Basierend ISO/IEC 29134 Datenschutz-Folgenabschätzung – Leitfaden. Online, zitiert am 2017-11-18; Verfügbar unter <https://www.beuth.de/de/norm/iso-iec-29134/276510955>

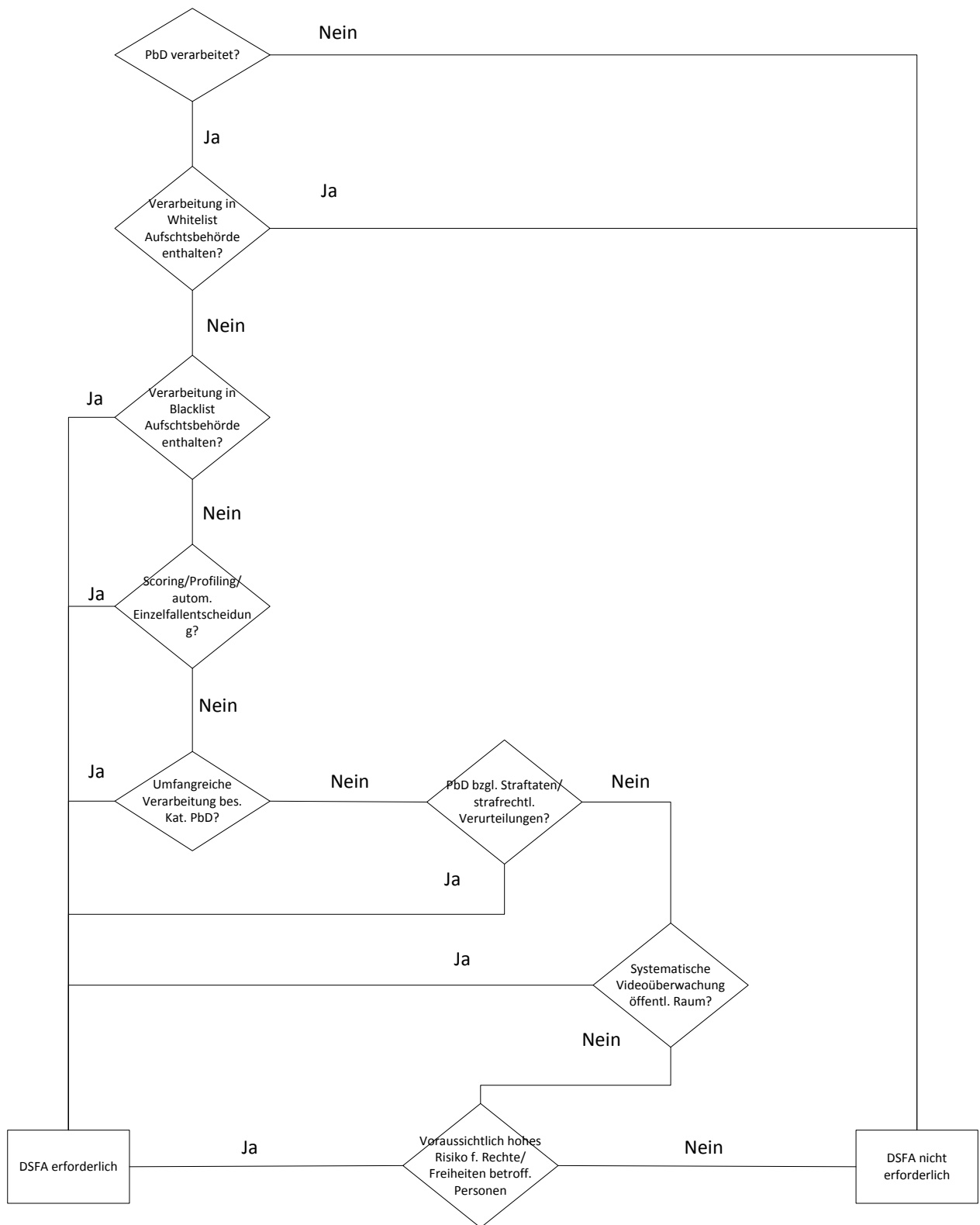


Abbildung 1: Entscheidungsbaum bzgl. Durchführung einer DSFA

5.1.1 Keine Datenschutz-Folgenabschätzung erforderlich?

Eine DSFA ist nicht erforderlich, wenn eine der folgenden Fragen mit „ja“ beantwortet werden kann.

	Ja	Nein
Steht die Verarbeitung auf einer „White-List“ gemäß Art. 35 Abs. 5 DS-GVO?		
Liegt eine Datenschutz-Folgenabschätzung im Sinne des Art. 35 Abs. 10 DS-GVO vor und wurde seitens des für den Verantwortlichen geltenden Mitgliedsstaates keine darüber hinausgehende DSFA angeordnet?		
Existiert eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohem Risiko i.S.v. Art. 35 Abs. 1 Satz 2 DS-GVO?		

5.1.2 Fälle, in denen eine Datenschutz-Folgenabschätzung durchgeführt werden muss

Eine Datenschutz-Folgenabschätzung ist – abgesehen von der veröffentlichten Liste der Aufsichtsbehörden sowie der in Art. 35 Abs. 10 DS-GVO erwähnten Ausnahme – insbesondere dann erforderlich, wenn einer der folgenden Umstände vorliegt:

- 1) Mit der Verarbeitung soll die Persönlichkeit des Betroffenen systematisch und automatisiert bewertet werden, sodass rechtliche oder andere intensive Eingriffe für den Betroffenen daraus resultieren bzw. resultieren können.
- 2) Es sollen umfangreiche Mengen von Daten, die zu den besonderen Kategorien gehören, verarbeitet werden.
Beispiel für das Gesundheitswesen: Verarbeitung von Gesundheitsdaten oder genetischen Daten
- 3) Es sollen umfangreiche Mengen von Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden.
- 4) Es sollen öffentlich zugängliche Räume überwacht werden.
Beispiel: Videoüberwachung in den öffentlich zugänglichen Bereichen der Notaufnahme oder Eingangshalle, in der Publikumsverkehr herrscht.

Weiterhin kann eine DSFA erforderlich sein, wenn die Verarbeitung der personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten der Betroffenen birgt. Indizien, dass eine DSFA durchzuführen ist, sind u.a.

- Einsatz neuer Verarbeitungstechnologien, d. h. Technologien, zu denen der Verantwortliche noch keine DSFA durchgeführt hat;
- Einsatz neuer Verarbeitungen, d. h. Verfahren der Verarbeitung personenbezogener Daten, zu denen der Verantwortliche noch keine DSFA durchgeführt hat;
- Verarbeitung großer Datenmengen;
- Verarbeitung von Daten einer großen Anzahl betroffener Personen;
- Verarbeitungen, welche betroffenen Personen die Wahrnehmung ihrer aus der DS-GVO resultierenden Rechte erschweren.

5.2 Vorbereitung

Ist eine DSFA durchzuführen (sei es eine neue oder die Überarbeitung einer vorhandenen DSFA), bestimmt der Verantwortliche die Leitung des DSFA-Teams. Gemeinsam mit der DSFA-Teamleitung wird

- die Aufgabe definiert
- der (Beurteilungs-) Umfang / Geltungsbereich bestimmt

- die Entscheidung zum Umfang⁴³ der DSFA getroffen
- die Zielgruppen bzw. die betroffenen Stakeholder benannt
- festgelegt, wer den DSFA-Bericht erhalten muss, ggf. auch, wer ihn zusätzlich bekommen darf.

Das Ergebnis wird schriftlich festgehalten. Danach stellt die DSFA-Leitung das DSFA-Team zusammen.

5.2.1 DSFA-Team

Die Durchführung einer DSFA benötigt ein interdisziplinär aufgestelltes Team, deren Mitglieder einerseits die verschiedenen Aspekte der benötigten Fachkenntnis (insbesondere Datenschutzrecht, IT-Sicherheit, Kenntnis bzgl. des betroffenen Fachgebietes) abdecken, andererseits müssen einige Mitglieder aber auch hinreichend tief in die Organisation des Unternehmens eingebunden sein, um Entscheidungen bzgl. der Finanzierbarkeit von Maßnahmen treffen zu können. Daher besteht das DSFA-Team mindestens aus je einer

- Person mit entsprechenden Entscheidungsbefugnissen; diese Person leitet das DSFA-Team und ist der Stellvertreter des Verantwortlichen im Rahmen der DSFA
- Person mit Fachkenntnis auf dem Niveau eines ausgebildeten Datenschutzbeauftragten auf dem jeweiligen Fachgebiet⁴⁴
- Person mit der Fachkenntnis eines IT-Sicherheitsbeauftragten
- Person aus der Informations- und Kommunikationstechnik des Unternehmens

sowie aus Vertretern der Fachbereiche oder Geschäftsfelder, die vom Projekt am meisten betroffen sind. Laut ISO/IEC 29134 sollte auch eine „abnehmende Person“ benannt werden. Dies ist die Person, welche den vorgelegten DSFA-Bericht im Namen des Unternehmens gegenzeichnet und somit die Umsetzung der im DSFA-Prozess festgelegten Prozesse verbindlich anordnet.

Der Datenschutzbeauftragte des Unternehmens steht dem DSFA-Team beratend zur Seite, um die notwendige datenschutzrechtliche Fachkenntnisse beizutragen. In diesem Fall ist der Datenschutzbeauftragte jedoch nicht mehr unvoreingenommen genug. Um die Ergebnisse der DSFA prüfen zu können, muss dies dann durch eine externe Fachkraft mit entsprechendem Fachwissen erfolgen. Alternativ wird von Anfang an eine externe Fachkraft mit Datenschutzkenntnissen in das Team integriert und der für das Unternehmen zuständige Datenschutzbeauftragte übernimmt am Ende die Prüfung; in diesem Fall kann er dem Team aber nur zu gelegentlichen Ratschlägen zur Verfügung stehen, wie es auch in Art. 35 Abs. 2 DS-GVO beschrieben ist („holt [...] den Rat des Datenschutzbeauftragten [...] ein“); eine Einbindung auch i.S.v. regelmäßiger Teilnahme an Sitzungsbesprechungen oder ähnlichem darf nicht erfolgen.

5.2.2 Einbeziehung der Stakeholder

Neben den betroffenen Personen und ihren Vertretern (Art. 35 Abs. 9 DS-GVO) können weitere interne und externe Gruppen von den in einer DSFA beschriebenen Prozessen betroffen sein bzw. zu deren Ergründung und Bewertung unverzichtbare Hinweise geben. Dies können insbesondere sein:

⁴³ Im Krankenhaus wird eine DSFA i.d.R. nur die eigenen Prozesse berühren. Ein Anbieter von einer institutionsübergreifenden Patientenakte, in die automatisiert Daten von verschiedenen Krankenhäusern, Arztpraxen usw. eingespielt werden, wird im Rahmen der dafür notwendigen DSFA auch die anderen Institutionen einbeziehen müssen.

⁴⁴ Hinweise auf die benötigte Qualifikation findet man im vom BvD erarbeiteten Berufsbild. Online, zitiert am 2017-12-17; Verfügbar unter <https://www.bvdnet.de/berufsbild/>

- Beschäftigte (im Rahmen der Gesundheitsversorgung insbesondere in den Prozess involvierte medizinische Fachgruppen wie z. B. ärztliches und pflegerisches Personal, aber auch Beschäftigte in der Verwaltung wie z. B. Beschäftigte in der IKT oder der Rechtsabteilung)
- Mitarbeitervertretung (Betriebsrat, Personalrat)
- Auftragnehmer sowie ggf. deren Unterauftragnehmer (insbesondere Hersteller von Informationssystemen, in denen die entsprechenden Daten verarbeitet werden).

Bereits bei der Planung der DSFA sollte man sich im DSFA-Team über die Art (zu welchen Aspekten soll welcher Stakeholder hinzugezogen werden) und den Umfang (in welche Tiefe der jeweiligen Prozessschritte dringt man vor) der Konsultation absprechen, aber naturgemäß ergeben sich einige Punkte erst bei der Konsultation selbst.

5.3 Durchführung

5.3.1 Analyse der Auswirkungen der Verarbeitungsprozesse

Zunächst muss eine Beschreibung des zu untersuchenden Tatbestandes (Prozess, eingesetztes IT-System, ...) erstellt werden. Dazu gehört insbesondere auch die Darstellung des Informationsflusses der Daten. Zu den Fragen, die hierbei beantwortet werden müssen, gehören insbesondere

- Wer sind die von der Verarbeitung ihrer Daten betroffenen Personen?
- Wer erhebt welche Daten bei wem?
- Für welche Zwecke werden welche Daten verarbeitet?
- Welche Vorteile erwachsen den betroffenen Personen aus der Verarbeitung? Welche Vorteile ggf. der Gemeinschaft aller, also dem Staat, bestehen?
- Wie erfolgt die Verarbeitung? Welchen Geschäftsprozessen dienen die Daten?

Ergänzende Angaben zu diesem Komplex sind

- o Welche Hard- und Software wird eingesetzt?
- o Über welche Kommunikationsnetze werden personenbezogene Daten ausgetauscht?
- o Existieren ggf. Daten in Papierform wie z. B. Ausdrucke?
- o Wie erfolgt das Identitäts- und Nutzermanagement in den eingesetzten IT-Systemen?
- o Welche Metadaten fallen an, werden genutzt,...?
- o Wie werden Daten gelöscht, Speichermedien entsorgt?
- o Ist eine Außerbetriebnahme des IT-Systems geplant (im organisatorischen, nicht im zeitlichen Sinne)?
- Wie werden die Betroffenenrechte gewahrt?
- Wer sind die Empfänger der Daten? Gibt es Empfänger in unsicheren Drittstaaten?
- Welche Auftragsverarbeiter und ggf. welche Unterauftragsverarbeiter existieren für welche Verarbeitungsvorgänge?
- Wie sind die Verantwortlichkeiten geregelt?
(Prozessverantwortung, wirtschaftliche Verantwortung)
- Was sind die rechtlichen Grundlagen der Verarbeitung?

D. h. der gesamte Lebenszyklus der Daten sollte dargestellt werden.

Darauf aufbauend werden die Folgen der Verarbeitung beschrieben. Dabei ist auch das Anwenderverhalten zu berücksichtigen, also z. B. ob ein Hinweistext vom Anwender voraussichtlich gelesen oder nur „weggeklickt“ wird. Ferner sind organisatorische Rahmenbedingungen zu berücksichtigen. Z. B. ob der Hinweistext ohne Lesen weggeklickt wird, weil der Inhalt durch eine

Schulung (oder auch durch regelmäßig stattfindende Wiederholungsunterweisungen) vermittelt wird und der Inhalt somit als „bekannt“ vorausgesetzt werden darf.

5.3.2 Abschätzung des datenschutzrechtlichen Risikos

5.3.2.1 Risikoevaluation

In einer Datenschutz-Folgenabschätzung geht es darum, den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger von der Verarbeitung betroffener Personen Rechnung zu tragen. D. h. es werden die diesbezüglichen Risiken betrachtet, nicht die Risiken für den Verantwortlichen, der diese Daten verarbeitet.

Zur Risikoevaluation gehört, neben den sich aus Kapitel 5.3.1 genannten Folgen der Verarbeitung, auch die Identifikation aller relevanten gesetzlichen, regulatorischen und geschäftlichen Faktoren mit Bezug auf den in der DSFA untersuchten Verarbeitungsprozess sowie die Darstellung des Resultats evtl. Verstöße dagegen, wenn diese ein Risiko im Sinne der DSFA darstellen. Insbesondere sollten auch die Risiken betrachtet werden, die sich aus den Folgen einer legitimen Verarbeitung ergeben können, z. B. Zweckänderung bei vorhandenen Daten, Umgang mit den Daten nach Erreichung des Zweckes, Verarbeitung auf Grund einer nicht eindeutigen Rechtsgrundlage oder auch der Verarbeitung basierend auf einer unwirksamen Einwilligung.

Des Weiteren gehört zur Risikoevaluation die Betrachtung der Gewährleistung der Betroffenenrechte. Wie werden Widerspruchsrechte gewährleistet, Auskunftsrechte usw.? Nicht zuletzt wohnen jeglichem Datentransfer Risiken inne: existiert ein wirksamer Schutz gegen unbefugtes Mitlesen der Daten? Wie sieht es mit dem Risiko des behördlichen Zugriffs in Drittländern aus, wenn dort Daten verarbeitet werden.

Zudem bestehen Risiken in jeder Verarbeitung selbst. Evtl. werden nicht-relevante Daten erhoben, die gelöscht werden müssen. Wie ist der Umgang mit doppelten Datenbeständen, welche ggf. sogar widersprüchliche Aussagen beinhalten? Wie werden fehlerhafte Daten erkannt? Gibt es eine Aktualisierungsstrategie? Existiert ein Auftragsverarbeitungsvertrag, wenn Auftragnehmer Daten verarbeiten? Alles Vorgenannte stellt Fragen dar, welche Risiken in der Verarbeitung aufdecken können.

5.3.2.2 Risiken bzgl. der betroffenen Personen

Insgesamt erhält man durch das in Kapitel 5.3.2.1 beschriebene Verfahren eine Liste von diversen potenziellen Tatbeständen, aus denen Risiken für die betroffene Person erwachsen können. Diese abstrakten Risiken müssen nun für die betroffene Person identifiziert werden. So kann etwa eine widerrechtliche Verarbeitung (z. B. in Form einer unbefugte Kenntnisnahme medizinischer Daten) u. a. das Risiko der Diskriminierung für die betroffene Person beinhalten. Daher muss nun eine Zuordnung der gefundenen Tatbestände und der daraus resultierenden möglichen Risiken erfolgen.

Eine Kategorisierung der Risiken, die bei einer Verarbeitung personenbezogener Daten auftreten können, lässt sich wie folgt darstellen⁴⁵:

1. Strukturelle Risiken
 - a. Gesellschaftlich-politische Risiken

⁴⁵ Stefan Drackert (2014) Die Risiken der Verarbeitung personenbezogener Daten - Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN '978-3-428-1 4730-4

- i. Informationsmacht
 - ii. Konformistische Verhaltensanpassung durch Überwachungsdruck
 - iii. Verantwortungsnegation
 - b. Wirtschaftliche Risiken
 - i. Handelshemmnisse
 - ii. Nachfragerückgang durch Vertrauensverlust
- 2. Individuelle Risiken
 - a. Erhöhung individueller Verletzlichkeit für Straftaten
 - b. Schamgefühl und Ansehensverlust
 - c. Selektivitätsschäden
 - i. Diskriminierung
 - ii. Stigmatisierung
 - d. Dauerhafte Verfügbarkeit (negativer) Informationen
 - e. Systematische Verzerrung von Inhalten (Entkontextualisierung)
 - i. Kontextdefizit
 - ii. Verknüpfung/Vermischung verschiedener Kontexte
 - f. Auftauchen (negativer) Informationen (Informationsemergenz)
 - g. Informationsfehlerhaftigkeit
- 3. Risiken für Gesellschaft und Individuum
 - a. Behandlung des Menschen als bloßes Objekt
 - b. Bildung eines Persönlichkeitsprofils
 - c. Fremdbestimmung
 - d. Enttäuschung von Vertraulichkeitserwartungen
- 4. Grenzfälle
 - a. Werbung und Zielgruppenpräzisierung
 - b. Bonitätsprüfungen, Forderungsmanagement
 - c. Arbeitsrechtlicher Kontext

Dies ist keine abschließende Aufzählung, jedoch verdeutlicht diese beispielhafte Darstellung, welche Risiken zu betrachten sind.

5.3.2.3 Risikobewertung

Wurden die Risiken für die Verarbeitung benannt, so erfolgt anschließend eine Bewertung der Risiken. Hierzu müssen drei Schritte absolviert werden:

1. Der (potenzielle) Schaden muss klassifiziert werden.
2. Die Eintrittswahrscheinlichkeit muss abgeschätzt werden.
3. Basierend auf diesen beiden Ergebnissen wird das Risiko klassifiziert.

5.3.2.3.1 Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit kann wie folgt klassifiziert werden:

Hoch	Tritt wahrscheinlich auf, oft, häufig
Mittel	Kann auftreten, jedoch nicht häufig
Niedrig	Unwahrscheinliches Auftreten, selten, fernliegend

5.3.2.3.2 Schadensklassifikation

Definitionen des Schweregrads:

Katastrophal:	Erhöhung individueller Verletzlichkeit für Straftaten
---------------	---

Kritisch:	Diskriminierung, Stigmatisierung
Ernst:	Wirtschaftliche Folgen, Folgen im Berufsleben
Gering:	Bildung eines Persönlichkeitsprofils
Vernachlässigbar:	Unannehmlichkeiten

5.3.2.3.3 Risikoklassifizierung

Innerhalb einer Risikomatrix wird das Risiko für die einzelnen Gefahrenpotenziale dargestellt:

Potenzielles Risiko		Eintrittswahrscheinlichkeit	Schadensklassifikation
Strukturelle Risiken			
	Gesellschaftlich-politische Risiken		
	Informationsmacht		
	Verhaltensanpassung durch Überwachungsdruck		
	Verantwortungsnegation		
	Wirtschaftliche Risiken		
	Handelshemmnisse		
	Nachfragerückgang		
Individuelle Risiken			
	Erhöhung individueller Verletzlichkeit für Straftaten		
	Schamgefühl und Ansehensverlust		
	Selektivitätsschäden		
	Diskriminierung		
	Stigmatisierung		
	Dauerhafte Verfügbarkeit (negativer) Informationen		
	Systematische Verzerrung von Inhalten		
	Kontextdefizit		
	Verknüpfung/Vermischung verschiedener Kontexte		
	Auftauchen (negativer) Informationen		
	Informationsfehlerhaftigkeit		
Risiken für Gesellschaft und Individuum			
	Behandlung des Menschen als bloßes Objekt		
	Bildung eines Persönlichkeitsprofils		
	Fremdbestimmung		
	Enttäuschung von Vertraulichkeitserwartungen		
Grenzfälle			
	Werbung und Zielgruppenpräzisierung		
	Bonitätsprüfungen, Forderungsmanagement		
	Arbeitsrechtlicher Kontext		

5.3.3 Umgang mit den datenschutzrechtlichen Risiken

Grundsätzlich existieren vier Möglichkeiten zum Umgang mit potenziellen Risiken:

- 1) Risikovermeidung: Das Risiko wird vollständig vermieden, z. B. durch ändern der Rahmenbedingungen oder durch Verzicht auf die Verarbeitung.
- 2) Risikominimierung: bei Eintritt des Risikos werden die Folgen durch die Maßnahmen nur verringert, jedoch nicht vollständig abgewendet.
- 3) Risikohandhabung: Bereits bestehende Maßnahmen behandeln das Risiko im ausreichenden Umfang, es besteht kein Bedarf für weitere Maßnahmen. Die Risikohandhabung stellt eine Untergruppe der Risikominimierung dar.
- 4) Risikoübertragung: Hier erfolgt eine teilweise oder vollständige Verlagerung auf externe Partner, z. B. durch eine Versicherung, die Konsequenzen aus dem Eintritt des Risikos begegnet, oder externer Überwachung von Systemen inkl. Eingriffsmöglichkeit (z. B. Betreuung einer Firewall durch externe Dienstleister; die Einbindung externer Partner kann grundsätzlich neue Risiken erzeugen, die betrachtet und ggf. auch behandelt werden müssen.

Bei Risiken mit hoher Schadensklassifikation („kritisch“ oder „katastrophal“) stellt ausschließlich die Risikovermeidung eine Option dar, alles andere ist der betroffenen Person nicht zumutbar.

Bei Risiken mit darunterliegender Schadensklassifikation kommen alle Optionen in Betracht. Dementsprechend müssen Kosten und Aufwand bei der Auswahl der Risikostrategie berücksichtigt werden. Ferner sind Kosten und Aufwand sowie die Art der Berücksichtigung nachvollziehbar zu dokumentieren, da die DSFA abschließend ja von einem unabhängigen Gutachter bewertet wird, der bei den Diskussionen des DSFA-Teams nicht anwesend war.

Zuletzt wird festgelegt, zu welchen der in Kapitel 5.3.1 ermittelten Folgen der Verarbeitung und den daraus resultierenden Risiken welche Maßnahmen ergriffen werden.

Wichtig dabei ist, dass die Maßnahmen bzw. deren Auswirkungen auch kontrollierbar sind. Es sollten z. B. Kennzahlen angegeben werden, anhand derer überprüft werden kann, ob das Schutzziel erreicht wurde oder nicht. Auch die Kontrollmöglichkeiten müssen dokumentiert werden, desgleichen wie häufig eine Überprüfung erforderlich ist und wie mit Abweichungen umgegangen wird. Wer wird kontaktiert, wenn ein Schutzziel nicht erreicht wird? Wer ist für weitergehende Maßnahmen verantwortlich? Usw.

5.4 Bericht

Der DSFA-Bericht stellt einerseits eine Prozessübersicht inkl. der beteiligten Akteure, der Prozesse/Verfahren, der Datenverarbeitungen sowie der daraus erwachsenden Folgen und Risiken dar und bietet damit zugleich auch eine gute Grundlage für die Arbeit anderer Organisationseinheiten wie dem Controlling. Andererseits dient er dem Nachweis des Umgangs mit Datenschutzrisiken im Unternehmen, bildet die Grundlage für eine künftige DSFA und ermöglicht durch die Nachverfolgbarkeit eine stetige Optimierung der Schutzmaßnahmen.

Dementsprechend sind sowohl der Empfängerkreis wie auch der Grad der Vertraulichkeit seitens des Unternehmens auszuwählen. Grundsätzlich steht der vollumfängliche Bericht der Datenschutzaufsichtsbehörde zur Verfügung. Sofern Interesse besteht, kann der Bericht der Öffentlichkeit zur Verfügung gestellt werden: dann müssen ggf. vertrauliche Einzelheiten wie Namen entfernt werden.

Die Struktur des Berichts kann wie folgt aussehen (Einzelheiten siehe Kapitel 6):

1. Beschreibung des Verarbeitungsverfahrens
 - a) Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien
2. Welche Daten werden verarbeitet?
 - a) Welche Datenarten werden verarbeitet?
 - b) Wo werden die Daten erhoben?
 - c) Darstellung der potenziellen Risiken
3. Zwecke und Mittel der Verarbeitung
 - a) Begründung, warum die Informationen verarbeitet werden müssen
 - b) Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung
 - c) Darstellung der Erlaubnistatbestände
 - d) Darstellung der Speicherdauer
 - e) Darstellung der potenziellen Risiken
4. Weitergabe der Daten
 - a) Mit wem werden die Daten geteilt?
 - b) Darstellung der potenziellen Risiken
5. Wahrung der Betroffenenrechte
 - a) Information des Betroffenen
 - b) Auskunftsrecht
 - c) Widerspruchsrecht
 - d) Recht auf Berichtigung und Vervollständigung
 - e) Recht auf Löschen („Vergessenwerden“)
 - f) Recht auf Einschränkung der Verarbeitung („Sperrung“)
 - g) Recht auf Datenübertragbarkeit
6. Gewährleistung der Sicherheit der Daten
 - a) Darstellung der Erbringung der Anforderungen aus Art. 32 DS-GVO „Sicherheit der Verarbeitung“
7. Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung
8. Fazit
 - a) Abschließende Bewertung
 - b) Entscheidung bzgl. Information Aufsichtsbehörde

6 Vorschlag für die strukturierte Dokumentation einer Datenschutz-Folgenabschätzung (DSFA-Bericht)

6.1 Beschreibung des Verarbeitungsverfahrens

Eine Beschreibung des bzw. der Verarbeitungsverfahren(s) soll insbesondere die folgenden Fragen beantworten:

- a) Wer sind die von der Verarbeitung ihrer Daten betroffenen Personen?
- b) Welchem/Welchen Zweck(en) dient die Verarbeitung? Was soll damit erreicht werden?
- c) Wie erfolgt die Verarbeitung? Wer macht was zu welchem Zeitpunkt mit welchen Daten?
- d) Welche Vorteile erwachsen den betroffenen Personen aus der Verarbeitung? Welche Vorteile ggf. der Gemeinschaft aller, also dem Staat?
- e) Wie erfolgt die Verarbeitung? Welchen Geschäftsprozessen dienen die Daten?
- f) Welche IT-Systeme werden eingesetzt?
- g) Wie werden die Daten wo für welchen Zeitraum gespeichert? Gibt es ein Archivierungskonzept? Gibt es ein Löschkonzept?
- h) Welche Arten von Daten werden verarbeitet?
- i) Wer hat unter welchen Bedingungen zu welchen Zeitpunkten von welchem Ort aus Zugriff auf die Daten?
- j) Wie können die Daten von wem abgefragt werden? Können die Daten mit Daten aus anderen Systemen verknüpft werden?
- k) Werden die Daten in andere Systeme übermittelt?
- l) Handelt es sich um eine Stand-alone-Anwendung? Oder besteht eine Vernetzung mit anderen Systemen? Wenn ja, welche? Wie sieht die Verbindung aus? Welche Standards werden verwendet, welche proprietären Lösungen⁴⁶ sind im Einsatz? Wie werden die Daten geschützt, insbesondere vor unbefugten Zugriffen?

6.1.1 Darstellung der Einhaltung der grundlegenden datenschutzrechtlichen Prinzipien

Beschreibung, wie die aus Art. 5 DS-GVO resultierenden grundlegenden Prinzipien eingehalten werden:

- Rechtmäßigkeit der Verarbeitung: Wie ist die Verarbeitung legitimiert?
- Transparenz: Werden die Informationspflichten eingehalten?
- Zweckbindung: Erfolgt die Verarbeitung für festgelegte, eindeutige und legitime Zwecke?
- Datenminimierung: Beschränkt sich die Verarbeitung auf das zur Erreichung der Zwecke notwendige Minimum an Daten? D. h. werden nur die absolut erforderlichen Daten verarbeitet?
- Verhältnismäßigkeitsprinzip: Ist die Verarbeitung im Verhältnis zur Zweckerreichung angemessen?
- Richtigkeit: Wie wird gewährleistet, dass die Daten richtig sind? Wie wird sichergestellt, dass die Daten auf dem neuesten Stand bleiben, wenn dies zur Erreichung der Zwecke erforderlich ist?
- Speicherbegrenzung: Werden die Daten (vorbehaltlich gesetzlicher Aufbewahrungspflichten) nur solange gespeichert, bis die Zwecke erreicht sind?
- Integrität und Vertraulichkeit: Welche Maßnahmen werden getroffen, um die Daten zu schützen?

⁴⁶ I.S.v. eigenständigen, für den individuellen Fall angepasste Lösungen

6.2 Welche Daten werden verarbeitet?

6.2.1 Welche Datenarten werden verarbeitet?

Die Datenarten müssen hinreichend genau beschrieben werden, damit die Notwendigkeit der Verarbeitung zur Erreichung des Zweckes auch dargestellt werden kann.

6.2.2 Wo werden die Daten erhoben?

1. Direkt bei der betroffenen Person
 - a. Persönliches Treffen
 - b. Telefongespräch
 - c. E-Mail
 - d. Fax
 - e. Online per Internet-Webseite
 - f. Andere (spezifizieren)
2. Indirekt bei der betroffenen Person
 - a. Ergebnisse aus diagnostischen Maßnahmen (z. B. Daten aus Laboruntersuchungen oder Funktionstests)
 - b. Ergebnisse aus der bildgebenden Diagnostik (z. B. Daten aus Labor- oder radiologischen Untersuchungen)
 - c. Ergebnisse aus Operationen (z. B. Sekundärbefund bei Laparoskopie)
 - d. Ergebnisse aus nicht operativen therapeutischen Maßnahmen (z. B. Allergische Reaktion)
 - e. Andere (spezifizieren)
3. Bevollmächtigte / Vertreter / Sonstige Personen
 - a. Ehepartner, Eltern und andere Verwandte, Freunde
 - b. Gerichtlich bestellte Betreuer
 - c. Mit-/nachbehandelnde Seelsorger
 - d. Mit-/nachbehandelnde Sozialdienst
 - e. Mitpatienten
 - f. Vor-, Mit- und Nachbehandler
 - g. Pflegeheim, Altenheim
 - h. Krankenkassen, gesetzliche Unfallversicherungen
 - i. Andere (spezifizieren)
4. Staatliche Quellen
 - a. Meldeauskunft
 - b. Polizeiliches Führungszeugnis
 - c. Krankheitsregister, z. B: Krebsregister
 - d. Andere (spezifizieren)
5. Öffentlich verfügbare Quellen
 - a. Frei zugängliche Internetseiten
 - b. Social Media
 - c. Andere (spezifizieren)
6. Nicht-öffentlich verfügbare Quellen
 - a. Vereine
 - b. Kommerzielle Datenhändler
 - c. Andere (spezifizieren)

6.2.3 Darstellung der potenziellen Risiken

An dieser Stelle werden die potenziellen Risiken/Gefährdungen dargestellt, die sich aus der Art der verwendeten Daten wie auch aus der Erhebung ergeben.

6.3 Zwecke und Mittel der Verarbeitung

6.3.1 Begründung, warum die Informationen verarbeitet werden müssen

1. Zweck: Der Zweck muss hinreichend genau angegeben werden, damit die Notwendigkeit der Verarbeitung der Datenarten dargestellt werden kann. Wird der Zweck zu allgemein dargestellt, ist die Notwendigkeit ggf. nicht begründbar, da das allgemeinere Ziel der Verarbeitung auch ohne bestimmte Daten erreicht werden kann.
2. Begründung
 - a. Gesetzliche Vorgaben
 - b. Vertragliche Verpflichtungen
 - c. Andere (spezifizieren)

6.3.2 Darstellung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitung

Beschreibe, warum die in Abschnitt 6.2.1 beschriebenen Daten sowie die Erhebungsmethoden für die dargestellten Zwecke notwendig sind. Hierzu gehört auch eine Darstellung, aus welcher ersichtlich wird, dass die Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck gewahrt wird.

6.3.3 Darstellung der Erlaubnistatbestände

Die Darstellung der Rechtmäßigkeit der Verarbeitung erfordert die Darlegung des Grundes, warum die Daten verarbeitet werden dürfen.

6.3.4 Darstellung der Speicherdauer

- Wie lange werden die Daten aus welchen Gründen wo unter welchen Umständen gespeichert?
- Wer hat während der Speicherdauer aus welchen Gründen unter welchen Bedingungen Zugriff auf die Daten?
- Wie ist die Löschung der Daten gewährleistet?

6.3.5 Darstellung der potenziellen Risiken

An dieser Stelle werden die potenziellen Risiken/Gefährdungen dargestellt, die sich aus der Art der Verarbeitung, insbesondere auch der Speicherung der Daten, ergeben.

6.4 Weitergabe der Daten

6.4.1 Mit wem werden die Daten geteilt?

Empfänger	Art der Weitergabe			
	Fall-zu-Fall	Vollständige Übermittlung	Direkter Zugriff	Andere (spezifizieren)
Innerhalb der Legaleinheit				
Innerhalb des Konzerns				
Staatliche Empfänger (spezifizieren)				
Nicht-staatliche Empfänger (spezifizieren)				

6.4.2 Darstellung der potenziellen Risiken

An dieser Stelle werden die potenziellen Risiken/Gefährdungen dargestellt, die sich aus der Weitergabe bzw. der Art der Übermittlung der Daten ergeben, sowie die Maßnahmen, welche die dargestellten Risiken entweder beseitigen oder derart minimieren, sodass das Risiko aus Sicht der betroffenen Person tragbar ist.

6.5 Wahrung der Betroffenenrechte

Wie werden die aus der DS-GVO resultierenden Betroffenenrechte gewahrt? An dieser Stelle muss eingetragen werden, wie in der jeweiligen Verarbeitung der Betroffene seine Rechte wahrnehmen kann, desgleichen, inwieweit diese auf Grund welcher Rechtsgrundlage eingeschränkt werden. Zu jedem Bereich wird ein kurzes Beispiel zur Veranschaulichung eingefügt.

6.5.1 Information des Betroffenen

Beispiel: Bei Aufnahme erhält jeder Patient eine Information, in welcher die notwendigen Angaben entsprechend Art. 13 resp. Art. 14 DS-GVO enthalten sind. Auf dieser Information befindet sich auch ein Link auf die Internetseite unseres Krankenhauses, welche die von uns beauftragten Auftragsverarbeiter enthält:

- Namen des Auftragsverarbeiters
- die Tätigkeit (z. B. Betreuung Krankenhausinformationssystem)
- wann das Vertragsverhältnis begann
- ggfs. wann das Vertragsverhältnis endete (offenes Enddatum = Vertragsverhältnis dauert an).

Sofern die Weitergabe von Daten nicht alle Patienten betrifft wie z. B. die Weitergabe von Daten an ein Krebsregister, wird der betroffene Patient hierüber individuell informiert. Hierzu werden ggf. Formulare der datenempfangenden Stelle genutzt. Die Informationen werden dabei stets in einer klaren und einfachen Sprache vermittelt, wie es Art. 12 DS-GVO fordert.

6.5.2 Auskunftsrecht

Beispiel: Jeder Patient hat das Recht auf Auskunft bzgl. der bei uns gespeicherten Daten. Dies wird ihm im Rahmen der unter Abschnitt 6.5.1 genannten Information mitgeteilt. In dieser Information wird hierzu sowohl eine Telefonnummer als auch eine spezielle nicht-personalisierte E-Mailadresse, die somit auch bei einem Wechsel des zuständigen Sachbearbeiters erhalten bleibt, genannt.

6.5.3 Widerspruchsrecht

Beispiel: Jeder Patient wird auf sein Recht zum Widerspruch gegen eine Datenverarbeitung hingewiesen (Information gemäß Abschnitt 6.5.1). Zugleich wird der Patient darauf hingewiesen, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt wird, z. B. eine Speicherung aufgrund gesetzlicher Bestimmungen trotz seines Widerspruchs erfolgen muss.

6.5.4 Recht auf Berichtigung und Vervollständigung

Beispiel: Jeder Patient wird darauf hingewiesen, dass ein Recht auf die Berichtigung fehlerhaft gespeicherter Daten besteht. Zugleich wird jeder Patient darauf hingewiesen, dass ggf. auch ein Recht auf die Vervollständigung unvollständiger personenbezogener Daten (u. U. auch mittels einer ergänzenden Erklärung) besteht. Beides erfolgt durch die o. g. Information.

6.5.5 Recht auf Löschen („Vergessenwerden“)

Beispiel: Durch die in Abschnitt 6.5.1 beschriebene Information wird jeder Patient darauf hingewiesen, dass er ein Recht auf Löschung seiner Daten hat. Zugleich wird er darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen, eingeschränkt wird.

6.5.6 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Beispiel: Durch die in Abschnitt 6.5.1 beschriebene Information wird jeder Patient darauf hingewiesen, dass er ein Recht eine Einschränkung der Verarbeitung seiner Daten hat. Zugleich wird er darauf hingewiesen, dass dieses Recht ggf. durch gesetzliche Bestimmungen, z. B. durch die Vorgabe gesetzlicher Verarbeitungszwecke wie beispielsweise der Verarbeitung im Rahmen der gesetzlichen Qualitätssicherung entsprechend § 137a SGB V, eingeschränkt wird

6.5.7 Recht auf Datenübertragbarkeit

Beispiel: Jeder Patient wird in dem in Abschnitt 6.5.1 genannten Information darauf hingewiesen, dass Daten, die auf Grundlage seiner Einwilligung in die Datenverarbeitung verarbeitet werden, ihm auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format entsprechend den Vorgaben von Art. 20 DS-GVO zur Verfügung gestellt werden. In dieser Information wird auch darauf hingewiesen, dass weiterhin ebenfalls das Recht besteht, diese Daten einem anderen Verantwortlichen auf Wunsch des Patienten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln. Es wird dabei aber auch darauf hingewiesen, dass kein Empfänger dieser Daten gesetzlich dazu verpflichtet ist, diese Daten überhaupt oder auch in dem von uns bereitgestellten Format anzunehmen.

6.6 Gewährleistung der Sicherheit der Daten

Hier erfolgt eine Darstellung, wie die Daten geschützt werden. Möglichkeiten hierzu sind u. a.

1. Auditierung und Zertifizierung des Verfahrens nach Norm ...
2. Angemessene Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff wurden getroffen.
Dies sind
 - a. ...
3. Es erfolgt ein kontinuierliches Monitoring von
 - a. ...
4. Vertragspartner, die Zugriff auf die Daten haben, wurden vertraglich zur Einhaltung der nachfolgenden technischen und organisatorischen Maßnahmen verpflichtet:
 - a. ...
5. Personen mit Zugriff auf die Daten werden speziell geschult. Zur Schulung gehört/gehören

- a. IT-Sicherheit
- b. Datenschutz
- c. ...

Die Schulung der Personen wird [Zeitraum] wiederholt.

6. ...

6.6.1 Darstellung der Erbringung der Anforderungen aus Art. 32 DS-GVO „Sicherheit der Verarbeitung“

6.6.1.1 Pseudonymisierung personenbezogener Daten

In diesem Kapitel muss dargestellt werden, wie mit der Anforderung zur Pseudonymisierung umgegangen wird. Erfolgt eine Pseudonymisierung? Wenn ja, muss hier das „Wie“ beschrieben werden. Wenn nicht, muss hier die Begründung zu finden sein, warum darauf verzichtet wird.

Beispiel: Standardmäßig ist eine Pseudonymisierung im KIS nicht möglich, ohne hierbei zugleich eine Gefährdung der Gesundheit von Patienten zu riskieren. Durch das Rollen- und Berechtigungskonzept ist gewährleistet, dass auf Patientendaten nur Berechtigte Zugriff haben. Bedingt durch die Notwendigkeit, sich bei der medizinischen Behandlung eines Patienten untereinander zu besprechen, müssen die Patientendaten in identifizierender Form vorliegen.

In wenigen Fällen besonderer Personengruppen, z. B. Personen des öffentlichen Lebens („Very Important Person, VIP“) oder Angestellten unseres Krankenhauses selbst, kann eine Pseudonymisierung trotz der damit verbundenen Risiken, die dies für die jeweilige Person bedeutet, sinnvoll sein. Ob dann eine Pseudonymisierung erfolgt und die damit verbundenen gesundheitlichen Risiken in Kauf genommen werden, entscheidet die betroffene Person selbst nach entsprechender Aufklärung.

Für die Testdatenbank, welche für Schulungszwecke eingesetzt wird, wird ein Anonymisierungstool verwendet, welches u. a. die nachfolgenden Funktionen hat:

- Anonymisierung von Personendaten wie Vorname, Name, Geburtsdatum etc.
- Anonymisierung von Adressdaten wie Straße, Hausnummer, Postleitzahl, Ort etc.
- Generierung neuer Patientenidentifikatoren (PIDs)
- Generierung neuer Fallnummern
- Umbenennung bzw. Sperrung von Applikationsbenutzern
- Anonymisierung oder Umbenennung von Organisationseinheiten
- Löschen von Schnittstellen- und Auditdaten

6.6.1.2 Verschlüsselung personenbezogener Daten

In diesem Abschnitt muss dargestellt werden, wie mit der Anforderung zur Verschlüsselung personenbezogener Daten umgegangen wird. Erfolgt eine Verschlüsselung? Wenn ja, muss hier beschrieben werden, wie die Verschlüsselung erfolgt (z. B. Welche Algorithmen werden verwendet?). Werden die Daten nicht verschlüsselt, so muss hier die Begründung zu finden sein, warum dies nicht geschieht.

Beispiel:

- Bei elektronischer Übertragung von Patientendaten an externe Empfänger erfolgt regelmäßig eine Verschlüsselung. Im Rahmen von gesetzlich vorgeschriebenen Übermittlungen sind die rechtlichen Vorgaben bindend.

- Bei einem elektronischen Export (z. B. als pdf-Datei) von Patientendaten entscheidet der jeweilige Anwender, ob eine Verschlüsselung erfolgen soll oder nicht, grundsätzlich wird die Verschlüsselung hierbei empfohlen.
- Verbindliche Vorgaben der betroffenen Person werden beachtet.
- Bzgl. der Verschlüsselungstechnik können nur die Möglichkeiten unseres KIS-Herstellers genutzt werden, der sich an den Vorgaben des BSI orientiert

6.6.1.3 Beschreibung des Verfahrens zur Gewährleistung der Verfügbarkeit der personenbezogenen Daten

In diesem Kapitel wird beschrieben, wie die Verfügbarkeit der Daten gewährleistet wird.

Beispiel: Näheres siehe Archivierungs- und Backupkonzept, hier erfolgt nur eine kurze Beschreibung zur Darstellung der getroffenen Maßnahmen.

- Einsatz eines Spiegelservers:
Alle Daten werden auf einen anderen Server „gespiegelt“, d. h. es wird also ein 1:1-Abbild erstellt. Der Spiegelserver steht dabei in einem anderen Brandabschnitt als der eigentliche Server. Die Synchronisierung erfolgt asynchron, daher ist das „Spiegelbild“ nicht immer aktuell. Vielmehr erfolgt die Spiegelung stündlich.

Bei einem Zwischenfall erfolgt hierdurch einerseits nur ein möglichst geringer Datenverlust, andererseits wird der Produktivverlust begrenzt, da seitens der Anwender die Ausfallzeit minimiert wird.

- Backup:
Ein Sicherungs-System wird zentral bereitgestellt. Dabei erfolgt eine Datensicherung nach dem „Generationenprinzip“. D. h. es wird gewährleistet, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen („Großvater“, „Vater“ und „Sohn“, daher Generationenprinzip) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu haben. Die Tagessicherung entspricht dabei dem „Sohn“, die Wochensicherung dem „Vater“ und die Monatsicherung dem „Großvater“.

Die Langzeitsicherung erfolgt grundsätzlich auf entsprechenden Bändern oder einem vergleichbaren Sicherungsmedium. Die Lagerung der Bandsicherungen erfolgt in einem anderen Brandabschnitt als dem Standort der Server.

Eine „Rücksicherung“ wird probenhalber quartalsweise für einzelne Datensätze, 1xjährlich für die gesamte Datenbank in einem Testsystem durchgeführt.

6.6.1.4 Beschreibung des Verfahrens zur Gewährleistung, den Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

In diesem Kapitel wird beschrieben, wie der Zugang zu personenbezogenen Daten nach einem physischen oder technischen Zwischenfall rasch wiederhergestellt wird.

Beispiel: Dies wird durch den Einsatz des Spiegelservers wie auch des Backup-Konzepts gewährleistet

6.6.1.5 Beschreibung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

In diesem Abschnitt wird das Verfahren dargestellt, welches zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der einzusetzenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung genutzt wird.

Beispiel: Interne Prüfungen der Einhaltung der vorliegend definierten Standards können zu jeder Zeit, auch unangekündigt, durch den Datenschutzbeauftragten bzw. IT-Sicherheitsbeauftragten durchgeführt werden. Grundsätzlich erfolgen interne Prüfungen regelmäßig. Die Ergebnisse einer entsprechenden Prüfung werden dem zuständigen IT Verantwortlichen und dem zuständigen Geschäftsführer in Berichtform übersendet. Zur Ergänzung interner Prüfaktivitäten können auch externe Prüfungen durch den Verantwortlichen veranlasst werden. Die Vorgehensweise bei externen Prüfungen ist vergleichbar mit dem Vorgehen bei internen.

6.7 Darstellung der Auswirkungen der Sicherheitsmaßnahmen auf die Risiken, Restrisikobewertung

Darstellung, welche Maßnahmen welche Risiken adressieren und ob die dargestellten Risiken beseitigt oder derart minimiert wurden, dass das Risiko aus Sicht der betroffenen Person tragbar ist.

Beispiel: Grundsätzlich stellt jede Verarbeitung von personenbezogenen Daten für die betroffenen Personen ein Risiko bzgl. des Missbrauchs ihrer Daten dar. Bedingt durch die Sensibilität sowohl von Gesundheitsdaten als auch von genetischen Daten, die bei der Patientenbehandlung zwangsläufig verarbeitet werden müssen, ist auch das Risiko für die betroffenen Personen entsprechend hoch.

Daher wurden Maßnahmen getroffen, die das Risiko für betroffene Personen minimieren:

- Ein Berechtigungskonzept beschränkt den berechtigten Zugriff auf die Personen, die entsprechend dem „Need-to-know“-Prinzip Zugriff auf die Daten benötigen
- Pseudonymisierung wird dort eingesetzt, wo es möglich ist.
- Wann immer es angebracht ist, werden Daten verschlüsselt. Eine elektronische Übermittlung erfolgt nur verschlüsselt.
- Sicherheitskonzepte wie der Einsatz eines Spiegelungsservers als auch ein differenziertes Backupkonzept gewährleisten eine Minimierung von Ausfallzeiten und die Wiederherstellbarkeit der Daten.
- Eine Firewall bewacht den Datenverkehr nach extern.
- Ein Intrusion Detection System überwacht den internen Netzbereich auf unerwünschte Vorgänge.
- Regelmäßige Schulungen unserer Beschäftigten zu Fragen bzgl. Datenschutz und IT-Sicherheit gewährleisten eine entsprechende Awareness bei dem bei uns eingesetzten Personal.

Sämtliche Maßnahmen zur Gewährleistung der Sicherheit der Daten wurden dabei stets aus dem Blickwinkel „Safety first“ gewählt. D. h. an erster Stelle steht in unserem Krankenhaus immer die Sicherheit der Patientenversorgung und die Minimierung von Risiken für die Gesundheit unserer Patienten.

6.8 Fazit

6.8.1 Abschließende Bewertung

6.8.2 Entscheidung bzgl. Information Aufsichtsbehörde

Die Einbeziehung der Aufsichtsbehörde

ist

ist nicht

notwendig, weil ...

7 Beispiele

Je nach Verarbeitung ist ggf. eine Mehrfachnennung notwendig, z. B. weil eine Verarbeitung zugleich mehrere Zwecke bedient oder mehrere Datenarten benötigt.

7.1 Beispiele für die Darstellung der Datenarten

1. Identifizierende Daten
 - a. Sozialversicherungsnummer
 - b. Personalausweisnummer
 - c. Reisepassnummer
 - d. Führerschein-ID
 - e. Kreditkartennummer
 - f. Krankenversicherungsnummer
 - g. Patient-ID aus Informationssystem (ggf. benennen aus welchem)
 - h. Andere (spezifizieren)
2. Stammdaten
 - a. Name/Vorname
 - b. Geburtsname
 - c. Geburtsdatum
 - d. Geburtsort
 - e. Geschlecht
 - f. Alter
 - g. Religionszugehörigkeit
 - h. Anschrift
 - i. Kontaktdaten (Telefon, Fax, E-Mail, ...)
 - j. Ethnische Zugehörigkeit
 - k. Ausbildung
 - l. Titel
 - m. Krankenkasse
 - n. Andere (spezifizieren)
3. Beschäftigtendaten
 - a. Gelernte(r) Beruf(e)
 - b. Ausgeübter Beruf
 - c. Job-Beschreibung
 - d. Dienstliche Anschrift
 - e. Dienstliche Kontaktdaten (Telefon, Fax, E-Mail, ...)
 - f. Gehalt/Vergütung
 - g. Bisheriges Arbeitsleben (bisherige Arbeit- bzw. Auftraggeber, ...)
 - h. Zugehörigkeit zu Berufsverbänden oder anderen Organisationen
 - i. Andere (spezifizieren)
4. Biometrische Daten
 - a. Fingerprint
 - b. Handflächen-Scan
 - c. Stimmerkennung
 - d. Fotos (Gesicht)
 - e. Besondere Kennzeichen (Narben, Tätowierungen, ...)
 - f. Gefäß-Scan

- g. Retina/Iris-Scan
 - h. DNA-Profil
 - i. Andere (spezifizieren)
5. Administrative Daten
 - a. User-ID
 - b. IP-Adresse
 - c. Datum/Uhrzeit von Zugriffen (An-/Abmelden vom System, Zugriff auf bestimmte Daten)
 6. Gesundheitsdaten
 - a. Physiologische Auffälligkeiten
 - b. Allgemeine Gesundheitsdaten (z. B. von Fitness-Trackern)
 - c. Klinische Informationen
 7. Andere Informationen
 - a. Spezifizieren

7.2 Beispiele für Verarbeitungszwecke

1. Administrative Zwecke
2. Aus- und Weiterbildung
 - a. Studierende in der Gesundheitsversorgung
 - b. Auszubildende in der Gesundheitsversorgung
 - c. Ärztliches Personal
 - d. Nicht-ärztliches medizinisches Personal
 - e. Administratives Personal
3. Gesundheitsversorgung
 - a. Ambulante Versorgung
 - b. Klinische Versorgung
 - c. Notfallversorgung
 - d. Öffentliches Gesundheitsmanagement
 - e. Überwachung der öffentlichen Gesundheit, Krankheitsbekämpfung
4. Nutzung durch die behandelte Person
 - a. Selbstversorgung und Pflege der eigenen Gesundheit
 - b. Wellness-Management und Lebensstilplanung
 - c. Häusliche Pflege
 - d. Information von Familie und/oder interessierten Dritten über die Krankengeschichte (z. B. Einholung einer Zweitmeinung)
 - e. Übergabe der Gesundheitsversorgung an einen anderen Erbringer (z. B. zum Zwecke der Nach- oder Weiterbehandlung)
 - f. Für Anforderungen aus Anstellungsverfahren (z. B. Einstellungsuntersuchungen, Impfstatus)
 - g. Für Anforderungen aus Einwanderungsverfahren
 - h. Für Anforderungen aus Reisen in andere Länder (z. B. Impfnachweis)
5. Forschung
 - a. Durchführung von klinischen Versuchen, für die eine Zustimmung erforderlich ist
 - b. Durchführung von populationsbasierten Forschungen,
 - c. Durchführung von Rekrutierungsmaßnahmen für klinische Versuche oder sonstige Forschungsstudien

6. Qualitätssicherung von Gesundheitsdienstleistungen
 - a. Interne Qualitätssicherung
 - b. Externe Qualitätssicherung
7. Juristische Zwecke
 - a. Nutzung von Patientenakten durch die Polizei, Gerichte oder sonstige gesetzlich autorisierte Behörden
 - b. Rechtsstreit
 - c. Strafverfolgung
 - d. Zivilrechtliche Zwecke
8. Eigene Zwecke
 - a. Abrechnung erbrachter Gesundheitsdienstleistungen
 - b. Marktstudien
 - c. Personalmanagement
 - d. Werbung
9. Andere
 - a. ...

7.3 Erlaubnistatbestände

In der DS-GVO existieren unterschiedliche Erlaubnistatbestände, die teilweise nebeneinander zu betrachten sind.

Art. 6 DS-GVO regelt die „Rechtmäßigkeit der Verarbeitung“ im Allgemeinen sofern „normale“ Daten verarbeitet werden, z. B. Mitarbeiterdaten im Rahmen eines Berechtigungskonzeptes bzw. dessen Umsetzung in einem Informationssystem. Art. 9 DS-GVO regelt die „Verarbeitung besonderer Kategorien personenbezogener Daten“ im Speziellen und trägt damit der besonderen Sensibilität dieser Daten Rechnung. Letzteres wird insbesondere an erhöhten Rechtmäßigkeitsvoraussetzungen deutlich.

Im Folgenden werden in einer exemplarischen Übersicht die Regelungen nebst Beispielen dargestellt, welche Verarbeitung unter welchen Tatbestand zu subsumieren ist.

1. Einwilligung der betroffenen Person
(Art. 6 Abs. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DS-GVO)
2. Gesetzlicher Erlaubnistatbestand
 - a. Daten, auf die Art. 6 DS-GVO zutrifft
 - i. Zur Vertragserfüllung notwendig
(Art. 6 Abs. 1 lit. b DS-GVO)
 - ii. Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich
(Art. 6 Abs. 1 Lit c DS-GVO)
 - iii. Erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
(Art. 6 Abs. 1 lit. d DS-GVO)
 - iv. Verarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung öffentlicher Gewalt
(Art. 6 Abs. 1 lit. e DS-GVO)

- v. Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht
(Art. 6 Abs. 1 lit. f DS-GVO)
- b. Besondere Kategorien von personenbezogenen Daten
 - i. Patientenbehandlung
(Art. 9 Abs. 2 lit. h i.V.m. Art. 9 Abs. 3 DS-GVO i.V.m. § 630a ff. BGB)
Zu beachten: Art. 9 Abs. 2 lit. h DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erfolgt
 - ii. Weitergabe von Daten an Mit-/Nachbehandler
(Art. 9 Abs. 2 lit. h i.V.m. Art. 9 Abs. 3 DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. h DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs beruht
 - iii. Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben
(Art. 9 Abs. 2 lit. c DS-GVO)
 - iv. Abrechnung von Leistungen
(Art. 9 Abs. 2 lit. f, h DS-GVO i.V.m. z. B. § 301 SGB V)
 - v. Qualitätssicherung der Patientenversorgung
(Art. 9 Abs. 2 lit. i DS-GVO i.V.m. § 299 SGB V i.V.m. § 136 SGB V bzw. den Richtlinien des G-BA)
Zu beachten: Art. 9 Abs. 2 lit. i DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht
 - vi. Gesetzlich geregelte Krankheitsregister
(Art. 9 Abs. 2 lit. h, i DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. h DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs beruht
 - vii. Gesundheitsstatistik des Bundes und der Länder
(Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. j DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht
 - viii. Arbeitsmedizinische Untersuchung
(Art. 9 Abs. 2 lit. b, h i.V.m. Art. 9 Abs. 3 DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. h DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs beruht
 - ix. Untersuchung durch Gesundheitsamt
(Art. 9 Abs. 2 lit. i DS-GVO i.V.m. z. B. §§ 6, 8 IfSG)
Zu beachten: Art. 9 Abs. 2 lit. i DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht

- x. Impfungen in Schule usw. durch Ämter
(Art. 9 Abs. 2 lit. i DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. i DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht
- xi. Verteidigung der behandelnden Person vor Gericht
(Art. 9 Abs. 2 lit. f DS-GVO⁴⁷)
- xii. Wissenschaftliche u. historische Forschung
(Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DS-GVO i.V.m. Regelungen in deutschen Gesetzen wie bspw. Landeskrankenhausgesetzen, Arzneimittelgesetz Medizinproduktegesetz usw.)
Zu beachten: Art. 9 Abs. 2 lit. j DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht
- xiii. Gesetzlich vorgeschriebene Archivierung zu historischen Zwecken
(Art. 9 Abs. 2 lit. j i.V.m. Art. 89 Abs. 1 DS-GVO)
Zu beachten: Art. 9 Abs. 2 lit. j DS-GVO bedingt u. a., dass die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats beruht
- xiv. Verarbeitung von seitens der betroffenen Person öffentlich zugänglich gemachten Daten
(Art. 9 Abs. 2 lit. e DS-GVO)

Das in Art. 9 Abs. 2 lit. h, i, j DS-GVO angesprochene „Recht eines Mitgliedstaats“ kann in Deutschland durch die Spezialgesetzgebungen z. B. aus den Sozialgesetzbüchern, dem Arzneimittel- oder Medizinproduktegesetz gegeben sein, wenn diese Gesetze den Anforderungen der DS-GVO genügen. Gleiches gilt für landesrechtliche Regelungen, wie sie z. B. in den Landeskrankenhausgesetzen zu finden sind. Auch diese können – sofern die Regelungen den Anforderungen der DS-GVO genügen – Erlaubnistatbestände i.S.d. Art. 9 Abs. 4 DS-GVO darstellen.

7.4 Beispiele für Risiken und Ursachen aus der DS-GVO

ErwGr. 75 führt beispielhaft einige Risiken auf, die bei einer Datenschutz-Folgenabschätzung berücksichtigt werden sollten:

Risiko	Mögliche Folgen
<ul style="list-style-type: none"> – Diskriminierung – Identitätsdiebstahl – Identitätsbetrug – Finanziellen Verlust – Rufschädigung – Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten – Unbefugte Aufhebung der Pseudonymisierung – Anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen 	<ul style="list-style-type: none"> – Betroffene Personen werden um ihre Rechte und Freiheiten gebracht – Betroffene Personen werden daran gehindert, die sie betreffenden personenbezogenen Daten zu kontrollieren – Verarbeitung besonderer Kategorien von Daten, d. h. Daten bzgl. <ul style="list-style-type: none"> • Rassistische oder ethnische Herkunft • Politische Meinungen • Religiöse oder weltanschauliche Überzeugungen • Zugehörigkeit zu einer Gewerkschaft

⁴⁷ Art. 9 Abs. 2 lit. f DS-GVO benötigt zwar keinen nationalen Erlaubnistatbestand; Landesregelungen können gemäß Art. 9 Abs. 4 DS-GVO die Verarbeitung zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten. Daher sind die Regelungen in den jeweiligen Landeskrankenhausgesetzen, sofern vorhanden, zu beachten.

	<ul style="list-style-type: none"> • Genetische Daten • Gesundheitsdaten • Sexualleben • Strafrechtliche Verurteilungen und Straftaten <ul style="list-style-type: none"> – Bewertung persönliche Aspekte, insbesondere Daten betreffend <ul style="list-style-type: none"> • Arbeitsleistung • Wirtschaftlicher Lage • Gesundheit • Persönliche Vorlieben oder Interessen • Zuverlässigkeit • Verhalten • Aufenthaltsort • Ortswechsel – Verarbeitung von Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern – Großer Verarbeitungsumfang <ul style="list-style-type: none"> • Große Menge personenbezogener Daten betreffend • Große Anzahl von betroffenen Personen betreffend
--	--

ErwGr. 83 benennt ebenfalls verschiedene Risiken, die berücksichtigt werden sollen:

- Vernichtung personenbezogener Daten
- Verlust personenbezogener Daten
- Veränderung personenbezogener Daten
- Unbefugte Offenlegung personenbezogener Daten
- Unbefugter Zugang zu personenbezogenen Daten

Dabei ist es unerheblich, ob die Risiken durch eine beabsichtigte, unbeabsichtigte oder auch unrechtmäßige Handlung entstehen. D. h. der Verantwortliche muss im Rahmen der Datenschutzfolgenabschätzung auch unrechtmäßige Handlungen berücksichtigen.

7.5 Beispiele für Risiken aus dem IT-Einsatz⁴⁸

Eingesetzte IT	Tatbestand	Risiko für betroffene Person	Beispiel
Hardware	Beschädigung	Verlust von Daten	Sturz, Tritt gegen den Rechner
Server-Hardware	Bedienungsfehler	Verlust von Daten	Betrieb außerhalb Spezifikation, z. B. Umgebung zu warm
Server-Anwendung	Bedienungsfehler	Unautorisierter Zugriff auf Daten	Fehlerhafte Freigabe von Ordnern
Server-Anwendung	Manipulation bzw.	Unautorisierter Zugriff	Interner

⁴⁸ Zitiert aus ISO/IEC 29134 „Guidelines for privacy impact assessment“, Stand: 2017-06. Online, zitiert am 2017-07-21; Verfügbar unter <https://www.iso.org/standard/62289.html>

Eingesetzte IT	Tatbestand	Risiko für betroffene Person	Beispiel
	gezielte Fehlbedienung der Software	auf Daten	Hackerangriff

8 Checkliste

1) Wurde der Datenschutzbeauftragte einbezogen?

2) Ist eine Datenschutz-Folgenabschätzung erforderlich?

Indizien, die für die Erforderlichkeit einer DSFA sprechen, sind insbesondere:

- Einsatz neuer Technologien, zu denen der Verantwortliche noch keine DSFA durchführte
- Neue Verarbeitungsvorgänge, zu denen der Verantwortliche noch keine DSFA durchführte
- Verarbeitung großer Datenmengen
- Verarbeitung der Daten einer hohen Anzahl von Personen
- Verarbeitung von Daten der besonderen Kategorien entsprechend Art. 9 DS-GVO
- Profiling/Scoring
- Erschwerte Rechtsausübung für die betroffenen Personen
- Systematische Verarbeitungen
- Öffentliche Überwachung

Eine DSFA ist nicht erforderlich, weil

- ...

3) Werden bei der Durchführung der DSFA alle relevanten Gesichtspunkte berücksichtigt?

Bei der Durchführung der DSFA sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Vorgaben der Aufsichtsbehörden insbesondere des Europäischen Datenschutz-Ausschusses
- Ähnliche Verarbeitungsvorgänge, für welche bereits eine DSFA existiert oder die bei der aktuellen durchzuführenden DSFA mit berücksichtigt werden sollten
- Berücksichtigung wirtschaftlicher/ökonomischer Gesichtspunkte

4) Entspricht die DSFA formal den Anforderungen der DS-GVO?

Die DSFA sollte mindestens beinhalten:

- Systematische Beschreibung der Verarbeitungsvorgänge
- Systematische Beschreibung der Verarbeitungszwecke (ggf. einschließlich berechtigter Interessen)
- Prüfung der Notwendigkeit und Verhältnismäßigkeit
- Prüfung der Folgen bei einer Weitergabe an Dritte
- Wahrung/Einschränkung Betroffenenrechte
- Bewertung der Risiken
- Ggf. Einbeziehung betroffener Personen bzw. Personengruppen/Vertreter
- Darstellung der Abhilfemaßnahmen/Maßnahmen zur Risikominimierung
- Abschließende Bewertung
- Entscheidung bzgl. Information/Einbeziehung der Aufsichtsbehörde

5) Ist die DSFA hinreichend dokumentiert, dass Externe sowohl die relevanten Risikofaktoren als auch die Entscheidung prüfen können?

9 Abkürzungen

Abs	Absatz
Art	Artikel
Artt	Artikel (Mehrzahl)
BayKrG	Bayerisches Krankenhausgesetz
BbgKHEG	Brandenburgisches Krankenhausentwicklungsgesetz
BremKHDSG	Bremisches Krankenhausdatenschutzgesetz
BVerfG	Bundesverfassungsgericht
DIN	Deutsches Institut für Normung e. V.
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
ErwGr	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
GDStG	Gesundheitsdatenschutzgesetz
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
HmbKHG	Hamburgisches Krankenhausgesetz
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches...
Kap	Kapitel
KHG	Krankenhausgesetz
KMU	Kleines, mittelständisches Unternehmen
LDSG	Landesdatenschutzgesetz
lit	littera (lat. „Buchstabe“)
LKHG	Landeskrankenhausgesetz
PIA	Privacy Impact Assessment
SächsKHG	Sächsisches Krankenhausgesetz
SDM	Standard-Datenschutzmodell
ThürKHG	Thüringer Krankenhausgesetz
TK	Telekommunikation(s-)
Ziff	Ziffer

10 Begriffserklärungen

Artikel-29-Datenschutzgruppe	Ein auf Artikel 29 der Richtlinie 95/46/EG beruhendes und unabhängig agierendes Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes
Automatische Verarbeitung	Verarbeitung unter Nutzung von EDV; also z. B. Word- oder Excel-Datei, aber auch KIS, RIS, PACS, unabhängig ob Client-Server-Lösung oder Stand-alone PC, Tablet oder anderweitige Hardware genutzt wird
Betroffener	Genau genommen „betroffene Person“, in der gesamten Literatur aber als "Betroffener" aufgeführt; Art. 4 Ziff. 1 DS-GVO „'Personenbezogene Daten' alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“
Datei	Im informationstechnischem Sinn: Gruppe von gespeicherten oder als eine Einheit bearbeiteten Aufzeichnungen (Quelle: ISO/IEC 2382:2015)
Daten/Datum	Im Informationstechnischem Sinn: Die re-interpretierbare Darstellung von Information in einer formalisierten für Kommunikation, Interpretation, oder Bearbeitung geeigneten Weise (Quelle: ISO/IEC 2382:2015)
Datenlöschung	Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt (Quelle: DIN CEN ISO/TS 14265)
Datenschutz-Ausschuss	Einrichtung der Europäischen Union entsprechend Art. 68 DS-GVO, welche gewährleisten soll, dass die Datenschutz-Grundverordnung in den EU-Mitgliedstaaten einheitlich angewandt wird. Die personelle Besetzung entspricht dabei im Prinzip der Artikel-29-Datenschutzgruppe
Erforderlichkeit, Notwendigkeit ⁴⁹	Die Begrifflichkeiten „Erforderlichkeit“ und „Notwendigkeit“ werden oftmals synonym verwendet. Im juristischen Schrifttum besagt der Grundsatz der Verhältnismäßigkeit, dass kollidierende Interessen, Freiheiten oder Rechtsprinzipien nur dann in einem angemessenen Verhältnis zueinander stehen, wenn das zu wahrende Interesse, Freiheitsrecht oder Rechtsprinzip schwerer wiegt als das zu seinen Gunsten geopfert. Auch im Sinne dieses Grundsatzes können die Begrifflichkeiten „Erforderlichkeit“ und „Notwendigkeit“ synonym verwendet werden. In der DS-GVO selbst wird der Begriff der „Erforderlichkeit“ bzw. „Notwendigkeit“ nicht definiert. Allerdings finden sich in den Erwägungsgründen Kriterien, welche die Beurteilung der Erforderlichkeit erleichtern. Die Verarbeitung von Daten ist insbesondere dann erforderlich bzw. notwendig, wenn <ul style="list-style-type: none"> – der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder – der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen

⁴⁹ Zitiert aus: GMDS/bvigt: Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen. Online, zitiert 2017-11-20; Verfügbar unter <https://gesundheitsdatenschutz.org/>

	<p>Person liegt (Erwägungsgrund 112). D. h. damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht. Um die Erforderlichkeit / Notwendigkeit beurteilen zu können, müssen daher drei Fragen beantwortet werden:</p> <ol style="list-style-type: none"> 1) Gibt es ein anderes Mittel? 2) Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen? 3) Ist dieses Mittel ein milderes, also die Rechte der betroffenen Person weniger belastendes Mittel?
Genetische Daten	<p>Art. 4 Ziff. 13 DS-GVO „'Genetische Daten' personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“</p>
Gesundheitsdaten	<p>Art. 4 Ziff. 15 DS-GVO „'Gesundheitsdaten' personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“</p>
Klinische Information	<p>Informationen über eine Person, die für deren Gesundheit oder Gesundheitsversorgung von Bedeutung sind (Quelle: DIN CEN ISO/TS 14265)</p>
Normadressat	<p>Rechtssubjekt (z. B. natürliche Person, juristische Person, Personenvereinigung), an die sich die Regelung eines Gesetzes (= einer Norm) richtet</p>
Notwendigkeit	<p>Siehe „Erforderlichkeit, Notwendigkeit“</p>
Offenlegung	<p>Preisgabe von Daten an Personen, die nicht routinemäßig über die entsprechende Berechtigung verfügen Quelle: DIN CEN ISO/TS 14265)</p>
Verantwortlicher	<p>Art. 4 Ziff. 7 DS-GVO „'Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“</p>
Verarbeitung	<p>Art. 4 Ziff. 2 DS-GVO „'Verarbeitung' jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“</p>

11 Literatur

11.1 Fachzeitschriften

- 1) Drackert S. (2014) Die Risiken der Verarbeitung personenbezogener Daten- Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN '978-3-428-1 4730-4
- 2) Eman KE, Dankar KF, Vaillancourt, R, Roffey, T, Lysyk M. (2009) Evaluating the Risk of Re-identification of Patients from Hospital Prescription Records. Can J Hosp Pharm 62(4): 307–319
- 3) Haas A, Hofmann A. (2014) Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. ZVersWiss (103): 377–407
- 4) Hansen M. (2016) Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge? DuD: 587-591
- 5) Kaufmann N. (2012) Meldepflichten und Datenschutz-Folgenabschätzung - Kodifizierung neuer Pflichten in der EU-Datenschutz-Grundverordnung. ZD: 358-362
- 6) Piatkowska E, Bajraktari A, Chhajed D, Smith P. (2017) Tool support for data protection impact assessment in the smart grid. Iektrotechnik & Informationstechnik (134/1): 26–29
- 7) Schmitz B, von Dall'Armi J. (2017) Datenschutz-Folgenabschätzung – verstehen und anwenden. ZD: 57-64
- 8) Schuster F, Hunzinger S. (2017) Pflichten zur Datenschutzeignung von Software - Wie die Pflichten zur Verwendung datenschutzkonformer IT-Lösungen auf die vertragliche Sollbeschaffenheit von Software durchschlagen. CR: 141-148
- 9) Thode J-C. (2016) Die neuen Compliance-Pflichten nach der Datenschutz-Grundverordnung. CR: 714-721
- 10) Wichtermann M. (2016) Die Datenschutz-Folgenabschätzung in der DS-GVO. DuD: 797-801
- 11) Wright D. (2013) Making Privacy Impact Assessment More Effective. The Information Society,29: 307–315

11.2 Standardisierungsorganisationen

- 1) ISO 22307: Financial services -- Privacy impact assessment. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.iso.org/standard/40897.html>
- 2) ISO/IEC 29134: Privacy impact assessment – Guidelines. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.iso.org/standard/62289.html>
- 3) HL7 Guidance: Standards Privacy Impact Assessment (SPIA), Release 1 (2016). Online, zitiert am 2017-04-27; Verfügbar unter http://wiki.hl7.org/index.php?title=HL7_SPIA_Cookbook_Project
- 4) •W3C Specification for Privacy Assessment (SPA)). Online, zitiert am 2017-04-27; Verfügbar unter <http://yrlesru.github.io/SPA/>

11.3 Internet

11.3.1 Ausarbeitungen

- 1) Forum Privatheit (2016) White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz. Online, zitiert am 2017-04-27; Verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf
- 2) Healthcare Information and Management Systems Society (HIMSS) (2013) Privacy Impact Assessment Guide v2. Online, zitiert am 2017-04-27; Verfügbar unter <http://www.himss.org/library/healthcare-privacy-security/impact-assessment>

11.3.2 Aufsichtsbehörden

- 1) Australia
 - Office of the Australian Information Commissioner (2013) Guide to undertaking privacy impact assessments. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>
- 2) Canada
 - The Office of the Privacy Commissioner of Canada (2011) A Guide for Submitting Privacy Impact Assessments. Online, zitiert am 2017-04-27; Verfügbar unter https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_201103/
 - Information and Privacy Commissioner/Ontario (2005) Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act. Online, zitiert am 2017-04-27; Verfügbar unter <http://govdocs.ourontario.ca/node/23322>
 - Information and Privacy Commissioner/Ontario (2015) Planning for Success: Privacy Impact Assessment Guide. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.ipc.on.ca/resource/planning-for-success-privacy-impact-assessment-guide/>
- 3) Deutschland
 - AK Technik (2013) Anforderungen an Privacy Impact Assessments aus Sicht der Datenschutzaufsichtsbehörden. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.datenschutz-mv.de/datenschutz/publikationen/informat/pia/pia.pdf>
 - Bayerisches Landesamt für Datenschutzaufsicht (2016) Datenschutz-Folgenabschätzung (DSFA) - Art. 35 DS-GVO. Online, zitiert am 2017-04-27; Verfügbar unter https://www.lida.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf
 - Datenschutzkonferenz (DSK): Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Stand: 24.07.2017. Online, zitiert am 2017-11-13; Verfügbar unter https://www.lida.bayern.de/de/datenschutz_eu.html
- 4) Europäische Union
 - Article 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679. Online, zitiert am 2017-04-27; Verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- 5) Frankreich
 - CNIL (2015) Privacy Impact Assessment (PIA) - Methodology (how to carry out a PIA). Online, zitiert am 2017-04-27; Verfügbar unter <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>
 - CNIL (2015) Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases). Online, zitiert am 2017-04-27; Verfügbar unter <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>
 - CNIL (2012) Privacy Impact Assessment (PIA) - Measures for the privacy risk treatment. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf>
- 6) Neuseeland
 - Privacy Commissioner (2015) Privacy Impact Assessment Toolkit. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/>

- Privacy Commissioner (2015) Part 2: How to do a Privacy Impact Assessment (PIA). Online, zitiert am 2017-04-27; Verfügbar unter <https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/>
- Privacy Commissioner (2015) Privacy Impact Assessment Handbook. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment-handbook/>

7) United Kingdom

- Information Commissioner's Office (2008) Privacy Impact Assessment - an overview. Online, zitiert am 2017-04-27; Verfügbar unter http://informationsharing.co.uk/wp-content/uploads/2012/08/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW1.pdf
- Trilateral Research & Consulting (2013) Privacy impact assessment and risk management. Online, zitiert am 2017-04-27; Verfügbar unter <https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf>
- Information Commissioner's Office (2014) Conducting privacy impact assessments code of practice. Online, zitiert am 2017-04-27; Verfügbar unter <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
- Information Commissioner's Office (2007) Privacy Impact Assessment Handbook. Online, zitiert am 2017-04-27; Verfügbar unter <http://www.rogerclarke.com/DV/PIAHbk-v1.0.pdf>
- Information Commissioner's Office (2016) Privacy Impact Assessment Handbook. Online, zitiert am 2017-04-27; Verfügbar unter <http://www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf>

11.3.3 Behörden/öffentliche Einrichtungen

1) British Columbia

- a. Ministry of Technology, Innovation and Citizens' Services (2013) Privacy Impact Assessment Guidelines. Online, zitiert am 2017-04-27; Verfügbar unter <http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/resources>
- b. Privacy Impact Assessments. Online, zitiert am 2017-04-27; Verfügbar unter <http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments>

2) Deutschland

- a. Bundesamt für Sicherheit in der Informationstechnik (2011) Privacy Impact Assessment Guideline. Online, zitiert am 2017-04-27; Verfügbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/RadioFrequencyIdentification/PIA/pia_node.html
- b. Bundesamt für Sicherheit in der Informationstechnik (2011) Privacy Impact Assessment Guideline for RFID Applications. Online, zitiert am 2017-04-27; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.html

3) Europäische Union

- a. European Commission (2012) PIAF A Privacy Impact Assessment Framework for data protection and privacy rights. Online, zitiert am 2017-04-27; Verfügbar unter http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- b. European Commission (2012) Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the

- European Union. Online, zitiert am 2017-04-27; Verfügbar unter http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf
- c. European Commission (2012) Recommendations for a privacy impact assessment framework for the European Union. Online, zitiert am 2017-04-27; Verfügbar unter <http://www.vub.ac.be/LSTS/pub/Dehert/506.pdf>
 - d. Wright D, Wadhwa K. (2012) A step-by-step guide to privacy impact assessment. Online, zitiert am 2017-04-27; Verfügbar unter http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf
- 4) Irland
- a. Health Information and Quality Authority (2010) Guidance on Privacy Impact Assessment in Health and Social Care. Online, zitiert am 2017-04-27; Verfügbar unter https://www.hiqa.ie/sites/default/files/2017-03/Hi_Privacy_Impact_Assessment.pdf
 - b. Health Information and Quality Authority (2016) Privacy Impact Assessment for the Individual Health Identifier (IHI). Online, zitiert am 2017-04-27; Verfügbar unter <http://www.ehealthireland.ie/Library/Document-Library/IHI-Documents/PIA-IHI.pdf>
- 5) United Kingdom
- a. Health & Social Care Information centre (2013) Privacy Impact Assessment; Functions of the Health and Social Care Information Centre. Online, zitiert am 2017-04-27; Verfügbar unter http://content.digital.nhs.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy_impact_assessment_2013.pdf
 - b. Ministry of Justice (2013) Justice Data Lab - Privacy Impact Assessment Report. Online, zitiert am 2017-04-27; Verfügbar unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/372076/justice-data-lab-privacy-impact-assessment.pdf
- 6) United Nations
- a. UN Refugee Agency (2015) Privacy Impact Assessment of UNHCR Cash Based Interventions. Online, zitiert am 2017-04-27; Verfügbar unter http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf
- 7) USA
- a. U.S. Securities and Exchange Commission (2007) Privacy Impact Assessment (PIA) Guide. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.sec.gov/about/privacy/piaguide.pdf>
 - b. Homeland Security (2010) Privacy Impact Assessments - The Privacy Office Official Guidance. Online, zitiert am 2017-04-27; Verfügbar unter https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf
 - c. United States Office of Personal Management (2010) Privacy Impact Assessment (PIA) Guide. Online, zitiert am 2017-04-27; Verfügbar unter <https://www.opm.gov/information-management/privacy-policy/privacy-references/piaguide.pdf>
 - d. Global Advisory Committee (2011) Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities. Online, zitiert am 2017-04-27; Verfügbar unter https://it.ojp.gov/documents/d/Guide%20to%20Conducting%20Privacy%20Impact%20Assessments_compliant.pdf

Anlage 1: Gesetzeswortlaut von Art. 35 DS-GVO

- (1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.
- (2) Der Verantwortliche holt bei der Durchführung einer Datenschutzfolgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.
- (3) Eine Datenschutzfolgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:
 - a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
 - b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
 - c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;
- (4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutzfolgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.
- (5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutzfolgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.
- (6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.
- (7) Die Folgenabschätzung enthält zumindest Folgendes:
 - a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
 - b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
 - c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
 - d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

- (8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutzfolgenabschätzung, gebührend zu berücksichtigen.
- (9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
- (10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.
- (11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.“