Leitfaden für die Erstellung von Datenschutzkonzepten im Gesundheitswesen

Eine Zusammenarbeit von

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

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG)

Version 1.1

Stand der Bearbeitung: 12. Dezember 2016

Inhaltsverzeichnis

Copyright 5

Vorwort 6

Vorgehen bei der Erstellung eines Datenschutzkonzeptes 6

Teil I: Aufbau und Struktur eines Datenschutzkonzeptes 8

1 Zusammenfassung/Management Summary 9

2 Einleitung 9

3 Definitionen/Begrifflichkeiten 9

4 Fachliche und organisatorische Hintergründe zum Vorhaben 10

5 Beschreibung und Zielsetzung des Vorhabens 10

5.1 Ziele 10

5.2 Zweckbestimmung 10

5.3 Zu verarbeitende Daten 10

5.3.1 Schutzbedarf der Daten 11

5.4 Rechtsgrundlage der Datenverarbeitung 12

5.5 Lebenszyklus der personenbezogenen Daten 13

5.5.1 Erheben, Sammeln der Daten 13

5.5.2 Übertragung der Daten 13

5.5.3 Verwendung der Daten 13

5.5.4 Speichern der Daten 14

5.5.5 Migration der Daten 14

5.5.6 Maßnahmen zur Zugriffsverhinderung 14

6 Akteure/Beteiligte 15

6.1 Verantwortliche Stelle 15

6.1.1 Angaben zur verantwortlichen Stelle 15

6.1.2 Grundsätzliche Einstellung des Unternehmens/der Institution/der Organisation/der Behörde zum Datenschutz 16

6.2 Datenverarbeitende 16

7 Datenschutzbezogene Anforderungen 16

7.1 Geeignetheit 16

7.2 Erforderlichkeit 16

7.3 Grundsatz der Datenvermeidung und -sparsamkeit 17

7.4 Verhältnismäßigkeit der Datenverarbeitung/Übermaßverbot 17

7.5 Zweckbindung, Aufbewahrungsfristen 17

7.6 Betroffenenrechte 17

7.6.1 Recht auf Benachrichtigung über die Datenerhebung 17

7.6.2 Recht auf Auskunft 17

7.6.3 Aushändigung einer Kopie der Daten 18

7.6.4 Recht auf Datenübertragbarkeit (Migration der Daten) 18

7.6.5 Recht zum Widerspruch bzgl. der Datennutzung 18

7.6.6 Recht auf Berichtigung, Sperrung oder Löschung 18

7.6.7 Verpflichtung, Betroffene bzgl. Datenpannen zu informieren 18

7.6.8 Anspruch auf Anrufung der Datenschutzkontrollinstanz 18

7.7 Darstellung der Gewährleistungsziele/Schutzziele 18
7.7.1 Wahrung der Vertraulichkeit 18
7.7.2 Authentizität (Zurechenbarkeit) 18
7.7.3 Integrität der Daten 18
7.7.4 Verfügbarkeit 18
7.7.5 Intervenierbarkeit (Eingreifbarkeit) 19
7.7.6 Nichtverkettbarkeit (Zweckbindung) 19
7.7.7 Transparenz 19
7.7.8 Validität 19
7.7.9 Nutzungsfestlegungen 19
7.8 Darstellung der Rechtskonformität 20
7.8.1 Allgemeines 20
7.8.2 Rechtssicherheit/Gerichtsverwertbarkeit der Datenverarbeitung 20
7.8.3 Revisionsfähigkeit/Beweisfestigkeit von Datenverarbeitungen 20
7.8.4 Nicht-Abstreitbarkeit von Datenübermittlungen 20
8 Implementierte bzw. zu implementierende Datenschutzmaßnahmen 20
8.1 Darstellung der Umsetzung des Grundsatzes der Datenvermeidung und –sparsamkeit 22
8.2 Vorgehen bei Abwägung zwischen dem schutzwürdigen Interesse des Betroffenen und den eigenen Geschäftsinteressen 22
8.2.1 Darstellung der möglichen und der getroffenen Maßnahmen zur Risikominimierung 22
8.2.2 Darstellung der verbliebenen Restrisiken für Betroffene 22
8.3 Beschreibung der Gewährleistung von Betroffenenrechten 22
8.3.1 Recht auf Benachrichtigung über die Datenerhebung 22
8.3.2 Recht auf Auskunft 22
8.3.3 Recht auf Aushändigung einer Kopie der Daten 22
8.3.4 Daten von Betroffenen in ein neues System migrieren können 22
8.3.5 Recht zum Widerspruch bzgl. der Datennutzung 22
8.3.6 Recht auf Berichtigung, Sperrung oder Löschung 22
8.3.7 Betroffene über erfolgte Angriffe informieren 22
8.3.8 Anspruch auf Anrufung der Datenschutzkontrollinstanz 22
8.4 Beschreibung der Maßnahmen zur Verteidigung der Gewährleistungsziele/Schutzziele 22
8.4.1 Wahrung der Vertraulichkeit 22
8.4.2 Authentizität (Zurechenbarkeit) 22
8.4.3 Integrität der Daten 22
8.4.4 Verfügbarkeit 22
8.4.5 Intervenierbarkeit (Eingreifbarkeit) 22
8.4.6 Nichtverkettbarkeit (Zweckbindung) 22
8.4.7 Transparenz 22
8.4.8 Validität 22
8.4.9 Nutzungsfestlegungen 22
9 Konzeptuelle Risikobetrachtung 23
10 Mitgeltende Unterlagen 23
11 Bereichsspezifische Ergänzungen 24

Teil II: Ergänzende Materialien 25

1 Mapping zu anderen Anforderungen 26
1.1 Europäische Datenschutz-Grundverordnung (DS-GVO) 26
1.2 SDM der Datenschutzaufsichtsbehörden 28

2 Begriffsdefinitionen 30

3 Akteure 42
3.1 Juristische und natürliche Personen 42
3.2 Nicht-Personen 43

4 Risikobewertung 45
4.1 Warum eine Risikobewertung? 45
4.2 Welche Risiken sollten immer betrachtet werden? 45
4.3 Risikobewertung 46
4.3.1 Eintrittswahrscheinlichkeit 46
4.3.2 Schadensklassifikation 46
4.3.3 Risikoklassifizierung 47

5 Feststellung des Schutzbedarfs 48

6 Abkürzungsverzeichnis 49

7 Weiterführende Literatur 50
7.1 Empfehlungen 50
7.1.1 Bundesamt für Sicherheit in der Informationstechnik (BSI) 50
7.1.2 Datenschutz-Aufsichtsbehörde 50
7.2 Normen 50
7.2.1 Allgemeine Datenschutz-Anforderungen 50
7.2.2 Anonymisierung/Pseudonymisierung 50
7.2.3 Archivierung 50
7.2.4 Berechtigungsmanagement 51
7.2.5 Datenschutzkonzept 51
7.2.6 ID-Management 51
7.2.7 IT-Sicherheit 51
7.2.8 Klassifikation 51
7.2.9 Löschung 51
7.2.10 Patientenakte 52
7.2.11 Protokollierung 52
7.2.12 Verschlüsselung 52
7.2.13 Wartung/Fernwartung 52
7.3 Zeitschriften 52

Historie

Version 1.0

Autoren (alphabetisch)

Treinat, Lars	ZTG Zentrum für Telematik und Telemedizin GmbH
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

Stand: 25.11.2015

Version 1.1

Autoren (alphabetisch)

Isele, Christoph	Cerner Deutschland
Mempel, Lukas	Sana Kliniken AG
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH
Spyra, Gerald	Kanzlei Spyra
Treinat, Lars	ZTG Zentrum für Telematik und Telemedizin GmbH
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

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

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Im folgenden Text werden daher, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.

Vorwort

In allen Stellen, welche Gesundheitsdaten verarbeiten, ist der Schutz dieser Daten vor unberechtigten Zugriffen unabdingbar. Ein wirkungsvoller Schutz benötigt letztlich auch ein Datenschutzkonzept, in welchem festgelegt wird, wie der Schutz der informationellen Selbstbestimmung der betroffenen Personen von der verarbeitenden Stelle sichergestellt wird.

Der grundsätzliche Aufbau eines derartigen Datenschutzkonzepts sollte wie folgt aussehen:

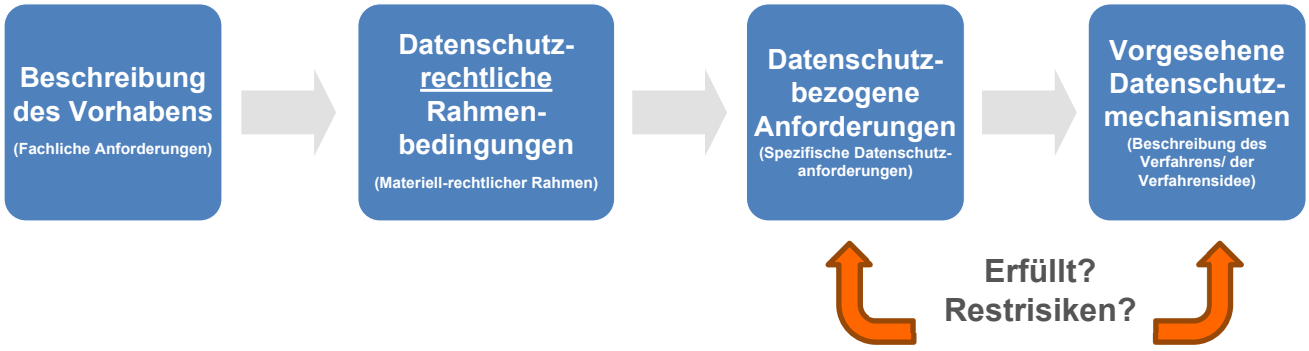
Kapitel 1	Zusammenfassung/Management Summary
Kapitel 2	Einleitung
Kapitel 3	Definitionen/Begrifflichkeiten
Kapitel 4	Fachliche Hintergründe zum Vorhaben (Produkt, Projekt, usw.)
Kapitel 5	Beschreibung und Zielsetzung des Vorhabens
Kapitel 6	Akteure/Beteiligte
Kapitel 7	Datenschutzbezogene Anforderungen
Kapitel 8	Implementierte bzw. zu implementierende Datenschutzmaßnahmen
Kapitel 9	Konzeptionelle Risikobetrachtung
Kapitel 10	Mitgeltende Unterlagen
Kapitel 11	Bereichsspezifische Ergänzungen.

Jedem dieser Kapitel wird in dieser Ausarbeitung ein eigenes Kapitel gewidmet, in welchem die grundlegenden Fragestellungen betrachtet werden. D. h. hier finden sich Hinweise, was im jeweiligen Datenschutzkonzept zu beschreiben ist. Es finden sich keine vorformulierten Texte, denn ähnlich wie ein Qualitätsmanagementhandbuch muss auch ein Datenschutzkonzept individuell für die jeweilige Datenverarbeitung geschrieben werden. Dementsprechend kann auch nur individuell entschieden werden, welche der hier vorgestellten Bestandteile der Kapitel 1 bis 10 in das für das jeweilige individuelle Vorhaben geltende Datenschutzkonzept übernommen werden müssen.

Ein Kapitel 11 widmet sich den Besonderheiten der föderalen Gesetzgebung in Deutschland, d. h. hier werden – soweit vorhanden und den Autoren bekannt – spezifische Anforderungen dargestellt, die in einem Bundesland erhoben werden, aber nicht als allgemeine Anforderung für Deutschland gelten kann.

Vorgehen bei der Erstellung eines Datenschutzkonzeptes

Das Vorgehen zur Erstellung eines Datenschutzkonzeptes kann als eine Folge von Einzelschritten verstanden werden, die von der nachfolgenden Skizze in Übersichtsform dargestellt werden:



Schritt 1: Beschreibung des Vorhabens

Zunächst erfolgt eine (grobe) einleitende Beschreibung des Vorhabens, sodass die grundlegenden Gedanken des Vorhabens erkennbar sind. In diesem Schritt werden weiterhin die fachlichen Anforderungen des Vorhabens beschrieben. Dies kann durchaus die Genauigkeit eines Lastenheftes abbilden. In diesem Schritt wird dargestellt, wer welches Ziel mit der Verarbeitung von welchen Daten durch wen erreichen will.

Schritt 2: Datenschutzrechtliche Rahmenbedingungen

In diesem Schritt werden die für das Vorhaben relevanten datenschutzrechtlichen Normen identifiziert. D. h. es werden sowohl die entsprechenden Gesetze und Verordnungen als auch die daraus erwachsenden Regelungen identifiziert. Neben Datenschutzgesetzen gehören hierzu natürlich auch andere Gesetze und Verordnungen, aus denen datenschutzrechtliche Anforderungen erwachsen können, wie beispielsweise die Berufsordnung der Ärztinnen und Ärzte, die Röntgenverordnung oder auch das Strafgesetzbuch.

Schritt 3: Datenschutzbezogene Anforderungen

Anschließend erfolgt ein Abgleich des im Schritt 2 identifizierten materiell-rechtlichen Rahmens mit den in Schritt 1 dargelegten fachlichen Anforderungen. Daraus ergeben sich die wesentlichen Anforderungen, die für das geplante Datenverarbeitungsvorhaben und dementsprechend auch im Datenschutzkonzept zu berücksichtigen sind.

Schritt 4: Vorgesehene Datenschutzmechanismen

Nun werden Mechanismen zur Gewährleistung der in Schritt 3 herausgearbeiteten datenschutzrechtlichen Anforderungen identifiziert und dargestellt, wie diese Mechanismen konkret im Vorhaben umgesetzt werden.

Schritt 5: Überprüfung der Maßnahmen

Abschließend erfolgt eine Beurteilung, ob alle Datenschutz-Anforderungen durch die vorgesehenen Datenschutzmechanismen erfüllt werden können, wie groß ggf. weiterhin vorhandene Risiken für die Betroffenen sind und eine Einschätzung, inwieweit die identifizierten Restrisiken als vertretbar eingeschätzt werden.

Sollte trotz aller Maßnahmen das Restrisiko nicht auf ein vertretbares Maß reduziert werden können, so darf die Datenverarbeitung weder begonnen noch durchgeführt werden.

Teil I:
Aufbau und Struktur eines Datenschutzkonzeptes

1 Zusammenfassung/Management Summary

Bitte beschreiben bzw. skizzieren Sie Ihre ausgearbeitete Gesamtlösung. Der Leser soll einen Überblick über das konzipierte Verfahren erhalten. Beispiel: Skizzen, Screenshots usw.

2 Einleitung

Die Einleitung sollte in aller Kürze das Vorhaben vorstellen. Es geht hierbei nicht um eine möglichst genaue Darstellung, vielmehr soll den Lesenden des Datenschutzkonzeptes ein Überblick geboten werden.

Die Einleitung soll die folgenden Fragen beantworten:

- Wie nenne ich das Vorhaben?
- Worum geht es?
- Wer führt das Vorhaben durch bzw. ist die verantwortliche Stelle für das Vorhaben?
- Gibt es weitere Beteiligte?
- Welche Aufgaben erfüllen die Parteien?
- Welchen Zweck hat das Verfahren/Vorhaben?

3 Definitionen/Begrifflichkeiten

Der Leitfaden enthält eine Reihe von Vorschlägen (siehe zweiter Teil dieser Ausarbeitung, Kapitel 2 Begriffsdefinitionen auf Seite 30), welche die Abbildung der Begriffsbestimmungen im eigenen Datenschutzkonzept erleichtern sollen. Hierzu müssen die im eigenen Datenschutzkonzept geltenden Definitionen aus Teil III in diesen Anschnitt übertragen werden.

Die Verwendung von gleichartigen Definitionen soll ein einheitliches Verständnis bei der Interpretation von verschiedenen Datenschutzkonzepten ermöglichen, sowohl bei Datenschutzexperten (z. B. bei externen Audits oder Aufsichtsbehörden) als auch bei den betroffenen Personen selbst. Die Zielgruppe der Datenschutzkonzepte kann Konsument der Angebote sein; eine gleiche Nutzung von Begrifflichkeiten führt somit zu einem leichteren Verständnis der Schutzmaßnahmen beim Dateninhaber, also den Betroffenen. Letztlich handelt es sich hierbei also um eine vertrauensbildende Maßnahme gegenüber den medizinisch zu versorgenden Menschen. Zusätzlich ermöglicht die einheitliche Verwendung von Begrifflichkeiten die Vergleichbarkeit von Datenschutzkonzepten bei der Erstellung von Gutachten und der Durchführung von Audits.

Sollten Sie z. B. aufgrund den von Ihnen anzuwendenden Gesetzen andere Definitionen als im Glossar des Leitfadens benutzen müssen, weisen Sie bitte in diesem Kapitel darauf hin und listen Sie Ihre Definition hier auf bzw. verweisen Sie auf Ihre Quelle.

4 Fachliche und organisatorische Hintergründe zum Vorhaben

In diesem Kapitel wird dargestellt, was zu dem Vorhaben führte, wer an dem Vorhaben beteiligt ist, welche Infrastruktur erforderlich ist und welche Infrastruktur genutzt wird bzw. werden soll.

Nach dem Lesen dieses Kapitels müssen die folgen Fragen beantwortet sein:

- Warum wird das Vorhaben durchgeführt?
- Was ist die Motivation für die Durchführung?
- Welche Fragestellungen, Anforderungen oder Herausforderungen sollen durch die Umsetzung des Vorhabens gelöst werden?
- Welche Geschäftspartner sind an dem Vorhaben beteiligt?
- Welche Infrastruktur ist für die Umsetzung des Vorhabens erforderlich?
- Welche Infrastruktur (bezogen auf das Datenschutzkonzept) steht von eigener Seite zur Verfügung, welche wird von Geschäftspartnern zur Verfügung gestellt?

5 Beschreibung und Zielsetzung des Vorhabens

In diesem Kapitel erfolgt die detaillierte Beschreibung des Vorhabens: die genauen Ziele werden vorgestellt, die Zweckbestimmung der Datenverarbeitung benannt, die zur Erreichung des Zwecks notwendigen Daten sowie deren Schutzbedarf werden beschrieben, die Rechtsgrundlage für die Datenverarbeitung dargelegt und der Lebenszyklus der Daten abgebildet

5.1 Ziele

- Welche fachlichen Anforderungen sind bekannt?
- Welche Geschäftsprozesse sollen realisiert oder unterstützt werden? (Beschreibung der entsprechenden Geschäftsprozesse)
- Was soll die Lösung leisten?
- Welche Fragestellungen sollen durch das Ergebnis des Vorhabens beantwortet werden?
- Welche Auswertungen werden von wem aus welchem Grund wann vorgenommen?
- Welche Daten werden im- und/oder exportiert?

5.2 Zweckbestimmung

- Im Folgenden ist eine ausführliche Beschreibung und Begründung zu liefern, für welchen Zweck die personenbezogenen und -beziehbaren Daten im betreffenden Informationssystem verarbeitet werden und warum diese Verarbeitung (unbedingt) erforderlich ist.
- Wenn es mit vertretbarem Aufwand möglich ist, sind Daten entsprechend den gesetzlichen Vorgaben grundsätzlich ohne Personenbezug (anonymisiert, ggf. pseudonymisiert) zu verarbeiten. Es muss daher begründet werden, warum dies nicht möglich ist.
- Werden Daten aus anderen Quellen verwendet, ist zu prüfen, ob dies mit dem Zweck dieser Erhebung vereinbar ist. Ändert sich der Zweck, so ist die Zweckänderung darzulegen.

5.3 Zu verarbeitende Daten

Hier sind neben den eigentlichen personenbezogenen Daten wie Name oder Geburtsdatum ebenfalls derartige Datenarten zu dokumentieren, die bei der Verarbeitung (im Sinne von Art. 4 Ziff. 2 DS-GVO) in Verbindung mit einer Person angezeigt und/oder ausgewertet werden und somit dieser Person

zugeordnet werden können (sog. personenbeziehbare Daten). Idealerweise werden die Daten katalogisiert dargestellt, z. B.

a. Patientendaten
   Bei dem betroffenen Personenkreis handelt es sich um alle Patientinnen und Patienten des jeweiligen Krankenhauses bzw. der Organisation. Bei den Daten handelt es sich einerseits um Daten der Patientin bzw. des Patienten selbst (z. B. Geburtsdatum bzw. Alter zum Zeitpunkt der Aufnahme), andererseits um bei deren Diagnostik und Behandlung anfallende Daten als auch – überwiegend bei epidemiologischen Studien – um Ortsdaten (z. B. Geburtsort, -land, Wohnort, -land) der in (Name der Einrichtung) betreuten Patientinnen und Patienten. Die Daten werden zu Zwecken der
   a. Medizinischen Versorgung,
   b. Lehre,
   c. Forschung
   d. und der Qualitätssicherung

   eingesetzt, entsprechend den Aufgaben, welche das Krankenhaus/die Organisation zu erfüllen hat.
b. Kundendaten
c. Lieferantendaten
d. Beschäftigtendaten
   a. Gehaltsabrechnung/Personalverwaltung
   b. Mitarbeiterinnen- und Mitarbeiterbeurteilung
   c. QM-System/Organigramm
   d. Dienstplanung
   e. ...
e. Aktionärsdaten
f. Mitgliederdaten
g. Personenbezogene Daten für Geschäftszwecke
h. ...

5.3.1 Schutzbedarf der Daten

Für alle Daten bzw. Datenkategorien muss der individuelle Schutzbedarf dargestellt werden. Allgemeine Fragen hierzu

- Wie viel Schutz benötigen die Daten bzw. Daten-Objekte[1]?
- Welche Daten bzw. Daten-Objekte benötigen mehr Sicherheit, bei welchen genügen elementare Schutzmaßnahmen?
- Die Einschätzungen des Schutzbedarfs müssen Außenstehenden (Aufsichtsbehörde, internen und externen Auditoren) gegenüber begründbar und von diesen nachvollziehbar sein.

[1] Daten werden in Datenobjekten gespeichert. Das Datum an sich ist zunächst allgemeiner Natur im Sinne von einem bestimmten Wissen. Damit es beispielsweise in Datenbanken angelegt werden kann, muss es in einem Objekt gespeichert werden. In diesem Sinne wird es auch von der Orientierungshilfe zu Krankenhausinformationssystemen der Datenschutzaufsichtsbehörden (online z. B. unter https://www.datenschutz-bayern.de/technik/orient/oh-kis.pdf verfügbar) Deutschlands angewendet.

Zur Schutzbedarfsfeststellung gehören die folgenden Aktivitäten[2]:

1) die auf Ihre Organisation zugeschnittene Definition der Schutzbedarfskategorien "normal", "hoch" und "sehr hoch",
2) die Feststellung des Schutzbedarfs der Anwendungen, die in der Strukturanalyse erfasst wurden, mit Hilfe der definierten Kategorien,
3) die Ableitung des Schutzbedarfs der IT-Systeme aus dem Schutzbedarf der Anwendungen,
4) daraus abgeleitet die Feststellung des Schutzbedarfs der Kommunikationsverbindungen und Räume sowie
5) die Dokumentation und Auswertung der vorgenommenen Einschätzungen.

Als Beispiel für die Schutzbedarfskategorien kann die folgende Eingruppierung dienen[3]:

1) Normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht durch eigene Aktivitäten zu heilen
2) Hoch: die Schadensauswirkungen werden für Betroffene als beträchtlich eingeschätzt, z. B. weil der Wegfall einer von einer Organisation zugesagten Leistung die Gestaltung des Alltags nachhaltig veränderte und die Betroffenen nicht aus eigener Kraft handeln können, sondern auf Hilfe angewiesen wären
3) Sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existenziell bedrohliches, katastrophales Ausmaß für Betroffene an.

5.4 Rechtsgrundlage der Datenverarbeitung

Welche Rechtsgrundlage ermöglicht die Datenverarbeitung des Vorhabens bzw. wer/was erlaubt mir, das geplante Vorhaben durchzuführen? Dies beinhaltet eine Darstellung der datenschutzrechtlichen Rahmenbedingungen. Somit ist zu fragen, ob die Grundlage der Tätigkeit(en) gesetzlicher, vertraglicher oder gewillkürter[4] Art ist.

Damit verbunden ergeben sich die normativen Anforderungen, die bei der Konzeption zu berücksichtigen sind:

a) Wirksame Einwilligung des Betroffenen; zu den Anforderungen an eine rechtswirksame Einwilligung siehe bspw. §§4(1), 4a BDSG, entsprechende Landesdatenschutzgesetze (etwa § 4 DSG NW) oder zukünftig gemäß Art. 7 DS-GVO
b) Erlaubnis durch ein Gesetz; bspw. §§13 ff. bzw. 28ff. BDSG, LDSG (etwa §§12 ff DSG NW) oder andere Rechtsvorschriften (etwa §§67a, 67b SGB X u.a., §10 GDSG NW oder auch Betriebsvereinbarungen)

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Schulung - Kapitel 4: Schutzbedarfsfeststellung. [Online, zitiert am 2016-02-08]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/Schutzbedarfsfeststellung/schutzbedarfsfeststellung_node.html

[3] Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Standard-Datenschutzmodell. [Online, zitiert am 2016-02-08]; Verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Standard-Datenschutzmodell/SDM-Handbuch_V09a.pdf

[4] Gewillkürt ist eine Qualifikation des Geschehens. Hier geschieht etwas durch den Willen, also z. B. gewillkürte Erbfolge. Der Gegensatz dazu wäre die Kraft Gesetzes eintretende Bewirkung, also im Beispiel die gesetzliche Erbfolge.

Idealerweise erfolgt die Darstellung der Rechtsgrundlage mit Referenzierung auf die Datenkategorien, also z. B.

a. Rechtsgrundlage für die Datenverarbeitung von Patientendaten
   Die Rechtsgrundlage zur Nutzung der erhobenen Patientendaten zu Patientenversorgung, Lehre, Forschung und Qualitätssicherung bilden die nachfolgend genannten Gesetze.
   a. Patientenversorgung:
      – ... (hier würden die entsprechenden Rechtsgrundlagen stehen, z. B. § 28 Abs. 7 BDSG
   b. Lehre:
      – ...
   c. Forschung:
      – ... (z.B. bei Arzneimittelforschung §§ 40-42a AMG)
   d. Qualitätssicherung:
      – §135a SGB V
      – §137 SGB V
      – Richtlinie gemäß § 137 Abs. 1 SGB V i. V. m. § 135 a SGB V über Maßnahmen der Qualitätssicherung für nach § 108 SGB V zugelassene Krankenhäuser
      – ... .

5.5 Lebenszyklus der personenbezogenen Daten

5.5.1 Erheben, Sammeln der Daten

– Wo werden die Daten erhoben? (Bei den Betroffenen direkt?)
– Durch wen erfolgt die Datenerhebung?
– Welche Voraussetzungen gelten für die Erhebung ohne Mitwirkung des Betroffenen?

5.5.2 Übertragung der Daten

– Werden Daten übermittelt?
– An wen/von wem werden Daten übermittelt?
– Wer ist verantwortliche Stelle?
– Bei automatisierten Abrufverfahren:
  - Sind Anlass und Zweck des Abrufverfahrens sowie die daran beteiligte(n) Stellen festgelegt?
  - Sind die Abrufberechtigungen festgelegt und werden sie kontrolliert?
  - Sind Art und Umfang der bereitgehaltenen Daten festgelegt?
  - Ist festgelegt, in welchen Fällen die speichernde Stelle von der abrufenden Stelle informiert werden muss? (Z. B. bei welchem Vorfall?)
  - Welche Maßnahmen wurden gegen einen unbefugten Abruf getroffen?[5]

5.5.3 Verwendung der Daten

– Welche technischen Systeme werden eingesetzt?
– Wie werden die Daten verarbeitet? Beschreibung der organisatorischen und personellen Prozesse der Verarbeitung von Daten mit den Systemen

[5] Bundesamt für Sicherheit in der Informationstechnik. M 2.510 Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten. [Online, zitiert am 2016-10-31]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02510.html?nn=6610630

5.5.4 Speichern der Daten

- An welchen Standorten werden personenbezogene Daten gespeichert? (intern, externes Rechenzentrum)?
- Gerichtsstand der Lokationen, an denen Daten gespeichert werden?
- Welche Aufbewahrungsfristen existieren für welche Daten(arten)?
- Wie lange darf ich welche Daten(arten) maximal aufbewahren?

5.5.5 Migration der Daten

- Wie werden Daten migriert?
- Wie wird eine Migration technisch unterstützt? (Darstellung der Lösung)?

5.5.6 Maßnahmen zur Zugriffsverhinderung

5.5.6.1 Löschen

- Wie sieht das Löschkonzept aus?
- Welche gesetzlichen Löschfristen existieren für welche Daten(arten)?
- Wann muss ich zwingend löschen?
- Wie werden Daten(träger) vernichtet?
- Wie sieht das Entsorgungskonzept aus?
- Wird ein Entsorgungsunternehmen eingesetzt? Wenn ja, welches?
- Können Daten automatisiert gelöscht werden?
- Können die Datenarten mit verschiedenen Aufbewahrungsfristen getrennt gelöscht werden? Eventuell Speicherkonzept (Datenbankentwurf) überarbeiten

5.5.6.2 Sperren

- Voraussetzung für die Sperrung
- Wie erfolgt die Sperrung der Daten?

5.5.6.3 Anonymisieren

- Existiert ein Anonymisierungskonzept?
- Ist die Methodik der Anonymisierung dokumentiert?
- Erfolgt die Anonymisierung automatisiert?
- Wie werden Daten anonymisiert?
- Der Aufwand bei der Erlangung der originalen Information aus einem anonymisierten Datenbestand muss für jedermann unverhältnismäßig hoch sein[6]. Unverhältnismäßig hoch bedeutet, dass der Aufwand für die Erlangung der personenidentifizierenden Informationen aus den anonymisierten Daten höher ist, als die erneute Erhebung der Daten selbst[6]. Ist dies gewährleistet?
- Ist gewährleistet, dass das Anonymisierungsverfahren auch Freitextfelder, Kommentarfelder, Anlagen usw. im Hinblick auf die Ersetzung identifizierenden Daten berücksichtigt?

5.5.6.4 Pseudonymisieren

- Ist die Methodik der Pseudonymisierung dokumentiert?
- Existiert ein „Konzept“?
- Unter welchen Bedingungen erfolgt eine Re-Identifikation?

[6] ErwGr. 26 S. 4 EU DS-GVO; §3 Abs. 6 BDSG

    - Sind die Bedingungen für eine Re-Identifikation vor Beginn der Pseudonymisierung festgelegt?
    - Sind die Bedingungen für eine Re-Identifikation im Vorfeld mit dem bzw. der zuständigen Datenschutzbeauftragten abgesprochen?
- Erfolgt die Pseudonymisierung automatisiert?
- Wie werden Daten pseudonymisiert?
- Ist gewährleistet, dass das Ergebnis der Identifikationsschutzmaßnahmen eine nicht zu unterschreitende Mindestgröße ergibt. D. h., die Gruppenmenge zur Pseudonymisierung hoch genug ist? Wenn ja, wie groß ist die kleinste Gruppenmenge?
- Wer hat Zugriff auf Pseudonymisierungslisten?
- Ist sichergestellt, dass, wenn pseudonymisierte Daten ohne Verwaltung des Schlüssels in einem Trust Center verwendet werden, die Anwender/Nutzer der pseudonymisierten Daten keinen Zugriff auf den Pseudonymisierungsschlüssel erhalten und dass ein Abgleich der pseudonymiserten Daten mit den Daten der Echtumgebung ausgeschlossen ist[7]?
- Ist gewährleistet, dass die Einhaltung der Bedingungen für eine Rückzuordnung in jedem Einzelfall durch den oder die Verantwortlichen geprüft wird?
- Ist sichergestellt, dass die Zuordnungsschlüssel nach Beendigung des Verfahrens vernichtet werden?
- Ist gewährleistet, dass das Pseudonymisierungsverfahren auch Freitextfelder, Kommentarfelder, Anlagen usw. im Hinblick auf die Ersetzung von identifizierenden Daten berücksichtigt?

6 Akteure/Beteiligte

Akteure sind Entitäten, die über Transaktionen miteinander interagieren. Dementsprechend können Akteure natürliche oder juristische Personen sein, aber ebenso gut EDV-Systeme wie beispielsweise ein KIS oder RIS. Zur Erleichterung der Benennung im eigenen Umfeld sind in dem in Teil II enthaltenen Kapitel 3 (Seite 42) beispielhaft verschiedene Akteure benannt.

Die Darstellung der Akteure sollte folgende Fragen beantworten:

- Wer sind die Beteiligten und welche Rollen haben sie?
- In welcher rechtlichen Beziehung stehen die Beteiligten zu einander?
    - Welche Weisungsbefugnisse gibt es?
    - Wer sind die Verantwortlichen des Vorhabens?
    - Wird das Konstrukt „Funktionsübertragung“ genutzt? Wenn ja, bitte beschreiben.
    - Wird das Konstrukt „Auftragsverarbeitung“ genutzt? Wenn ja, bitte beschreiben.
- Wer benutzt das Informationssystem?
- Wer führt Wartungsarbeiten durch?
- Greift jemand aus welchen Gründen, die nicht dem eigentlichen Zweck entsprechen, auf die Daten zu? Wenn ja: warum und mit welcher Berechtigung?

6.1 Verantwortliche Stelle

6.1.1 Angaben zur verantwortlichen Stelle

- Wer ist bei der verantwortlichen Stelle für was zuständig und wie erreichbar?

[7] ErwGr. 29 S. 1 EU DS-GVO

– Wer hat ggf. außerhalb der verantwortlichen Stelle Einflussmöglichkeiten auf die Datenverarbeitung?

6.1.2 Grundsätzliche Einstellung des Unternehmens/der Institution/der Organisation/der Behörde zum Datenschutz

– Gibt es eine eindeutige Positionierung der obersten Leitung/der Geschäftsführung hinsichtlich des Stellenwertes von Datenschutz und IT-Sicherheit im Unternehmen/in der Institution?
– Ist gewährleistet, dass keine Verarbeitung personenbezogener Daten ohne datenschutzrechtliche Freigabe der oder des Datenschutzbeauftragten erfolgt?
– Angemessenheit:
  Darstellung, dass nur geeignete und für die Verarbeitung erforderliche Daten erhoben werden.
– Verhältnismäßigkeit:
  Wie steht das Unternehmen zur Verhältnismäßigkeit bei der Datenverarbeitung? Lassen sich die fachlichen Anforderungen ggf. auch mit Verfahren erfüllen, die weniger Einschnitte in die informationelle Selbstbestimmung der Betroffenen erfordern?
– Zweckbindung der Daten:
  Erfolgt bei einer Zweckänderung der Datennutzung
    - die Überprüfung der Rechtmäßigkeit der Zweckänderung?
    - eine Information an die Betroffenen?
– Schulung Management und Beschäftigte
    - Sind verantwortliche Entscheidungsträger, Administratoren sowie die jeweiligen Anwender hinsichtlich Datenschutz und IT-Sicherheit geschult?
    - Erfolgen regelmäßig Sensibilisierungsmaßnahmen?
    - Gibt es unabhängig von Schulungsmaßnahmen Informationsmaterial zum Thema, so dass im Bedarfsfall etwas nachgelesen werden kann?

6.2 Datenverarbeitende

– Darstellung, wer (Rolle/Funktion) welche Daten bearbeitet
– Ggf. bestehende Verschwiegenheitspflichten
– Darstellung Schulung der Beschäftigten bzgl. Datensicherheit/IT-Sicherheit

7 Datenschutzbezogene Anforderungen

In diesem Kapitel werden die Anforderungen dargelegt, die aus den verschiedenen normativen Regelungen des Datenschutzes resultieren. Die nachfolgenden Aspekte sollten beschrieben werden, falls diese im Kontext des Vorhabens zutreffend sind. Bitte geben Sie im Falle von zusätzlichen Anforderungen, die sich beispielweise aus spezialgesetzlichen Regelungen ergeben und die Sie ggf. in Kapitel 5.4 Rechtsgrundlage der Datenverarbeitung identifiziert haben, diese ebenfalls an.

7.1 Geeignetheit

– Ist das Datenverarbeitungsverfahren geeignet, den angestrebten Zweck zu erfüllen?

7.2 Erforderlichkeit

– Sind das gewählte Gesamtverfahren, die Daten, die einzelnen Verarbeitungen erforderlich, um den angestrebten Zweck zu erreichen?

- Gibt es „mildere Mittel“ zur Erreichung des beabsichtigen Zweckes, deren Verwendung geringere Eingriffe in die Persönlichkeitsrechte verursachen? (Beschreibung, warum es kein milderes Mittel gibt.)

7.3 Grundsatz der Datenvermeidung und -sparsamkeit

- Wie ist der Grundsatz der Datenvermeidung und der -sparsamkeit beim beschriebenen Datenverarbeitungsvorhaben vorgesehen?
- Welche Techniken lassen sich sinnvoll einsetzen, um den Personenbezug weiter einzuschränken, ohne dass der Zweck gefährdet wird?
- Sind nachfolgende Maßnahmen sinnvoll einsetzbar: Anonymisierung, Pseudonymisierung, Trennung von personenidentifizierenden Daten?

7.4 Verhältnismäßigkeit der Datenverarbeitung/Übermaßverbot

- Ist die Art und Weise der Verarbeitung, um den Zweck zu erreichen, verhältnismäßig?
  Die Frage ist insbesondere bei der Datenverarbeitung von besonderen Arten personenbezogener Daten (z. B. medizinische Daten) oder dem Einsatz einer automatisierten Einzelentscheidung (etwa §6a BDSG) bedeutsam.
- Welches Missbrauchsrisiko besteht für die betroffene Person, wenn Daten in „falsche“ Hände gelangen?
  Um die Verhältnismäßigkeit im Sinne einer Güterabwägung durchführen zu können, muss das Missbrauchsrisiko der Daten bekannt sein, sonst lässt sich das Risiko für den Betroffenen nicht richtig abschätzen.
- Steht das Risiko in einem vertretbaren Verhältnis zum Nutzen der Datenverarbeitung?

7.5 Zweckbindung, Aufbewahrungsfristen

- Beschreiben Sie den Zweck der Datenverarbeitung. Stellen Sie sich bei der Antwort einen Text vor, der einer betroffenen Person erläutert, in was und warum sie einwilligen soll und warum.
- Zwecke sind regelmäßig zeitbegrenzt oder anlassbegrenzt:
  - Welche Fristen gelten daher bei unserem Datenverarbeitungsvorhaben für die Daten?
  - Wie lange dürfen/müssen die Daten aufbewahrt werden?
  - Wie sieht unser Lösch- und Sperrkonzept aus?
- Wie wird geregelt bzw. wie wird sichergestellt, dass die Daten nicht für andere Zwecke genutzt werden? (Wie wird dies überprüft?)

7.6 Betroffenenrechte

- Welche Rechte von Betroffenen sind zu erfüllen (z. B. Recht auf Auskunft, Berichtigung, Widerruf etc.)?
- Wie wird der Wahrung dieser Rechte nachgekommen (z. B. an wen wenden sich Betroffene, wer kann Auskunft zu den nachfolgenden Punkten erteilen)?

7.6.1 Recht auf Benachrichtigung über die Datenerhebung

- Wie können sich Betroffene über eine Datenerhebung benachrichtigen lassen?

7.6.2 Recht auf Auskunft

- Wie sieht das Konzept zum Umgang mit Auskunftsersuchen von Betroffenen aus? (Prozessbeschreibung)

7.6.3 Aushändigung einer Kopie der Daten

- Wie können Betroffene eine Kopie ihrer Daten erhalten (z. B. auf Grund § 630g Abs. 2 BGB)? (Konzept, Prozessbeschreibung)

7.6.4 Recht auf Datenübertragbarkeit (Migration der Daten)

- Wie können Daten von Betroffenen in ein neues System migriert werden?

7.6.5 Recht zum Widerspruch bzgl. der Datennutzung

- Wird auf eine Widerspruchsmöglichkeit, besonders wenn die Verarbeitung auf einer Einwilligung basiert, hingewiesen?
- Wie wird mit einem Widerspruch umgegangen (Konzept?)

7.6.6 Recht auf Berichtigung, Sperrung oder Löschung

- Gibt es ein entsprechendes Verfahren?

7.6.7 Verpflichtung, Betroffene bzgl. Datenpannen zu informieren

- Wie kann eine Datenpanne festgestellt werden?
- Gibt es einen Prozess, wie bei einer Datenpanne zu verfahren ist? (Prozessbeschreibung)
  Z. B. Ablaufplan zur Meldung unrechtmäßiger Kenntnisnahme oder Schäden am Datenbestand (Verlust, Manipulation etc.).

7.6.8 Anspruch auf Anrufung der Datenschutzkontrollinstanz

- Wie wird die betroffene Person auf ihr Recht, die Datenschutzaufsichtsbehörde anzurufen, hingewiesen?

7.7 Darstellung der Gewährleistungsziele/Schutzziele

Die Gewährleistungsziele/Schutzziele müssen angemessen umgesetzt werden. Es ist immer ein Abwägungsprozess.

7.7.1 Wahrung der Vertraulichkeit

- Ist bei dem Vorhaben die Vertraulichkeit und/oder die Schweigepflicht zu wahren?
- Welche Anforderungen sind hieran zu stellen?
- Wie wird sichergestellt, dass die Daten nicht von Unbefugten eingesehen werden können?
- Existiert ein Rechte-Rollen-Konzept bzgl. der Zugriffsmöglichkeit hinsichtlich der Daten?

7.7.2 Authentizität (Zurechenbarkeit)

- Wie wird die Eindeutigkeit der Urheberschaft eines Dokuments/eines Eintrages sichergestellt?
- Wie werden Änderungen an den Daten dokumentiert?

7.7.3 Integrität der Daten

- Welche Anforderungen an die Integrität (Unversehrtheit der Daten) sind für das Vorhaben essenziell?
- Wie wird die Unverändertheit und Vollständigkeit der Daten sichergestellt? (Hinweis: Dies schließt auch den korrekten Zeitpunkt der Erstellung/Bearbeitung mit ein.)

7.7.4 Verfügbarkeit

- Welche Anforderungen bestehen an die Verfügbarkeit der Datenverarbeitungssysteme und der Daten?

7.7.5 Intervenierbarkeit (Eingreifbarkeit)

- Welche Maßnahmen sind vorgesehen, etwa Sperrung bei unrichtigen Daten, Nachvollziehbarkeit von Änderungen?

7.7.6 Nichtverkettbarkeit (Zweckbindung)

- Gibt es ein abgestuftes Rollen- und Rechtekonzept?
- Werden Schnittstellen auf Erforderlichkeit geprüft?

7.7.7 Transparenz[8]

- Gibt es ein Betriebskonzept mit Darstellung aller Schnittstellen und technischen sowie organisatorischen Abläufe?
- Gibt es ein Protokollierungskonzept?
- Welche Protokollfunktionen werden eingesetzt?
- Welche Ereignisse werden protokolliert? [9]
    - Einrichten von Benutzerinnen und Benutzern
    - Erstellung von Rechteprofilen
    - Einspielen und Änderung von Anwendungssoftware
    - Änderungen an der Dateiorganisation
    - Durchführung von Datensicherungsmaßnahmen
    - Aufruf von Administrations-Werkzeugen
    - Versuche unbefugten Einloggens
    - Versuche der Überschreitung von Befugnissen
    - Eingabe/Änderung von Daten
    - Datenübermittlungen
    - Benutzung von automatisierten Abrufverfahren
    - Löschung von Daten
    - Aufruf von Programmen
- Ist die Zweckbindung hinsichtlich der Nutzung der Protokolldaten gewährleistet?
- Ist die maximale Aufbewahrungsdauer von Protokolldaten festgelegt?
- Ist das Löschen der Protokolldaten gewährleistet und sind entsprechende Regelungen niedergelegt?

7.7.8 Validität

- Welche Anforderungen an die Qualität der Daten sind gegeben, um den Zweck zu erreichen?
- Sind die Daten aktuell und in einer für den Verarbeitungszweck genügenden Qualität?
- Relevant etwa bei Bilddokumenten, um den medizinischen Zweck erreichen zu können.

7.7.9 Nutzungsfestlegungen

- Können für personenbezogene Daten/Dokumente der Kreis der Nutzer und deren Nutzungsrechte (z. B. lesen, schreiben, ändern) abgestuft geregelt werden?
- Wie wird dieses sichergestellt (eventuell durch Rollenkonzepte)?

---

[8] Transparenz im Sinne von Art. 5 Abs. 1 lit. a DS-GVO: Daten werden einer für die betroffene Person nachvollziehbaren Weise verarbeitet

[9] Bundesamt für Sicherheit in der Informationstechnik. M 2.110 Datenschutzaspekte bei der Protokollierung. [Online, zitiert am 2016-10-31]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02110.html?nn=6610630

7.8 Darstellung der Rechtskonformität

7.8.1 Allgemeines

- Wie wird eine ausreichende Vorabkontrolle gewährleistet?
  Bzw. bei Geltung der DS-GVO: Wie wird die Datenschutz-Folgenabschätzung durchgeführt?
- Ist gewährleistet, dass alle Verfahren im Verfahrensverzeichnis gelistet sind?
  Bzw. bei Geltung der DS-GVO: Ist gewährleistet, dass alle entsprechenden Verarbeitungen im Verzeichnis aller Verarbeitungstätigkeiten aufgeführt werden?
- Sind Datenschutz-Audits zur Überprüfung der Einhaltung der im Datenschutzkonzept beschriebenen Maßnahmen vorgesehen?
- Bei einer Verarbeitung von Daten in einem Drittland: wie wird die Verarbeitung abgesichert?
- Ist gewährleistet, dass Entscheidungen, welche für eine betroffene Person rechtliche Folgen nach sich ziehen oder sie erheblich beeinträchtigen können, nicht ausschließlich auf einer automatisierten Verarbeitung, welche der Bewertung einzelner Persönlichkeitsmerkmale dient, beruhen?

7.8.2 Rechtssicherheit/Gerichtsverwertbarkeit der Datenverarbeitung

- Besteht die Möglichkeit, dass die Daten ggf. vor Gericht als Beweismittel angesehen werden?
- Wenn ja, wie wird dies sichergestellt? (Z. B. durch Einsatz einer qualifizierten elektronischen Signatur entsprechend Art. 25 der eIDAS-Verordnung[10]))

7.8.3 Revisionsfähigkeit/Beweisfestigkeit von Datenverarbeitungen

- Ist es bei dem Vorhaben wichtig, dass Änderungen an Daten protokolliert werden, d. h., dass das System revisionsfähig ist?
- Wie wird sichergestellt, dass unberechtigte Manipulationen an den Daten aufgedeckt und nachvollzogen werden können?
- Wie wird sichergestellt, dass die Urheberschaft an einer Information oder einer Änderung daran (ggf. gerichtsfest) nachgewiesen werden kann?

7.8.4 Nicht-Abstreitbarkeit von Datenübermittlungen

- Besteht die Möglichkeit, dass Dateneingaben, Übermittlungen usw. so dokumentiert werden, dass sowohl Sender und Empfänger das Versenden bzw. das Erhalten nicht abstreiten können?
- Wie wird sichergestellt, dass die Urheberschaft an einer Information oder einer Änderung daran (ggf. gerichtsfest) nachgewiesen werden kann?

8 Implementierte bzw. zu implementierende Datenschutzmaßnahmen

Zu den in Kapitel 7 identifizierten Datenschutzanforderungen: Mit welchen Maßnahmen werden die in Kapitel 7 dargestellten Datenschutz-Anforderung umgesetzt?

Die Inhalte dieses Kapitels basieren auf den in Kapitel 7 genannten Anforderungen, daher können hier keine allgemeingültigen Hinweise gegeben werden, was im Einzelnen beschrieben werden muss.

[10] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. [Online, zitiert am 2016-09-17]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

Hilfestellungen bei der Angabe und Umsetzung einzelner Maßnahmen bieten z. B. die IT-Grundschutz-Standards und IT-Grundschutz-Kataloge des BSI.

Beispiele wären etwa die Datentrennung, Pseudonymisierung, Zugriffskontrolle/rollenbasierte Zugriffskonzepte, Verschlüsselung etc. Die nachfolgend aufgelisteten Kapitelüberschriften dienen der Strukturierung und Überprüfung der Vollständigkeit der Maßnahmen zur Gewährleistung der datenschutzrechtlichen Anforderungen.

8.1 Darstellung der Umsetzung des Grundsatzes der Datenvermeidung und -sparsamkeit

8.2 Vorgehen bei Abwägung zwischen dem schutzwürdigen Interesse des Betroffenen und den eigenen Geschäftsinteressen

8.2.1 Darstellung der möglichen und der getroffenen Maßnahmen zur Risikominimierung

8.2.2 Darstellung der verbliebenen Restrisiken für Betroffene

8.3 Beschreibung der Gewährleistung von Betroffenenrechten

8.3.1 Recht auf Benachrichtigung über die Datenerhebung

8.3.2 Recht auf Auskunft

8.3.3 Recht auf Aushändigung einer Kopie der Daten

8.3.4 Daten von Betroffenen in ein neues System migrieren können

8.3.5 Recht zum Widerspruch bzgl. der Datennutzung

8.3.6 Recht auf Berichtigung, Sperrung oder Löschung

8.3.7 Betroffene über erfolgte Angriffe informieren

8.3.8 Anspruch auf Anrufung der Datenschutzkontrollinstanz

8.4 Beschreibung der Maßnahmen zur Verteidigung der Gewährleistungsziele/Schutzziele

8.4.1 Wahrung der Vertraulichkeit

8.4.2 Authentizität (Zurechenbarkeit)

8.4.3 Integrität der Daten

8.4.4 Verfügbarkeit

8.4.5 Intervenierbarkeit (Eingreifbarkeit)

8.4.6 Nichtverkettbarkeit (Zweckbindung)

8.4.7 Transparenz

8.4.8 Validität

8.4.9 Nutzungsfestlegungen

9 Konzeptuelle Risikobetrachtung

Bei dieser konzeptuellen Risikobetrachtung ist nicht zwingend die klassische Risikoanalyse aus der IT Sicherheits-Analyse gemeint. Vielmehr sollen anhand der unter Kapitel 8 beschriebenen Lösung/Konzeption mögliche Angriffsszenarien durchspielt werden (etwa: eine unbefugte Person gibt sich für einen Patienten aus und verlangt die Löschung seiner Daten; beim Übertragen von Röntgenbildern per eMail werden die eMails abgefangen, um sie zu lesen usw.)?

Die konzeptuelle Risikobetrachtung dient der Darstellung, wie groß/relevant das Risiko dieser Angriffsszenarien ist und welche der getroffenen Maßnahmen welche jeweiligen Angriffe wie effizient abwehren würden.

Nach Durcharbeitung aller wesentlichen Angriffsszenarien muss geprüft werden, welche Restrisiken anhand der getroffenen Maßnahmen noch verbleiben: Ist das verbleibende Restrisiko durch weitere verhältnismäßige Maßnahmen reduzierbar oder ist das Risiko vertretbar oder müssen ggf. Einschränkungen beim angestrebten Zweck gemacht werden?

10 Mitgeltende Unterlagen

Einige zur Darstellung der Einhaltung des Datenschutzes bzw. zur Erfüllung datenschutzrechtlicher Anforderungen werden ggf. in externen Dokumenten dargestellt, z. B. Aufbewahrungsfristen in einem Archivierungskonzept, Löschfristen und -vorgaben in einem Löschkonzept. Dieses Kapitel dient der Auflistung, welche Dokumente ggf. ergänzend zu diesem Datenschutzkonzept für die Abbildung datenschutzrechtlicher Anforderungen betrachtet werden müssen. Beispielsweise:

a) Berechtigungskonzept
   (Rollen- und Rechtekonzept)
b) Datenschutzrichtlinie
c) Verfahrensverzeichnis der verantwortlichen Stelle[11] bzw. Verzeichnis von Verarbeitungstätigkeiten[12]
d) Protokollierungskonzept
e) Löschkonzept
f) Sicherheitskonzept
g) Notfall-Handbuch
h) Archivordnung
i) Musterdokumente wie
   - Patienteninformation
   - Patientenaufklärung
   - Patienteneinwilligung
   - Schweigepflichtentbindung
   - usw.

[11] §4g Abs. 2 BDSG i. V. m. §4e BDSG
[12] Art. 30 EU DS-GVO

11 Bereichsspezifische Ergänzungen

Auf Grund der föderalen Strukturen der Bundesrepublik Deutschland existieren im Bereich des Datenschutzrechts neben den Regelungen des Bundes korrespondierende rechtliche Vorgaben der Länder. Dies gilt ebenso für Bereiche wie etwa das Gesundheitswesens wie auch im konfessionellen Bereich.

Daher ist im jeweiligen Einzelfall zwingend zu prüfen, ob für die geplante Erhebung oder Verarbeitung besondere rechtliche Anforderungen bestehen. Diese sind zu benennen.

Teil II:
Ergänzende Materialien

1 Mapping zu anderen Anforderungen

1.1 Europäische Datenschutz-Grundverordnung (DS-GVO)

Anforderungen DS-GVO	Vorliegende Ausarbeitung
Art. 5 Abs. 1 lit. a: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Kap. 5.4, 7.6 und 8.3
Art. 5 Abs. 1 lit. b: Zweckbindung	Kap. 5.2
Art. 5 Abs. 1 lit. c: Datenminimierung	Kap. 7.3
Art. 5 Abs. 1 lit. d: Richtigkeit	Kap. 7.8.2, 7.8.4 sowie 8.4.2, 8.4.3 und 8.4.8
Art. 5 Abs. 1 lit. e: Speicherbegrenzung	Kap. 5.5 und 7.5
Art. 5 Abs. 1 lit. f: Integrität und Vertraulichkeit	Kap. 8.4.3 und 8.4
Art. 5 Abs. 2: Rechenschaftspflicht	Das Datenschutzkonzept selbst enthält den Nachweis, welche Daten wozu mit welcher Rechtsgrundlage verarbeitet wurden, wie der Schutzbedarf der Daten zum Zeitpunkt der Verarbeitung ist und welche Schutzmaßnahmen vorhanden sind
Art. 25 Abs. 1, Art. 32 Abs. 1: Berücksichtigung „Stand der Technik[13]“	Abhängig von der Umsetzung, siehe Kap. 8
Art. 25 Abs. 2: Geeignete technische und organisatorische Maßnahmen (Gewährleistung angemessener Datenschutz, Datensicherheit)	Kap. 8
Art. 32 Abs. 1 lit. a Nutzung von Pseudonymisierung und Verschlüsselung personenbezogener Daten	Abhängig von der Umsetzung, siehe Kap. 8
Art. 32 Abs. 1 lit. b: Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	Kap. 8.4, 8.4.3, 8.4.4
Art. 32 Abs. 1 lit. c: Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	Kap. 8.4.4
Art. 32 Abs. 1 lit. d: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der	Abhängig von der Umsetzung, siehe Kap. 8

[13] Begrifflichkeit „Stand der Technik“ siehe auch

- BVerfG Urt. v. 08.08.1978 Az.: 2 BvL 8/77. Online, zitiert am 2016-05-13; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Text=2%20BvL%208/77
- §3 Abs. 2 Patentgesetz. Online, zitiert am 2016-05-13; Verfügbar unter http://www.gesetze-im-internet.de/patg/__3.html
- DIN EN 45020:2007-03. Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe.

Anforderungen DS-GVO	Vorliegende Ausarbeitung
technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	
Art. 32 Abs. 2: Beurteilung des angemessenen Schutzniveaus beinhaltend eine Risikobetrachtung	Kap 5.3.1
Art. 32 Abs. 4: Gewährleistung, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten	Berechtigungskonzept, Anlage zum Datenschutzkonzept
Art. 33: Meldung von Datenpannen an Behörden	Abhängig von der Umsetzung, siehe Kap. 8
Art 34: Meldung von Datenpannen an betroffene Personen	Abhängig von der Umsetzung, siehe Kap. 8
Art. 35: Datenschutz-Folgenabschätzung	Abhängig von der Umsetzung, siehe Kap. 8

1.2 SDM der Datenschutzaufsichtsbehörden

Das Standard-Datenschutzmodell (Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele), kurz SDM genannt, wurde vom Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder entwickelt. Das SDM soll „sowohl im öffentlich-rechtlichen als auch im privat-rechtlichen Bereich" einen „systematischen und nachvollziehbaren Vergleich" zwischen „Sollvorgaben, die sich aus Normen, Verträgen, Einwilligungserklärungen und Organisationsregeln ableiten" und ihrer Umsetzung „sowohl auf organisatorischer wie auch informationstechnischer Ebene" ermöglichen[14]. Aktuell existiert die Version 0.9 vom 30. September und 1. Oktober 2015.

Die in den vorhergehenden Kapiteln dargestellten Anforderungen wurden bzgl. den Darstellungen im SDM abgeglichen. Im Einzelnen findet sich:

- Kap. 5.2 SDM Die zentralen datenschutzrechtlichen Anforderungen
    - Zweckbindung → In dieser Ausarbeitung in Kapitel 7.5 zu finden
    - Begrenzung der Datenverarbeitung → In dieser Ausarbeitung in Kapitel 7.2, 7.3 und 7.4 zu finden
    - Berücksichtigung der Betroffenenrechte → In dieser Ausarbeitung in Kapitel 7.6 zu finden
    - Transparenz von Verfahren → In dieser Ausarbeitung zwar kein eigenes Kapitel, aber implizit in Kapitel 7.2, 7.4 und 7.8 enthalten; in Kapitel 7.7.7 als Schutzziel verankert
    - Datensicherheit der eingesetzten Komponenten zur Datenverarbeitung → In dieser Ausarbeitung in Kapitel 7.7 zu finden
- Kap. 5.3 SDM → In dieser Ausarbeitung in Kapitel 7.3 zu finden
- Kap. 5.4 SDM Die elementaren Gewährleistungsziele → Schutzziele zu finden in Kapitel 7.7
    - Verfügbarkeit → zu finden in Kapitel 7.7.4
    - Integrität → zu finden in Kapitel 7.7.3
    - Vertraulichkeit → zu finden in Kapitel 7.7.1
    - Nichtverkettbarkeit → zu finden in Kapitel 7.7.6
    - Transparenz → zu finden in Kapitel 7.7.7
    - Intervenierbarkeit → zu finden in Kapitel 7.7.5
- Kap. 5.5 SDM Weitere abgeleitete Gewährleistungsziele
    - Authentizität → zu finden in Kapitel 7.7.2
    - Revisionsfähigkeit → zu finden in Kapitel 7.8.2
- Kap. 7 SDM Die generischen Maßnahmen zur Umsetzung der Gewährleistungsziele → zu finden in Kapitel 8.4
- Kap. 8 SDM Die Verfahrenskomponenten → zu finden in Kapitel 5
    - die personenbezogenen Daten
      → zu finden in Kapitel 5.3

[14] Das Standard-Datenschutzmodell: Konzept zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. [Online, zitiert am 2016-11-11]; Verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Standard-Datenschutzmodell/Standard-Datenschutzmodell.php

    - die beteiligten technischen Systeme (Hardware, Software und Infrastruktur)
      → zu finden in Kapitel 5.5.3
    - die organisatorischen und personellen Prozesse der Verarbeitung von Daten mit den Systemen
      → zu finden in Kapitel 5.5.3
- Kap. 9 SDM Der Schutzbedarf → zu finden in Kapitel 5.3.1
- Kap. 9.3 Definition der Schutzbedarfskategorien → zu finden in Kapitel 5.3.1
- Kap. 9.4 SDM Schadensszenarien für Betroffene → zu finden in Kapitel 8.2.1

2 Begriffsdefinitionen

Begriff	Erklärung
Akte	Jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist. (Quelle: §3 Abs. 6 DSG NRW)
Akteur	Urheber einer Handlung; neben natürlichen und juristischen Personen können auch Rollen oder Funktionen als Akteur agieren.
Angriff	Versuch, einen Wert zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff auf ihn zu erlangen oder ihn ohne Berechtigung zu nutzen. (Quelle: DIN ISO IEC 27000)
Anonymisieren	Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. (Quelle: §3 Abs. 6 BDSG)
Archiv, elektronisches	siehe „Elektronisches Archiv“
Audit	Systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Audit-Trail	Chronologische Aufzeichnung der Aktivitäten von Nutzern eines Informationssystems, die die getreue Wiederherstellung früherer Zustände der betreffenden Informationen ermöglicht. (Quelle: DIN CEN ISO/TS 14265)
Auftragsdatenverarbeitung	ist die (→) Datenverarbeitung personenbezogener Daten durch einen Auftragnehmer im Auftrag und nach ausdrücklicher Weisung eines Auftraggebers
Aufzeichnung	Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt. (Quelle: DIN ISO IEC 27000)
Ausdrückliche Zustimmung	Genehmigung, die aus freien Stücken und unmittelbar gegeben und entweder mündlich oder schriftlich zum Ausdruck gebracht wird (Quelle: DIN CEN ISO/TS 14265)
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. (Quelle: DIN EN ISO 22600-1)
Authentisierung, starke	siehe „starke Authentisierung“
Authentizität	Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt. (Quelle: DIN ISO IEC 27000)
Automatisierte Datenverarbeitung	Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. (Quelle: §3 Abs. 2 BDSG)

Begriff	Erklärung
Autorisierung	Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen. (Quelle: DIN EN ISO 22600-1)
Bedrohung	Möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden des Systems oder der Institution führen kann. (Quelle: DIN ISO IEC 27000)
Beschäftigte	Beschäftigte sind: 1. Arbeitnehmerinnen und Arbeitnehmer, 2. zu ihrer Berufsbildung Beschäftigte, 3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden), 4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte, 5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte, 6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten, 7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, 8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende (Quelle: §3 Abs. 11 BDSG)
Betroffener	eine bestimmte oder bestimmbare natürliche Person (Quelle: §3 Abs. 1 BDSG)
Daten, personenbezogene	siehe „Personenbezogene Daten“
Datenbearbeiter	jegliche Personen (andere als die Mitarbeiter des Datenbeauftragten), die die Daten im Auftrag des Datenbeauftragten bearbeiten (Quelle: DIN EN 15713)
Datenbeauftragter (controller)	Person, die (entweder alleine oder gemeinsam mit anderen Personen) die Verwendungszwecke der Daten und die Art und Weise, in der personenbezogene Daten bearbeitet werden oder bearbeitet werden sollen, festlegt. (Quelle: DIN EN 15713)
Datenintegrität	Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind. (Quelle: DIN EN ISO 27799)
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)
Datennutzung	Handhabung von oder Umgang mit Informationen für einen spezifischen Zweck. (Quelle: DIN CEN ISO/TS 14265)
Datenschutz	Festgelegte technische und soziale Vorgehensweise für die Verhandlung, Verwaltung und Sicherstellung von Geheimhaltung, Vertraulichkeit und Sicherheit von Informationen (Quelle: DIN CEN ISO/TS 14265)

Begriff	Erklärung
Datenschutzkontrolle	Technische und organisatorische Maßnahmen, die dazu dienen, Risiken zu minimieren, die zu Datenschutzverletzungen führen könnten (Quelle: DIN CEN ISO/TS 14265)
Datenschutzpolitik	Festlegung von Zielen, Regeln, Pflichten und Datenschutzkontrollen im Hinblick auf die Verarbeitung von persönlichen Gesundheitsinformationen in einer bestimmten Umgebung (Quelle: DIN CEN ISO/TS 14265)
Datenschutzverletzung	Situation, in der Daten einer Person auf illegale Weise oder unter Verletzung einer oder mehrerer relevanter Datenschutzbestimmungen verarbeitet wurde (Quelle: DIN CEN ISO/TS 14265)
Datenschutzvorgaben	Ausdrückliche oder stillschweigende Entscheidungen einer Einzelperson darüber, wie ihre Daten verarbeitet werden sollen (Quelle: DIN CEN ISO/TS 14265)
Datenverarbeiter (processor)	jegliche Personen (andere als die Mitarbeiter des Datenbeauftragten), die die Daten im Auftrag des Datenbeauftragten bearbeiten (Quelle: DIN EN 15713)
Datenverarbeitung	Datenverarbeitung ist das Erheben, Verarbeiten sowie Nutzen personenbezogener Daten. Im Einzelnen ist – Erheben ist das Beschaffen von Daten über den Betroffenen (Quelle: §3 Abs. 3 BDSG) – Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung (Quelle: §3 Abs. 4 Ziff. 1 BDSG) – Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter personenbezogener Daten (Quelle: §3 Abs. 4 Ziff. 2 BDSG) – Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft, (Quelle: §3 Abs. 4 Ziff. 3 BDSG) – Sperren (Sperrung) das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken (Quelle: §3 Abs. 4 Ziff. 4 BDSG) – Löschen (Löschung) das Unkenntlichmachen gespeicherter personenbezogener Daten (Quelle: §3 Abs. 4 Ziff. 5 BDSG) – Nutzen (Nutzung) ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (Quelle: §3 Abs. 5 BDSG)
Datenverarbeitung im Auftrag	siehe „Auftragsdatenverarbeitung“

Begriff	Erklärung
Datenverarbeitung, automatisierte	siehe „Automatisierte Datenverarbeitung“
Datenverwendung	Handhabung von oder Umgang mit Informationen für einen spezifischen Zweck. (Quelle: DIN CEN ISO/TS 14265)
Datum, personenbezogenes	siehe „Personenbezogenes Datum“
Delegierung	Übertragung eines Privilegs von einer Entität, die dieses Privileg besitzt, auf eine andere Entität (Quelle: DIN EN ISO 22600-1)
Dokument	a) als Einheit gehandhabte Zusammenfassung oder Zusammenstellung von Informationen, die nicht-flüchtig auf einem Informationsträger gespeichert sind b) festgelegte und strukturierte Menge von Informationen, die als Einheit verwaltet und zwischen Anwendern und Systemen ausgetauscht werden kann (Quelle: DIN 06789)
Dritter	jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. (Quelle: §3 Abs. 8 BDSG)
Drittland	Land, welches nicht an die gesetzlichen Anforderungen der EU-Datenschutz-Direktive gebunden ist (Land außerhalb des EWR) (Quelle: DIN EN 14484)
Drittland, sicheres	siehe „Sicheres Drittland“
Effizienz	Beziehung zwischen den erzielten Ergebnissen und dem Grad der Nutzung der Ressourcen (Quelle: DIN ISO IEC 27000)
Einhaltung	Handlung, die erforderlich ist, um eine festgelegte Anforderung zu erfüllen (Quelle: DIN CEN ISO/TS 14441)
Einwilligung	Handlung, etwas zu genehmigen, das einen betrifft; im Sinne des Datenschutzrechts eine auf freier Entscheidung beruhende Genehmigung des Betroffenen zur Verarbeitung der der betroffenen Person zuordenbaren Daten
Elektronisches Archiv	Sammlung von Dokumenten in einem Speicher für historische Zwecke oder als Sicherungsmaßnahme. (Quelle: DIN 06789)
Empfänger	jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle (Quelle: §3 Abs. 8 BDSG)
Entität	natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Entpersonalisierung	allgemeine Bezeichnung für jeden Prozess, bei dem der Bezug eines identifizierenden Datensatzes auf die betreffende Person aufgehoben wird (Quelle: DIN CEN ISO/TS 14265)

Begriff	Erklärung
Ereignis	Auftreten von ungewöhnlichen Umständen (Quelle: DIN ISO IEC 27000)
Freigabe	a) eine bestimmten Anweisungen entsprechende Genehmigung nach abgeschlossener Prüfung b) formelle Aktion einer autorisierten Person/Organisation, mit der ein Dokument für einen deklarierten Zweck im Prozessablauf gültig erklärt wird (Quelle: DIN 06789)
Geheimhaltung	Verhinderung des Eindringens in das Privatleben oder die Angelegenheiten einer Person, sofern dieses Eindringen aus der unzulässigen oder illegalen Erfassung und Nutzung von Daten über diese Person resultiert. (Quelle: DIN CEN ISO/TS 14265)
Genehmigung	Bestätigung einer autorisierten Person/Organisation, dass etwas zuvor festgelegten Anforderungen entspricht. (Quelle: DIN 06789)
Gesundheitsinformationen, persönliche (personal health information, PHI)	siehe „Persönliche Gesundheitsinformationen“
Gesundheits-Informations-System	Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen, in einer von Computern zu verarbeitenden Form, sicher gespeichert und übermittelt sowie zugänglich für mehrere autorisierte Benutzer. (Quelle: DIN CEN ISO/TS 14441)
Identifikation	Erkennung einer Person in einem bestimmten Bereich mithilfe einer Reihe ihrer Attribute. (Quelle: DIN CEN ISO/TS 14441)
Identifizierbare Person	Person, die direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind. (Quelle: DIN EN 14484)
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen. (Quelle: DIN EN ISO 22600-1)
Identitätsdaten	Identitätsdaten sind (u.a.): – Familiennamen, Vornamen, Geburtsnamen, frühere Namen und Titel – Geburtstag (Tag im Geburtsmonat), Monat und Jahr der Geburt – Straße und Hausnummer der Wohnanschrift zum Zeitpunkt der Meldung. – Geschlecht – Postleitzahl und Wohnort zum Zeitpunkt der Erkrankung/Meldung – Tag, Monat und Jahr Diagnose – Tag, Monat und Jahr des Todes. (Quelle: §3 Abs. 2,3 KRG NRW)
Informationen, klinische	siehe „klinische Informationen“

Begriff	Erklärung
Informationssicherheits-Ereignis	Erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die Leitlinie zur Informationssicherheit, das Versagen von Maßnahmen oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt. (Quelle: DIN ISO IEC 27000)
Informationssicherheits-Risiko	Möglichkeit, dass eine vorhandene Bedrohung die eine Schwachstelle eines Wertes oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte. (Quelle: DIN ISO IEC 27000)
Informationssicherheits-Vorfall	einzelnes oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheits-Ereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird. (Quelle: DIN ISO IEC 27000)
Informationswert	Wissen oder Daten, die von Wert für die Institution sind (Quelle: DIN ISO IEC 27000)
Inspektion	Untersuchung der Entwicklungs- und Konstruktionsunterlagen eines Produktes, eines Prozesses oder einer Anlage und Ermittlung seiner/ihrer Konformität mit spezifischen Anforderungen oder, auf der Grundlage einer sachverständigen Beurteilung, mit allgemeinen Anforderungen. (Quelle: DIN ISO IEC 27000)
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert wird. (Quelle: DIN EN ISO 22600-2)
Klinische Informationen	Informationen über eine Person, die für deren Gesundheit oder Gesundheitsversorgung von Bedeutung sind. (Quelle: DIN CEN ISO/TS 14265)
Konformitätsbewertung	Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Korrekturmaßnahme	Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation. (Quelle: DIN ISO IEC 27000)
Leitlinie	Vom Management formell ausgedrückte Gesamtintention und -richtung (Quelle: DIN ISO IEC 27000)
Maßnahme	Mittel zum Management von Risiken, einschließlich von Leitlinien, Verfahren, Richtlinien, Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können. (Quelle: DIN ISO IEC 27000)
Maßnahmenziel	Beschreibung, was durch die Umsetzung von Maßnahmen als Ergebnis erreicht werden soll. (Quelle: DIN ISO IEC 27000)

Begriff	Erklärung
Mobile Datenträger	Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger, 1. die an den Betroffenen ausgegeben werden, 2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und 3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann. (Quelle: §3 Abs. 10 BDSG)
Nicht-Abstreitbarkeit	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden. (Quelle: DIN ISO IEC 27000)
Notfallzugriff	Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen. (Quelle: DIN CEN ISO/TS 14265)
Offenlegung	Preisgabe von Daten an Personen, die nicht routinemäßig über die entsprechende Berechtigung verfügen. (Quelle: DIN CEN ISO/TS 14265)
Person, identifizierbare	siehe „Identifizierbare Person“
Personenbezogene Daten	Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Quelle: §3 Abs. 1 BDSG)
Persönliche Gesundheitsinformationen (personal health information, PHI)	Informationen über eine identifizierbare Person, die sich auf den körperlichen oder geistigen Gesundheitszustand der betreffenden Person oder auf die Erbringung von Gesundheitsdienstleistungen für die betreffende Person beziehen. (Quelle: DIN CEN ISO/TS 14441)
Policy	Menge von gesetzlichen, politischen, organisatorischen, funktionellen und technischen Verpflichtungen, die sich auf Kommunikation und Kooperation beziehen. (Quelle: DIN EN ISO 22600-1)
Policy-Vereinbarung	schriftliche Vereinbarung, nach der sich alle Beteiligten zur Einhaltung einer festgelegten Reihe von Policies verpflichten. (Quelle: DIN EN ISO 22600-1)
Privileg	Kapazität, die einer Entität von einer Behörde entsprechend dem Attribut dieser Entität zugewiesen wird. (Quelle: DIN EN ISO 22600-1)
Prozess	Satz von in Wechselbeziehung oder -wirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt. (Quelle: DIN ISO IEC 27000)

Begriff	Erklärung
Pseudonymisieren	Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. (Quelle: §3 Abs. 3a BDSG)
Psychische Krankheiten	Behandlungsbedürftige Psychosen sowie andere behandlungsbedürftige psychische Störungen und Abhängigkeitserkrankungen von vergleichbarer Schwere (Quelle: §1 Abs. 2 PsychKG NRW)
Restrisiko	Nach der Risikobehandlung verbleibende Risiko (Quelle: DIN ISO IEC 27001)
Revisionssicherheit	Der Begriff „Revisionssicherheit“ bezieht sich die Anforderungen a) des Handelsgesetzbuches (§§ 239, 257 HGB) b) der Abgabenordnung (§§ 146, 147 AO), c) der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) d) ... d. h., auf praktisch ausnahmslos steuerrechtliche bzw. handelsrechtliche Vorgaben. Andere gesetzlichen Vorgaben werden hierbei nicht beachtet. Die revisionssichere Archivierung ist nur ein Bestandteil der rechtsicheren Archivierung. So beinhaltet eine revisionssichere Archivierung beispielsweise keine datenschutzrechtlichen Vorgaben, z. B. bzgl. des Zugriffs auf die archivierten Daten. Hingegen beinhaltet eine revisions- und rechtssichere Archivierung auch alle rechtlichen Anforderungen.
Richtlinie	Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen (Quelle: DIN ISO IEC 27000)
Richtlinienvereinbarung	schriftliche Vereinbarung, mit der sich alle beteiligten Parteien zur Einhaltung einer festgelegten Reihe von Richtlinien verpflichten (Quelle: DIN CEN ISO/TS 14265)
Risiko	Kombination aus der Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen (Quelle: DIN ISO IEC 27000)
Risikoakzeptanz	Entscheidung, ein Risiko zu akzeptieren (Quelle: DIN ISO IEC 27000)
Risikoanalyse	systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos (Quelle: DIN ISO IEC 27000)
Risikobehandlung	Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos (Quelle: DIN ISO IEC 27000)
Risikobestimmung	Tätigkeit, bei der der Wahrscheinlichkeit und den Auswirkungen eines Risikos Werte zugeordnet werden (Quelle: DIN ISO IEC 27000)
Risikobewertung	Prozess, in dem das eingeschätzte Risiko mit den festgelegten Risikokriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen (Quelle:) DIN ISO IEC 27000

Begriff	Erklärung
Risikoeinschätzung	gesamter Prozess der Risikoanalyse und Risikobewertung (Quelle: DIN ISO IEC 27000)
Risikokommunikation	Austausch oder gemeinsame Nutzung von Informationen über Risiken zwischen Entscheidungsträgern und anderen Stakeholdern (Quelle: DIN ISO IEC 27000)
Risikokriterien	Bezugsrahmen für die Einschätzung der Bedeutung eines Risikos (Quelle: DIN ISO IEC 27000)
Risikomanagement	koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution in Bezug auf Risiken (Quelle: DIN ISO IEC 27000)
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen (Quelle: DIN EN ISO 22600-1)
Schlüssel	Symbolfolge, die die Verschlüsselungs- und Entschlüsselungsoperationen steuert (Quelle: DIN EN ISO 22600-1)
Schlüssel, öffentlicher	Schlüssel, der mit einem asymmetrischen Verschlüsselungsalgorithmus verwendet wird und öffentlich zugänglich gemacht werden kann (Quelle: DIN EN ISO 22600-1)
Schlüssel, privater	Schlüssel, der sich im Besitz einer begrenzten Anzahl von Entitäten (in der Regel nur einer Entität) befindet und mit einem asymmetrischen Verschlüsselungsalgorithmus verwendet wird (Quelle: DIN EN ISO 22600-1)
Schwachstelle	Schwäche eines Werts oder einer Maßnahme, die von einer Bedrohung ausgenutzt werden kann (Quelle: DIN ISO IEC 27000)
Sensibilität	Eigenschaft einer Ressource, die deren Wert oder Wichtigkeit impliziert (Quelle: DIN EN ISO 22600-2)
Schreddern	mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe (Quelle: DIN EN 15713)
Sicheres Drittland	Land, dessen Gesetzgebung den Anforderungen der EU-Datenschutz-Direktive entspricht und dessen Datenschutzniveau von der Europäischen Kommission als angemessen erkannt wurde (Quelle: DIN EN 14485)
Sicherheit	Kombination von Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit (Quelle: DIN EN ISO 22600-1)
Sicherheitsdienst	Dienst, der von einer Schicht miteinander kommunizierender offener Systeme bereitgestellt wird und die Sicherheit der Systeme oder der Datenübertragung in angemessenem Maße sicherstellt (Quelle: DIN EN ISO 22600-1)
Sicherheits-Policy	Plan oder Vorgehensweise für die Sicherstellung der Rechnersicherheit (Quelle: DIN EN ISO 22600-1)
Signaturen, elektronische	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind, und die zur Authentifizierung dienen (Quelle: §2 Abs.1 SigG)

Begriff	Erklärung
Starke Authentisierung	Authentisierung mittels kryptographisch abgeleiteter multifaktorieller Identitätsnachweise. (Quelle: DIN EN ISO 22600-1)
Stelle, verantwortliche	siehe „Verantwortliche Stelle“
Stillschweigende Zustimmung	freiwilliges Einverständnis mit dem, was getan oder vorgeschlagen wird, das sich in vernünftigem Rahmen aus den Handlungen oder Unterlassungen der betreffenden Person ableiten lässt (Quelle: DIN CEN ISO/TS 14265)
Systemintegrität	Eigenschaft, dass ein System seine vorgesehene Funktion in einer unbeeinträchtigten Art und Weise, frei von vorsätzlicher oder zufälliger unberechtigter Veränderung des Systems ausführt (Quelle: DIN EN ISO 27799)
Unleugbarkeit	Dienstleistung, die einen Nachweis für die Integrität und die Herkunft der Daten (beides auf fälschungssichere Art und Weise) erbringt, der von einer beliebigen anderen Partei verifiziert werden kann (Quelle: DIN EN ISO 22600-2)
Unterlagen	Urkunden, Amtsbücher, Akten, Schriftstücke, amtliche Publikationen, Karteien, Karten, Risse, Pläne, Plakate, Siegel, Bild-, Film- und Tondokumente und alle anderen, auch elektronischen Aufzeichnungen, unabhängig von ihrer Speicherungsform, sowie alle Hilfsmittel und ergänzenden Daten, die für die Erhaltung, das Verständnis dieser Informationen und deren Nutzung notwendig sind. (Quelle: §2 Abs. 1 ArchivG NRW)
Verantwortliche Stelle	jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (Quelle: §3 Abs. 7 BDSG)
Verarbeitung	Erfassung, Aufzeichnung, Aufbewahrung, Änderung, Abruf, Löschung oder Offenlegung von Daten (Quelle: DIN CEN ISO/TS 14265)
Verfahren	festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: DIN ISO IEC 27000)
Verfälschung	unzulässige Änderung des Inhaltes eines Dokumentes nach dessen Freigabe (Quelle: DIN 06789)
Verfügbarkeit	Eigenschaft, auf Anforderung einer autorisierten Entität zugänglich und nutzbar zu sein (Quelle: DIN EN ISO 22600-1)
Verlässlichkeit	Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen (Quelle: DIN ISO IEC 27000)
Vernichtung	Reduzierung der Größe, wodurch die Unterlagen so weit wie möglich unlesbar, unleserlich und nicht rekonstruierbar gemacht werden (Quelle: DIN EN 15713)
Vertrauen	im Allgemeinen kann davon ausgegangen werden, dass eine Entität einer anderen Entität „vertraut“, wenn sie annehmen kann, dass sich die zweite Entität genauso, wie von der ersten Entität erwartet, verhalten wird (Quelle: DIN EN ISO 22600-2)

Begriff	Erklärung
Vertraulichkeit	Eigenschaft, die dazu führt, dass die betreffende(n) Information(en) keinen Personen, Entitäten oder Prozessen, die nicht über die entsprechende Autorisation verfügen, verfügbar gemacht oder diesen gegenüber offengelegt wird (Quelle: DIN EN ISO 22600-1)
Vorbeugungsmaßnahme	Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation (Quelle: DIN ISO IEC 27000)
Weisung	Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).
Wert	ist wiederum definiert als „alles, was für die Institution von Wert ist“ (Quelle: DIN ISO IEC 27000)
Wirksamkeit	Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden (Quelle: DIN ISO IEC 27000)
Zeitstempel	Nicht personengebundene elektronische Signatur-Methode (Quelle: DIN 06789)
Zeitstempel, qualifizierte	Elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben (Quelle: §2 Abs.14 SigG)
Zerfasern	Mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe auf mechanische Weise, kleinere Größen als mittels Schreddern erreichbar (Quelle: DIN EN 15713)
Zertifikatsaussteller	Institution, die von einer oder mehreren vertrauenden Parteien als vertrauenswürdig erachtet wird, um Zertifikate erstellen, zuweisen und verwalten zu können. Wahlweise darf die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen (Quelle: in Anlehnung an DIN EN ISO 22600-1)
Zertifizierung	Bestätigung durch eine dritte Stelle bezogen auf Produkte, Prozesse, Systeme oder Personen (Quelle: DIN CEN ISO/TS 14441)
Zertifizierungsstelle	Institution, die von einer oder mehreren vertrauenden Parteien als vertrauenswürdig erachtet wird, um Zertifikate erstellen, zuweisen und verwalten zu können. Wahlweise darf die Zertifizierungsstelle die Schlüssel der vertrauenden Parteien erzeugen (Quelle: Anlehnung an DIN EN ISO 22600-1)
Ziel	Ressource, auf die von einem Anwärter zugegriffen wird (Quelle: DIN EN ISO 22600-1)

Begriff	Erklärung
Zugriffskontrolle	Verhinderung der unbefugten Nutzung einer Ressource einschließlich Verhinderung der Nutzung einer Ressource auf nicht autorisierte Art und Weise (Quelle: DIN CEN ISO/TS 14265)
Zugriffssteuerung	Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können (Quelle: DIN EN ISO 22600-1)
Zurechenbarkeit	Eigenschaft, durch die sichergestellt wird, dass die Aktionen einer Entität eindeutig auf diese zurückgeführt werden können (Quelle: DIN EN ISO 22600-1)
Zustimmung	Von einer Person aus freien Stücken erteilte spezifische und informierte Genehmigung zur Verarbeitung von diese Person betreffenden persönlichen Daten (Quelle: DIN CEN ISO/TS 14265)
Zustimmung, ausdrückliche	siehe „ausdrückliche Zustimmung“
Zustimmung, stillschweigende	siehe „stillschweigende Zustimmung“

3 Akteure

3.1 Juristische und natürliche Personen

Akteur	Beschreibung
Angreifer	Person, die versucht, mögliche Schwachstellen eines biometrischen Systems auszunutzen (Quelle: DIN EN ISO 25237)
Anwender	Person, die ein Gerät oder eine Software verwendet
Aufsichtsbehörde	eine von einem Mitgliedstaat gemäß Artikel 51 DS-GVO eingerichtete unabhängige staatliche Stelle (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Auftragsverarbeiter	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Bediener	Siehe „Anwender“
Betroffene/Betroffener	Siehe „Person, betroffene“
Datenschutzbeauftragte/ Datenschutzbeauftragter	Natürliche Person, die auf die Einhaltung des Datenschutzes im Unternehmen hinwirken soll
Datenschutzkoordinator	Natürliche Person, welche über eine Basisausbildung im Datenschutz verfügt und vom Datenschutzbeauftragten delegierte Teilaufgaben abarbeitet
Datensubjekt	behandelte Person (Quelle: DIN CEN ISO/TS 14441)
Dritter	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Empfänger	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. (Quelle: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Entität	natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Heilberufler	Person, die von einer anerkannten Stelle autorisiert ist, zur Erbringung gewisser medizinischer Dienstleistungen qualifiziert zu sein (Quelle: DIN CEN ISO/TS 14441)

Akteur	Beschreibung
Hersteller	natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung oder Kennzeichnung eines Medizinprodukts, für den Zusammenbau eines Systems oder für die Anpassung eines Medizinprodukts vor dem Inverkehrbringen oder der Inbetriebnahme verantwortlich ist, unabhängig davon, ob diese Tätigkeiten von dieser Person selbst oder stellvertretend für diese von einer dritten Person ausgeführt werden (Quelle: DIN EN ISO 14971)
Maßnahmenverantwortlicher	Verantwortlicher zur Umsetzung einer oder mehrerer Maßnahme(n)
Patient	eine oder mehrere Personen, die terminlich eingeplant sind, eine Leistung des Gesundheitswesens zu erhalten, diese gerade erhalten oder diese bereits erhalten haben (Quelle: DIN CEN ISO/TS 14441)
Person, behandelte	Siehe „Patient“
Person, betroffene	Personen, auf die sich Daten beziehen (Quelle: DIN EN ISO 25237)
Person, identifizierbare	jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind (Quelle: DIN CEN ISO/TS 14441)
Risikoinhaber	Verantwortlicher zur Verwaltung und Beobachtung eines Risikos
Unternehmen	natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Verantwortlicher (für die Verarbeitung)	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 (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Vertreter	eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))

3.2 Nicht-Personen

Akteur	Beschreibung
Anwendungssystem	System bestehend aus Hardware und Anwendungssoftware zur Unterstützung definierter Aufgaben
Archiv, digitales	Informationssystem und Strategie, welche den Erhalt und die Verfügbarkeit von Informationen in digitaler Form bei bestimmungsgemäßen Gebrauch gewährleistet
Arzneimittelinformationssystem	Softwarelösung, welche umfangreiche Informationen zu Arzneimitteln bereitstellt

Akteur	Beschreibung
Arzt-Informations-System	Softwarelösung für die Unterstützung der in einer Arztpraxis anfallenden Geschäftsprozesse
Arztpraxisinformationssystem	Ein oder mehrere Informationssysteme zur Erhebung und Speicherung sowie Bereitstellung von in einer Arztpraxis anfallenden Daten eines Patienten
Dokumenten-Management-System	Softwarelösung für das Management von digitalen Dokumenten (Erfassen, Strukturieren, Speichern, Bereitstellen)
Gesundheitsinformationssystem	Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen; die in einer von Computern zu verarbeitenden Form sicher gespeichert und zugänglich für mehrere autorisierte Benutzer dargestellt werden (Quelle: DIN CEN ISO/TS 14441)
Hospital Information System	Siehe „Krankenhaus-Informationssystem“
Kommunikationsserver	Softwarelösung um Empfang und zur Verteilung von digitalen Nachrichten zwischen verschiedenen Informationssystemen wie bspw. KIS, RIS, LIS
Krankenhaus-Informationssystem	Gesamtheit aller in einem Krankenhaus eingesetzten informationstechnischen Systeme zur Verwaltung und Dokumentation elektronischer Patientendaten. Dabei handelt es sich in aller Regel um einen Verbund selbständiger Systeme meist unterschiedlicher Hersteller. Auf einzelne Fachbereiche beschränkte Verfahren wie z. B. Labor-, Radiologie- oder Diagnosesysteme gehören als Subsysteme ebenfalls zum Krankenhausinformationssystem (Quelle OH KIS, 2. Fassung Stand März 2014)
Labor-Informationssystem	Softwarelösung für die Unterstützung der in einem Labor anfallenden Geschäftsprozesse
Medizinprodukt	Entsprechend EU Richtlinie 93/42/EWG Art. 1 Abs.2 lit. a[15]
Modalität	Gerät zur Erzeugung medizinischer Bilddaten
Patientendatenmanagementsystem	Softwarelösung, welche in Krankenhäusern die patientenbezogenen Informationen erfasst, speichert und zugänglich für mehrere autorisierte Benutzer darstellt
Picture Archiving and Communication System	Softwarelösung, welche den Erhalt und die Verfügbarkeit von medizinischen Bilddaten gewährleistet
Point-Of-Service-System	System, das an der Versorgungsstelle bei der Erbringung klinischer Dienstleistungen gegenüber der behandelten Person verwendet wird (Quelle: DIN CEN ISO/TS 14441)
Radiologisches Informationssystem	Softwarelösung für die Unterstützung der in der Radiologie anfallenden Geschäftsprozesse

[15] Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte. [Online, zitiert am 2016-09-01]; Verfügbar unter http://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:31993L0042

4 Risikobewertung

4.1 Warum eine Risikobewertung?

Die europäische Datenschutzgrundverordnung fordert in verschiedenen Artikeln eine Risikobetrachtung und -bewertung. Z. B.: muss laut Art. 35 Abs. 7 lit. c DS-GVO in der Datenschutz-Folgenabschätzung „eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen“ integriert sein, wobei Art. 25 Abs. 1 DS-GVO referenziert wird., d. h. Risiken „für die Rechte und Freiheiten natürlicher Personen“ müssen betrachtet werden. Ebenso sieht es in anderen Bereichen der DS-GVO aus, beispielsweise:

- Gemäß Art. 24 Abs. 1 DS-GVO muss der Verantwortliche „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen“ entsprechende geeignete technische und organisatorische Maßnahmen ergreifen.
- Entsprechend Artt. 25 Abs. 1, Art. 32 Abs. 1 DS-GVO ist es zwingend erforderlich, „Risiken für die Rechte und Freiheiten natürlicher Personen“ zu bewerten, um darzustellen, welche Mittel entsprechend dem Stand der Technik zum Schutz anzuwenden sind.
- Laut Art. 32 Abs. 2 DS-GVO muss bei der Beurteilung des angemessenen Schutzniveaus die Risiken für die Rechte und Freiheiten natürlicher Personen beachtet werden.
- Die Meldepflichten referenzieren u.a. die vorhandenen Risiken für die Rechte und Freiheiten natürlicher Personen bzgl. der Entscheidung, ob ein Vorfall gemeldet werden muss /Artt. 33,34 DS-GVO).
- Bei einer Übermittlung in Drittstaaten gemäß Art. 49 DS-GVO muss die/der Betroffene über die Risiken aufgeklärt werden.

Damit ergibt sich die Notwendigkeit, eine Risikobewertung bzgl. der Verarbeitung personenbezogener Daten aufzustellen. Dazu müssen natürlich zunächst einmal die Risiken für „Rechte und Freiheiten natürlicher Personen“ benannt werden.

In Deutschland werden bisher überwiegend materielle Risiken (Finanzen, Gesundheit, ...) benannt, was u.a. an unserer zivilrechtlichen Rechtsprechung bzgl. Haftung liegt. Europarechtlich sind aber auch immaterielle Risiken zu betrachten. Die folgenden Kapitel sollen helfen, diese Thematik für die eigenen Fragestellungen zu behandeln.

4.2 Welche Risiken sollten immer betrachtet werden?

In seiner Dissertation[16] erarbeitete Herr Drackert eine Kategorisierung der Risiken, die bei einer Verarbeitung personenbezogener Daten auftreten können.

1. Strukturelle Risiken
   a. Gesellschaftlich-politische Risiken
      i. Informationsmacht
      ii. Konformistische Verhaltensanpassung durch Überwachungsdruck
      iii. Verantwortungsnegation
   b. Wirtschaftliche Risiken
      i. Handelshemmnisse
      ii. Nachfragerückgang durch Vertrauensverlust

[16] 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

2. Individuelle Risiken
    a. Erhöhung individueller Verletzlichkeit für Straftaten
    b. Schamgefühl und Publizitätsschäden
    c. Selektivitätsschäden
        i. Diskriminierung
        ii. Stigmatisierung
    d. Informationspermanenz
    e. Entkontextualisierung
        i. Kontextdefizit
        ii. Kontextinfiltration
    f. 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

4.3 Risikobewertung

Hierzu müssen drei Schritte absolviert werden:

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

4.3.1 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

4.3.2 Schadensklassifikation

Definitionen des Schweregrads:

Katastrophal:	Führt zum Tod der Patientin/des Patienten
Kritisch:	Führt zu dauernder Behinderung oder einer lebensbedrohlichen Schädigung
Ernst:	Führt zu einer Schädigung oder Behinderung, die ein sachkundiges medizinisches Eingreifen erfordert

Gering: Führt zu einer zeitweiligen Schädigung oder Behinderung, die kein sachkundiges medizinisches Eingreifen erfordert

Vernachlässigbar: Unannehmlichkeiten oder zeitweilige Beschwerden

4.3.3 Risikoklassifizierung

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

Potentielles 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 Publizitätsschäden		
	Selektivitätsschäden		
	Diskriminierung		
	Stigmatisierung		
	Informationspermanenz		
	Entkontextualisierung		
	Kontextdefizit		
	Kontextinfiltration		
	Informationsemergenz		
	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 Feststellung des Schutzbedarfs

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erläutert in Kapitel 4.3 im BSI-Standard 100-2[17] das Vorgehen bei einer Schutzbedarfsfeststellung. Daher werden hier nur einige allgemeine Hinweise bzgl. des Vorgehens gegeben, nähere Einzelheiten sind in der Ausarbeitung des BSI zu finden.

Zur Schutzbedarfsanalyse müssen folgende Schritte vollzogen werden:

1) Definition der Schutzbedarfskategorien
2) Schutzbedarfsfeststellung für Anwendungen
3) Schutzbedarfsfeststellung für IT-Systeme
4) Schutzbedarfsfeststellung für Räume
5) Schutzbedarfsfeststellung für Kommunikationsverbindungen
6) Schlussfolgerungen aus den Ergebnissen 2) bis 5).

Die Definition der Schutzbedarfskategorien muss auf die eigenen Bedürfnisse erfolgen. Begrifflichkeiten wie „normal“, „hoch“ und „sehr hoch“ werden zwar universell eingesetzt, die Bedeutung, was unter „normal“ und den anderen allgemeinen Begrifflichkeiten im Einzelfall zu verstehen ist, kann aber nur im jeweiligen Einzelfall definiert werden.

Zu betrachtende Schadensszenarien bedingen natürlich auch die Betrachtung evtl. Verstöße gegen Gesetze und Verordnungen und daraus resultierende Schäden wie Bußgelder oder andere Haftungsfolgen. Andererseits müssen natürlich auch die Folgen evtl. auftretender negativer Innen- und/oder Außenwirkung betrachtet werden, aus denen Schaden erwachsen kann, z. B. durch verlorene Kundinnen und Kunden. Je nach erfolgter Verarbeitung kann für Betroffene auch eine Beeinträchtigung der körperlichen oder seelischen Unversehrtheit mit entsprechendem Schadensersatzanspruch resultieren. Letztlich muss also auch bei der Betrachtung eines potentiellen Schadens der jeweilige Einzelfall betrachtet werden. Die Schadensszenarien sind letztlich auch Ergebnisse der Risikobewertung (siehe entsprechendes Kapitel auf Seite 45).

Sind Schutzbedarfskategorien definiert und potentielle Schadensszenarien identifiziert erfolgt die Schutzbedarfsfeststellung für die jeweils potentiell bedrohten Ressourcen. Auch hierzu finden sich in der Ausarbeitung des BSI Beispiele.

Ist der Schutzbedarf festgestellt, so resultiert daraus als Ergebnis, welche Ressource gegen welche Bedrohung zu schützen ist. Idealerweise lassen sich aus der Identifikation des Risikos auch direkt Maßnahmen zum Schutz der Ressource ableite. Dies ist aber nicht immer der Fall, sodass hier ggf. auch externes Wissen zur Risikominimierung eingekauft werden muss.

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. [Online, zitiert am 2016-09-27]; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile

6 Abkürzungsverzeichnis

Abs	Absatz
AIS	Arzt-Informations-System
AMIS	Arzneimittelinformationssystem
AMTS	Arzneimitteltherapiesicherheit
Art	Artikel
Artt	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
DB	Datenbank
DBMS	Datenbankmanagementsystem
DIN	Deutsche Institut für Normung e. V.
DMS	Dokumentenmanagementsystem
DSG	Datenschutzgesetz
DS-GVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EFA	Elektronische Fallakte
EGA	Elektronische Gesundheitsakte
EPA	Elektronische Patientenakte
EU	Europäische Union
GDSG	Gesundheitsdatenschutzgesetz
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
HIS	Hospital Information System
HW	Hardware
IS	Informationssystem
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap	Kapitel
KAS	Klinisches Arbeitsplatzsystem
KIS	Krankenhaus-Informationssystem
KMU	Kleines, mittelständisches Unternehmen
LDSG	Landesdatenschutzgesetz
LIS	Labor-Informationssystem
lit	littera (lat. „Buchstabe“)
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
NRW	Nordrhein-Westfalen
PACS	Picture Archiving and Communication System
PDMS	Patientendatenmanagementsystem
RIS	Radiologisches Informationssystem
RZ	Rechenzentrum
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
SW	Software
TK	Telekommunikation(s-)
ZTG	ZTG Zentrum für Telematik und Telemedizin GmbH

7 Weiterführende Literatur

7.1 Empfehlungen

7.1.1 Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Bundesamt für Sicherheit in der Informationstechnik (2013) IT-Grundschutz-Kataloge: M 2.503 Aspekte eines Datenschutzkonzeptes. [Online, zitiert am 2015-12-09]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02503.html

7.1.2 Datenschutz-Aufsichtsbehörde

- Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015) Das Standard-Datenschutzmodell (SDM). [Online, zitiert am 2015-12-09]; Verfügbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Standard-Datenschutzmodell/Standard-Datenschutzmodell.php
- Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen (2006) Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes. [Online, zitiert am 2015-12-09]; Verfügbar unter https://ssl.bremen.de/datenschutz/sixcms/media.php/13/oh_Datenschutzkonzept.pdf
- Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen (2007) Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen. [Online, zitiert am 2015-12-09]; Verfügbar unter https://ssl.bremen.de/datenschutz/sixcms/media.php/13/datenloeschung.pdf
- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Standard-Datenschutzmodell. [Online, zitiert am 2016-02-08]; Verfügbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Standard-Datenschutzmodell/SDM-Handbuch_V09a.pdf

7.2 Normen

7.2.1 Allgemeine Datenschutz-Anforderungen

- DIN EN 14484: „Internationaler Austausch von unter die EU-Datenschutzrichtlinie fallenden persönlichen Gesundheitsdaten - Generelle Sicherheits-Statements“
- DIN EN 14485: „Anleitung zur Verwendung von persönlichen Gesundheitsdaten in internationalen Anwendungen vor dem Hintergrund der EU-Datenschutzrichtlinie“

7.2.2 Anonymisierung/Pseudonymisierung

- DIN EN ISO 25237: „Pseudonymisierung“

7.2.3 Archivierung

- DIN 6878-1: „Digitale Archivierung in der medizinischen Radiologie“, Teil 1: Allgemeine Anforderungen an die Archivierung von Bildern
- ISO 21547: „Archivierung elektronischer Gesundheitsakten“, Teil 1: Prinzipien und Anforderungen
- ISO 21548: „Archivierung elektronischer Gesundheitsakten“, - Teil 2: Leitlinien
- DIN 31644: „Kriterien für vertrauenswürdige digitale Langzeitarchive“
- DIN 31645: „Leitfaden zur Informationsübernahme in digitale Langzeitarchive“

7.2.4 Berechtigungsmanagement

- DIN EN 12251: „Sichere Nutzeridentifikation im Gesundheitswesen“, Management und Sicherheit für die Authentifizierung durch Passwörter
- ISO/TS 21298: „Funktionelle und strukturelle Rollen“
- DIN EN ISO 22600-1: „Privilegienmanagement und Zugriffssteuerung“, Teil 1: Übersicht und Policy-Management
- DIN EN ISO 22600-2: „Privilegienmanagement und Zugriffssteuerung“, Teil 2: Formale Modelle
- DIN EN ISO 22600-3: „Privilegienmanagement und Zugriffssteuerung“, Teil 3: Implementierungen
- ISO/IEC DIS 29146: „Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung“
- ISO/IEC 29146: „Security techniques - A framework for access management”

7.2.5 Datenschutzkonzept

- ISO/IEC 29100: „Rahmenwerk für Datenschutz“
- ISO/IEC 29101: „Rahmenwerk für Datenschutzarchitektur“

7.2.6 ID-Management

- ISO/IEC 24760-1: „Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement“, Teil 1: Terminologie und Konzept
- ISO/IEC 24760-2: „Sicherheitsverfahren - Ein Rahmenwerk für das Identitätsmanagement“, Teil 2: Referenzarchitektur und Anforderungen

7.2.7 IT-Sicherheit

- DIN EN 13606-4: „Kommunikation von Patientendaten in elektronischer Form“, Teil 4: Sicherheit
- DIN CEN/TS 16850; DIN SPEC 14001: „Leitfaden für das Sicherungsmanagement in Gesundheitseinrichtungen“
- DIN EN ISO 27799: „Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“
- DIN EN 61511-1: „Sicherheitstechnische Systeme für die Prozessindustrie“, Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware
- DIN EN 61511-2: „Sicherheitstechnische Systeme für die Prozessindustrie“, Teil 2: Informative Anleitungen zur Anwendung des Teils 1
- DIN EN 61511-3: „Sicherheitstechnische Systeme für die Prozessindustrie“, Teil 3: Informative Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel

7.2.8 Klassifikation

- DIN CEN ISO/TS 14265: „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“

7.2.9 Löschung

- DIN EN 15713: „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“
- DIN 66398: „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“
- DIN 66399-1: „Vernichten von Datenträgern“, Teil 1: Grundlagen und Begriffe
- DIN 66399-2: „Vernichten von Datenträgern“, Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern
- DIN 66399-3: „Vernichten von Datenträgern“, Teil 3: Prozess der Datenträgervernichtung

7.2.10 Patientenakte

- DIN EN ISO 10781: „Funktionales Modell für ein elektronisches Gesundheitsaktensystem (EHRS FM)“
- DIN CEN ISO 14441: „Sicherheits- und Datenschutzanforderungen für die Konformitätsprüfung von EGA-Systemen“
- ISO/TR 20514: „Elektronische Gesundheitsakte - Definition, Anwendungsbereich und Kontext“
- DIN EN ISO 21091: „Verzeichnisdienste für Anbieter, zu Behandelnde und andere Entitäten im Gesundheitswesen“
- DIN EN 61907: „Zuverlässigkeit von Kommunikationsnetzen“

7.2.11 Protokollierung

- DIN EN ISO 27789: „Audit-Trails für elektronische Gesundheitsakten“

7.2.12 Verschlüsselung

- ISO/TR 11636: „Dynamisch abrufbares virtuelles privates Netzwerk für die Informationsinfrastruktur im Gesundheitswesen“
- ISO/IEC 18033-1: „Verschlüsselungsalgorithmen“, Teil 1: Allgemeines Modell
- ISO/IEC 18033-2: „Verschlüsselungsalgorithmen“, Teil 2: Asymmetrische Chiffren
- ISO/IEC 18033-3: „Verschlüsselungsalgorithmen“, Teil 3: Blockziffern
- ISO/IEC 18033-4: „Verschlüsselungsalgorithmen“, Teil 4: Stromchiffren
- ISO/IEC 19772: „Authentifizierte Verschlüsselung“

7.2.13 Wartung/Fernwartung

- ISO/TR 11633-1: „Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen“, Teil 1: Anforderungen und Risikoanalyse
- ISO/TR 11633-2: „Informationssicherheitsmanagement für die Fernwartung für Medizinprodukte und Informationssysteme im Gesundheitswesen“, Teil 2: Implementierung eines ISMS

7.3 Zeitschriften

- Bedner M, Ackermann T. (2010) Schutzziele der IT-Sicherheit. DuD: 323-2010
- Bock K, Meissner S. (2012)Datenschutz-Schutzziele im Recht. DuD: 425-431
- Conrad I, Hausen D. (2011) Datenschutzgerechte Löschung personenbezogener Daten. ITRB: 35-40
- Dewitz A, Jürgens P. (2008)Zu viele Regeln im Sicherheitskonzept? DuD: 583-587
- Flieder K. (2008) Identity- und Access-Management mit EAI-Konzepten und -Technologien. DuD: 532-536
- Fraenkel R, Hammer V. (2007) Rechtliche Löschvorschriften. DuD: 899-904
- Greveler U, Wegener C. (2010) Ein Ansatz zur Umsetzung von Löschvorschriften mittels Verschlüsselung. DuD: 467-471
- Hammer V, Fraenkel R. (2007) Löschkonzept. DuD: 905-910
- Hammer V, Fraenkel R. (2011) Löschklassen - Standardisierte Fristen für die Löschung personenbezogener Daten. DuD: 890-895
- Katko P, Knöpfle K, Kirschner T (2014) Archivierung und Löschung von Daten - Unterschätzte Pflichten in der Praxis und ihre Umsetzung. ZD: 238-241
- Kühling J, Klar M. (2014) Löschpflichten vs. Datenaufbewahrung - Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten. ZD: 506-510

- Probst T. (2012) Generische Schutzmaßnahmen für Datenschutz-Schutzziele. DuD 36(6): 439-444
- Rost M, Bock K. (2011) Privacy By Design und die Neuen Schutzziele. DuD: 30-35
- Rost M, Pfitzmann A. (2009) Datenschutz-Schutzziele – revisited. DuD: 353-358
- Rost M. (2011) Datenschutz in 3D - Daten, Prozesse und Schutzziele in einem Modell. DuD: 351-354
- Thomsen S. (2006) Sicherheitskonzepte für den Datenschutz. DuD: 17-19