

11 Datenschutzmanagement

Zwar kennt die DSGVO den Begriff des Datenschutzmanagements nicht, doch enthält sie mehrere Regelungen, die unter diesem Begriff zusammengefasst werden können. Zweck des Datenschutzmanagements ist es, die **datenschutzrelevanten Prozesse** so zu organisieren und zu dokumentieren (Art. 5 Abs. 2 DSGVO), dass sämtlichen Datenschutz-Anforderungen zu jeder Zeit genügt werden kann.⁶⁵⁴ Das Datenschutzmanagement obliegt dem Verantwortlichen. Damit ist es letztlich die Aufgabe der jeweiligen Stellenleitung, darauf zu achten; dass alle datenschutzrechtlich geforderten Maßnahmen umgesetzt werden. Dem Datenschutzbeauftragten (s.u. Kap. 11.1) sind insofern spezielle Aufgaben übertragen. Dies ändert aber an der Letztverantwortung der Stellenleitung nichts. Im Rahmen der vorliegenden Ausarbeitung kann zum Datenschutzmanagement keine umfassende Darstellung erfolgen. Wohl aber sollen die Aspekte behandelt werden, die im Rahmen von medizinischen Forschungsprojekten von besonderer praktischer Relevanz sind. Dabei handelt es sich um die Benennung eines Datenschutzbeauftragten, die Erstellung von Verarbeitungsverzeichnissen, die Durchführung einer Datenschutz-Folgenabschätzung sowie die Notwendigkeit eines umfassenden Datenschutzkonzepts.

⁶⁵⁴ Roßnagel in SHS, Art. 5 Rn. 101, 176.

11.1 Datenschutzbeauftragter

Nach Art. 37 Abs. 1 DSGVO besteht in jedem Fall die **Verpflichtung zur Benennung** eines Datenschutzbeauftragten für öffentliche Stellen (lit. a). Bei nicht-öffentlichen Stellen besteht die Verpflichtung, wenn deren Kerntätigkeit in der systematischen Überwachung von Betroffenen (lit. b) oder in der umfangreichen Verarbeitung sensibler Daten nach Art. 9 DSGVO (lit. c) besteht. Weiterhin besteht die Verpflichtung zu einer solchen Benennung bei nicht-öffentlichen Stellen gemäß § 38 Abs. 1 S. 1 BDSG, soweit „in der Regel mindestens zwanzig Personen mit der automatisierten Verarbeitung personenbezogener Daten“ beschäftigt werden.⁶⁵⁵

Die Benennungspflicht besteht für den Verantwortlichen oder Auftragsverarbeiter und damit regelmäßig für die jeweilige **juristische Person**. Werden von dieser neben Aufgaben der (medizinischen) Forschung weitere Aufgaben wahrgenommen, so kommt es auf die Gesamtsicht an. Eine spezifische Benennung von nur für die Forschungsdatenverarbeitung zuständigen Datenschutzbeauftragten ist nicht vorgesehen. Vielmehr ist der Datenschutzbeauftragte z.B. auch für Fragen der Verarbeitung von Beschäftigtendaten oder von Daten aus dem Verwaltungs- und dem Produktionsbereich zuständig.

Datenschutzbeauftragter kann sowohl eine natürliche Person wie auch eine (externe) juristische Person sein (Art. 37 Abs. 6 DSGVO).⁶⁵⁶ Es ist – insbesondere bei größeren Stellen – möglich, dass ein Datenschutzbeauftragter nachgeordnete Mitarbeiter mit spezialisierten Zuständigkeitsbereichen hat, d. h., dass besondere Mitarbeiter ausschließlich für den (medizinischen) Forschungsbereich zuständig sind. Die Letztverantwortung für die Aufgabenwahrnehmung bleibt aber beim Datenschutzbeauftragten (zu möglichen Interessenkonflikten s.o. Kap. 10.4).

Erfolgt die Forschungstätigkeit im organisatorischen Rahmen einer **öffentlichen Stelle**, so ist in jedem Fall ein Datenschutzbeauftragter zu benennen (Art. 37 Abs. 1 lit. a DSGVO). Dies ist der Fall bei öffentlich-rechtlichen Forschungseinrichtungen, Universitäten, Universitätskliniken, Kommunen, bei denen in Gesundheitsämtern geforscht wird, Kliniken der Bundeswehr sowie Kliniken unter Landes- oder kommunaler Verantwortung sowie bei sonstigen öffentlichen Körperschaften, Stiftungen oder Anstalten.

Der in Art. 37 DSGVO verwendete Begriff der **Kerntätigkeit** bezieht sich auf die Haupttätigkeit einer Stelle und umfasst auch solche Aufgaben, die mit einer Haupttätigkeit untrennbar verbunden sind.⁶⁵⁷ Bei medizinischen Forschungseinrichtungen liegt in der Verarbeitung von Gesundheitsdaten deren Kerntätigkeit. Die Forschungstätigkeit von Universitätskliniken gehört zu deren Kerntätigkeit. Entsprechendes kann auch für Medizinproduktehersteller und für Pharmaunternehmen gelten.

Eine Benennungspflicht besteht auch bei einer **systematischen Überwachung von Betroffenen** (Art. 37 Abs. 1 lit. b DSGVO). Diese knüpft an der Kritikalität der Datenverarbeitung an und basiert auf der Risikoorientierung, die der gesamten DSGVO zu

⁶⁵⁵ Geändert durch das 2. DSAnpUG-EU v. 20.11.2019, BGBl. I S. 1626, zuvor 10 Personen.

⁶⁵⁶ Jaspers/Reif in SJTK, Art. 37 Rn. 45; zweifelnd Bergt in Kühling/Buchner, Art. 37 Rn. 36 m.w.N.

⁶⁵⁷ Drewes in SHS, Art. 37 Rn. 16.

Grunde liegt.⁶⁵⁸ Systematische Überwachung erfordert ein gezieltes, planmäßiges Vorgehen mit einer größeren Zahl von Betroffenen oder einer umfangreicheren räumlichen Ausdehnung.⁶⁵⁹ Die Intention der Überwachung spielt keine Rolle; erfasst wird auch eine Überwachung zu Forschungszwecken, etwa im Rahmen der „NAKO-Gesundheitsstudie“. Ebenso können durch diese Regelung Krankheitsregister oder Biobanken erfasst sein.

Eine **umfangreiche sensitive Datenverarbeitung** begründet ebenso eine Benennungspflicht (Art. 37 Abs. 1 lit. c DSGVO). Die Verarbeitung von Daten zur Gesundheit, zu genetischen Anlagen oder zur sexuellen Disposition sind derartige sensitive Daten (Art. 9 Abs. 1 DSGVO). Der große Umfang lässt sich an der Zahl der Betroffenen festmachen, an der Größe der jeweiligen Datensätze sowie an der Verarbeitungstiefe.⁶⁶⁰ Das reine Führen einer Patientendokumentation in einer kleineren Arztpraxis soll nicht genügen (ErwGr. 91 S. 4); verpflichtet sein sollen dagegen größere medizinische Labors und Arztpraxen, Krankenhäuser oder Beratungsstellen wie Familienhilfvereine.⁶⁶¹

11.2 Verarbeitungsverzeichnis

Art. 30 DSGVO verpflichtet verarbeitende Stellen zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten, in das Angaben zu **Verantwortlichen und Auftragsverarbeitern**, zu den Zwecken, Datenkategorien, Empfängern und – wenn möglich – zu Löschfristen und technisch-organisatorischen Maßnahmen aufzunehmen sind.⁶⁶² Dies ist Teil der Dokumentationspflichten gemäß Art. 5 Abs. 2, 24 DSGVO. Das Verzeichnis soll den Aufsichtsbehörden bei Kontrollen dienlich sein, es dient aber auch der jeweiligen Stelle selbst zur Wahrnehmung von deren datenschutzrechtlichen Pflichten. Es ist zudem geeignet als Grundlage für die Erarbeitung einer Datenschutzfolgenabschätzung und eines projektbezogenen Datenschutzkonzepts.

Zentrales Ordnungskriterium des Verarbeitungsverzeichnisses ist der **Zweck der Datenverarbeitung**. Dieser ist so präzise wie möglich zu benennen, er muss eindeutig und aussagekräftig sein; bei medizinischen Forschungsvorhaben ist also deren Fragestellung aufzuführen (s.o. Kap. 8.2).⁶⁶³ Das Verzeichnis ist laufend auf dem aktuellen Stand zu halten.⁶⁶⁴ Eine Änderung der wissenschaftlichen Fragestellung muss sich im Verzeichnis ebenso widerspiegeln wie Änderungen beim Datenumfang, bei den Betroffenen oder den Empfängern.

⁶⁵⁸ Drewes in SHS, Art. 37 Rn. 12.

⁶⁵⁹ Drewes in SHS, Art. 37 Rn. 26f.

⁶⁶⁰ Drewes in SHS, Art. 37 Rn. 23.

⁶⁶¹ Bergt in Kühling/Buchner, Art. 37 Rn. 24; Klug ZD 2016, 317; Paal in Paal/Pauly, Art. 37 Rn.

⁶⁶² DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Stand Februar 2018, <https://www.datenschutzzentrum.de/uploads/dsgvo/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf>.

⁶⁶³ Hartung in Kühling/Buchner, Art. 30 Rn. 18.

⁶⁶⁴ Hartung in Kühling/Buchner, Art. 30 Rn. 31.

11.3 Datenschutz-Folgenabschätzung

Darüber hinausgehende Anforderungen stellt Art. 35 DSGVO, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein besonders hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Der Verantwortliche muss in diesem Fall eine Datenschutz-Folgenabschätzung⁶⁶⁵ durchführen. Gemäß Art. 35 Abs. 3 DSGVO ist ein **besonders hohes Risiko** insbesondere anzunehmen bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, wenn automatisierte Entscheidungen (Art. 22 DSGVO) erfolgen sollen (lit. a), sowie bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO. Mit der Regelung zur Datenschutz-Folgenabschätzung wird der Risikoansatz konkretisiert, der der gesamten DSGVO zugrunde liegt.⁶⁶⁶

Da medizinische Forschungsvorhaben regelmäßig nicht auf **konkrete Entscheidungen** abzielen, ist Art. 22 DSGVO nicht anwendbar (Art. 35 Abs. 3 lit. a DSGVO). Etwas anderes gilt, wenn ein Forschungsprojekt so in eine medizinische Behandlung integriert ist, dass die über die automatisierte Datenverarbeitung erlangten Erkenntnisse, etwa über maschinenlernende Systeme, direkt in die Therapie einfließen.

Wenn bei medizinischen Forschungsprojekten in einem großen Umfang **Gesundheitsdaten** verarbeitet werden, was regelmäßig der Fall ist, besteht die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.⁶⁶⁷ Entsprechendes gilt für die forschende Verarbeitung von biometrischen und genetischen Daten, Daten zum Sexualleben oder zur sexuellen Orientierung oder Daten zu bestimmten Einstellungen oder zur rassischen oder ethnischen Herkunft.⁶⁶⁸

Umfangreich ist eine Verarbeitung, wenn eine große Zahl von Betroffenen und eine große räumliche Verbreitung gegeben ist (ErwGr 91 S. 1). Ebenso ist von einem großen Umfang auszugehen, wenn eine Datensammlung über einen längeren Zeitraum hinweg erfolgt sowie wenn zu jeder Person eine Vielzahl von Merkmalen erfasst wird. Keine Pflicht besteht aber, wenn sich dabei die Verarbeitung auf Einzelfälle beschränkt.⁶⁶⁹ Die Verarbeitung durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs ist nicht umfangreich (ErwGr 91 S. 4). Bei der Speicherung von Metadaten zum Zweck des Forschungsdatenmanagements kann eine Folgenabschätzung auch dadurch nötig werden, dass über die Forschenden umfassende Profile erstellt werden können.⁶⁷⁰ Big-Data-Anwendungen können für Forschungszwecke zulässig sein, bedürfen aber regelmäßig einer umfassenden Folgenabschätzung.⁶⁷¹

Gemäß Art. 35 Abs. 4, 5 DSGVO wird **von den Aufsichtsbehörden aufgelistet**, wann eine Folgenabschätzung nötig ist und wann nicht. Diese Liste findet sich im Inter-

⁶⁶⁵ Zum Begriff Friedewald u.a., 7.

⁶⁶⁶ Friedewald u.a., 17f.

⁶⁶⁷ Zu klinischen Prüfungen Bischoff/Wiencke ZD 2019, 13.

⁶⁶⁸ Roßnagel ZD 2018, 163.

⁶⁶⁹ Wedde in DWWS, Art. 35 Rn. 50; siehe aber nächster Absatz.

⁶⁷⁰ Syckor/Strufe/Lauber-Rönsberg ZD 2019, 393.

⁶⁷¹ Raum in Ehmann/Selmayr, Art. 89 Rn. 44.

net.⁶⁷² Darin wird klargestellt, dass auch bei einer umfangreichen Verarbeitung von Sozial- und Berufsgeheimnissen eine Folgenabschätzung durchzuführen ist (dort Nr. 3). Unter Nr. 15 wird als weiterer Anwendungsfall aufgeführt:

„Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte“.

Unter ausdrücklicher Nennung von „Telemedizin-Lösungen“ wird unter Nr. 16 als Regelbeispiel aufgeführt:

„Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO – auch wenn sie nicht als ‚umfangreich‘ im Sinne des Art. 35 Abs. 3 lit. b) anzusehen ist – sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.“

Nicht ausdrücklich aufgeführt wird in der Liste die **Verarbeitung für Forschungszwecke**. Die dabei geltende enge Zweckbindung kann zu einem geringeren Risiko führen als bei einer Verarbeitung mit einer operativen Zielsetzung. Insbesondere bei sensiblen Daten sowie einer umfangreichen Verarbeitung bleibt aber weiterhin technisch-organisatorisch wie auch personell ein hohes Risiko bestehen. Daher kann für eine Forschungsverarbeitung in Bezug auf Art. 35 DSGVO grundsätzlich keine rechtliche Freistellung angenommen werden.⁶⁷³ Dies gilt umso mehr, als die in der DSGVO vorgesehenen Privilegierungen hinsichtlich der Zweckänderung und der Betroffenenrechte normativ die DSGVO-Schutzstandards zweckbedingt reduzieren. ErwGr. 91 S. 1 nennt als einen Anlass für eine Folgenabschätzung, wenn die „*Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren*“.

Folgende **Risikoindikatoren** können im Forschungsbereich besonders relevant sein: Sensitivität und Höchstpersönlichkeit der Daten, Verletzlichkeit der Betroffenen, der Umfang der Daten bzw. die Komplexität und der Umfang der Datenverarbeitung, die systematische Beobachtung von Betroffenen, die Neuartigkeit der eingesetzten Technik, die individuelle Bewertung von Betroffenen, die Art der Datenverknüpfung, der Einsatz automatisierter Entscheidungsverfahren oder der Einsatz sog. Künstlicher Intelligenz.⁶⁷⁴

Bei der Durchführung der Datenschutz-Folgenabschätzung hat der Verantwortliche den **Rat des Datenschutzbeauftragten** (s.o. Kap. 11.1) einzuholen, sofern ein solcher benannt wurde (Art. 35 Abs. 2 DSGVO).⁶⁷⁵

Art. 35 Abs. 9 DSGVO legt dem Verantwortlichen nahe, „*den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge einzuholen*.“ Die-

672 DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DSK_DSFA-Liste-1_1.pdf.

673 Friedewald u.a., 26.

674 EDPS 2020, 24; Martin/Mester/Schiering/Friedewald/Hallinan DuD 2020, 152.

675 Jandt in Kühling/Buchner, Art. 35 Rn, 18; Martin/Schiering/Friedewald DuD 2020, 156.

ser **Standpunkt der betroffenen Personen** kann durch Patienteninitiativen oder durch Verbraucherschutzorganisationen vertreten werden.⁶⁷⁶

Art. 35 Abs. 7 DSGVO beschreibt die **Inhalte**, die zumindest in eine Folgenabschätzung aufgenommen werden müssen:

„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.“

Die in Abs. 7 genannten unabdingbaren Inhalte a) bis d) bauen aufeinander auf und sind demgemäß auch so darzustellen.⁶⁷⁷ Die **systematische Beschreibung** kann an das Verarbeitungsverzeichnis nach Art. 30 DSGVO anknüpfen⁶⁷⁸, darf sich jedoch nicht hierauf beschränken, da es zusätzlich auf die Systematik der Verarbeitungsschritte ankommt. Es geht also nicht nur um die Beschreibung der einzelnen zum Einsatz kommenden Verfahren, sondern um eine ablauf- bzw. prozessorientierte Gesamtschau unter Einbeziehung der Hardware, der Software, der Vernetzung, der Schnittstellen und der Rollen der Anwendenden.⁶⁷⁹

Ergeben sich wesentliche Änderungen in Bezug auf die Datenverarbeitung oder die Risiken, so ist eine **Fortschreibung** der Folgenabschätzung nötig.⁶⁸⁰

Hinsichtlich der **Form** gibt es keine expliziten normativen Vorgaben. Da die Dokumentation aber verfügbar sein und auf Nachfrage vorlegt werden können muss, bedarf es einer textlichen Darstellung, die analog oder digital vorgehalten werden kann.⁶⁸¹

11.4 Datenschutzkonzept

Art. 5 Abs. 2 DSGVO verpflichtet den Verantwortlichen, die Rechtmäßigkeit der von ihm veranlassten Datenverarbeitung nachzuweisen. Im Rahmen dieser Gesamtver-

⁶⁷⁶ Wedde in DWWS, Art. 35 Rn. 104f.

⁶⁷⁷ Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 48, Roßnagel ZD 2019, 163f.; zum Gesamtprozess Friedewald u.a., 19ff.

⁶⁷⁸ Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 51; Goosen/Schramm ZD 2017, 11; Ferik in SJTK, Art. 35 Rn. 164.

⁶⁷⁹ Karg in SHS, Art. 35 Rn. 76.

⁶⁸⁰ Friedewald u.a., 33.

⁶⁸¹ Piltz K&R 2016, 716; Sassenberg/Schwendemann in Sydow, Art. 35 Rn. 37; Ferik in SJTK, Art. 35 Rn. 163; Raum in Auernhammer, Art. 35 Rn. 39; a.A. Baumgartner in Ehmann/Selmayr, Art. 35 Rn. 49: schriftlich.

antwortung hat er vor Beginn der Verarbeitung Risikoanalysen und Datenschutz-Folgenabschätzungen vorzunehmen (s.o. Kap. 11.3) und ein Verarbeitungsverzeichnis (s.o. Kap. 11.2) zu erstellen. Weitere **zu dokumentierende Umstände** sind die technisch-organisatorischen Maßnahmen (Art. 32 DSGVO) sowie im Fall von „Verletzungen des Schutzes personenbezogener Daten“, also von Datenlecks, Meldungen an die Aufsichtsbehörde sowie evtl. an die Betroffenen (Art. 33, 34 DSGVO).

Eine **ausdrückliche Verpflichtung** zur Erstellung eines umfassenden Datenschutzkonzeptes enthält die DSGVO nicht.⁶⁸² Etwas anderes gilt für die Durchführung von Forschungsprojekten durch öffentliche Stellen in Hessen, wo § 24 Abs. 1 S. 2 HDSIG Folgendes regelt:

„Vor dem Beginn des Forschungsvorhabens ist ein Datenschutzkonzept zu erstellen, das der zuständigen Aufsichtsbehörde auf Nachfrage vorzulegen ist.“

Eine weitergehende Regelung enthält § 75 Abs. 1 S. 4 SGB X. Danach ist im Fall einer Übermittlung von Sozialdaten für Forschungszwecke „*der nach Absatz 4 Satz 1 zuständigen Behörde [...] ein Datenschutzkonzept vorzulegen. Zuständige Behörde ist nach Abs. 4 S. 1 die oberste Bundes- oder Landesbehörde, die für den Bereich, aus dem die Daten herrühren, zuständig ist.*“ Dabei handelt es sich regelmäßig um das jeweilige Sozialministerium, welches die Datenübermittlung gemäß Abs. 4 S. 1 zu genehmigen hat. In dem Datenschutzkonzept soll der Antragsteller, also der forschende Verantwortliche, darlegen, dass er die technischen und organisatorischen Anforderungen des Datenschutzes sowie des Grundsatzes der Datenminimierung erfüllt.⁶⁸³ Dabei wird auf Art. 32 DSGVO sowie § 22 Abs. 2 BDSG Bezug genommen.

Auch wenn es eine ausdrückliche Regelung nicht gibt, vertreten die deutschen Datenschutzbehörden die Ansicht, dass die für ein Forschungsprojekt Verantwortlichen den „zur Prüfung der ethischen und datenschutzrechtlichen Vereinbarkeit zuständigen Stellen“ ein „**Forschungskonzept**“ vorlegen müssen gemeinsam mit der Prüfung der Vereinbarkeit mit dem Datenschutzrecht, einschließlich der „zugrunde liegenden Beweggründe sowie die Sicherstellung der o.g. Sicherheitsmaßnahmen“. ⁶⁸⁴ Eine entsprechende Dokumentationspflicht kann mit Art. 5 Abs. 2 DSGVO begründet werden, der den Verantwortlichen dazu verpflichtet, die Einhaltung der in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze nachweisen zu können einschließlich der in Art. 89 DSGVO auferlegten Garantien.

Eine präzise Umschreibung dessen, was ein Datenschutzkonzept enthalten muss, ist den Regelungen nicht zu entnehmen. Wohl aber ergibt sich aus einer Gesamtschau der rechtlichen Vorgaben, dass die **Inhalte des Datenschutzkonzeptes** eine umfassende Darstellung der Datenverarbeitung enthalten müssen, aus der sich deren Rechtmäßigkeit ableiten lässt. Erfasst werden damit

- das Verarbeitungsverzeichnis (s.o. Kap. 11.2),
- die Darstellung der technisch-organisatorischen Maßnahmen (s.o. Kap. 9) und
- die Datenschutz-Folgenabschätzung (s.o. Kap. 11.3).

⁶⁸² Bischoff/Wiencke ZD 2019, 13; Empfehlung; Weichert in Kühling/Buchner § 22 Rn. 43.

⁶⁸³ BT-Drs. 18/12611, 109.

⁶⁸⁴ DSK, Beschluss zur Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ in Erwägungsgrund 33 der DS-GVO v. 03.04.2019; Weichert ZD 2020, 23; als Empfehlung bei klinischen Prüfungen Bischoff/Wiencke ZD 2019, 13.

Nimmt eine Stelle die Privilegierungen bei der Zweckbindung (s.o. Kap. 8.1) sowie hinsichtlich der Einschränkung der Betroffenenrechte (s.u. Kap. 12) in Anspruch, so sind hierfür geeignete Garantien vorzusehen, die zu dokumentieren sind ebenso wie die Abwägung der Interessen der forschenden Stelle mit den Betroffeneninteressen. Letztlich handelt es sich bei diesen vorzunehmenden **Abwägungen** um zu dokumentierende Bestandteile der Datenschutz-Folgenabschätzung.⁶⁸⁵

Es bestehen keine Vorgaben für die Form der o.g. Dokumente. Insbesondere das Verarbeitungsverzeichnis und die Folgenabschätzung können in separate Dokumente aufgenommen werden. Es empfiehlt sich jedoch, diese in **ein umfassendes Dokument** aufzunehmen, das allen Anforderungen genügt. Dieses Dokument sollte in einer Weise strukturiert sein, dass es zeitlich fortgeschrieben werden kann.

⁶⁸⁵ Karg in SHS, Art. 35 Rn. 13.