Austausch von Gesundheitsdaten - Datenschutzrechtliche Anforderungen an Datenaustauschplattformen im Gesundheitswesen

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

IHE Deutschland e.V.

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Inhaltsverzeichnis

Rechtliches

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Die Autoren sind größtenteils keine Juristen. Insofern können und dürfen sie keine rechtsverbindlichen Auskünfte geben. Daher ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen. Eine Haftung für die Angaben übernehmen die Autoren nicht. Insgesamt stellt diese Veröffentlichung keine Rechtsberatung dar und verfolgt ausschließlich den Zweck, bestimmte Aspekte anzusprechen und dafür zu sensibilisieren. Sie erhebt keinen Anspruch auf Vollständigkeit. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen für die jeweilige Situation anhand der geltenden rechtlichen Vorschriften geprüft und angepasst werden.

Urheber- und Kennzeichenrecht

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

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Stand der Bearbeitung ist 13. März 2016.

Copyright

Präambel

In der heutigen Zeit werden immer öfter Gesundheitsdaten über das Internet ausgetauscht. Häufig werden sowohl zur Erfassung wie auch zum Austausch der Gesundheitsdaten im Internet „Portallösungen“ genutzt. Ein Portal wird dabei in der Wikipedia[1] wie folgt beschrieben: „*Das ideale Portal eröffnet einen gemeinsamen, personalisierten Zugang zu Daten, Expertisen und Anwendungen.*“

Neben den klassischen Web-Portalen gibt es eine Reihe weiterer auf Plattformen basierenden Lösungsangeboten mit denen Gesundheitsdaten gesammelt werden. Beispiele hierfür sind Krankheitsregister oder auch Kollaborationslösungen für Versorgung und Forschung. Allen diesen Lösungen ist gemeinsam, dass Gesundheitsdaten im Internet vorhanden sind; es sind Werkzeuge zur Zusammenarbeit, wobei grundsätzlich schon bei der Planung einer Lösung für einen gemeinsamen Zugriff auf Gesundheitsdaten die Sensibilität dieser Daten berücksichtigt werden muss. D.h. es müssen dem (potentiellen) Missbrauch der Gesundheitsdaten entsprechende Schutzmaßnahmen vorgesehen werden, wenn derartige Daten unter Nutzung des Mediums Internet anderen Personen zur Verfügung gestellt werden sollen. Zusammenfassend sprechen wir in dieser Ausarbeitung von „Datenaustauschplattformen“.

Diese Ausarbeitung beschreibt Anforderungen an Datenaustauschplattformen und bietet damit eine Orientierungshilfe für die Einführung und den Betrieb derartiger internetbasierter Lösungen. Dabei treffen nicht alle hier beschriebenen Anforderungen auf jede Plattformlösung zu. Vielmehr muss bei der Konzeption der jeweiligen Plattform festgehalten werden, welche Anforderungen zutreffend sind und welche nicht, wobei Letzteres selbstverständlich begründet werden muss - es geht bei Gesundheitsdaten ja um Daten, die den höchstmöglichen Schutzbedarf beinhalten.

Dabei ist die Ausarbeitung derart aufgeteilt, dass in einem Kapitel die Anforderungen dargestellt werden. Datenschützer, Hersteller und Betreiber von derartigen Plattformlösungen finden hier nicht nur Anforderungen dargestellt, sondern zu jeder Anforderung auch Erläuterungen: „Aus welchen Gründen wird diese Anforderung erhoben? Was soll mit dieser Anforderung erreicht werden?“ Damit besteht die Möglichkeit, für die konkret geplante oder vorliegende Plattformlösung festzustellen, ob die dargestellte Anforderung erfüllt werden sollte oder nicht.

In einem weiteren Kapitel wird beispielhaft dargestellt, ob die Anforderungen rein organisatorisch (z.B. mit Verfahrensanweisungen) zu lösen sind, oder ob eine technische Unterstützung denkbar ist. Ist Letzteres der Fall, wird auch hier beispielhaft skizziert, wie eine technische Unterstützungsmaßnahme aussehen könnte. Dieses Kapitel dient Hersteller und Betreibern als Ausgangspunkt für Anregungen und Ideen zur Realisierung der eigenen Lösung.

Wir hoffen, mit den vorliegenden Empfehlungen allen, die eine Datenaustauschplattform für das Gesundheitswesen einführen oder betreiben wollen, eine Orientierungshilfe zu bieten, an was man zum Schutz der Gesundheitsdaten vor Missbrauch denken sollte.

[1] Wikipedia: Portal (Informatik). [Online, zitiert 2016-03-05] Verfügbar unter https://de.wikipedia.org/wiki/Portal_(Informatik)

1 Abgrenzung

1.1 Thematische Umgrenzung

Diese Ausarbeitung beschäftigt sich ausschließlich mit den deutschen datenschutzrechtlichen Anforderungen bei der Nutzung von internetbasierten Datenaustauschplattformen. Nicht Bestandteil dieser Ausarbeitung sind andere Anforderungen, seien sie rechtlicher Natur wie beispielsweise Haftungsfragen oder Empfehlungen der entsprechenden medizinischen Fachorgane. Hier wird auf die gängige Literatur verwiesen.

1.1.1 Mobile Geräte und Mobile Application Software („Apps“)

Aus datenschutzrechtlicher Betrachtung heraus macht es keinen Unterschied, ob auf Daten mittels eines Laptops, eines Smartphones, eines Tablets oder einem anderen IT-Gerät zugegriffen wird. Die Daten müssen gegen den Zugriff von Unbefugten geschützt werden, hier gelten bei Datenaustauschplattformen dieselben Anforderungen, wie sie auch für mobile Arbeitsplätze beispielsweise in Krankenhäusern oder Arztpraxen gelten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinen IT-Grundschutz-Katalogen die entsprechenden Rahmenbedingungen, sodass an dieser Stelle auf diese Thematik nicht noch einmal eingegangen werden muss[2]. Insbesondere sei auf

- Kapitel B2 Infrastruktur[3], insbesondere
  - Abschnitt B2.10 „Mobiler Arbeitsplatz“,
  - Abschnitt B2.8 „Häuslicher Arbeitsplatz“
- Kapitel B3 IT-Systeme[4], insbesondere
  - Abschnitt B3.203 „Laptop“,
  - Abschnitt B3.208 „Internet-PC“,
  - Abschnitt B3.404 „Mobiltelefon“
  - Abschnitt B3.405 „PDA“
- Kapitel B5 Anwendungen[5], insbesondere
  - Abschnitt B5.8 „Telearbeit“,
  - Abschnitt B5.14 „Mobile Datenträger“
  - Abschnitt B5.21 „Webanwendungen“

hingewiesen. Natürlich müssen auch die aus den Bausteinen resultierenden Maßnahmenkataloge berücksichtigt werden.

Mobile Application Software, sogenannte „Apps“, unterscheiden sich rechtlich nicht von anderer Software, sodass auch hier aus datenschutzrechtlicher Sicht keine besondere Betrachtung erfolgen muss.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. [Online, zitiert 2015-04-06] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kapitel B2 Infrastruktur. [Online, zitiert 2015-04-06] Verfügbar unterhttps://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02.html

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kapitel B3 IT-Systeme. [Online, zitiert 2015-04-06] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03.html

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kapitel B5 Anwendungen. [Online, zitiert 2015-04-06] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05.html

1.2 Datenschutzrechtliche Rahmenbedingungen

Die Aufteilung der Zuständigkeiten zwischen dem Bund und den Ländern werden in den Artikeln 70 bis 75 Grundgesetz (GG) behandelt („Föderalismus“). Entsprechend Artikel 74 GG existiert im Bereich des Gesundheitswesens eine konkurrierende Gesetzgebung, sodass die länderspezifische Betrachtung bei einer Datenerhebung in Deutschland nicht zu umgehen ist. Datenaustauschplattformen werden häufig von ausgegründeten Unternehmen, die als GmbH oder gGmbH arbeiten, betrieben. Für diese gilt als datenschutzrelevante gesetzliche Vorschrift das Bundesdatenschutzgesetz (BDSG). Gerade für Krankenhäuser, die als wichtige Akteure bei der Bereitstellung von Gesundheitsdaten anzusehen sind, gelten landes- und kirchenrechtliche Bestimmungen, die zum Teil sehr detailliert beschreiben, was mit den Daten der Patienten geschehen muss oder auch darf. Für Sozialdaten (Legaldefinition siehe §67 Abs. 1 SGB X) gilt der Sozialdatenschutz, der überwiegend im Zehnten Buch Sozialgesetzbuch (Sozialverwaltungsverfahren und Sozialdatenschutz SGB X[6]) beschrieben wird.

In dieser Ausarbeitung werden die Anforderungen so gut wie möglich berücksichtigt, auch wenn die jeweiligen landes- oder kirchenrechtlichen Regelungen nicht explizit genannt werden. Dennoch muss jede Leserin / jeder Leser die für ihn geltenden rechtlichen Bestimmungen im Einzelfall prüfen und ggfs. Anforderungen ergänzen, um- oder neu definieren.

1.3 Schweigepflicht

Die Verpflichtung zur Einhaltung einer ärztlichen Schweigepflicht ist sowohl im Strafgesetzbuch (§203 StGB) als auch in den Berufsordnungen der Landesärztekammern (§9 BO) festgelegt. Der strafrechtlichen Schweigepflicht unterliegen auch die bei einem Arzt berufsmäßig tätigen Gehilfen und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen. Daraus wird schon ersichtlich, dass die ärztliche Schweigepflicht nicht Gesundheitsdaten allgemein betrifft, sondern die Schweigepflicht ausschließlich jenen Bereich betrifft, wo einem Arzt im Rahmen seiner ärztlichen Tätigkeit Patienten ihre persönlichen Daten anvertrauen. Diese einem Arzt anvertrauten Daten sind gesetzlich geschützt. Damit diese Daten von einem Dritten, also nicht vom betroffenen Patienten selbst, in eine Datenaustauschplattform integriert werden können, muss eine Schweigepflichtentbindung vom Betroffenen erteilt werden, sofern nicht ein gesetzlicher Erlaubnistatbestand eine Offenbarung des Patientengeheimnisses gestattet. Da zum Thema „ärztliche Schweigepflicht“ schon diverse Literatur existiert, wird im Rahmen dieser Ausarbeitung das Thema nicht weiter besprochen. Dessen ungeachtet muss das Thema im Rahmen von Datenaustauschplattformen selbstverständlich beachtet werden.

Außer Ärzten gilt die Schweigepflicht ebenfalls für Angehörige „eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert“. Demnach gehören u.a. auch folgende medizinische Berufsgruppen zu den unter §203 StGB fallenden Berufszweigen:

- Diätassistentin/ Diätassistent
- Heilpraktikerin / Heilpraktiker
- Podologin/ Podologe
- Altenpfleger
- Hebamme / Entbindungspfleger
- Physiotherapeut
- Ergotherapeut
- Gesundheits- und Kinderkrankenpflegerin/ Gesundheits- und Kinderkrankenpfleger
- Gesundheits- und Krankenpflegehelferin/ Gesundheits- und Krankenpflegehelfer
- Gesundheits- und Krankenpflegerin/ Gesundheits- und Krankenpfleger

[6] Zehntes Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz. [Online, zitiert 2015-02-13] Verfügbar unter http://www.gesetze-im-internet.de/sgb_10/

- Notfallsanitäter.

An Literatur hierzu empfehlen wir (ohne Anspruch auf Vollständigkeit):

(1) Ärztekammer Berlin. (2008) Merkblatt Schweigepflicht. Online, zitiert am 2014-10-03]; Verfügbar unter http://www.aerztekammer-berlin.de/10arzt/30_Berufsrecht/08_Berufsrechtliches/06_Behandlung_von_Patienten_Pflichten_Empfehlungen/35_Merkblatt_Schweigepflicht.pdf
(2) Bräutigam P. (2011) §203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416
(3) Bruns W, Andreas M, Debong B. (1999) Ärztliche Schweigepflicht im Krankenhaus. ArztRecht: 32 - 37
(4) Buchner B. (2013) Outsourcing in der Arztpraxis – zwischen Datenschutz und Schweigepflicht. MedR: 337 - 342
(5) Conrad I, Fechtner S. (2013) IT-Outsourcing durch Anwaltskanzleien nach der Inkasso-Entscheidung des EuGH und dem BGH, Urteil vom 7.2.2013 - Datenschutzrechtliche Anforderungen. CR: 137-148
(6) Ehrmann C. (2008) Outsourcing von medizinischen Daten – strafrechtlich betrachtet. Online, zitiert am 2014-10-03]; Verfügbar unter http://opus.bibliothek.uni-wuerzburg.de/files/2494/OutsourcingDissEhrmann.pdf
(7) Frewer A, Säfken C. (2003) Ärztliche Schweigepflicht und die Gefährdung Dritter - Medizinethische und juristische Probleme der neueren Rechtsprechung. Ethik Med: 15 – 24
(8) Giesen T. (2012) Zum Begriff des Offenbarens nach §203 StGB im Falle der Einschaltung privatärztlicher Verrechnungsstellen. NStZ: 122ff
(9) Heghmanns M, Niehaus H. (2008) Outsourcing im Versicherungswesen und der Gehilfenbegriff des §203 III 2 StGB. NStZ: 57ff
(10) Hoenike M, Hülsdunk L. (2004) Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung? MMR:788ff
(11) Huffer H. (2002) Schweigepflicht im Umbruch. NJW: 1382-1386
(12) Jandt S, Roßnagel A, Wilke D. (2011) Outsourcing der Verarbeitung von Patientendaten - Fragen des Daten- und Geheimnisschutzes. NZS: 641ff
(13) Kern BR. (2006) Der postmortale Geheimnisschutz. MedR: 205 - 208
(14) Klein H. (2010) Schweigepflicht versus Offenbarungspflicht. RDG: 172ff
(15) Klöcker I. (2001) Schweigepflicht des Betriebsarztes im Rahmen arbeitsmedizinischer Vorsorgeuntersuchungen. MedR: 183 - 187
(16) Kort M. (2011) Strafbarkeitsrisiken des Datenschutzbeauftragten nach §STGB §203 StGB beim IT-Outsourcing, insbesondere in datenschutzrechtlich „sichere“ Drittstaaten. NstZ: 193 - 195
(17) Kroschwald S, Wicker M. (2012) Kanzleien und Praxen in der Cloud – Strafbarkeit nach §203 StGB. CR: 758-764
(18) Leisner W. (2010) Einschaltung Privater bei der Leistungsabrechnung in der Gesetzlichen Krankenversicherung - Verfassungsrechtliche Vorgaben für eine anstehende gesetzliche Neuregelung. NZS: 129 -136
(19) Lensdorf L, Mayer-Wegelin C, Mantz R. (2009) Outsourcing unter Wahrung von Privatgeheimnissen - Wie das mögliche Hindernis des § 203 Abs. 1 StGB überwunden werden kann. CR: 62-68
(20) Lewinski K. (2004) Schweigepflicht von Arzt und Apotheker - Datenschutzrecht und aufsichtsrechtliche Kontrolle. MedR: 95-104
(21) Menzel HJ. (2013) Auftragsdatenverarbeitung im Sozial- und Gesundheitswesen. RDV: 59 - 66
(22) Moderegger C. (2001) Leitfaden zur Telearbeit. ArbRB: 90-92
(23) Parzeller M, Wenk M, Rothschild MA. (2005) Zertifizierte Medizinische Fortbildung: Die ärztliche Schweigepflicht. Dtsch Arztebl; 102(5): A-289 / B-237 / C-224 (Online, verfügbar unter https://www.aerzteblatt.de/pdf.asp?id=45243
(24) Paul JA, Gendelev B. (2012) Outsourcing von Krankenhausinformationssystemen -

Praxishinweise zur rechtskonformen Umsetzung. ZD: 315-321
(25) Sosna S. (2014) Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich. 1.Aufl. ISBN: 978-3-8487-1701-9
(26) Spickhoff A. (2005) Postmortaler Persönlichkeitsschutz und ärztliche Schweigepflicht. NJW: 1982-1984
(27) Szalai S, Kopf R. (2012) Verrat von Mandantengeheimnissen - Ist Outsourcing strafbar nach §203 StGB? ZD: 462-468
(28) Ulmer CD. (2012) Datenverarbeitung und Datenschutz im Gesundheitswesen – technische Möglichkeiten und rechtliche Grundlagen. RDG: 272-278
(29) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Erklärung zur Entbindung von der Schweigepflicht. Online, zitiert am 2014-10-03]; Verfügbar unter https://www.datenschutzzentrum.de/medizin/arztprax/entbind.htm
(30) Waider, H. (2006) Ärztliche Schweigepflicht im psychiatrischen Krankenhaus. Recht & Psychiatrie 24: 65-74
(31) Weichert T. (2004) Die Krux mit der ärztlichen Schweigepflichtentbindung für Versicherungen. NJW: 1695ff
(32) Welke WA. (2008) Zulässigkeit von Durchsuchungen in Arztpraxen - Anmerkung zum Beschluss des BVerfG vom 21. 1. 2008 – 2 BvR 1219/07. MedR: 732 - 734
(33) Wienke A, Sauerborn J. (2000) EDV-gestützte Patientendokumentation und Datenschutz in der Arztpraxis. MedR: 517-519

2 Einführung in das Thema

Der Austausch von Gesundheitsdaten oder - als Spezialisierung der Gesundheitsdaten - von Patientendaten zur Mit- und Weiterbehandlung war schon immer einer der Grundpfeiler für die Optimierung der Gesundheitsversorgung der Bevölkerung. Die moderne EDV löst dabei mehr und mehr die klassische papiergebundene Kommunikation ab, so dass eine einrichtungsübergreifende und dabei häufig auch sektorenübergreifende Kommunikation unter Nutzung moderner Möglichkeiten der Informations- und Kommunikationstechnik immer stärker genutzt wird. Dabei finden verschiedene Formen des Datenaustausches statt:

- über von Bürgern (insbesondere auch von Patienten) geführte elektronische Aktensysteme, die von einer Organisation zur Verfügung gestellt werden sowie
- elektronische Aktensysteme, welche von einer medizinischen Einrichtung wie einem Krankenhaus mit der Einwilligung des jeweiligen Patienten (oder basierend auf einer rechtlichen Erlaubnisnorm) geführt werden

oder auch

- durch Nutzung fallbasierter Patientenaktensysteme, die Informationen zu genau einer bestimmten Erkrankung bereitstellen.

Weiterhin werden immer häufiger von Bürgern selbst Daten in zentralen Speicherorten abgelegt: eigene Gesundheitsdaten werden mittels „Wearable Computing“, am ehesten mit „tragbarer Datenverarbeitung“ zu übersetzen, gesammelt und in einem auf Internettechnologie basierendem Portal abgelegt, um diese Daten für eigene Zwecke zu verarbeiten oder mit anderen Nutzern zu teilen. Hierbei handelt es sich oftmals nicht um Patienten im Sinne einer in einer konkreten Behandlungssituation befindlichen Person, sondern insbesondere um gesundheitsbewusste Menschen, die ihre Gesundheit selbst überwachen wollen. Daher wird im folgendem Text auf die Verwendung des Begriffs „Patient“ weitestgehend verzichtet und stattdessen der Begriff „Betroffener“ genutzt, wobei sowohl der Begriff „Patient“ wie auch der Begriff „Betroffener“ geschlechtsneutral genutzt wird.

Gesundheitsdaten gehören entsprechend §3 Abs. 9 BDSG zu den „besondere Arten personenbezogener Daten“, dementsprechend existiert ein hoher Schutzbedarf für diese Daten[7]. Alle oben genannten Datenaustauschplattformen, egal welcher Form, müssen daher diesen hohen Schutzbedarf gewährleisten. Die vorliegende Ausarbeitung will hierzu eine Hilfestellung bieten, indem die wesentlichen Anforderungen an einen datenschutzgerechten Betrieb einer derartigen Datenaustauschplattform für Gesundheitsdaten dargestellt werden.

2.1 Hinweis zu den nachfolgend genannten Anforderungen

Viele der nachfolgend beschriebenen Anforderungen wie beispielsweise die Ausführungen zu Passwörtern stellen den aktuellen Stand der Technik dar. Hier werden Anforderungen den aktuellen Standards zur IT Sicherheit entsprechend benannt. Diese Standards werden regelmäßig weiterentwickelt und dementsprechend müssen die hier gelisteten Anforderungen immer unter dem Gesichtspunkt „was ist der aktuelle Stand der Technik“ interpretiert und ggfs. angepasst werden.

In vielen Fällen wird bei den nachfolgend dargestellten Anforderungen auf die Protokollierung der Aktivitäten von Anwendern eingegangen. Die gesetzlichen Vorgaben bzgl. der Nachvollziehbarkeit beim Zugriff auf personenbezogene oder personenbeziehbare Gesundheitsdaten müssen eingehalten werden, der einzig praktikable Weg hierzu ist eine entsprechende Protokollierung der Aktivitäten eines Nutzers von Gesundheitsdaten im erforderlichen Umfang. Grundsätzlich gilt auch hierbei das Gebot der Datensparsamkeit, sodass nur die erforderlichen Daten gesammelt werden dürfen, um den rechtlichen Anforderungen bzgl. der Nachvollziehbarkeit zu genügen.

[7] kes spezial (2014) Datenschutz und IT-Sicherheit in Arztpraxis und Klinik. [Online, zitiert 2015-02-13] Verfügbar unter http://2014.kes.info/archiv/material/e-health2014/ehealth-2014.pdf

Eine Abwägung zwischen dem evtl. vorhandenen Wunsch eines Anwenders, dass seine Aktivitäten nicht protokolliert werden, und dem Schutzbedarf eines Betroffenen bzgl. Nachverfolgbarkeit des Zugriffs auf seine Daten ist hierbei aus rechtlichen Gründen nicht möglich, auch eine Mitarbeitervertretung kann den rechtlichen Rahmen nicht ändern. Eine Abwägung ist lediglich bzgl. der Detailtiefe der Protokollierung sowie deren Auswertung möglich und muss auch erfolgen.

Da es sich hierbei aber trotz allem um eine Maßnahme handelt, die letztlich auch der Kontrolle von Mitarbeitern dienen könnte, muss - ebenfalls aus rechtlichen Gründen - die jeweilige Mitarbeitervertretung, sofern vorhanden, in den Prozess integriert werden.

Weiterhin muss beachtet werden, dass technische Maßnahmen nur organisatorische Maßnahmen unterstützen können. Allein mit technischen Maßnahmen kann keine der nachfolgend dargestellten Anforderungen umgesetzt werden. Beispiel: eine Passwortlänge und ein Passwortalter muss zunächst organisatorisch definiert werden, die Einhaltung der Vorgaben kann dann technisch herbeigeführt werden.

In diesem Sinne gibt es Anforderungen, die "rein" organisatorisch (also ohne technische Unterstützung) erfüllt werden können und Anforderungen, bei denen organisatorische Maßnahmen durch technische Maßnahmen begleitet werden können.

3 Begriffsbestimmungen

Es gelten insbesondere die Begriffsbestimmungen aus §3 BDSG.

3.1 Was ist eine Datenaustauschplattform?

Eine Datenaustauschplattform ist eine „Informations- und Telekommunikationstechnik (ITK) Lösung, welche den elektronischen Datenaustausch zwischen

- einem oder mehreren Leistungserbringern im Gesundheitswesen (primärer Datenverarbeiter)

sowie

- definierten Dritten (z.B. Mit- und Weiterbehandler, Betroffenen, Forschungseinrichtungen)
- unter Nutzung des Internets ermöglicht,
- mit der Zielsetzung,
  - eine sichere technische Plattform bzw. Portallösung
  - für den elektronischen Informationsaustausch
  - von Daten der Gesundheitsversorgung (inklusive der medizinischen Forschung)

zwischen diesen Stellen anzubieten.

3.2 Akteure

(1) Hersteller einer Datenaustauschplattform

Hersteller einer Datenaustauschplattform ist, wer das Produkt hergestellt hat. Als Hersteller gilt

- jeder, der sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt,
- jeder, der ein Produkt zum Zweck des Verkaufs, der Vermietung, des Mietkaufs oder einer anderen Form des Vertriebs mit wirtschaftlichem Zweck im Rahmen seiner geschäftlichen Tätigkeit in den Geltungsbereich des Abkommens über den Europäischen Wirtschaftsraum einführt oder verbringt.

Kann der Hersteller des Produkts nicht festgestellt werden, so gilt jeder Lieferant als dessen Hersteller. Dies gilt auch für ein eingeführtes Produkt.

(2) Betreiber einer Datenaustauschplattform

Betreiber einer Datenaustauschplattform ist jede natürliche oder juristische Person,

- die eigene oder fremde Gesundheitsdaten zur Nutzung bereithält oder
- den Zugang zur Nutzung von Gesundheitsdaten vermittelt oder
- welche die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert.

(3) Datenlieferant

Datenlieferant ist jede natürliche oder juristische Person, welche Gesundheitsdaten eines Betroffenen in eine Datenaustauschplattform einstellt.

(4) Nutzer einer Datenaustauschplattform

Nutzer einer Datenaustauschplattform ist jede natürliche oder juristische Person, welche Daten einer Datenaustauschplattform nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

(5) Betroffener bei Nutzung einer Datenaustauschplattform

Betroffener bei Nutzung einer Datenaustauschplattform ist jede natürliche Person, deren Gesundheitsdaten in einer Datenaustauschplattform erhoben, verarbeitet oder genutzt werden.

3.3 Verschiedene Austauschplattformen – Unterscheidung durch die Zweckbestimmung

Vorbemerkung: Austauschplattformen bilden i.d.R. nicht einen oder mehrere Geschäftsprozesse in einer Einrichtung ab und deshalb ist die verantwortliche Stelle nicht auf Anhieb zu erkennen. Aus den Rollen, den vertraglichen Zusicherungen und Leistungsangeboten ergibt sich manchmal eine differenzierte Sicht, die meisten Austauschplattformen leben durch eine Arbeitsteilung: Kein Geschäftspartner könnte wirtschaftlich eine Austauschplattform anbieten, wenn er nicht auf Spezialisten im Sinn der Auftragsdatenverarbeitung (ADV) zurückgreifen könnte. Daher ist das Thema „Datenaustauschplattform" immer eng mit dem Thema „Auftragsdatenverarbeitung" verknüpft. Bzgl. des Themas „Auftragsdatenverarbeitung" verweisen wir auf die Ausarbeitung der Verbände bvitg, BvD, GDD und GMDS[8].

3.3.1 „Klassische" Gesundheitsportale

Bei den Gesundheitsportalen muss man zwischen den Portalen unterscheiden, in denen ein Betroffener selbst seine Daten einstellt und den Portalen, in denen ein Dritter Daten des Betroffenen einstellt.

Für Ersteres sind typische Vertreter Patienten-Infoportale (z.B. Bewertungs-Portale, Portale von Selbsthilfegruppen) oder auch Gesundheits- bzw. Fitnessplattformen, wo z.B. Gesundheitsdaten mittels „Wearable Computing" in die Plattform integriert werden. Hier gibt der Betroffene die Daten selbst ein, ist somit alleiniger Entscheidungsträger, welche seiner Informationen er in die Datenaustauschplattform einstellt und zunächst bei Eingabe der Daten auch „Herr seiner Daten". Verarbeitet oder nutzt der Plattformbetreiber die Daten für eigene Zwecke (z.B. zu einer Pseudonymisierung/Anonymisierung zwecks späterer Verwendung), so ist auch der Plattformbetreiber als „Herr der Daten" und somit als datenschutzrechtlich verantwortlich anzusehen. Nur in den Fällen, wo der Betroffene alleiniger Verarbeiter/Nutzer seiner Daten ist, ist er auch als alleiniger Verantwortlicher für die Sicherheit seiner Daten anzusehen.

Beispiele für die zweite Variante, also Portale, in welche ein Dritter Daten eines Patienten einstellt, sind beispielsweise

- Krankenhaus-Infoportal (z.B. Zugriff auf KIS- oder auch PACS-Daten über Webseite)
- Behandlungsportale (z.B. Tumorboard, Schlaganfall-Netzwerk)
- Krankheitsregister (wie beispielsweise das „Nationale Register für angeborene Herzfehler", das „Nationale Hospiz- und Palliativregister" oder auch das TraumaRegister der Deutschen Gesellschaft für Unfallchirurgie).

In Zusammenhang mit diesen Portalen ist nicht der Patient als Betroffener „Herr der Daten", sondern ein Dritter, oftmals ein Krankenhaus; die Einflussmöglichkeit des Patienten ist oftmals auf die Gabe oder Verweigerung seiner Einwilligung hinsichtlich der Einstellung seiner Daten in die Datenaustauschplattform beschränkt.

3.3.2 E-Collaboration

Kollaborationssoftware ermöglicht über IT-Netze gemeinsam an einem Projekt zu arbeiten, d.h. in einer Gruppe zu kommunizieren und die Daten gemeinsam zu verwalten. In der Medizin, wo die interdisziplinäre, institutionsübergreifende Zusammenarbeit eine immer stärkere Rolle spielt, bekommt der Einsatz einer Kollaborationssoftware eine immer größere Bedeutung.

[8] Krüger-Brand, HE. (2015) Auftragsdatenverarbeitung: Mustervertrag für das Gesundheitswesen. Dtsch Arztebl 2015; 112(10): A-422 / B-366 / C-358. Online verfügbar unter http://www.aerzteblatt.de/archiv/168571/Auftragsdatenverarbeitung-Mustervertrag-fuer-das-Gesundheitswesen?s=Datenschutz bzw. bei den jeweiligen Verbänden z.B. http://gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015

I.d.R. stellt Kollaborationssoftware eine Groupware-Funktionalität zur Verfügung, d.h. Funktionen wie ein Adressbuch, Kalender oder auch eine Aufgabenverwaltung sind in einem Team verfügbar. Zusätzlich werden die Funktionalitäten von Intranetportalen, insbesondere die Möglichkeit für den Aufbau und den Betrieb von sozialen Netzwerken (z.B. für ein Patientenforum) sowie ein Content-Management-System, welches mittels Dokumentenmanagement-Funktionen wie Inhaltsverwaltung, Definition von Metadaten zu den Dokumenten und einer benutzeranpassbaren Suchfunktion den Dokumentenaustausch in der medizinischen Versorgung ermöglicht, genutzt.

Bei der Installation von Software zur Zusammenarbeit verschiedener Einrichtungen oder Stellen muss von der die Software einrichtenden verantwortlichen Stelle geprüft werden, ob die Zusammenarbeit aufgrund gesetzlicher Regelungen oder aufgrund der ausdrücklichen Einwilligung des Betroffenen zulässig ist.

3.3.3 Einrichtungsübergreifende elektronische Patientenakte (eEPA)

Bei der einrichtungsübergreifenden elektronischen Patientenakte (eEPA) werden unter ärztlicher Moderation Daten und Dokumente der Behandlungen eines Patienten gesammelt, um so die Kommunikation zwischen Krankenhäusern, niedergelassenen Ärzten und anderen Gesundheitsdienstleistern sowie dem Patienten selbst zu unterstützen. Dabei entscheidet nur der Patient, beraten durch eine ärztliche Vertrauensperson, wer auf diese Daten zugreifen darf. Der Patient sieht alle eingestellten Dokumente, kann selbst welche hinzufügen und die Zugriffsrechte auf die Dokumente in Absprache mit der ärztliche Vertrauensperson detailliert festlegen.

3.3.4 Persönliche einrichtungsübergreifende elektronische Patientenakte (pEPA)

Der Inhalt einer persönlichen einrichtungsübergreifenden elektronischen Patientenakte (pEPA) liegt, wie es der Name schon andeutet, ausschließlich in der Hoheit des Patienten, unabhängig davon, ob dieser die Informationen in die Akte selbst einstellt oder ggf. einen Dritten (Pflegedienst, Arzt, Krankenhaus, usw.) damit beauftragt. Die pEPA dient ebenfalls der Optimierung der Kommunikation zwischen Behandlern und Patient, wobei den Verwendungszweck ausschließlich der Patient bestimmt.

3.3.5 Fallbezogene einrichtungsübergreifende elektronische Patientenakte (eFA)

Eine fallbezogene einrichtungsübergreifende elektronische Patientenakte (eFA) liegt in ärztlicher Verwaltungshoheit, d.h. wird ausschließlich ärztlicherseits geführt: nur Ärzte entscheiden, welche Informationen hier gespeichert werden. Der Patient bestimmt lediglich, welche Personen Zugriff auf die Informationen erhalten, hat jedoch bzgl. der dargestellten Informationen kein Mitspracherecht, es gilt das „Alles-oder-Nichts“-Prinzip. Zweck einer eFA ist die Schaffung eines gemeinsamen Wissensstandes zur Koordination der Behandlung des betroffenen Patienten. Da der Fokus einer eFA auf einen konkreten Behandlungsfall gerichtet ist, ist auch die Nutzungsdauer einer eFA zeitlich begrenzt; ist der Behandlungsfall abgeschlossen, so sind die Daten innerhalb der eFA zu löschen bzw. zu sperren, wenn eine Löschung aus den in Kapitel 4.5.3 genannten Gründen nicht möglich ist.

3.4 Datenaustauschplattform und Cloud Computing

Cloud Computing ist eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen durch i.d.R. nicht fest zugeordnete IT-Ressourcen über Netze. D.h. man versteht darunter die automatisierte Verarbeitung von Daten in einem entfernten Rechenzentrum bzw. die Bereitstellung von Software-Programmen, die nicht auf dem lokalen Rechner des Anwenders installiert sind und genutzt werden, sondern in der Cloud. Die für das Cloud Computing benötigte IT-Infrastruktur ist für den Anwender dabei nur abstrakt vorhanden, d.h. der Anwender weiß i.d.R. nicht, wo die von ihm benutzten Ressourcen sich befinden.

3.4.1 Cloud Computing: eine Begriffsbestimmung

Cloud Computing wird hier im Sinne des BSI[9] verstanden, d.h. entsprechend der BSI-Definition:

> „Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Dementsprechend charakterisieren fünf Eigenschaften einen Cloud-Service (zitiert nach [7]):

1. On-demand Self Service: Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service Provider ab.
2. Broad Network Access: Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
3. Resource Pooling: Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
4. Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
5. Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Daraus resultiert, dass bei der Nutzung von Cloud-Diensten einem Betroffenen nicht mitgeteilt werden kann,

- wo seine Daten gespeichert werden
- auf welchen (Betriebs-) Systemen seine Daten mit welchen Schutzmechanismen gespeichert werden
- welche Person zu welchem Zeitpunkt im Rahmen von Wartung oder Fehlerbehebung auf die Daten des Betroffenen wann an welchem Ort zugreift.

Damit wird die Information eines Betroffenen, welche ihn in die Lage versetzt, aufgeklärt über eine Einwilligung in die Cloud-Nutzung hinsichtlich seiner Daten zu entscheiden, stark erschwert.

3.4.2 Arten von Cloud Computing

Weitgehend akzeptiert ist die Einteilung der Dienstleistungen in drei Ebenen, allen drei Ebenen ist gemeinsam, dass die IT-Leistungen als Dienste („as a Service") bereitgestellt werden[10]:

- Infrastructure as a Service
  Infrastructure as a Service (IaaS) beschreibt im Cloud Computing die Bereitstellung von virtualisierter IT-Infrastruktur über Netze.
- Platform as a Service
  Platform as a Service (PaaS) liefert Anwendungs-Infrastruktur in Form von technischen Frameworks (Datenbanken und Middleware) oder die gesamte Anwendungssoftware.
- Software as a Service
  Software as a Service (SaaS) ist eine Form von Cloud Computing, bei der Nutzer eine

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI): Cloud Computing Grundlagen. [Online, zitiert 2015-04-11] Verfügbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Dossiers/Anwender/AnwenderManagement/anwenderManagement_node.html

[10] siehe hierzu auch: European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR) - eHealth Toolkit. [Online, zitiert 2016-01-23] Verfügbar unter http://www.cocir.org/uploads/media/15013.COC_2.pdf

Applikation über Netze beziehen.

Unter Betriebs-, Eigentums- und Organisationsaspekten unterscheidet man weiterhin zwischen einer „Private Cloud“ (auch „Enterprise Cloud“ genannt) sowie der „Public Cloud“, wobei sich beide Formen in der technischen Realisierung nicht grundsätzlich unterscheiden. In der Realität werden auf absehbare Zeit wohl überwiegend Mischformen, sogenannte „Hybrid Clouds“, genutzt. Hybrid Clouds sind mögliche Nutzungskombinationen von Private Clouds, Public Clouds und traditioneller IT-Umgebung.

3.4.3 Cloud Computing und die Speicherung von Gesundheitsdaten

Bei der Nutzung von Cloud Computing zur Speicherung von Gesundheitsdaten ist zu beachten, dass der genaue Ort der Speicherung der Gesundheitsdaten bei der Einholung der Einwilligung des Betroffenen genannt werden muss; ein Speicherort „Deutschland“ wird keinesfalls ausreichen, um dem Betroffenen in die Lage zu versetzen, die Bedeutung und Tragweite seiner Entscheidung überblicken zu lassen (siehe hierzu auch Kapitel 4.1.1). Zudem gehen verschiedene landesrechtliche Rechtsnormen auf den Speicherort von Gesundheitsdaten (insbesondere Patientendaten, z.B. im Krankenhausrecht) ein, sodass auch von dieser Seite die Nutzung von Cloud Computing begrenzt wird.

Gesundheitsdaten dürfen nur dann in einer Cloud gespeichert werden, wenn sichergestellt ist, dass Dritte (Cloud-Betreiber, IT-Dienstleister) keinen unbefugten Zugriff auf diese Daten erhalten.

Für eEPA, pEPA und eFA wie auch bei anderen Formen einer Datenaustauschplattform im Gesundheitswesen, welche der ärztlichen Schweigepflicht unterliegende Patientendaten für eine Optimierung zur Kommunikation zwischen Patienten und Behandlern integrieren will, wird man daher zu dem Schluss kommen müssen, dass der rechtssichere Einsatz von Cloud Computing nur sehr schwierig zu realisieren ist. (Hinsichtlich Beschlagnahmeschutz siehe Kapitel 4.3.1)

Anders hingegen sieht es aus, wenn der Betroffene seine selbst erhobenen Gesundheitsdaten in ein internetbasiertes Gesundheitsportal (häufig als Gesundheits- oder Fitnessplattform bezeichnet) ablegen will. Dies ist selbstverständlich möglich, dennoch müssen Gesundheitsdaten natürlich ebenfalls vor unbefugtem Zugriff Dritter geschützt werden. Neben den in dieser Ausarbeitung dargestellten Anforderungen sollte die Orientierungshilfe „Cloud Computing“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Stand 09.10.2014[11]) beachtet werden, desgleichen die Ausarbeitung der Artikel-29-Datenschutzgruppe aus dem Jahr 2012 zum Thema.[12]

Auch integrierte das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Baustein „Cloud-Nutzung“ in die IT-Grundschutz-Kataloge, weiterhin bietet das BSI diverse Informationsmaterialien zum Thema „Cloud Computing“ an.[13]

[11] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder - Orientierungshilfe Cloud-Computing. [Online, zitiert 2015-02-13] Verfügbar unter http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=28691&article_id=99460&_psmand=48

[12] Artikel-29-Datenschutzgruppe. Opinion 05/2012 on Cloud Computing. [Online, zitiert 2015-02-13] Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI): Cloud Computing. [Online, zitiert 2015-02-13] Verfügbar unter https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html

4 Datenschutzrechtliche Anforderungen

Es ist zu beachten, dass Gesundheitsdaten durch Bereitstellung in öffentlichen Netzen wie z.B. im Internet i.d.R. einer höheren Gefährdung bzgl. einer Vertraulichkeitsverletzung ausgesetzt sind, als wenn sich die Daten nur im geschützten lokalen Netzwerk befinden, das vom Internet getrennt ist.

In den folgenden Unterkapiteln wird oftmals darauf hingewiesen, dass die Anforderungen schriftlich dokumentiert werden müssen. Eine grundsätzliche Dokumentation aller Verfahren wird im Verfahrensverzeichnis festgehalten. Hier erfolgt oftmals jedoch nur eine sehr oberflächliche Darstellung der getroffenen Schutzmaßnahmen, was datenschutzrechtlich im jeweiligen Einzelfall statthaft sein kann, denn das Verfahrensverzeichnis dient dazu, einen generellen Überblick über die Verfahren zu behalten.. In diesen Fällen müssen die Anforderungen an anderer Stelle präziser ausformuliert werden, damit diese auch entsprechend umgesetzt werden können.

Es spricht aber auch nichts dagegen, die Dokumentation im Verfahrensverzeichnis zu führen, wenn dies seitens der verantwortlichen Stelle so gewünscht ist. Die Autoren können und wollen hier keine Vorgaben treffen, vielmehr muss individuell die Entscheidung erfolgen, wo die Dokumentation erfolgt.

4.1 Rechtmäßigkeit der Datenverarbeitung

4.1.1 Einwilligung vs. gesetzlicher Grundlage

Die Erhebung, Verarbeitung und Nutzung (bzgl. Begriffsbestimmung siehe hierzu §3 Abs. 3-5 BDSG) personenbezogener oder personenbeziehbarer Daten sind nur zulässig, soweit ein gesetzlicher Erlaubnistatbestand dies gestattet oder sogar anordnet oder der Betroffene eingewilligt hat (§4 BDSG).

In einigen Landesdatenschutzgesetzen gibt es eine Regelung zu „gemeinsamen Verfahren“ (Z.B. Hessen mit §15 HessDSG). Diese Regelungen gelten einerseits ausschließlich für den öffentlichen Bereich, also z.B. nicht für Arztpraxen, Apotheken, private Krankenhäuser. Im Bereich der öffentlichen geführten Krankenhäuser (z.B. städtische Krankenhäuser) ist zu beachten, dass in den Landesdatenschutzgesetzen die spezialgesetzlichen Regelungen (z.B. Krankenhausgesetze) vorrangig zu beachten sind. Somit können Regelungen aus den Landesdatenschutzgesetzen bzgl. gemeinsamer Verfahren nicht als Erlaubnisnorm für die hier vorgestellten Datenaustauschplattformen dienen. Auch in anderen Gesetzen findet sich keine gesetzliche Erlaubnisnorm, im Sinne einer internetbasierten Datenaustauschplattform, die ohne eine Einwilligung des Betroffenen auskommt.

Für die hier vorgestellten internetbasierten Datenaustauschplattformen existiert keine gesetzliche Grundlage, sodass hier immer zwingend eine Einwilligung des Betroffenen notwendig ist. Die Übermittlung von zulässig erhobenen und verarbeiteten Gesundheitsdaten über eine Datenaustauschplattform muss zunächst technisch sicher sein und damit beispielsweise den Anforderungen an die im SGB V gesetzlich geregelte Telematikplattform oder einer ähnlich sicheren Kommunikationslösung entsprechen. Darüber hinaus bedarf es der Einwilligung des Betroffenen zur sicheren elektronischen Übermittlung an die von ihm bestimmten Personen oder Stellen im Rahmen der Mit- und Weiterbehandlung.

Entsprechend der geltenden Rechtsprechung ist einwilligungsfähig nur, wer Art, Bedeutung und Tragweite (Risiken) der Maßnahme erfassen kann[14]. Eine datenschutzrechtliche Einwilligung setzt daher insbesondere voraus (§4a BDSG):

- dass die Einwilligung auf der freien Entscheidung des Betroffenen beruht

[14] BGH Urteil vom 28.11.1957 - 4 Str 525/57 [Online, zitiert 2015-02-13] Verfügbar unter http://dejure.org/dienste/vernetzung/rechtsprechung?Text=4%20StR%20525%2F57&Suche=4%20Str%20525%2F57;
BGH Urteil vom 16.11.1971 - VI ZR 76/70 [Online, zitiert 2015-02-13] Verfügbar unter http://dejure.org/dienste/vernetzung/rechtsprechung?Text=NJW 1972, 335

- dass der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen wurde
- dass die Einwilligung sich ausdrücklich auf die Daten der besonderen Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) bezieht
- dass die Schriftform gewahrt wird
- dass die Einwilligung, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt wird, besonders hervorgehoben wurde
- dass der Betroffene darüber aufgeklärt wurde, dass die Einwilligung jederzeit, ohne Angabe von Gründen widerrufen werden kann.

Es ist dabei zu beachten, dass eine ordnungsgemäße Aufklärung nur dann vorliegt, wenn sie zum richtigen Zeitpunkt stattfindet, und dies ist grundsätzlich nur der Fall, wenn der Betroffene noch Gelegenheit hat, zwischen der Aufklärung und Maßnahme das Für und Wider der Einwilligung in die Maßnahme abzuwägen[15]. Eine wirksame Einwilligung setzt also immer voraus, dass der Erklärende eine im Wesentlichen zutreffende Vorstellung davon hat, worin er einwilligt, und die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag[16,17].

Anforderung 1: Jegliche Erhebung, Verarbeitung und Nutzung personenbezogener oder personenbeziehbarer Daten - insbesondere durch den Einsatz von Datenaustauschplattformen, die an das Internet angebunden sind - bedarf einer datenschutzrechtlich wirksamen Einwilligung des Betroffenen.

Anforderung 2: Vor der Erteilung der Einwilligung zu einer Erhebung, Verarbeitung (= Speichern, Verändern, Übermitteln, Sperren und Löschen) oder Nutzung (alles, was nicht als Erhebung oder Verarbeitung aufzufassen ist) seiner Daten muss der Betroffene insbesondere über

- Sitz/Land des Dienstanbieters
- das Empfängerland (soweit bekannt; Internet ermöglicht globalen Zugriff, je nach Austauschplattform ist jedoch nur aus definierten Ländern ein Zugriff möglich)
- die im Empfängerland, soweit dieses von seinem Heimatland abweicht, vorhandenen oder nicht vorhandenen Datenschutzregelungen, insbesondere von den von seinem Heimatland abweichenden Regelungen
- die Form der Gewährleistung des europäischen Datenschutzniveaus insbesondere über den Schutz vor Zugriff auf seine Daten durch Unbefugte (dies schließt auch alle staatlichen Ermittlungsbehörden ein, ausgenommen die staatlichen Ermittlungsbehörden im Land des Betroffenen)
- die Gewährleistung seiner datenschutzrechtlich garantierten Rechte wie
  - die Möglichkeiten der Korrektur der ihn betreffenden Daten (wie werden seine Daten auf seine Anforderung hin korrigiert)
  - die Möglichkeiten zur Löschung der ihn betreffenden Daten (wie werden seine Daten auf seine Anforderung hin gelöscht bzw. gesperrt, sowohl aus dem Arbeitsbereich wie auch aus Backupdateien)

informiert werden, sodass er die Gefährdung seiner Daten ausreichend beurteilen kann.

[15] BGH Urteil vom 07.04.1992 - VI ZR 192/91 [Online, zitiert 2015-02-13] Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=07.04.1992&Aktenzeichen=VI%20ZR%20192/91

[16] BGH Urteil vom 10.10.2013 - III ZR 325/12 [Online, zitiert 2015-02-13] Verfügbar unter http://dejure.org/dienste/vernetzung/rechtsprechung?Text=III%20ZR%20325%2F12&Suche=Az.%20III%20ZR%20325%2F12

[17] Artikel-29-Datenschutzgruppe. Stellungnahme 15/2011 zur Definition von Einwilligung. [Online, zitiert 2015-04-23] Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

Die Einwilligung muss auf einer freien Entscheidung des Betroffenen beruhen. Sie ist mithin nicht geeignet, die Datenverarbeitungen zu legitimieren, wenn der Betroffene keine echte Wahl hat, sondern faktisch dazu gezwungen ist, sich einverstanden zu erklären. Da eine Einwilligung stets freiwillig erfolgt, besteht für den Betroffenen jederzeit die Möglichkeit seine Einwilligung zu widerrufen. Dies kann jedoch nur für zukünftige Ereignisse gelten, da die Vergangenheit nicht geändert werden kann. (Das Recht auf Löschen der Daten bleibt hiervon selbstverständlich unberührt, siehe Kapitel 3.5 bzgl. der Gewährleistung der Betroffenenrechte.)

Anforderung 3: Eine Einwilligung muss für den Betroffenen jederzeit mit Wirkung für die Zukunft widerrufbar sein.

Für jeden Betroffenen muss nachvollziehbar sein, welche seiner Daten in der Datenaustauschplattform erhoben, verarbeitet und genutzt werden und an wen ggfs. eine Weitergabe der Daten erfolgt. Hierzu müssen entsprechende Datenschutzhinweise veröffentlicht werden.

Anforderung 4: Jede Datenaustauschplattform muss Datenschutzhinweise veröffentlichen und darin die getroffenen Datensicherheitslösungen allgemeinverständlich beschreiben.

Anforderung 5: Datenschutzhinweise müssen unmittelbar von der Startseite der Datenaustauschplattform aus aufrufbar bzw. erreichbar sein[18].

Anforderung 6: Datenschutzhinweise müssen für den Betroffenen jederzeit abrufbar sein.

Anforderung 7: Bei nachträglicher Änderung ist der Betroffene zu informieren und sein Einverständnis erneut einzuholen.

4.1.2 Telemedien

4.1.2.1 Anwendung Telemediengesetz (TMG)

Die Vorschriften im Telemediengesetz regeln die Erhebung und Verwendung personenbezogener Daten, die bei der Nutzung von Telemedien anfallen. Zu den Telemedien zählen alle elektronischen Informations- und Kommunikationsdienste, außer Telekommunikationsdienste gemäß § 3 Nr. 24 des Telekommunikationsgesetzes, telekommunikationsgestützte Dienste gemäß § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk gemäß § 2 des Rundfunkstaatsvertrages.[19]

Die Datenaustauschplattform stellt einen solchen Telemediendienst dar.

Bereits bei der Nutzung einer Webseite fallen eine Vielzahl personenbezogener Daten über Webseitenbesucher an, die in den Schutzbereich des Telemediengesetzes fallen. Nutzer im Sinne des TMG sind Personen, die eine Webseite besuchen, um Informationen über z.B. einen potentiellen Arbeitgeber zu erlangen oder ihre Daten dem Unternehmen für ein Bewerbungsverfahren online zur Verfügung stellen.[20]

Datenschutzrechtliche Bestimmungen zur Erhebung und Verwendung personenbezogener Daten bei der Nutzung von Telemedien finden sich im 4. Abschnitt, in den Regelungen der §§ 11-15 TMG, die sowohl Erlaubnistatbestände zur Verarbeitung personenbezogener Daten bei der Nutzung von Telemedien beinhalten sowie auch besondere Pflichten für die Anbieter von Telemedien.

---

[18] Z.B. LG Frankfurt a.M. mit Urteil v. 18.02.2014, Az. 3-10 O 86/12:
"bb) Zweck der Regelung in § 15 Absatz 3, Absatz 1 TMG ist es, den Datenverarbeitungsvorgang schon zu Beginn des Nutzungsvorgangs für den Nutzer transparent zu gestalten. Die konkrete Gestaltung der Unterrichtung liegt zwar - mangels weiterer gesetzlicher Angaben - im Ermessen des Diensteanbieters. Sie muss aber u. a. klar und zuverlässig wahrnehmbar sein [...]. Diesen Anforderungen entspricht beispielsweise eine Einbindung in den Nutzervorgang, indem der Nutzer über eine Website zwangsläufig mit den Informationen in Berührung kommt oder ein deutlich hervorgehobener Hinweis mit einem Hyperlink auf der Startseite vorhanden ist ..."
Ein direkter Zugang ist aus Sicht dieses Urteils unumgänglich.

[19] Vgl. § 1 Abs.1 TMG

[20] Vgl. § 11 Abs. 2 TMG

Die §§ 14 und 15 im TMG haben eine Doppelfunktion. Zum einen definieren sie die Begrifflichkeiten, zum anderen beinhalten sie die generellen Voraussetzungen für die Erhebung und Verwendung der anfallenden Daten.[21]

4.1.2.2 Abgrenzung BDSG / TMG / TKG

Die Abgrenzung der Anwendungsbereiche der unterschiedlichen datenschutzrechtlichen Normen erfolgt nach dem sogenannten „Schichtenmodell". Während sich die datenschutzrechtliche Zulässigkeit des Datentransports (Telekommunikation) nach dem Telekommunikationsgesetz (TKG) richtet, beurteilt sich die Zulässigkeit der Interaktion zwischen Nutzer und Anbieter nach dem TMG. Für Datenverarbeitungen, bei denen ein Telemedium lediglich als Übertragungsmedium genutzt wird, ist weiterhin das BDSG anzuwenden. [22]

4.1.2.3 Bestandsdaten

Es ist einem Diensteanbieter gestattet, Bestandsdaten eines Nutzers zu erheben, zu verarbeiten und zu nutzen, soweit dies für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich ist. [23]

Dazu zählen Angaben wie zum Beispiel Name, Anschrift, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Bankverbindung, Kreditkartennummer, öffentlicher Schlüssel oder die User-ID des Dienstenutzers.

Normadressaten sind Diensteanbieter, die ihre Dienste auf Basis eines Vertragsverhältnisses anbieten[24].

4.1.2.4 Nutzungsdaten

Die Daten, die erforderlich sind, um Telemediendienste überhaupt nutzen und abrechnen zu können, dürfen zulässigerweise von einem Diensteanbieter erhoben und verwendet werden, soweit sie für diese Zwecke erforderlich sind. Dazu zählen beispielsweise Angaben über genutzte Medien, Identifikationsmerkmale, Angaben über Beginn, Ende und Umfang der Nutzung.[25]

4.1.2.5 Inhaltsdaten

Unter „Inhaltsdaten" sind diejenigen personenbezogenen Daten zu verstehen, die der Diensteanbieter vom Nutzer erhält, wenn zwischen diesen beiden Parteien bei der Nutzung des Telemediendienstes eine zweite vertragliche Beziehung über die Lieferung oder Leistung einer Ware oder Dienstleistung begründet wird.[26]

Danach zählen zu den Inhaltsdaten auch alle Informationen, die ein Nutzer über eine Webseite dem Datenaustauschplattformbetreiber zur Verfügung stellt. Hierzu gehören digitale Dokumente wie z.B. Entlassbriefe, Operationsberichte, Röntgenbilder oder Laborbefunde oder die Angaben, die mit einem Online-Fragebogen erhoben und die über die Webseite auf einen Server hochgeladen werden können.

Weil im TMG aber nicht, wie bei den Bestands-, oder Nutzungsdaten auch Inhaltsdaten normiert sind, besteht weiterhin Unklarheit darüber, welche Regelungen dafür anzuwenden sind.

Nach dem Wortlaut des § 11 Abs. 1 TMG gelten die datenschutzrechtlichen Vorschriften des TMG für „personenbezogene Daten der Nutzer von Telemedien".

---

[21] Zscherpe in: Taeger/Gabel, BDSG, 2010, § 15 TMG, Rn. 11
[22] Rockstroh/Leuthner in Taeger, Law as a Service (Laas) Band 1 , 2013 , S.128
[23] Vgl. Zscherpe in: Taeger/Gabel; BDSG; 2010; § 14 TMG; Rn. 6
[24] Vgl. § 14 Abs.1 TMG
[25] Vgl. §15 Abs. 1-7 TMG
[26] Zscherpe in: Taeger/Gabel, BDSG, 2010, § 14 TMG , Rn. 19

Demnach wären grundsätzlich auch solche Daten eines Telemediennutzers erfasst, die nicht unmittelbar im Zusammenhang mit den genutzten Telemedien stehen, sondern für andere Rechtsverhältnisse anfallen, die durch oder mit Hilfe der Telemedien begründet werden. Entsprechend würden diese Inhaltsdaten dem TMG unterfallen und dürften gemäß § 12 Abs. 1 TMG nur mit ausdrücklicher Einwilligung des Nutzers, welcher nicht notwendigerweise mit dem Betroffenen, dessen Daten in der Austauschplattform vorhanden sind, übereinstimmen muss, erhoben, verarbeitet und genutzt werden.[27]

Dies würde bedeuten, dass für die Erhebung, Verarbeitung und Speicherung grundsätzlich eine ausdrückliche Einwilligung erforderlich wäre sowie die Anwendung der strengeren Datenschutz-Auflagen des TMG (Abschnitt 4 TMG §§ 11-15 TMG) zur Geltung kommen. Entsprechend §12 Abs. 1 TMG ist auch für die Erhebung und Verwendung von personenbezogenen oder personenbeziehbaren Daten eine Rechtsgrundlage oder die Einwilligung des Betroffenen erforderlich, hier gilt das in Kapitel 4.1.1 Gesagte. Allerdings gestattet §13 Abs. 2 TMG eine elektronische Einwilligung, wenn folgende Voraussetzungen erfüllt sind:

1) Der Nutzer hat seine Einwilligung bewusst und eindeutig erteilt.
2) Die Einwilligung wird protokolliert.
3) Der Nutzer kann den Inhalt der Einwilligung jederzeit abrufen.
4) Der Nutzer kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen.

Anforderung 8: Wird die Einwilligung des Betroffenen elektronisch eingeholt, so muss der Vorgang protokolliert werden und der Inhalt der Einwilligung für den Betroffenen jederzeit abrufbar sein.

4.1.3 Anonymisierung bzw. Pseudonymisierung

Entsprechend §3a Satz 2 BDSG sind personenbezogene Daten „zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert“.

Die Artikel-29-Datenschutzgruppe veröffentlichte im Mai 2014 eine Stellungnahme zum Thema Anonymisierungstechniken[28]. Nach der Ausarbeitung der Artikel-29-Datenschutzgruppe ist "Anonymisierung als ein auf personenbezogene Daten angewandtes technisches Verfahren nach dem aktuellen Stand der Technik" anzusehen, d.h. das Ergebnis einer Anonymisierung muss "so dauerhaft sein wie eine Löschung“. Bei Anerkennung dieser Definition ist im Rahmen von Datenaustauschplattformen im Gesundheitswesen wohl immer von einer Pseudonymisierung auszugehen, da bei hinreichendem Zusatzwissen eine Re-Identifizierung nie gänzlich ausgeschlossen werden kann, wie verschiedene Studien (z.B. [29,30,31,32]) zeigen.

Anforderung 9: Personenbezogene oder personenbeziehbare Daten müssen pseudonymisiert werden, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

---

[27] Zscherpe in: Taeger/Gabel, BDSG, 2010, § 14 TMG, Rn.22; Vgl. ebenfalls LfDI Niedersachsen, OH für Diensteanbieter von Telemedien, Grundsätzliches zur Verarbeitung, personenbezogener Daten, S. 3

[28] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. [Online, zitiert 2015-02-13] Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[29] Montjoye YA, Radaelli L, Singh VK, Pentland A. (2014) Unique in the shopping mall: On the reidentifiability of credit card metadata. Science Vol. 347 no. 6221: 536-539

[30] Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. (2013) Identifying Personal Genomes by Surname Inference. Science Vol. 339 no. 6117: 321-324

[31] Bohannon J. (2013) Genealogy Databases Enable Naming of Anonymous DNA Donors. Science Vol. 339 no. 6117: 262

[32] Christl W. (2014) Kommerzielle digitale Überwachung im Alltag. [Online, zitiert 2015-02-13] Verfügbar unter http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf

Es bietet sich also an, bei der Nutzung von Datenaustauschplattformen mit abstrakten Kodierungen (z.B. separate Nummernkreise) etc. zu arbeiten, sofern das im Rahmen der Behandlung akzeptabel und beherrschbar ist. Bereits bei der Arztbriefschreibung wird das jedoch nicht mehr möglich sein.

4.1.4 Automatisierte Abrufverfahren

Nach § 10 BDSG ist die Einrichtung eines automatisierten Abrufverfahrens zulässig soweit es unter Abwägung der schutzwürdigen Interessen der Betroffenen und den Aufgaben bzw. Geschäftszwecken der beteiligten Stellen angemessen ist. Geschäftszweck einer Datenaustauschplattform ist, dass Gesundheitsdaten für einen elektronischen Abruf bereitgestellt werden, d.h. Aufgabe/Geschäftszweck einer Datenaustauschplattform beinhaltet automatisierte Verfahren. Dementsprechend muss den datenschutzrechtlichen Anforderungen bzgl. automatisierter Abrufverfahren entsprochen werden.

Anforderung 10: Die beteiligten Stellen haben schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens
2. Dritte, an die übermittelt wird
3. Art der zu übermittelnden Daten
4. Die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen (TOMs) [33]

Die Verantwortung für die Aufzeichnungspflicht des jeweiligen Datenabrufs liegt beim Empfänger (§29 Abs. 2 S. 4 BDSG). Insbesondere sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung aufzuzeichnen (§29 Abs. 2 S. 3 BDSG). Die übermittelnde Stelle muss stichprobenartig die Aufzeichnungen kontrollieren und hierbei auch das berechtigte Interesse einzelfallbezogen prüfen (§29 Abs. 2 S. 5 BDSG).

Anforderung 11: Die speichernde Stelle muss vertraglich dazu verpflichtet werden, dass bei einer Übermittlung der gesetzlich geforderten Aufzeichnungspflicht genügt wird.

Anforderung 12: Die übermittelnde Stelle muss stichprobenartig die Aufzeichnungen der empfangenden Stelle prüfen, insbesondere ist hierbei das berechtigte Interesse der empfangenden Stelle einzelfallbezogen zu prüfen.

4.1.5 Richtlinie 2002/58/EG

Die Richtlinie 2002/58/EG[34] des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (sogenannte „Cookie-Richtlinie“) beschreibt verbindliche Mindestvorgaben für den Datenschutz in der Telekommunikation innerhalb der EU. Daraus resultieren Anforderungen für den Umgang mit Cookies sowie die Auswertung des Nutzungsverhaltens eines Internetauftritts (sogenannte „Web-Statistik“).

4.1.5.1 Cookies

Anforderung 13: Der Betroffene muss der Nutzung von Cookies explizit zustimmen.

Leider wurde diese Cookie-Richtlinie nach der Auffassung der Datenschutzbeauftragten des Bundes und der Länder (Umlaufentschließung vom 05.02.2015) in Deutschland nicht entsprechend der Vorgaben der EU-Richtlinie in nationales Recht umgesetzt. Es reicht in der Praxis derzeit aber aus, wenn in der Datenschutzerklärung oder über einen Link in einem entsprechenden Banner auf die Verwendung von Cookies hingewiesen wird und eine Opt-out-Möglichkeit besteht.

Anforderung 14: Die Verwendung von Cookies durch Drittanbieter muss auf die Erstellung anonymer Nutzungsstatistiken beschränkt sein.

---

[33] Schutze-Melling in Taeger/Gabel, BDSG, 2010 § 10

[34] Richtlinie 2002/58/EG [Online, zitiert 2015-02-13] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32002L0058

Anforderung 15: Das Handling der Drittanbieter-Cookies muss durch den Betroffenen steuer- und nachvollziehbar sein.

Anforderung 16: Soweit möglich, müssen Drittanbieter temporäre Cookies verwenden.

Anforderung 17: Die Gültigkeit persistenter Cookies von Drittanbietern darf nicht länger als 30 Tage betragen.

4.1.5.2 Auswertung bzgl. Nutzung der Datenaustauschplattform („Web-Statistik")

Anforderung 18: Die Erhebung, Verarbeitung und Nutzung von Daten zur Erstellung von Nutzungsstatistiken von Webportalen muss dokumentiert werden.

Anforderung 19: Die Erstellung von Nutzungsstatistiken von Datenaustauschplattformen muss auf Basis anonymisierter Daten erfolgen.

Anforderung 20: Eine Analyse des Nutzerverhaltens (einschließlich Geolokalisierung) auf der Basis gekürzter IP-Adressen ist ohne Einwilligung des Betroffenen möglich, wenn durch die Kürzung der IP-Adresse ein Personenbezug ausgeschlossen wurde.

Anforderung 21: Beim Einsatz eines Dienstleisters ist ein ADV-Vertrag zu schließen. Hat der Dienstleister außerhalb des EWR seinen Geschäftssitz, sind die hier geltenden besonderen Anforderungen zu beachten[8].

4.2 Grundsatz der klaren Verantwortlichkeiten

Im Zentrum steht das Verhältnis zwischen dem Plattform-Nutzer, der die Daten in der Plattform speichert, und dem Plattformbetreiber (Provider), der die Plattform bereitstellt. Für die Frage, welches Datenschutzrecht die Rahmenbedingungen der Nutzung vorgibt, kommt es jedoch nicht nur auf dieses Verhältnis an, sondern auch auf das Verhältnis zwischen dem Plattformnutzer und dem Betroffenen / Patienten – also demjenigen, dessen Daten in der Plattform gespeichert und zum Abruf bereit gestellt werden. Ein Vertragsverhältnis selbst wird i.d.R. zwischen Plattformbetreiber und Plattformnutzer bestehen, jedoch kein direktes zwischen dem Betroffenem, also dem Betroffenen, und dem Plattformbetreiber. Vielmehr wird der Plattformnutzer häufig in die Behandlung des Betroffenen integriert sein. Jedoch gibt es auch genug Beispiele (z.B. Krankheitsregister), in welchem die Plattformnutzer nicht notwendigerweise in die Behandlung des Betroffenen integriert sind.

§3 Abs. 7 BDSG definiert eine „verantwortliche Stelle" als eine Person oder Stelle, welche personenbezogene oder personenbeziehbare Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Entsprechend der europäischen Datenschutzrichtlinie[35] kommt es bei der Feststellung des Verantwortlichen auf die tatsächlichen objektiven Umstände an: wer „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" (Art. 2 Nr. d) RL 5/46/EG) ist der für die Verarbeitung Verantwortliche.

Damit ein Betroffener diesem Verantwortlichen gegenüber seine Rechte wahrnehmen kann, müssen die entsprechenden Kontaktstellen benannt werden.

Anforderung 22: Es muss öffentlich verfügbar sein, wer innerhalb der verantwortlichen Stelle Entscheider ist und wie er kontaktiert wird; die Mindestanforderung ist ein Impressum entsprechend §5 TMG.

Anforderung 23: Der Kontakt zum Datenschutzbeauftragten der verantwortlichen Stelle sollte öffentlich verfügbar gemacht werden.

Anforderung 24: Es sollte benannt und öffentlich verfügbar gemacht werden, wer innerhalb der verantwortlichen Stelle Adressat einer Datenschutzfrage eines Betroffenen oder eines staatlichen Organs (z.B. der Datenschutzaufsicht) ist.

---

[35] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. [Online, zitiert 2015-02-13] Verfügbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML

Für den Betroffenen müssen die Prozesse bzgl. der Verarbeitung seiner Daten transparent gemacht werden können. Der öffentliche Teil des sogenannten „Verfahrensverzeichnisses“ (auch „Verfahrensübersicht“ oder „Jedermannverzeichnis“ genannt), also die Übersicht der in §4e BDSG genannten Angaben, muss Jedermann „auf Antrag in geeigneter Weise“ vom DSB zur Verfügung gestellt werden.

Anforderung 25: Die Übersicht der in §4e Ziff. 1-8 BDSG genannten Angaben muss für jeden Betroffenen öffentlich verfügbar gehalten werden.

✍ **Hinweis:** Stellt man die Übersicht der in §4e Ziff. 1-8 BDSG genannten Angaben als Download z.B. bei den Datenschutzhinweisen oder beim Impressum des eigenen Internet-Auftritts zur Verfügung, so kann dies die Anzahl der Anfragen reduzieren. Eine gesetzliche Pflicht, diese Angaben im Internet zur Verfügung zu stellen, existiert nicht.

4.2.1 Auftragsdatenverarbeitung

Selbstverständlich bedarf auch die Hard- und Software der hier beschriebenen Datenaustauschplattform einer regelmäßigen Wartung, die in den seltensten Fällen der Betreiber der Datenaustauschplattform selbst vornehmen wird. Vielmehr wird regelhaft der bzw. die Hersteller der eingesetzten Hard- und Software die Wartung übernehmen. Hierzu muss ein Auftragsdatenverarbeitungsvertrag („ADV-Vertrag“) abgeschlossen werden. Für die Erstellung eines ADV-Vertrages erarbeitete eine Gruppe, bestehend aus Mitgliedern der Organisationen/Verbände BvD, bvitg, GDD und GMDS, einen kommentierten Muster-ADV-Vertrag[36], welcher hier weitere Informationen bietet.

Innerhalb einer Auftragsdatenverarbeitung findet datenschutzrechtlich keine Übermittlung statt: da der Auftraggeber für die Verarbeitung der Daten beim Auftragnehmer verantwortlich bleibt, ist die Beauftragung der Datenverarbeitung beim Auftragnehmer somit vereinfacht (privilegiert) möglich und wird datenschutzrechtlich wie eine innerbetriebliche Weitergabe behandelt. Dienstleister außerhalb des Europäischen Wirtschaftsraumes (EWR), z.B. in den USA, unterliegen nicht dieser Vereinfachung, d.h. hier findet keine Auftragsdatenverarbeitung statt.

Besonders zu beachten ist, dass die Verarbeitung von sensitiven Daten / Gesundheitsdaten nur mit ausdrücklicher Einwilligung des Betroffenen außerhalb des Schutzbereiches des europäischen Datenschutzrechts stattfinden darf. Eine Auftragsdatenverarbeitung außerhalb der EU verbietet sich bei solchen Daten regelmäßig.

Wenn keine Auftragsdatenverarbeitung vorliegt (z.B. weil keine Weisungsbefugnis vorliegt), spricht man von einer Funktionsübertragung. Bei einer Funktionsübertragung wird der Auftragnehmer selbst die für die Datenverarbeitung verantwortliche Stelle, d.h. es findet datenschutzrechtlich eine Übermittlung statt, für die wiederum entweder eine rechtliche Erlaubnisnorm oder die Einwilligung eines Betroffenen vorliegen muss.

Für ausgewählte Länder[37] hat die EU-Kommission erklärt, dass in diesen Ländern ein dem EU-Recht entsprechendes angemessenes Datenschutzniveau vorhanden sein kann. Zur Auftragsverarbeitung mit Dienstleistern in Ländern, in denen seitens der EU-Kommission bisher kein der EU-Gesetzgebung entsprechendes angemessenes Datenschutzniveau festgestellt wurde, stellte die EU-Kommission „Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern“[38] zur Verfügung, die zur Auftragsverarbeitung in diesen Ländern eingesetzt werden

[36] „Muster eines Auftragsdatenverarbeitungsvertrags im Gesundheitswesen“. [Online, zitiert 2015-04-05] Verfügbar unter http://www.gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen bzw. http://gddak.eh-cc.de/materialien_und_links/ bzw.

[37] Commission decisions on the adequacy of the protection of personal data in third countries. [Online, zitiert 2015-04-05] Verfügbar unter http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[38] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des

können. Wird ein rechtsgültiger EU-Standardvertrag abgeschlossen, gilt entsprechend §4b Abs. 1 und Abs. 2 BDSG ebenfalls die oben beschriebene Privilegierung bei der Datenverarbeitung durch einen Dienstleister.

4.3 Grundsatz der Zweckbindung sowie der Datenvermeidung und Datensparsamkeit

Es dürfen nur solche Daten erhoben, gespeichert oder verarbeitet werden, die unmittelbar dem eigentlichen Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses mindestens notwendig sind (Prinzip der Datenvermeidung und Datensparsamkeit entsprechend §3a BDSG).

Eine Zweckänderung ist nur mit entsprechender Einwilligung des Betroffenen möglich oder eine andere Rechtsvorschrift wie z.B. Forschungsklauseln in den Krankenhausgesetzen der Länder erlauben die Nutzung.

Anforderung 26: Eine Zweckänderung bedarf einer Erlaubnisnorm (Einwilligung des Betroffenen oder gesetzlicher Erlaubnistatbestand).

Anforderung 27: Um die Sparsamkeit der Datenerhebung zu gewährleisten, ist der Verwendungszweck jedes Datums bzw. jeder Datenkategorie zu beschreiben.

Anforderung 28: Daten, die keinen zur Erfüllung der Aufgabe definierten Verwendungszweck haben, dürfen nicht erhoben, verarbeitet oder genutzt werden.

Der Verwendungszweck der Daten darf sich in keinem nachgelagerten Schritt der Verarbeitung, auch nicht nach einer Übermittlung ändern. Insbesondere bei Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, wird eine Änderung des Verwendungszweckes ohne gesetzliche Grundlage gemäß §39 BDSG verboten, d.h. eine Zweckänderung kann in diesen Fällen auch nicht mit einer Einwilligung des Betroffenen legalisiert werden.

Anforderung 29: Eine Änderung des Verwendungszweckes von Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ist untersagt und muss durch technische und organisatorische Maßnahmen verhindert werden.

Ein striktes Verbot der Zweckänderung besteht weiterhin entsprechend §31 BDSG für Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden.

Eine Änderung des Verwendungszweckes von Daten, die ausschließlich zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert wurden (§ 31 BDSG), ist untersagt und muss durch technische und organisatorische Maßnahmen verhindert werden. Verpflichtung zum Schutz der Daten

4.3.1 Zeugnisverweigerungsrecht und Beschlagnahmeverbot

Für Daten von Personenkreisen, die in §53 Abs. 1 Ziff. 1-3b StPO genannt werden (z.B. Ärzte, Zahnärzte, Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apotheker und Hebammen), existiert neben dem Zeugnisverweigerungsrecht gemäß §97 Abs. 1 StPO auch ein Beschlagnahmeverbot. Hier gilt, dass „über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist“, diese Personenkreise zur Verweigerung des Zeugnisses berechtigt sind, d.h. sie sind berechtigt vor Gericht und anderen staatlichen Ermittlungsbehörden wie beispielsweise der Polizei oder der Staatsanwaltschaft die Auskunft in Bezug auf den Patienten zu verweigern. Das Zeugnisverweigerungsrecht gilt nicht mehr, wenn eine Schweigepflichtentbindung vorliegt.

Europäischen Parlaments und des Rates. [Online, zitiert 2015-04-05] Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32010D0087

Entsprechend §53a StPO gilt das Zeugnisverweigerungsrecht auch für deren Gehilfen und anderen Personen, "die zur Vorbereitung auf den Beruf an der berufsmäßigen Tätigkeit teilnehmen", entsprechend §97 Abs. 2 S. 2 und Abs. 3 StPO ist hier auch ein Beschlagnahmeverbot gegeben. Bei dieser Vorschrift wird nach herrschender Meinung der Begriff „Gehilfe“ ebenfalls dahingehend interpretiert, dass derjenige, der nur faktisch tätig wird, ein Gehilfe sein kann[39]. Als maßgeblich wird die Veranlassung der Tätigkeit durch den Hauptberufsgeheimnisträger gesehen. Lediglich Tätigkeiten, die nicht im unmittelbaren Zusammenhang mit der Berufstätigkeit stehen, werden nicht vom Begriff des Gehilfen erfasst[40].

Werden Gesundheitsdaten in eine Datenaustauschplattform eingestellt, sodass diese Daten jemand einsehen kann, der

a) entweder nicht in die Behandlung integriert ist und diese Daten damit nicht in seiner Eigenschaft als zur Zeugnisverweigerung berechtigten Berufsgruppe zur Kenntnis nahm
b) oder die Daten zur Kenntnis nahm, aber selbst nicht unter den Kreis der zur Zeugnisverweigerung Berechtigten gehört,

so besteht kein Zeugnisverweigerungsrecht gegenüber Gerichten und staatlichen Ermittlungsbehörden.

Ob der Betreiber der Datenaustauschplattform bzw. die Personen, welche die Datenaustauschplattform warten und ggfs. Einsicht in die Daten bekommen, als Gehilfen im Sinne von §53a StPO anzusehen sind, kann nur im Einzelfall entschieden werden. Für Daten, für die entsprechend §53 StPO bzw. §53a StPO ein Zeugnisverweigerungsrecht bestehen, existiert gemäß §97 Abs. 1 StPO auch ein Beschlagnahmeverbot. Das Beschlagnahmeverbot gilt allerdings nur, wenn

a) sich die Daten im Gewahrsam der zur Verweigerung des Zeugnisses Berechtigten befinden oder
b) wenn diese sich im Gewahrsam einer Krankenanstalt oder eines Dienstleisters, der für die Genannten personenbezogene Daten erhebt, verarbeitet oder nutzt, befinden.

Ob Daten in einer Datenaustauschplattform durch ein Beschlagnahmeverbot geschützt sind, kann ebenfalls nur im Einzelfall beurteilt werden.

4.3.2 Bestellung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten

Entsprechend §4f Abs. 1 S. 6 BDSG ist ein Beauftragter für den Datenschutz (DSB) zu bestellen, wenn eine automatisierte Verarbeitung von Daten, die einer Vorabkontrolle unterliegen, erfolgt oder „personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung“ verarbeitet werden. Darüber hinaus ist ein DSB zu bestellen, wenn mehr als 9 Personen in einer verantwortlichen Stelle personenbezogene Daten automatisiert verarbeiten.

Unter einer automatisierten Verarbeitung ist gemäß §3 Abs. 2 BDSG eine Verarbeitung z.B. unter Nutzung eines Datenverarbeitungsanlage zu verstehen. Entsprechend §4d Abs. 5 BDSG ist eine Vorabkontrolle insbesondere dann durchzuführen, wenn besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden.

Datenschutzrechtlich wird entsprechend §3 Abs. 4 Ziff. 3 BDSG unter „übermitteln“ das Bekanntgeben personenbezogener Daten an einen Dritten verstanden, indem entweder die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Eine Datenaustauschplattform beinhaltet den Zweck, Gesundheitsdaten anderen Personen oder Stellen zur Ansicht zu präsentieren oder durch Download zur Verfügung zu stellen, d.h. im datenschutzrechtlichen Sinne die Daten zu übermitteln.

[39] Meyer-Goßner, StPO, § 53a Rn. 2; Senge, in: Karlsruher Kommentar StPO, § 53a Rn. 2; Rogall, in: Systematischer Kommentar StPO, § 53a Rn. 8; Lemke, in: Heidelberger Kommentar StPO, § 53a Rn. 2
[40] Senge, in: Karlsruher Kommentar StPO, § 53a Rn. 2

Daraus ergibt sich für einen Betreiber einer Datenaustauschplattform die gesetzliche Verpflichtung einen Beauftragten für den Datenschutz zu bestellen.

Anforderung 30: Es muss ein Beauftragter für den Datenschutz bestellt werden.

4.3.3 Verpflichtung der auf die Daten Zugreifenden

Gemäß §5 BDSG sind Personen (Mitarbeiter/-innen) bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Gilt für den Betreiber der Datenaustauschplattform das Telekommunikationsgesetz, so muss ebenfalls eine Verpflichtung auf das Fernmeldegeheimnis entsprechend §88 TKG erfolgen. Idealerweise erfolgt zugleich eine Information der vorgenannten Mitarbeiter/-innen, dass sie nach §17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) zur Wahrung von Geschäftsgeheimnissen, zu welchen letztlich auch die in der Datenaustauschplattform gespeicherten Gesundheitsdaten gehören, verpflichtet sind.

Anforderung 31: Alle Personen, welche auf die gespeicherten Gesundheitsdaten zugreifen können, müssen vor dem erstmaligen Zugriff auf die Wahrung des Datengeheimnisses verpflichtet worden sein.

4.3.4 Telemediengesetz

§13 Abs. 6 TMG gebietet, dass die Nutzung von Telemedien nach Möglichkeit anonym oder unter Pseudonym zu ermöglichen ist. Zugleich muss der Betreiber einer Datenaustauschplattform einem Betroffenen jederzeit Auskunft geben können, wer auf die Daten des Betroffenen wann zugegriffen hat. Dies ist bei einer anonymen Nutzung nicht möglich, daher ist eine anonyme Nutzung im Umfeld der hier besprochenen Austauschplattformen für Gesundheitsdaten regelhaft nicht statthaft.

Anforderung 32: Ein anonymer Zugriff des Plattformbetreibers sowie der Nutzer der Plattform auf personenbezogene oder personenbeziehbare Gesundheitsdaten ist zu unterbinden.

Bei einem Zugriff auf die gespeicherten Gesundheitsdaten mittels eines Pseudonyms muss dem Betroffenen auf Nachfrage die zugreifende Person entpseudonymisiert mitgeteilt werden.

§13 Abs. 4 TMG verlangt, dass der Telemedien-Anbieter durch technische und organisatorische Vorkehrungen gewährleistet, dass insbesondere folgende Anforderungen erfüllt sind:

- die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder gesperrt (= Vorliegen von gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen) werden,
- der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann (Verschlüsselung der Kommunikation und der gespeicherten Daten),
- die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
- Nutzungsprofile nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

Aufgrund der Tatsache, dass Betroffenen gegenüber Auskunft gegeben werden muss, wer wann auf welche Daten zugegriffen hat, sind die Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar auf Datenaustauschplattformen im Gesundheitswesen zu sperren und nicht zu löschen.

Anforderung 33: Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung sind unmittelbar nach dem Zugriff bzw. ggfs. nach erfolgter Abrechnung der Dienstenutzung zu sperren und nur zu entsperren, wenn eine gesetzliche Bestimmung (z.B. Auskunftsersuchen eines Betroffenen) dies erlaubt.

Anforderung 34: Die Nutzung von Telemedien muss gegen die Kenntnisnahme unberechtigter Dritter geschützt werden.

4.4 Grundsatz der Gewährleistung der Betroffenenrechte

Jeder Betroffene besitzt entsprechend §6 BDSG grundlegende Rechte bzgl. der ihn betreffenden Daten. Zu diesen Rechten gehören das Recht auf Auskunft bzgl. seiner Daten sowie die Rechte auf Berichtigung, Löschung oder Sperrung seiner Daten.

4.4.1 Auskunft

Dem Betroffenen muss jederzeit Auskunft darüber gegeben werden,

a) wer wann auf welche seiner Daten aus welchen Gründen bzw. mit welcher Berechtigung zugegriffen hat und
b) wer wann welche seiner Daten aus welchen Gründen bzw. mit welcher Berechtigung an wen weitergegeben hat.

Damit dies gewährleistet ist, müssen entsprechende Zugriffe protokolliert werden.

Anforderung 35: Es muss protokolliert werden, wer wann auf welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung zugegriffen hat.

Anforderung 36: Es muss protokolliert werden, wer wann welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung exportiert oder ausgedruckt hat. Zu jedem Datenexport oder Ausdruck ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, zu welchem Zweck ein Datenexport oder ein Ausdruck erfolgte.

Es muss nachvollziehbar sein, wer wann welche Daten gespeichert, verändert, gesperrt oder gelöscht hat.

Anforderung 37: Es muss protokolliert werden, wer wann welche personenbezogenen oder personenbeziehbaren Daten gespeichert, verändert, gesperrt oder gelöscht hat. Bei jeder Löschung ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, wer aus welchem Grund welche Daten löschte.

Existiert in der Anwendung aufgrund eingetretener Umstände (z.B. eines Notfalls) die Möglichkeit auf Daten zuzugreifen, auf die die oder der Zugreifende laut Berechtigungskonzept keinen Zugriff hätte (z.B. mittels eines sogenannten „Notfall-Button“), so ist dieser Zugriff unter Angabe des Grundes zu protokollieren.

Anforderung 38: Es muss protokolliert werden, wer wann auf welche personenbezogenen oder personenbeziehbaren Daten durch die Nutzung erweiterter Systemprivilegien (z.B. durch den sogenannten „Notfall-Zugriff“) zugriff. Zu jedem Datenzugriff unter Nutzung von durch das System bereitgestellten Mechanismen zur Erweiterung der Zugriffsberechtigung ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, zu welchem Zweck ein Zugriff, ein Datenexport oder ein Ausdruck erfolgte.

Weiterhin muss nachvollziehbar sein, wenn jemand den Versuch unternahm, auf Daten unberechtigt zuzugreifen. Dies erfolgt durch eine Auswertung der Protokolldaten. Ergibt diese Auswertung, dass möglicherweise ein unberechtigter Zugriff erfolgte, so muss dies zu einer Alarmmeldung führen, wobei die Alarmmeldungen ebenfalls protokolliert werden.

Anforderung 39: Ereignisse, die potenziell dazu führen können, dass ein unberechtigter Zugriff auf personenbezogene oder personenbeziehbare Daten erfolgen könnte, sind zu protokollieren.

Beispielhaft hierfür wären folgende Ereignisse:

- 2 x gleichzeitige Anmeldung des Benutzers
- Anmeldung außerhalb Dienstzeit
- Anzahl Fehlanmeldungen >= 3

- Druck > n Dokument(e)[41]
- Druck > n Dokument(e)[41] ohne Begründung
- Export > n Dokument(e)[41]
- Export > n Dokument(e)[41] ohne Begründung
- Notfallanmeldung
- Notfallanmeldung ohne Begründung
- Änderung Systemrichtlinien
- Erweitern der Benutzerberechtigung zu administrativen Rechten
- Veränderung am Regelwerk zur Protokollierung
- Veränderung am Regelwerk zur Protokollierung ohne Begründung
- Zugriff auf Protokolldaten
- Zugriff auf Protokolldaten ohne Begründung
- Zugriff mit "Super-User"-Rechten außerhalb der Arbeit an der Systemkonfiguration.

Dabei muss berücksichtigt werden, dass entsprechend §31 BDSG „personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden“ auch nur für diese Zwecke verwendet werden dürfen. D.h. dass die entsprechenden Protokollierungsdaten, die dem Zweck der Erfüllung der datenschutzrechtlichen Bestimmungen dienen, auch nur zu diesen Zwecken benutzt werden dürfen.

Anforderung 40: Enthalten Protokolle personenbezogene oder personenbeziehbare Daten, so dürfen diese Protokolle nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes genutzt werden. Jegliche andere Nutzung ist durch technische und organisatorische Mittel zu verhindern.

Dem Betroffenen ist jederzeit Einsicht in alle zu seiner Person gespeicherten Daten inklusive ggfs. erfolgter Änderungen zu geben (siehe auch §630g Abs. 1 BGB). Auf Aufforderung muss der Betroffene einen Ausdruck oder einen Datenexport der zu seiner Person gespeicherten Daten erhalten (siehe auch §630g Abs. 2 BGB).

Anforderung 41: Der Betroffene muss die Möglichkeit haben, jederzeit Einblick in alle zu seiner Person gespeicherten Daten zu erhalten. Dies umfasst auch die Möglichkeit, Änderungen seiner gespeicherten Daten nachzuvollziehen.

Anforderung 42: Der Betroffene muss die Möglichkeit haben, einen Ausdruck oder einen für ihn verwertbaren Export aller zu seiner Person gespeicherten Daten zu erhalten.

4.4.2 Berichtigung falscher Daten

Der Betroffene hat das Recht, falsche Angaben zu seiner Person berichtigen zu lassen.

Anforderung 43: Es muss eine Möglichkeit geben, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren.

Erfolgen Berichtigungen der Daten zu einem Betroffenen, so ist dies eine Veränderung, die protokolliert werden muss. Es sollte möglich sein, dass der Ändernde dokumentieren kann, dass die Änderung auf Aufforderung des Betroffenen erfolgte.

Anforderung 44: Es muss protokolliert werden, wer wann welche Daten eines Betroffenen auf dessen Wunsch änderte. Es sollte die Eingabe der Begründung „Änderung erfolgte auf Wunsch

[41] „n“ ist bei den oben angeführten Anforderungen Platzhalter für eine konfigurierbare ganze Zahl, die entsprechend dem Schutzbedarf der Gesundheitsdaten der jeweiligen Gesundheitseinrichtung definiert wird, wobei die Zahl so gewählt werden sollte, dass ein unverhältnismäßiger Export der Gesundheitsdaten eines Betroffenen erkannt werden kann. Für verschiedene Systeme sollte die Zahl individuell festgelegt werden; die Anzahl der Ausdrucke aus einem Archivsystem beispielsweise dürfte sich von der aus einem Archivsystem unterscheiden.

des Betroffenen“ möglich sein.

Anforderung 45: Wurden Daten vom Betreiber der Datenaustauschplattform an andere Stellen übermittelt, so sollte der Betreiber der Datenaustauschplattform, sofern zumutbar, diese Stellen über erfolgte Berichtigungen informieren, sofern diese Benachrichtigung im Interesse des Betroffenen liegt.

4.4.3 Löschen bzw. Sperren

Daten, für welche die Grundlage zu ihrer Speicherung fehlt, müssen gelöscht werden.

Anforderung 46: Es muss eine Löschfunktion implementiert werden, welche eine Rekonstruktion gelöschter Informationen ausschließt.

Anforderung 47: Es ist in einem Löschkonzept festzulegen, wann welche Daten zu löschen sind.

Anforderung 48: Liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, sind die Daten auf Anweisung des Betroffenen unverzüglich zu löschen.

Anforderung 49: Entfällt der Verwendungszweck und es liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, sind die Daten unverzüglich zu löschen.

Anforderung 50: Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren Wiederverwendung datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet.

Anforderung 51: Eine Weitergabe von Datenträgern an externe Stellen zur datenschutzgerechten Entsorgung ist nur zulässig, wenn der Datenträger vor der Übergabe an die externe Stelle datenschutzgerecht gelöscht wurde.

Anforderung 52: Die Löschung der Daten ist unter Angabe des Löschgrunds sowie des Anwenders, der die Löschung vornahm, zu protokollieren.

An Stelle des Löschens kann entsprechend §20 BDSG bzw. §35 BDSG eine Sperrung der Daten vorgenommen werden, wenn

- einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
- Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
- eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Entsprechend §630f BGB müssen Berichtigungen und Änderungen von Eintragungen in der Patientenakte so durchgeführt werden, dass

a) der ursprüngliche Inhalt erkennbar bleibt und ebenso
b) wann die Berichtigungen und Änderungen vorgenommen wurden.

Die Aufzeichnungspflicht nach §630f BGB führt zudem im Rahmen von Haftungsansprüchen vor Gericht zu einer Beweislastumkehr: Hat der Behandelnde eine medizinisch gebotene, wesentliche Maßnahme und ihr Ergebnis entgegen § 630f Absatz 1 oder Absatz 2 nicht in der Patientenakte aufgezeichnet oder hat er die Patientenakte entgegen § 630f Absatz 3 nicht im Rahmen der Aufbewahrungspflichten archiviert, wird vermutet, dass er diese Maßnahme nicht getroffen hat (§630h BGB). Letztlich wird damit eine Aufbewahrung gefordert, welche die Daten vor Veränderung und Verfälschung schützt und vor Verlust sichert.

Dies führt zu einem Konflikt mit dem datenschutzrechtlichen Löschungsgebot: einerseits wird Löschen unzulässig gespeicherter Daten verlangt, andererseits eine nicht-löschbare und nicht-veränderbare Aufbewahrung. . Dieser Konflikt ist so aufzulösen, dass die Löschung (unter Beachtung der Sicherheitsanforderungen) im größtmöglichen Umfang und zum frühestmöglichen Zeitpunkt

(nach Beendigung der Aufbewahrungsfristen) vorzunehmen ist[42]. Technische und organisatorische Maßnahmen müssen gewährleisten, dass auf eigentlich zu löschende Daten nicht zugegriffen werden kann und auf diese Daten auch im Fall der Rekonstruktion eines Datenbestandes nur im unumgänglich notwendigen Ausmaß von einem im Vorfeld definierten Personenkreis zugegriffen werden kann.

Diese Ausnahmeregelung, wie sie unter anderem auch in §20 Abs. 3 Ziff. 3 BDSG bzw. in §35 Abs. 3 Ziff. 3 BDSG dargelegt wird, ist restriktiv auszulegen. D.h. der Gesetzestext ist im Sinne eines weitest gehenden Löschungsrechts auszulegen. Mit dieser Regelung sollen lediglich betriebswirtschaftlich unsinnige Forderungen ausgeschlossen werden[43].

Wird statt einer Löschung eine Sperrung vorgenommen, so ist dies stets zu begründen. Die Löschung muss unverzüglich erfolgen, wenn der Grund für die erfolgte Sperrung nicht länger gegeben ist, z.B. die gesetzliche Aufbewahrungsfrist abgelaufen ist.

Anforderung 53: Erfolgt statt einer Löschung eine Sperrung der Daten, so muss die Begründung, warum die Daten nicht gelöscht werden, festgehalten werden.

Anforderung 54: Ist der Grund für die Sperrung nicht länger gegeben, so muss unverzüglich eine Löschung erfolgen.

4.4.3.1 Was heißt „löschen“?

Entsprechend §3 Abs. 4 Ziff. 5 wird unter „Löschen“ „das Unkenntlichmachen gespeicherter personenbezogener Daten“ verstanden. „Unkenntlichmachen“ ist in den Datenschutzgesetzen nicht definiert. In Urteilen wird als Beispiel für „Unkenntlichmachen“ auch das Abdecken von Informationen bei Vorlage angeführt[44]. Im Standardkommentar zum BDSG (Simitis[45]) wird „Unkenntlichmachen“ als jede Handlung, die irreversibel bewirkt, dass eine Information nicht länger aus gespeicherten Daten gewonnen werden kann, bezeichnet. Dazu werden mehrere Möglichkeiten dargestellt, denen aber alle eine Forderung zugrunde liegt: Die Informationen dürfen nach der Löschung nicht wiederherstellbar sein. Unkenntlich im datenschutzrechtlichen Sinn sind Daten damit nur dann, wenn die Kenntnisnahme der den Daten innewohnenden Informationen unmöglich ist.

Ein Löschen der Daten kann daher auf verschiedenen Ereignissen beruhen, insbesondere zählen hierzu:

- Entfernen der Signale
  Daten werden hierbei durch Entfernung der die Daten speichernden Signale gelöscht, ohne dass hierbei jedoch die Integrität des Datenträgers selbst beeinträchtigt wird.
- Zerstörung des Datenträgers
  Daten werden durch das physikalische Zerstören des Datenträgers vernichtet und sind damit unkenntlich.
- Löschung der Verknüpfung
  Ergibt sich eine zu löschende Information aus der Verknüpfung zweier (oder mehrerer) Teilmengen, jedoch nicht aus den unverknüpften Teilmengen, so kann eine datenschutzrechtliche Löschung der Information auch durch eine irreversible Löschung der Verknüpfung erfolgen.

---

[42] §3 Abs 4 Ziff. 5 Rn 185 (Dammann U. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 7. Auflage. Nomos Verlag. ISBN 978-3-8329-4183-3)

[43] §35 Abs. 3 Ziff. 3 Rn. 30(Dix A. in Simitis (Hrsg.) Bundesdatenschutzgesetz. 7. Auflage. Nomos Verlag. ISBN 978-3-8329-4183-3)

[44] BGH Urteil vom 13.04.1983 - AZ IVb ZR 374/81 [Online, zitiert 2015-02-13] Verfügbar unter https://www.jurion.de/de/document/show/0:327554,0/
BGH Urteil vom 09. 11.2011 - Az. XII ZB 212/11 [Online, zitiert 2015-02-13] Verfügbar unter http://openjur.de/u/258298.html

[45] Prof. Dr. Dres. h. c. Spiros Simitis (Hrsg.) Bundesdatenschutzgesetz. 7. Auflage. Nomos Verlag. ISBN 978-3-8329-4183-3

4.5 Technisch-organisatorische Maßnahmen

Entsprechend §9 BDSG müssen Stellen, die personenbezogene oder personenbeziehbare Daten erheben, verarbeiten oder nutzen, technische und organisatorische Maßnahmen treffen, um diese zu schützen. Entsprechend der Anlage zu § 9 Satz 1 BDSG gehören zu diesen Maßnahmen insbesondere

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

4.5.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Räumlichkeiten, aus denen heraus der Zugriff auf personenbezogene Daten mittels Datenverarbeitungsanlagen möglich ist, zu verwehren. Damit dies möglich ist, müssen entsprechende Räumlichkeiten benannt werden.

Anforderung 55: Zu schützende Bereiche und deren Zutrittspunkte müssen benannt und schriftlich festgehalten werden. Der Schutzbedarf eines Raumes bzw. eines Gebäudes ist anhand des Schutzbedarfs der gespeicherten Daten festzustellen.

Anforderung 56: Es ist festzulegen, welche Voraussetzung eine Person erfüllen muss, um Zutritt zu erhalten. Der Kreis der Berechtigten ist auf das notwendige Minimum zu beschränken.

Anforderung 57: Zu schützende Räumlichkeiten sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Schließanlage) oder organisatorische (z.B. Pförtner) Maßnahmen gegen den Zutritt durch Unbefugte geschützt werden.

4.5.2 Zugangskontrolle

Eine starke Authentifizierung erfolgt immer auf Basis mehrerer (mindestens zwei) Merkmale wie z.B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft. Letzteres sind in der Regel biometrische Verfahren zur Authentisierung wie z.B. die Stimmerkennung oder ein Irisscan. Nicht alle biometrischen Techniken sind bereits verlässlich, zudem ergeben sich erhebliche sicherheitstechnische Anforderungen durch das notwendige Abspeichern persönlicher Merkmale, daher wird zum heutigen Zeitpunkt vom Einsatz biometrischer Verfahren abgeraten.

Mögliche Methoden, die zur Authentisierung genutzt werden können, sind:

- Benutzername/Passwort (statisch)
- Einmal Passwort / Hardware Token
- Einmal Passwort / Mobiltelefon
- PKI / zertifikatsbasierte Anmeldung
- SMS Passwort
- Sicherheitsfragen
- Geo-Lokalisation
- Verhaltensbasierend
- Geräte-Identifikation
- Virtuelle Smartcards

Anforderung 58: Da im Internet eine potenziell größere Gefährdung für einen unbefugten Zugriff auf personenbezogene Daten existiert, muss mindestens eine 2-Faktor-Authentifizierung erfolgen.

Damit statische Passwörter als sicher gelten können, müssen Mindestregeln eingehalten werden[46]:

a) Ein Passwort sollte mindestens zwölf Zeichen lang sein, sind sogenannte Offline-Attacken möglich, sollte es mindestens 20 Zeichen lang sein.
b) Es sollte aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen (?!%+…) bestehen.
c) Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter.
d) Wenn möglich sollte es nicht in Wörterbüchern vorkommen.
e) Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht „asdfgh“ oder „1234abcd“ und so weiter.
f) Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen ($! ? #), am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.
g) Einheitliche Passwörter für verschiedene Zwecke beziehungsweise Zugänge (Accounts) sind zu vermeiden.
h) Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden, mindestens halbjährlich.
i) Es ist zu beachten, dass Umlaute bei Reisen ins Ausland auf einer landestypischen Tastatur ggfs. nicht eingegeben werden können.
j) Passwörter dürfen nicht in unverschlüsselten E-Mails versendet oder in einer anderen Form ohne entsprechenden Schutz übertragen werden.
k) Passwörter dürfen nicht an Dritte weitergegeben werden.

Anforderung 59: Werden statische Passwörter zur Authentisierung eingesetzt, so müssen die Empfehlungen des BSI bzgl. der Generierung und des Umgangs eingehalten werden. D.h. es müssen technische und organisatorische Maßnahmen zu der Einhaltung der Empfehlungen des BSI getroffen werden.

Anforderung 60: Authentisierungsgeheimnisse dürfen nur gesichert in Netzwerken übertragen werden, d.h. es muss eine verschlüsselte Datenübertragung entsprechend dem Stand der Technik eingesetzt werden.

Anforderung 61: Passwörter und/oder entsprechende Formulareingaben dürfen nicht auf dem Client oder in seiner Umgebung unverschlüsselt gespeichert werden, eine Speicherung im Browser ist zu verhindern.

Es muss gewährleistet sein, dass wiederholte fehlerhafte Eingaben zu einer Sperrung des Zugangs führen, ohne dass hierbei der Zugriff auf die Gesundheitsdaten dauerhaft verhindert wird. Zugangsdaten, die über einen definierten Zeitraum (z.B. 40 Tage bei 30 Urlaubstagen im Jahr) hinweg ungenutzt bleiben, sind zu sperren.

[46] Empfehlung des BSI. [Online, zitiert 2015-02-13] Verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html

Anforderung 62: Nach wiederholter fehlerhafter Authentisierung muss der Zugang gesperrt werden.

Anforderung 63: Die Sitzung muss gesperrt oder beendet werden, wenn der Anwender eine definierte Zeitspanne in der Sitzung keine Aktivitäten durchführte (Sitzungs-Zeitlimit, Session Timeout).

Anforderung 64: Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden.

Anforderung 65: Die Anzahl der Fehlversuche, die zu einer Sperrung führt, ist schriftlich festzuhalten und den Anwendern gegenüber zu kommunizieren.

Anforderung 66: Benutzerkennungen, welche über einen definierten Zeitraum nicht benutzt wurden, sind zu sperren bzw. auf inaktiv zu setzen.

Sind in der Datenaustauschplattform Daten gespeichert, die in einer Notfallsituation wie beispielsweise einer Reanimation oder einem anaphylaktischen Schock benötigt werden, so muss gewährleistet sein, dass auf diese Informationen in der Notfallsituation zugegriffen werden kann. Im Rahmen eines „Notfallzugriffs“ können erleichterte Anmeldebedingungen vorherrschen, aber auch hier muss die Identität des Zugreifenden sichergestellt sein.

Anforderung 67: Sind in der Datenaustauschplattform Daten enthalten, die in einer medizinischen Notfallsituation zur Patientenbehandlung benötigt werden, so kann unter Berücksichtigung einer trotzdem erforderlichen Authentifizierung des Zugreifenden eine vereinfachte Form der Anmeldung genutzt werden. Hierbei sind der Zugreifende, eine Begründung des Notfallzugriffs sowie die gesichteten Daten zu protokollieren.

4.5.3 Zugriffskontrolle

In Organisationen und Firmen ist die richtige Zuordnung von Zugriffsrechten zu Subjekten unabdingbar. Zum Beispiel erstellt die Lohn- und Gehaltsabteilung Abrechnungen für die einzelnen Beschäftigten, andere Mitarbeiter sollen diese aus Datenschutzgründen aber nicht einsehen dürfen. Gesundheitsdaten gelten als besonders schützenswerte Daten, daher bestehen insbesondere für Patientendaten die höchsten Anforderungen bzgl. ihres Schutzes vor unbefugter Kenntnisnahme.

Daraus ergibt sich, dass das „Need-to-know-Prinzip“ (Kenntnis nur bei notwendigem Bedarf) einzuhalten ist. Das Need-to-know-Prinzip verlangt, das, auch wenn eine Person grundsätzlich Zugriff auf Informationen einer bestimmten Hierarchie hat, dieser Person der Zugriff auf die Daten zu verweigern ist, außer wenn die Person diese Daten unmittelbar für die Erfüllung einer konkreten Aufgabe benötigt.

Anforderung 68: Es muss ein Berechtigungs- und Rollenkonzept erstellt und gepflegt werden, aus dem eindeutig abzulesen ist, wer welche Rolle (funktionell und strukturell) und damit verbundene Rechte bzgl. des Datenzugriffs hat.

Anforderung 69: Bzgl. der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept ist das Need-to-know-Prinzip anzuwenden.

✍ **Hinweis:** Es existieren verschiedene Normen, die bei der Erstellung eines Berechtigungskonzeptes hilfreich sein können:

- 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 24760-1 „Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement“, Teil 1: Terminologie und Konzept
- ISO/TS 21298 „Funktionelle und strukturelle Rollen“

- ISO/IEC 29100 „Security techniques - Privacy framework“
- ISO/IEC 29101 „ Security techniques - Privacy architecture framework”
- ISO/IEC 29146 „Security techniques - A framework for access management”

Eine Trennung der Funktionsrollen ist festzulegen, zu dokumentieren und zu begründen, d.h. es ist im Berechtigungskonzept darzustellen, welche Funktionsrollen nicht miteinander vereinbar sind, also auch nicht von einer Person gleichzeitig wahrgenommen werden dürfen.

Anforderung 70: Im Berechtigungs- und Rollenkonzept muss beschrieben sein, welche Funktionsrollen nicht miteinander vereinbar sind und somit nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Es sind technische und organisatorische Maßnahmen zu ergreifen, um diese Trennung sicherzustellen.

Es ist zu vermeiden, dass durch eine geeignete Kombination von verschiedenen Rollen bzw. Zugriffsrechten auf eine Person diese in der Kombination mehr Rechte für Datenzugriffe bekommt, als für ihre Aufgabe benötigt werden.

Anforderung 71: Eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, ist zu verhindern. Es sind technische und organisatorische Maßnahmen zu ergreifen, um dies sicherzustellen.

Protokolldaten können sensible Informationen beinhalten. Es ist im Berechtigungskonzept festzulegen, wer unter welchen Umständen und zu welchem Zweck auf diese Daten zugreifen darf.

Anforderung 72: Im Berechtigungskonzept ist festzulegen, wer auf Grund welcher Geschehnisse auf Protokolldaten zugreifen darf.

Anforderung 73: Protokolldaten sind gegen unbefugten Zugriff in geeigneter Weise entsprechend dem Stand der Technik zu schützen.

Protokolldaten sind nach einer festgelegten Speicherdauer zu löschen. Die Aufbewahrungsfrist richtet sich nach den gesetzlichen Bestimmungen. Existieren keine gesetzlichen Bestimmungen, so ist die Aufbewahrungsdauer der Protokolldaten vom Anbieter der Datenaustauschplattform unter angemessener Berücksichtigung der Interessen der Betroffenen festzulegen. Die Begründung der Aufbewahrungsdauer und insbesondere die Berücksichtigung der Interessen der Betroffenen im Entscheidungsprozess sind schriftlich festzuhalten.

Anforderung 74: Die Aufbewahrungsdauer für Protolldaten ist schriftlich festzulegen.

Anforderung 75: Die Begründung für die Festlegung der Aufbewahrungsdauer ist schriftlich festzuhalten, sodass Dritte die Begründung nachvollziehen können.

4.5.4 Weitergabekontrolle

Bei einer Weitergabe an Dritte ist zu prüfen, ob die Weitergabe rechtens ist. Weiterhin ist festzuhalten, wer Daten an Dritte unter welchen Umständen auf welchem Weg weitergeben darf und wie die Daten auf dem Transportweg geschützt werden.

Anforderung 76: Werden Daten an Dritte weitergegeben (z.B. durch die Weitergabe eines elektronischen Datenexports oder Ausdrucks der Daten), so muss entweder eine gesetzliche Grundlage hierfür vorhanden sein oder der Betroffene der Weitergabe zugestimmt haben.

Anforderung 77: Es ist festzulegen, welche Stellen/Personen an wen welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies zu geschehen hat.

Soll eine Weitergabe von Daten ins Ausland erfolgen, so sind die gesetzlichen Einschränkungen vorab zu prüfen. Insbesondere die Übermittlung in Länder außerhalb der Europäischen Union ist grundsätzlich nur unter zusätzlichen Bedingungen möglich. Es ist zu beachten, dass bereits ein Zugriff aus anderen Ländern eine Übermittlung darstellt.

Anforderung 78: Die Rechtmäßigkeit der Übermittlung von Daten ins Ausland ist vor der Übermittlung zu prüfen.

Anforderung 79: Erfolgt eine Übermittlung in ein Drittland, also außerhalb des EWR, so muss zwischen Daten exportierender Stelle und dem Datenimporteur eine vertragliche Regelung zum Datenschutz existieren, welche ein der EU angemessenes Datenschutzniveau beim Datenimporteur garantiert. D.h. es muss eine Verpflichtung der Parteien auf die Einhaltung der EU-Datenschutzregelungen sowie das Ergreifen ausreichender technisch-organisatorischer Maßnahmen vorhanden sein. Diese vertragliche Regelung schließt auch jegliche Zweckänderung inklusive der Verwendung der Daten für eigene Zwecke beim Datenimporteur aus.

✍ **Hinweis:** Erfolgt eine Übermittlung in ein Drittland, welches keine seitens der EU-Kommission dem europäischen Datenschutzniveau entsprechenden datenschutzrechtlichen Regelungen aufweist, so kann entsprechend §4c Abs. 2 BDSG eine Genehmigung der für die Datenaustauschplattform zuständigen Aufsichtsbehörde eingeholt werden und sich der Betreiber der Datenaustauschplattform so die Rechtmäßigkeit einer Datenübermittlung absichern lassen.

Anforderung 80: Ist die Rechtmäßigkeit nicht eindeutig sichergestellt, ist die Übermittlung zu verhindern.

Eine sichere Datenübertragung ist sowohl zwischen Server und Client wie auch zwischen den Servern selbst bei jeglichem Zugriff zu gewährleisten.

Anforderung 81: Die Übertragung personenbezogener oder personenbeziehbarer Gesundheitsdaten zwischen Clients und Servern wie auch zwischen Servern selbst muss entsprechend dem jeweiligen Stand der Technik generell verschlüsselt erfolgen.

Alle Schnittstellen, die dem Austausch von personenbezogenen oder personenbeziehbaren Gesundheitsdaten dienen, sind zu dokumentieren. Die Dokumentation muss mindestens beinhalten:

- Der genaue Verwendungszweck für den Datentransfer
- Alle Datenfelder, welche personenbezogene oder personenbeziehbare Gesundheitsdaten beinhalten
- Die Richtung der Übermittlung, d.h. werden Daten im- oder exportiert
- Die empfangende Schnittstelle bzw. das empfangende Informationssystem, wenn Daten exportiert werden
- Die Art der Authentisierung an der Schnittstelle
- Der Schutz der Übertragung, d.h. wie erfolgt die Verschlüsselung der Daten.

Anforderung 82: Sind Schnittstellen im System vorhanden, welche dem Datenimport oder -export dienen, so ist diese Schnittstelle zu dokumentieren.

Werden Datenträger entsorgt, so ist dafür Sorge zu tragen, dass eine unberechtigte Kenntnisnahme der auf den Datenträgern gespeicherten Gesundheitsdaten nicht möglich ist. Daher ist ein Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern einzurichten und zu beschreiben. Diese Beschreibung muss Regelungen und Verfahren zur sicheren Sammlung bzw. Lagerung sowie zur Weitergabe inklusive des Transportwegs zur Vernichtung des Datenträgers beinhalten. Die Vernichtung der Datenträger muss für Dritte (z.B. Aufsichtsbehörden oder Auditoren) nachvollziehbar sein. Hinweise zum Vorgehen zur Vernichtung finden sich in der Normenreihe der DIN 66399[47], Anregungen zur Erstellung eines Löschkonzeptes in der Vornorm DIN 66398[48].

Anforderung 83: Es ist der Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von

[47] DIN 66399-1. Büro- und Datentechnik - Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe. (Ausgabedatum 2012-10)
DIN 66399-2. Büro- und Datentechnik - Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern. (Ausgabedatum 2012-10)
DIN SPEC 66399-3. Büro- und Datentechnik - Vernichten von Datenträgern - Teil 3: Prozess der Datenträgervernichtung. (Ausgabedatum 2013-02)

[48] E DIN 66398 (Norm-Entwurf). Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. (Ausgabedatum 2015-02)

Datenträgern festzulegen und schriftlich festzuhalten.

Anforderung 84: Dieser Prozess muss datenschutzgerechte Löschverfahren beinhalten.

Anforderung 85: Die vollständige, datenschutzgerechte und dauerhafte Löschung von Datenträgern ist zu protokollieren.

Eine Möglichkeit zur Kenntnisnahme von personenbezogenen Gesundheitsdaten durch Dienstleister, welche zu Wartungsarbeiten auf die Infrastruktur zugreifen müssen, ist zu vermeiden. Damit auch Datenbankadministratoren nicht unbefugt Kenntnis von den gespeicherten Gesundheitsdaten erhalten können, sind die Daten in der Datenbank dem Stand der Technik entsprechend verschlüsselt zu speichern.

Anforderung 86: Gesundheitsdaten sind entsprechend dem Stand der Technik verschlüsselt in der Datenbank zu speichern, sodass bei administrativen Zugriffen Wartungspersonal keinen unbefugten Zugriff auf die gespeicherten Daten erhalten kann.

4.5.5 Eingabekontrolle

Im Berechtigungskonzept muss festgelegt sein, welche Person aufgrund ihrer Aufgabenstellung befugt und verantwortlich ist, Eingaben oder Importe in die Datenaustauschplattform vorzunehmen oder zu veranlassen.

Anforderung 87: Nur Personen, die laut Berechtigungskonzept zu einer Eingabe berechtigt sind, dürfen personenbezogene oder personenbeziehbare Daten in eine Datenaustauschplattform eingeben.

Anforderung 88: Nur Personen, die laut Berechtigungskonzept zu einem Datenimport berechtigt sind, dürfen einen Import personenbezogener oder personenbeziehbarer Daten in eine Datenaustauschplattform durchführen oder veranlassen.

Die Eingaben wie auch der Import personenbezogener oder personenbeziehbarer Daten in eine Datenaustauschplattform muss protokolliert werden, damit die Eingabe kontrolliert werden kann.

Anforderung 89: Sowohl die Eingabe wie auch der Import personenbezogener oder personenbeziehbarer Daten muss protokolliert werden.

4.5.6 Auftragskontrolle

Generell sind die rechtlichen Rahmenbedingungen einer Auftragsdatenverarbeitung zu prüfen, insbesondere die Fragestellungen:

- Darf ich eine Auftragsdatenverarbeitung durchführen?
- Welche Voraussetzungen müssen beim Dienstleister erfüllt sein?
- An welchem Ort darf die Leistung erbracht werden?

Verantwortliche Stelle im Sinne des Datenschutzrechts bleibt der Plattformbetreiber als Auftraggeber. Daher kann der Auftraggeber seine gesetzlichen Pflichten (z. B. aus §203 StGB resultierendes Arztgeheimnis) an den Auftragnehmer nicht weiterreichen, sondern die Pflichten obliegen eindeutig allein dem Auftraggeber. Daraus resultiert auch, dass der Auftraggeber für die beim Auftragnehmer stattfindende Datenverarbeitung datenschutzrechtlich verantwortlich bleibt.

Der Gesetzgeber fordert vom Auftraggeber, dass er sich vor und nach Vertragsabschluss sowie während der Vertragslaufzeit von der Einhaltung der vertraglich vereinbarten Bedingungen, insbesondere der technisch-organisatorischen Maßnahmen (TOMs) überzeugt. Daher muss der Auftraggeber vor Abschluss des ADV-Vertrages und danach in regelmäßigen Abständen die Einhaltung der im ADV-Vertrag vereinbarten Pflichten des Auftragnehmers prüfen[49] und das Ergebnis der Prüfung dokumentieren[50].

[49] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit veröffentlichte in seinem Wiki Hinweise zur Prüfung: Checkliste Datenverarbeitung im Auftrag [Online] 2013 [Zitiert 2014-03-31] Verfügbar unter http://www.bfdi.bund.de/bfdi_wiki/index.php/Checkliste_Datenverarbeitung_im_Auftrag bzw.

Anforderung 90: Der Auftraggeber überzeugt sich vor sowie in regelmäßigen Abständen auch nach Erteilung der Auftragsvergabe von der Einhaltung der vertraglich vereinbarten datenschutzrechtlichen Vorgaben, insbesondere der TOMs.

Die meisten landesrechtlichen Regelungen für Krankenhäuser beispielsweise schränken die Möglichkeiten der Auftragsdatenverarbeitung ein: in einigen Ländern wird der Ort der Leistungserbringung eingeschränkt, in anderen landesrechtlichen Bestimmungen die Art der Leistungserbringung. Grundsätzlich gilt jedoch, dass ein Vertrag für eine Auftragsdatenverarbeitung existieren muss.

Anforderung 91: Wenn personenbezogene oder personenbeziehbare Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, so ist ein ADV-Vertrag abzuschließen.

Der Auftragnehmer hat durch eine geeignete Dokumentation die lückenlose Nachvollziehbarkeit der einzelnen im Rahmen der Auftragsausführung durchgeführten Arbeitsschritte zu gewährleisten. Auf Anforderung muss der Auftragnehmer nachweisen, dass der jeweils durchgeführte Auftrag genau den Weisungen des Auftraggebers entsprechend durchgeführt wurde.

Anforderung 92: Der Auftragnehmer dokumentiert die Auftragsausführung dergestalt, dass der Auftraggeber die ordnungsgemäße Durchführung eines Auftrags, d.h. die Durchführung des Auftrags gemäß den Anweisungen des Auftraggebers, kontrollieren kann.

4.5.7 Verfügbarkeitskontrolle

Um die Verfügbarkeit der Daten zu gewährleisten, müssen die Daten regelmäßig gesichert werden. Zu diesem Zweck muss ein Backup-Konzept vorhanden sein, das befugte Personen in die Lage versetzt, die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung zu stellen.

Anforderung 93: Es muss ein Backup-Konzept vorhanden sein, welches gewährleistet, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung gestellt werden können. In diesem Backup-Konzept muss berücksichtigt werden, dass nur berechtigte Personen Zugriff auf Backup-Daten erlangen können.

Anforderung 94: Es muss eine regelmäßige Prüfung stattfinden, ob mittels der gesicherten Daten eine Wiederherstellung möglich ist.

Entsprechend der Anforderung an die Verfügbarkeit der Datenaustauschplattform müssen Notfalleinrichtungen wie z.B. Notstromaggregate und Überspannungsschutzeinrichtungen vorhanden sein oder auch eine Verteilung der Daten auf verschiedene Rechenzentren.

Anforderung 95: Entsprechend der festzulegenden Anforderung an die Verfügbarkeit der Datenaustauschplattform müssen Notfalleinrichtungen vorhanden sein.

Es muss ein Notfallplan vorhanden sein, in dem beschrieben steht

- wer bei Ausfall der Datenaustauschplattform wie zu benachrichtigen ist
- welche Maßnahmen in welcher Reihenfolge für z.B. den Wiederanlauf zu ergreifen sind,

um so eine Minimierung des Schadens zu erzielen bzw. idealerweise den Schaden durch den Ausfall gänzlich abzuwenden.

Anforderung 96: Es muss ein Notfallplan vorhanden sein, dessen Befolgung eine Minimierung des Schadens bzw. eine Verhinderung des Eintretens eines Schadens zum Ziel hat.

4.5.8 Trennung

Die datenschutzrechtlichen Anforderungen bedingen eine Trennung von Daten, wenn Daten zu unterschiedlichen Zwecken erhoben wurden. D.h. wenn Daten zum Zwecke der Behandlung eines

---

Checkliste Datenverarbeitung Wartung [Online] 2013 [Zitiert 2014-03-31] Verfügbar unter http://www.bfdi.bund.de/bfdi_wiki/index.php/Checkliste_Datenverarbeitung_Wartung

[50] Hier ist zumindest die Textform entsprechend §126b BGB erforderlich

bestimmten Falls erhoben wurden (beispielsweise im Rahmen einer eFA), so müssen diese Daten von anderen Daten desselben Betroffenen (z.B. die Daten innerhalb einer eEPA) getrennt werden. Hinweise zur Mandantenfähigkeit finden sich in der entsprechenden Orientierungshilfe der Aufsichtsbehörden aus dem Jahr 2012[51].

Anforderung 97: Personenbezogene oder personenbeziehbare Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden.

Anforderung 98: Die Verarbeitung personenbezogener Daten verschiedener Mandanten muss physisch oder logisch getrennt voneinander erfolgen.

Anforderung 99: Die Aufbewahrung, Archivierung und Löschung von personenbezogenen Daten verschiedener Mandanten oder mit unterschiedlicher Zweckbindung muss getrennt voneinander möglich sein.

[51] Bayerisches Landesamt für Datenschutzaufsicht: Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur - Orientierungshilfe Mandantenfähigkeit. [Online] 2012 [Zitiert 2016-02-24] Verfügbar unter https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OrientierungshilfeMandantenfaehigkeit.pdf

5 Hinweise zur technischen Umsetzung der datenschutzrechtlichen Anforderungen

5.1 Allgemeines

In Kapitel 2.1 wurde darauf hingewiesen, dass Datenschutz zunächst eine organisatorische Aufgabe ist: das Unternehmen muss festlegen, welche Regelungen im Unternehmen gelten, um den gesetzlichen Anforderungen zu genügen. Dabei wird es Regelungen geben, bei deren Umsetzung technische Hilfsmittel wie beispielsweise IT-System unterstützen können. Andere Regelungen sind rein organisatorischer Natur und können technisch nicht begleitet werden.

In diesem Sinne gibt es Anforderungen, die "rein" organisatorisch (also ohne technische Unterstützung) erfüllt werden können und Anforderungen, bei denen organisatorische Maßnahmen durch technische Maßnahmen begleitet werden können. Dementsprechend werden in den nachfolgenden Kapiteln zu jeder Anforderung festgehalten, um es sich hier aus Sicht der Autoren um „rein organisatorische“ Anforderungen handelt, oder um Anforderungen, die „technisch unterstützt“ werden können.

5.2 Umsetzung der Anforderungen

5.2.1 Einwilligung vs. gesetzliche Grundlage

5.2.1.1 Anforderung 1

„Jegliche Erhebung, Verarbeitung und Nutzung personenbezogener oder personenbeziehbarer Daten - insbesondere durch den Einsatz von Datenaustauschplattformen, die an das Internet angebunden sind - bedarf einer datenschutzrechtlich wirksamen Einwilligung des Betroffenen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im Bereich von IHE XDS Anwendungen kann die Berechtigung feingranular bis auf Dokumentenebene geregelt werden. Hierzu wird das Profil Basic Patient Privacy Consents (BPPC) genutzt. Voraussetzung für die Nutzung von BPPC ist, dass vordefinierte Datenschutzrichtlinien (Privacy Policies) für den Zugriff auf Gesundheitsdaten existieren. Der Betroffene wählt aus diesen Policies die seinem Willen entsprechende Policy aus und BPPC sorgt dafür, dass die Policy beim Zugriff auf die Daten angewendet wird. Dabei kann der Betroffene für verschiedene Dokumente verschiedene Policies vergeben und so z.B. auf sein Diabetestagebuch nur seinem Hausarzt Zugriff erlauben, hingegen auf die Dokumente seines Krankenhauses allen seinen behandelnden Ärzten.

Die Einwilligungserklärung des Betroffenen (Basic Patient Privacy Acknowledgement Document) wird als ein CDA-Dokument gespeichert, welches die eindeutige ID der gewählten Policy beinhaltet und eine textuelle, also menschenlesbare Beschreibung der Einwilligung enthalten sollte.

Neben diesen Mechanismen bietet die Extensible Access Control Markup Language (XACML), ein XML-basierter OASIS-Standard, eine Möglichkeit um Policies, Authorisierungsanfragen und -antworten definieren zu können. In XACML wird außerdem spezifiziert, wie Policies ausgelegt werden müssen, z.B. um einen Dokumentenzugriff zu erlauben oder zu verweigern.

5.2.1.2 Anforderung 2

„Vor der Erteilung der Einwilligung zu einer Erhebung, Verarbeitung (= Speichern, Verändern, Übermitteln, Sperren und Löschen) oder Nutzung (alles, was nicht als Erhebung oder Verarbeitung aufzufassen ist) seiner Daten muss der Betroffene insbesondere über

- *Sitz/Land des Dienstanbieters*
- *das Empfängerland (soweit bekannt; Internet ermöglicht globalen Zugriff, je nach Austauschplattform ist jedoch nur aus definierten Ländern ein Zugriff möglich)*
- *die im Empfängerland, soweit dieses von seinem Heimatland abweicht, vorhandenen oder nicht vorhandenen Datenschutzregelungen, insbesondere von den von seinem Heimatland abweichenden Regelungen*
- *die Form der Gewährleistung des europäischen Datenschutzniveaus insbesondere über den Schutz vor Zugriff auf seine Daten durch Unbefugte (dies schließt auch alle staatlichen Ermittlungsbehörden ein, ausgenommen die staatlichen Ermittlungsbehörden im Land des Betroffenen)*
- *die Gewährleistung seiner datenschutzrechtlich garantierten Rechte wie*
  - *die Möglichkeiten der Korrektur der ihn betreffenden Daten (wie werden seine Daten auf seine Anforderung hin korrigiert)*
  - *die Möglichkeiten zur Löschung der ihn betreffenden Daten (wie werden seine Daten auf seine Anforderung hin gelöscht bzw. gesperrt, sowohl aus dem Arbeitsbereich wie auch aus Backupdateien)*

informiert werden, sodass er die Gefährdung seiner Daten ausreichend beurteilen kann. "

informiert werden und jederzeit Zugriff auf diese Informationen haben.

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.1.3 Anforderung 3

„Eine Einwilligung muss für den Betroffenen jederzeit mit Wirkung für die Zukunft widerrufbar sein.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Datenaustauschplattformen können dem Betroffenen internetbasierte Kontaktmöglichkeiten zur Verfügung stellen, in welchem der Betroffene seinen Widerruf erklären kann. Dies erfordert eine

a) eindeutige Identifizierung des Betroffenen
b) Aufklärung des Betroffenen bzgl. der Folgen seines Widerrufs, idealerweise mit Bestätigung der Kenntnisnahme durch den Betroffenen.

Eine Aufklärung des Betroffenen hinsichtlich der Folgen eines Widerrufs der Einwilligung erfolgte natürlich schon bei der Einholung der Einwilligung. Jedoch wird wahrscheinlich zwischen Widerruf und Einholung der Einwilligung eine hinreichende Zeitspanne vergangen sein, sodass man nicht

davon ausgehen kann, dass dem Patenten die Folgen des Widerrufes noch bewusst sind. Dies impliziert natürlich zugleich, dass überall dort, wo nur ein Mensch die Folgen eines Widerrufes dem Betroffenen erläutern kann, eine technische Unterstützung nur eingeschränkt zur Verfügung gestellt werden kann.

5.2.1.4 Anforderung 4

„Jede Datenaustauschplattform muss Datenschutzhinweise veröffentlichen und darin die getroffenen Datensicherheitslösungen allgemeinverständlich beschreiben."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im einfachsten Fall handelt es sich um hierbei um Webseiten, die aufgerufen werden. Der Zugriff auf die Informationen kann über Hyperlinks realisiert werden. Die Webseiten sollten sowohl in PC-Systemen wie auch auf mobilen Geräten gut sichtbar sein, z.B. durch die Nutzung entsprechender Möglichkeiten von HTML5. Eine Darstellung der Links in einer kleinen (kaum lesbaren) Schriftart und eine Informationsverschachtelung - der Link ist nur über einen weiteren Link usw. erreichbar - muss vermieden werden.

5.2.1.5 Anforderung 5

„Datenschutzhinweise müssen unmittelbar von der Startseite der Datenaustauschplattform aus aufrufbar bzw. erreichbar sein."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Das Design der Startseite muss entsprechend vorgegeben werden.

5.2.1.6 Anforderung 6

„Datenschutzhinweise müssen für den Betroffenen jederzeit abrufbar sein."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Auf der Startseite ist neben dem Link zum Impressum zugleich ein Link zu den Datenschutzhinweisen anzubringen.

5.2.1.7 Anforderung 7

„Bei nachträglicher Änderung ist der Betroffene zu informieren und sein Einverständnis erneut einzuholen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Ein Datenbanktrigger reagiert auf Änderungen in zuvor organisatorisch definierten Datenbankfeldern und erzeugt hierzu eine Änderungsmeldung, auf welche - automatisiert oder nach Bestätigung des Nutzers - eine Nachricht an den Betroffenen per E-Mail oder SMS (je nach Konfiguration) versendet wird.

5.2.2 Telemedien

5.2.2.1 Anforderung 8

„Wird die Einwilligung des Betroffenen elektronisch eingeholt, so muss der Vorgang protokolliert werden und der Inhalt der Einwilligung für den Betroffenen jederzeit abrufbar sein.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es existieren Frameworks zur Protokollierung wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, sodass die Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Das IHE-Profil Audit Trail and Node Authentication (ATNA) definiert die grundlegenden Sicherheitsanforderungen innerhalb einer IHE XDS-Umgebung. Ohne ATNA als Sicherheitsinfrastruktur kann eine IHE XDS-Domäne nicht betrieben werden. In ATNA wird beschrieben, wie und wann die Auditierung von Zugriffen auf Gesundheitsdaten bei welchen Ereignissen zu erfolgen hat. ATNA bildet die Grundlage für die DIN EN ISO 27789:2013-06 („Audit-Trails für elektronische Gesundheitsakten“).

Diese Protokolldaten müssen entsprechend aufbereitet und z.B. über eine Webseite zur Verfügung gestellt werden. Dabei muss darauf geachtet werden, dass ein Zugriff durch den Betroffenen erst nach dessen eindeutiger Authentifizierung erfolgen darf.

5.2.3 Anonymisierung bzw. Pseudonymisierung

5.2.3.1 Anforderung 9

„Personenbezogene oder personenbeziehbare Daten müssen pseudonymisiert werden, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Eine reine Bearbeitung von Namen, Anschrift und Geburtsdatum ist in den meisten Fällen nicht ausreichend, vielmehr müssen oftmals zur Pseudonymisierung auch medizinische Daten angepasst werden. Methoden zur Durchführung einer Pseudonymisierung sind hinlänglich bekannt und erprobt, jedoch kann aus den genannten Gründen nur im jeweiligen Kontext unter Berücksichtigung der konkreten Fragestellung festgelegt werden, welche Daten wie behandelt werden müssen, um eine Pseudonymität zu gewährleisten. Daher kann hier keine technische Umsetzung angegeben werden.

5.2.4 Automatisierte Abrufverfahren

5.2.4.1 Anforderung 10

„Die beteiligten Stellen haben schriftlich festzulegen:

1. *Anlass und Zweck des Abrufverfahrens*
2. *Dritte, an die übermittelt wird*
3. *Art der zu übermittelnden Daten*
4. *Die nach § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen (TOMs)"*

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.4.2 Anforderung 11

„Die speichernde Stelle muss vertraglich dazu verpflichtet werden, dass bei einer Übermittlung der gesetzlich geforderten Aufzeichnungspflicht genügt wird.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.4.3 Anforderung 12

„Die übermittelnde Stelle muss stichprobenartig die Aufzeichnungen der empfangenden Stelle prüfen, insbesondere ist hierbei das berechtigte Interesse der empfangenden Stelle einzelfallbezogen zu prüfen.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.5 Richtlinie 2002/58/EG

5.2.5.1 Anforderung 13

„Der Betroffene muss der Nutzung von Cookies explizit zustimmen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Der Umgang mit Cookies wird durch die sogenannte „Cookie-Richtlinie" (EU-Richtlinie 2009/136/EG zur Änderung u. a. der Richtlinie 2002/58/EG) beschrieben. Danach dürfen Cookies nur nach ausdrücklicher Zustimmung des Betroffenen genutzt werden. D.h. eine Zustimmungs-Vermutung reicht nach europäischem Recht nicht aus. Entsprechend §13 Abs. 2 TMG kann bei Telemedien eine Einwilligung elektronisch erfolgen, sodass eine Zustimmung entsprechend den Vorgaben der Cookie-Richtlinie rein elektronisch abgebildet werden kann.

Die Einholung der Zustimmung muss vor dem Setzen eines Cookie erfolgen. Hierzu wird empfohlen, ein Pop-Up-Fenster zu verwenden, in welchem der Verwendungszweck der Cookies eindeutig erklärt wird, zugleich dem Nutzer mitgeteilt wird, welche Folgen die Verweigerung der Einwilligung hat. Ein nicht vorbelegtes Ankreuzfeld kann vom Nutzer angehakt werden (= Zustimmung) und das Pop-Up-Fenster durch Anklicken eines OK-Buttons (= Zustimmung erteilt) oder Abbrechen-Buttons (= Zustimmung verweigert) geschlossen werden. Das Ergebnis wird inklusive eines Time-Stamps in einem Protokoll gespeichert.

Nach der Anmeldung in der Datenaustauschplattform hat der Nutzer jederzeit die Möglichkeit, sich in seinen Profildaten die protokollierte Zustimmung anzusehen (keine Änderungsmöglichkeit) oder auch die Einwilligung mit Hinblick auf die Zukunft zu widerrufen.

5.2.5.2 Anforderung 14

„Die Verwendung von Cookies durch Drittanbieter muss auf die Erstellung anonymer Nutzungsstatistiken beschränkt sein."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Innerhalb der Cookies werden keinerlei personenbezogene Daten gespeichert, lediglich eine ID. innerhalb der Datenaustauschplattform kann die ID des Cookies mit der Person verknüpft werden (Lookup-Table). Dritte haben keinen Zugriff auf diese Verknüpfungsmöglichkeit. Somit können Drittanbieter in ihren Cookies nur auf die ID verweisen, erhalten jedoch nie einen Zugriff auf personenidentifizierende Merkmale.

5.2.5.3 Anforderung 15

„Das Handling der Drittanbieter-Cookies muss durch den Betroffenen steuer- und nachvollziehbar sein."

Umsetzung:

	Rein Organisatorisch

X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Bevor ein Drittanbieter ein Cookie setzen kann, muss der Nutzer diesem Vorgehen explizit zustimmen (zweite Ankreuzmöglichkeit bei der Einwilligung). In seinen Profildaten kann ein Nutzer nach der Anmeldung die Einwilligung widerrufen oder auch nachträglich eine Einwilligung erteilen. Entsprechend der vorhandenen oder nicht vorhandenen Einwilligung steuert die Datenaustauschplattform den Einsatz von Drittanbieter-Cookies.

5.2.5.4 Anforderung 16

„Soweit möglich, müssen Drittanbieter temporäre Cookies verwenden."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

✍ **Hinweis:** Vertragsverhandlung mit Drittanbieter; letztlich kann nur der Drittanbieter das Verhalten seines Cookies beeinflussen**.**

5.2.5.5 Anforderung 17

„Die Gültigkeit persistenter Cookies von Drittanbietern darf nicht länger als 30 Tage betragen."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

✍ **Hinweis:** Vertragsverhandlung mit Drittanbieter; letztlich kann nur der Drittanbieter das Verhalten seines Cookies beeinflussen.

5.2.5.6 Anforderung 18

„Die Erhebung, Verarbeitung und Nutzung von Daten zur Erstellung von Nutzungsstatistiken von Webportalen muss dokumentiert werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Durch die Protokollierung entsprechender Ereignisse wird festgehalten, wer wann welche Daten zu welchem Zweck (Pop-Up-Fenster mit der Aufforderung den Zweck der Statistik anzugeben) verwendete.

5.2.5.7 Anforderung 19

„Die Erstellung von Nutzungsstatistiken von Datenaustauschplattformen muss auf Basis anonymisierter Daten erfolgen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Dies kann seitens der Datenaustauschplattform nur gewährleistet werden, wenn ausschließlich mit den Mitteln der Datenaustauschplattform Statistiken erhoben werden. Sobald freie SQL-Abfragen möglich sind – z.B. weil die Komplexität der Abfragen dies erfordert – kann eine anonyme Datenbasis technisch nicht mehr gewährleistet werden.

Im Rahmen der Nutzung von durch die Datenaustauschplattform zur Verfügung gestellten Reporting-Werkzeugen dürfen – sofern zuvor definiert wurde, welche Daten zwecks Anonymisierung wie zu behandeln sind – Daten nur in anonymer Form an Anfragende weitergegeben werden.

5.2.5.8 Anforderung 20

„Eine Analyse des Nutzerverhaltens (einschließlich Geolokalisierung) auf der Basis gekürzter IP-Adressen ist ohne Einwilligung des Betroffenen möglich, wenn durch die Kürzung der IP-Adresse ein Personenbezug ausgeschlossen wurde."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Zur statistischen Auswertung bzgl. des ortsbezogenen Nutzungszugriffs auf die Datenaustauschplattform ist ein Personenbezug nicht erforderlich. Im Bereich von IPv4 muss der letzte 8-Bit-Teil (ausgehend vom niedrigstwertigen Bit, also dem 4. Oktett) gelöscht bzw. durch Nullen ersetzt werden (IP-Adresskürzung). Ein größeres Maß an Kürzung bringt naturgemäß auch ein größeres Maß an Anonymität, verhindert aber ggfs. die Geolokalisierung.

Bei IPv6 muss anders vorgegangen werden. Hier bekommt ein Nutzer nur den Netzwerk-Teil von seinem Internet-Service-Provider zugewiesen, der Geräte-Teil wird vom Netzwerk-Adapter im genutzten Endgerät - also etwa PC, Tablet oder Smartphone – erzeugt. Das Standardverfahren von IPv6 sieht vor, dass der Geräte-Teil aus der MAC-Adresse generiert wird, somit ist diese Adresse weltweit eindeutig. Jedes Gerät kann für ausgehende Verbindungen temporäre IP-Adressen zufällig erzeugen (Privacy Extension), d.h. die Pseudonymisierung/Anonymisierung erfolgt auf der Client-Seite.

Allerdings muss beachtet werden, dass einzelne Bereiche im TKG und TMG die Speicherung der vollständigen IP-Adresse erfordern wie z.B. §113a Abs.2 Ziff. 5 TKG bei der Internet-Telefonie. In diesem Fall muss die IP-Adresse vollständig gespeichert werden und wird nur zu statistischen Auswertungszwecken verkürzt genutzt.

5.2.5.9 Anforderung 21

„Beim Einsatz eines Dienstleisters ist ein ADV-Vertrag zu schließen. Hat der Dienstleister außerhalb des EWR seinen Geschäftssitz, sind die hier geltenden besonderen Anforderungen zu beachten."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.6 Grundsatz der klaren Verantwortlichkeiten

5.2.6.1 Anforderung 22

„Es muss öffentlich verfügbar sein, wer innerhalb der verantwortlichen Stelle Entscheider ist und wie er kontaktiert wird; die Mindestanforderung ist ein Impressum entsprechend §5 TMG."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Impressum wird auf die Startseite verlinkt. Über einen „Impressumsgenerator" wird gewährleistet, dass die Mindestinformationen eines Impressums bei Inbetriebnahme vorhanden sind.

5.2.6.2 Anforderung 23

„Der Kontakt zum Datenschutzbeauftragten der verantwortlichen Stelle sollte öffentlich verfügbar gemacht werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Bei Inbetriebnahme der Datenaustauschplattform wird die Information abgefragt und integriert.

Auf der Startseite der Datenaustauschplattform wird auf die Datenschutzhinweise verlinkt. Hier wird, ebenso wie auf der Impressumseite, eine Kontaktmöglichkeit zum Datenschutzbeauftragten zur Verfügung gestellt.

Dass Änderungen der Information erfasst werden, muss jedoch organisatorisch gewährleistet werden; die Datenaustauschplattform bekommt diese Informationen nicht mit.

5.2.6.3 Anforderung 24

„Es sollte benannt und öffentlich verfügbar gemacht werden, wer innerhalb der verantwortlichen Stelle Adressat einer Datenschutzfrage eines Betroffenen oder eines staatlichen Organs (z.B. der Datenschutzaufsicht) ist."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Bei Inbetriebnahme der Datenaustauschplattform wird die Information abgefragt und integriert.

Auf der Startseite der Datenaustauschplattform wird auf die Datenschutzhinweise verlinkt. Hier wird, ebenso wie auf der Impressumseite, die Information zur Verfügung gestellt.

Dass Änderungen der Information erfasst werden, muss jedoch organisatorisch gewährleistet werden; die Datenaustauschplattform bekommt diese Informationen nicht mit.

5.2.6.4 Anforderung 25

„Die Übersicht der in §4e Ziff. 1-8 BDSG genannten Angaben muss für jeden Betroffenen öffentlich verfügbar gehalten werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die gesetzliche Anforderung lautet „auf Antrag verfügbar", sodass diese Information nicht dauerhaft im Internet verfügbar sein muss. Gleichwohl erleichtert es die Prozesse, wenn der auf Antrag verfügbar zu machende Teil des Verfahrensverzeichnisses im Internet verfügbar ist. So kann bei Nachfragen darauf verwiesen werden. Es wird empfohlen, dies als pdf-Datei im Bereich der Webseite mit den Datenschutzhinweisen zur Verfügung zu stellen.

5.2.7 Grundsatz der Zweckbindung sowie der Datenvermeidung und Datensparsamkeit

5.2.7.1 Anforderung 26

„Eine Zweckänderung bedarf einer Erlaubnisnorm (Einwilligung des Betroffenen oder gesetzlicher Erlaubnistatbestand)."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.7.2 Anforderung 27

„Um die Sparsamkeit der Datenerhebung zu gewährleisten, ist der Verwendungszweck jedes Datums bzw. jeder Datenkategorie zu beschreiben."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.7.3 Anforderung 28

„Daten, die keinen zur Erfüllung der Aufgabe definierten Verwendungszweck haben, dürfen nicht erhoben, verarbeitet oder genutzt werden.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.7.4 Anforderung 29

„Eine Änderung des Verwendungszweckes von Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ist untersagt und muss durch technische und organisatorische Maßnahmen verhindert werden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Extensible Access Control Markup Language (XACML), ein XML-basierter OASIS-Standard, bietet die Möglichkeit Policies, Authorisierungsanfragen und -antworten zu definieren. Da in XACML zudem spezifiziert wird, wie Policies ausgelegt werden, kann so die Nutzung in Hinsicht auf die Verwendungszwecke erlaubt werden. Die grundlegende Policy lautet dabei „Verwendung verboten, wenn nicht erlaubt“. Damit können Daten nur verwendet werden, wenn der Verwendungszweck dies gestattet. Eine Verwendung von Daten nach Änderung des Verwendungszweckes ist damit erst möglich, wenn die Policies angepasst wurden.

5.2.8 Bestellung Datenschutzbeauftragter

5.2.8.1 Anforderung 30

„Es muss ein Beauftragter für den Datenschutz bestellt werden.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.9 Verpflichtung der auf die Daten Zugreifenden

5.2.9.1 Anforderung 31

„Alle Personen, welche auf die gespeicherten Gesundheitsdaten zugreifen können, müssen vor dem erstmaligen Zugriff auf die Wahrung des Datengeheimnisses verpflichtet worden sein.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Bei Anlage eines Nutzers in der Datenaustauschplattform wird abgefragt, ob eine Verpflichtung zur Wahrung auf das Datengeheimnis erfolgte (Häkchen kann gesetzt werden). Eine Aktivierung des Accounts und somit eine Anmeldung am System ist erst möglich, wenn die Abfrage positiv beantwortet wurde (Häkchen gesetzt).

5.2.10 Telemediengesetz

5.2.10.1 Anforderung 32

„Ein anonymer Zugriff des Plattformbetreibers sowie der Nutzer der Plattform auf personenbezogene oder personenbeziehbare Gesundheitsdaten ist zu unterbinden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Um Gesundheitsdaten zu schützen, ist ein Zugriff ohne vorherige Authentifizierung nicht möglich. Eine Login-Prozedur verhindert einen Datenzugriff ohne Anmeldung.

5.2.10.2 Anforderung 33

„Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung sind unmittelbar nach dem Zugriff bzw. ggfs. nach erfolgter Abrechnung der Dienstenutzung zu sperren und nur zu entsperren, wenn eine gesetzliche Bestimmung (z.B. Auskunftsersuchen eines Betroffenen) dies erlaubt."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im Berechtigungskonzept muss festgelegt werden, welche Anwendergruppe auf welche Daten zu welchen Bedingungen zugreifen darf. Dies wird mittels BPPC resp. XACML umgesetzt. Dies beinhaltet auch die Festlegung von „Ablaufdaten" wie beispielsweise „6 Monate nach Rechnungsstellung".

5.2.10.3 Anforderung 34

„Die Nutzung von Telemedien muss gegen die Kenntnisnahme unberechtigter Dritter geschützt werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die Anmeldung an die Datenaustauschplattform ist zwingend zur Nutzung erforderlich, sodass nur authentifizierte und für den Datenzugriff autorisierte Nutzer Zugriff auf Daten bekommen. Der oder die Server selbst stehen in gesicherten Rechenzentren, so dass der physikalische Zugriff nur autorisiertem Personal möglich ist.

5.2.11 Recht auf Auskunft

5.2.11.1 Anforderung 35

„Es muss protokolliert werden, wer wann auf welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung zugegriffen hat."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Beispiel IHE XDS: In ATNA wird protokolliert, wer wann welche Zugriffe auf welche Gesundheitsdaten aufgrund welcher Berechtigung (z.B. Standardzugriff, Notfallzugriff) durchführte.

5.2.11.2 Anforderung 36

„Es muss protokolliert werden, wer wann welche personenbezogenen oder personenbeziehbaren Daten mit welcher Berechtigung exportiert oder ausgedruckt hat. Zu jedem Datenexport oder Ausdruck ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, zu welchem Zweck ein Datenexport oder ein Ausdruck erfolgte."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Beispiel IHE XDS: In ATNA wird protokolliert, wer wann welchen Datenexport (z.B. Ausdruck, externe Speicherung, Mail) auf welche Gesundheitsdaten aufgrund welcher Berechtigung (z.B. Standardzugriff, Notfallzugriff) durchführte.

5.2.11.3 Anforderung 37

„Es muss protokolliert werden, wer wann welche personenbezogenen oder personenbeziehbaren Daten gespeichert, verändert, gesperrt oder gelöscht hat. Bei jeder Löschung ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, wer aus welchem Grund welche Daten löschte."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Beispiel IHE XDS: In ATNA wird protokolliert, wer wann welche Zugriffe (Lesen, Ändern, Löschen) auf welche Gesundheitsdaten aufgrund welcher Berechtigung (z.B. Standardzugriff, Notfallzugriff)

durchführt. Über ein Pop-Up-Fenster wird bei einem Löschauftrag der Grund der Löschung abgefragt. Der Löschauftrag wird erst nach Eingabe des Löschgrundes physikalisch durchgeführt, ohne Angabe des Löschgrundes erfolgt eine Sperrung der Daten, der die Löschung veranlassende Nutzer wird auf den Umstand hingewiesen. Der Löschgrund wird in das Protokoll geschrieben.

5.2.11.4 Anforderung 38

„Es muss protokolliert werden, wer wann auf welche personenbezogenen oder personenbeziehbaren Daten durch die Nutzung erweiterter Systemprivilegien (z.B. durch den sogenannten „Notfall-Zugriff“) zugriff. Zu jedem Datenzugriff unter Nutzung von durch das System bereitgestellten Mechanismen zur Erweiterung der Zugriffsberechtigung ist die Eingabe einer Begründung notwendig, damit nachvollziehbar und überprüfbar ist, zu welchem Zweck ein Zugriff, ein Datenexport oder ein Ausdruck erfolgte.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Beispiel IHE XDS: In ATNA wird protokolliert, wer wann welche Zugriffe auf welche Gesundheitsdaten auf Grund welcher Berechtigung (z.B. Standardzugriff, Notfallzugriff) durchführte.

5.2.11.5 Anforderung 39

„Ereignisse, die potenziell dazu führen können, dass ein unberechtigter Zugriff auf personenbezogene oder personenbeziehbare Daten erfolgen könnte, sind zu protokollieren.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es existieren Frameworks zur Protokollierung wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, so dass die obige Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Im Bereich IHE XDS erlaubt ATNA eine Protokollierung entsprechender Ereignisse.

5.2.11.6 Anforderung 40

„Enthalten Protokolle personenbezogene oder personenbeziehbare Daten, so dürfen diese Protokolle nur zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes genutzt werden. Jegliche andere Nutzung ist durch technische und organisatorische Mittel zu verhindern.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die Nutzung von Daten muss im Berechtigungskonzept hinterlegt werden. Die Vorgaben des Berechtigungskonzepts werden in ein Regelframework (z.B. durch Nutzung von XACML) überführt.

D.h. wenn im Berechtigungskonzept die obige Forderung enthalten ist, wird dies auch im Regelwerk entsprechend berücksichtigt.

5.2.11.7 Anforderung 41

„Der Betroffene muss die Möglichkeit haben, jederzeit Einblick in alle zu seiner Person gespeicherten Daten zu erhalten. Dies umfasst auch die Möglichkeit, Änderungen seiner gespeicherten Daten nachzuvollziehen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Nach erfolgreicher Authentisierung gegenüber dem System erhält jeder Nutzer Zugriff auf die Daten, die ihm entsprechend Berechtigungskonzept zugewiesen sind. Hat ein Betroffener entsprechend Berechtigungskonzept Zugriff auf alle seine Daten, so gewährt ihm das System auch den Zugriff nach erfolgreicher Anmeldung.

Alternativ kann der Betroffene sich nicht selbst an der Datenaustauschplattform anmelden, aber in den Datenschutzhinweisen findet der Betroffene eine Kontaktmöglichkeit zu einer Person, die ihm in ihrem Beisein Einblick in die Daten gewährt.

5.2.11.8 Anforderung 42

„Der Betroffene muss die Möglichkeit haben, einen Ausdruck oder einen für ihn verwertbaren Export aller zu seiner Person gespeicherten Daten zu erhalten."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Dem Betroffenen müssen im Berechtigungskonzept die entsprechenden Rechte zugewiesen werden, dann kann er nach Anmeldung an der Datenaustauschplattform einen Export oder Ausdruck oder beides seiner Daten veranlassen.

Alternativ kann der Betroffene sich nicht selbst an der Datenaustauschplattform anmelden, aber in den Datenschutzhinweisen findet der Betroffene eine Kontaktmöglichkeit zu einer Person, die ihm einen Export oder Ausdruck oder beides seiner Daten zur Verfügung stellt.

5.2.12 Berichtigung falscher Daten

5.2.12.1 Anforderung 43

„Es muss eine Möglichkeit geben, auf Aufforderung des Betroffenen Daten zu seiner Person zu korrigieren."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Nach erfolgreicher Authentisierung gegenüber dem System erhält jeder Anwender Zugriff auf die Daten, die ihm entsprechend Berechtigungskonzept zugewiesen sind. Hat ein Betroffener entsprechend Berechtigungskonzept Zugriff auf alle seine Daten, so gewährt ihm das System auch den Zugriff nach erfolgreicher Anmeldung und er kann die Daten selbst korrigieren.

Alternativ kann der Betroffene sich nicht selbst an der Datenaustauschplattform anmelden, aber in den Datenschutzhinweisen findet der Betroffene eine Kontaktmöglichkeit zu einer Person, die ihm bzgl. Korrekturmöglichkeiten als Ansprechpartner zur Verfügung steht.

5.2.12.2 Anforderung 44

„Es muss protokolliert werden, wer wann welche Daten eines Betroffenen auf dessen Wunsch änderte. Es sollte die Eingabe der Begründung „Änderung erfolgte auf Wunsch des Betroffenen“ möglich sein.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es existieren Frameworks zur Protokollierung wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, sodass die obige Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Im Bereich IHE XDS erlaubt ATNA eine Protokollierung entsprechender Ereignisse.

Über ein Pop-Up-Fenster wird die Eingabe eines Begründungstextes realisiert, der Begründungstext selber wird ins Protokoll übernommen.

5.2.12.3 Anforderung 45

„Wurden Daten vom Betreiber der Datenaustauschplattform an andere Stellen übermittelt, so sollte der Betreiber der Datenaustauschplattform, sofern zumutbar, diese Stellen über erfolgte Berichtigungen informieren, sofern diese Benachrichtigung im Interesse des Betroffenen liegt.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Bei allen Datenübermittlungen werden von der Datenplattform die Empfänger festgehalten, sodass jederzeit eine Liste der zu benachrichtigenden Empfänger generiert werden kann. Automatisiert oder nach Freigabe eines Anwenders können die Empfänger über Berichtigungen informiert werden.

5.2.13 Löschen bzw. Sperren

5.2.13.1 Anforderung 46

„Es muss eine Löschfunktion implementiert werden, welche eine Rekonstruktion gelöschter Informationen ausschließt.“

Umsetzung:

	Rein Organisatorisch

X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im Löschkonzept muss beschrieben werden, welche Daten unter welchen Bedingungen gelöscht werden dürfen. Aufgrund gesetzlicher Aufbewahrungsfristen muss verhindert werden, dass Daten im Rahmen der vorgeschriebenen Aufbewahrungsfristen gelöscht werden. All dies muss im Löschkonzept berücksichtigt werden. Das Löschkonzept kann in ein Regelwerk überführt werden, das bei einem Löschauftrag einem Anwender entsprechende Hinweise gibt. Eine automatisierte Löschung wird aufgrund von Haftungsfragen nur schwer seitens eines Herstellers realisierbar sein, wenngleich eine technische Umsetzung natürlich möglich ist.

5.2.13.2 Anforderung 47

„Es ist in einem Löschkonzept festzulegen, wann welche Daten zu löschen sind..“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Ein Cronjob kann die Daten entsprechend zu den organisatorisch vorgegebenen Zeitpunkten löschen bzw. eine Löschliste generieren, sodass die letztmalige Löschung von einem Menschen autorisiert wird.

5.2.13.3 Anforderung 48

„Liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, sind die Daten auf Anweisung des Betroffenen unverzüglich zu löschen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im Löschkonzept muss beschrieben werden, welche Daten unter welchen Bedingungen gelöscht werden dürfen. (Siehe Ausführungen bzgl. Kapitel 5.2.13.1)

5.2.13.4 Anforderung 49

„Entfällt der Verwendungszweck und es liegt keine gesetzliche Grundlage zur Speicherung der Daten vor, sind die Daten unverzüglich zu lösch.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.13.5 Anforderung 50

„Unverschlüsselte Datenträger müssen aus Sicherheitsgründen vor deren Wiederverwendung datenschutzgerecht gelöscht werden. Die Formatierung ist als sicheres Löschverfahren ungeeignet.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Entsprechend den Ausführungen des BSI[52] kann davon ausgegangen werden, dass bei einem Überschreiben mit geeigneten Zeichenfolgen oder Zufallszahlen keine Daten mehr rekonstruiert werden können. Laut den Vorgaben des BSI sollte für den höheren Schutzbedarf die Überschreibprozedur aus mindestens zwei Durchläufen und einer Verifikation des Überschreibvorgangs bestehen.

5.2.13.6 Anforderung 51

„Eine Weitergabe von Datenträgern an externe Stellen zur datenschutzgerechten Entsorgung ist nur zulässig, wenn der Datenträger vor der Übergabe an die externe Stelle datenschutzgerecht gelöscht wurde.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es wird eine Löschung entsprechend den in Kapitel 5.2.13.4 vorgestellten Kriterien ermöglicht.

5.2.13.7 Anforderung 52

„Die Löschung der Daten ist unter Angabe des Löschgrunds sowie des Anwenders, der die Löschung vornahm, zu protokollieren.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es existieren Frameworks zur Protokollierung wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, sodass die obige Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Im Bereich IHE XDS erlaubt ATNA eine Protokollierung entsprechender Ereignisse.

Über ein Pop-Up-Fenster wird die Eingabe eines Begründungstextes realisiert, der Begründungstext selber wird ins Protokoll übernommen.

[52] Bundesamt für Sicherheit in der Informationstechnik (BSI). M 2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten. [Online, zitiert 2015-07-17] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02433.html

5.2.13.8 Anforderung 53

„Erfolgt statt einer Löschung eine Sperrung der Daten, so muss die Begründung, warum die Daten nicht gelöscht werden, festgehalten werden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Über ein Pop-Up-Fenster wird die Eingabe eines Begründungstextes realisiert, der Begründungstext selber wird ins Protokoll übernommen.

Es existieren Frameworks zur Abbildung von Protokollierungsfunktionalitäten wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, sodass die obige Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Im Bereich IHE XDS erlaubt ATNA eine Protokollierung entsprechender Ereignisse.

5.2.13.9 Anforderung 54

„Ist der Grund für die Sperrung nicht länger gegeben, so muss unverzüglich eine Löschung erfolgen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Eine automatisierte Löschung seitens der Software kann aufgrund haftungsrechtlicher Fragen einem Hersteller nicht empfohlen werden. Z.B. kann ja ein Grund für die Rücknahme einer Sperrung sein, dass der Betroffene sich wieder in Behandlung befindet und die Daten gebraucht werden. Oder telefonisch wurde zwischen Behandler und Betroffenen vereinbart, dass der Betroffene eine Woche nach Ablauf der Aufbewahrungsfrist erneut zur Behandlung kommt und die Daten noch gebraucht werden.

Jedoch kann in entsprechenden Arbeitslisten dargestellt werden, bei welchen Daten der Grund für die Sperrung aus Systemsicht nicht länger existiert, sodass ein Mensch die Listen abarbeiten kann.

5.2.14 Zutrittskontrolle

5.2.14.1 Anforderung 55

„Zu schützende Bereiche und deren Zutrittspunkte müssen benannt und schriftlich festgehalten werden. Der Schutzbedarf eines Raumes bzw. eines Gebäudes ist an Hand des Schutzbedarfs der gespeicherten Daten festzustellen.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.14.2 Anforderung 56

„Es ist festzulegen, welche Voraussetzung eine Person erfüllen muss, um Zutritt zu erhalten. Der Kreis der Berechtigten ist auf das notwendige Minimum zu beschränken."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.14.3 Anforderung 57

„Zu schützende Räumlichkeiten sowie deren Zutrittspunkte müssen gegen den Zutritt unbefugter Personen durch geeignete technische (z.B. Schließanlage) oder organisatorische (z.B. Pförtner) Maßnahmen gegen den Zutritt durch Unbefugte geschützt werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Der oder die Serverräume der Datenaustauschplattform sind dergestalt zu schützen, dass nur autorisiertem Personal Zutritt zu den Räumlichkeiten gestattet wird. Hinweise zum Schutz eines Serverraums finden sich beim BSI[53].

5.2.15 Zugangskontrolle

5.2.15.1 Anforderung 58

„Da im Internet eine potenziell größere Gefährdung für einen unbefugten Zugriff auf personenbezogene Daten existiert, muss mindestens eine 2-Faktor-Authentifizierung erfolgen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die Standardanmeldeprozedur bei internetbasierten Datenaustauschplattformen basiert auf der Benutzung von Anmeldenamen in Kombination mit einem Passwort. Ein zweiter Faktor erhöht einerseits die Sicherheit bzgl. der Authentisierung, verzögert oder schlimmstenfalls verhindert ggfs. in einem Notfall den Zugriff auf benötigte Daten. Daher muss für den Notfall eine 1-Faktor-

[53] Bundesamt für Sicherheit in der Informationstechnik (BSI). B 2.4 Serverraum. [Online, zitiert 2015-07-17] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b02/b02004.html

Authentifizierung möglich sein. Im Berechtigungskonzept muss festgelegt werden, welche Rollen einen Notfallzuggriff durchführen können, so kann das Missbrauchspotential begrenzt werden.

Beim Online-Banking hat sich die Kombination Benutzername/Passwort mit zusätzlicher hardwarebasierter Nutzung eines Einmal-Passworts (TAN) bewährt. Im Rahmen von internetbasierten Datenaustauschplattformen empfiehlt sich daher, dass eine TAN zur Anmeldung auf das Mobiltelefon der anmeldenden Person gesendet wird.

Hardwaretoken bieten zwar eine größere Sicherheit, haben jedoch den Nachteil, dass die Gefahr des „Liegenlassens“ sehr groß ist. Das Mobiltelefon entwickelte sich zu einem steten Begleiter, sodass diese Gefahr hier als relativ gering anzusehen ist. Gerade im Gesundheitswesen muss der Zugriffsmöglichkeit ein entsprechendes Gewicht eingeräumt werden, sodass hier ggfs. in einer entsprechenden Notfallsituation eine geringere Sicherheit in Kauf genommen werden muss.

Statische IP-Adressen vorausgesetzt, bietet sich auch die Geo-Lokalisierung als probates Mittel für ein Benutzername/Passwort ergänzendes Kriterium an, sofern gewährleistet werden kann, dass eine Anmeldung an der Datenaustauschplattform an fest definierte Orte (Krankenhaus, Arztpraxis usw.) gebunden werden kann.

5.2.15.2 Anforderung 59

„Werden statische Passwörter zur Authentisierung eingesetzt, so müssen die Empfehlungen des BSI bzgl. der Generierung und des Umgangs eingehalten werden. D.h. es müssen technische und organisatorische Maßnahmen zu der Einhaltung der Empfehlungen des BSI getroffen werden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es werden Regeln umgesetzt, welche die grundlegenden Empfehlungen des BSI[54] befolgen. Jedoch können nicht alle Regeln umgesetzt werden. Beispiel: das KFZ-Kennzeichen soll nicht als Passwort zu hinterlegen sein. Um dies zu verhindern, muss das KFZ-Kennzeichen dem System bekannt sein. Aus Gründen der Datensparsamkeit sowie der Zweckbindung ist eine Erhebung des KFZ-Kennzeichens zur Optimierung der Passwortwahl rechtlich nicht zulässig, somit kann das System die Eingabe nicht prüfen.

Es müssen daher organisatorisch die Regelungen zur Passwortvergabe hinterlegt werden. Diese Regelungen werden in der Datenaustauschplattform aktiviert.

Stand heute sind technisch im System i.d.R. die folgenden Regeln hinterlegt:

- Für die Erstanmeldung neuer Benutzer werden Einmalpasswörter vergeben, die der Benutzer nach erfolgreicher Anmeldung wechseln muss.
- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten mindestens zwei dieser Anforderungen umgesetzt sein.
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.
- Die Wahl von Trivialpasswörtern ("BBBBBBBB", "12345678", usw.) wird verhindert.
- Nach einer definierten Anzahl Fehlversuche wird das System gesperrt.

[54] Bundesamt für Sicherheit in der Informationstechnik (BSI). M 2.11 Regelung des Passwortgebrauchs. [Online, zitiert 2015-07-17] Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

- Erfolgreiche Anmeldung wird protokolliert.
- Fehlgeschlagene Anmeldung wird protokolliert.
- Das Passwort muss regelmäßig gewechselt werden, der Passwortwechsel wird vom System initiiert.
- Sperrung des Accounts ab Datum xx.xx.2xxx
- Sperrung des Accounts bei Inaktivität > x Tagen.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden. Eine Passworthistorie verhindert die Nutzung der letzten x Passwörter, die somit nicht mehr genutzt werden können.

Auch zur Abbildung derartiger Regeln existieren Frameworks für verschiedene Programmiersprachen. In Java kann z.B. Passay (http://www.passay.org/) genutzt werden.

5.2.15.3 Anforderung 60

„Authentisierungsgeheimnisse dürfen nur gesichert in Netzwerken übertragen werden, d.h. es muss eine verschlüsselte Datenübertragung entsprechend dem Stand der Technik eingesetzt werden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Internetbasierte Datenaustauschplattformen können jederzeit mit TLS verschlüsselt betrieben werden. Ob eine Verschlüsselung genutzt wird und wie stark die Verschlüsselung ist, entscheidet der Betreiber der Datenaustauschplattform autonom.

5.2.15.4 Anforderung 61

„Passwörter und/oder entsprechende Formulareingaben dürfen nicht auf dem Client oder in seiner Umgebung unverschlüsselt gespeichert werden, eine Speicherung im Browser ist zu verhindern.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Eine temporäre Speicherung im Arbeitsspeicher des Clients lässt sich natürlich nicht verhindern, da Formulardaten ja versandt werden müssen und somit eine Verarbeitung der Formulardaten unumgänglich ist.

In der Datenaustauschplattform selbst werden Passwörter nur zugriffssicher gespeichert, d.h. mittels Hashfunktionen.

5.2.15.5 Anforderung 62

„Nach wiederholter fehlerhafter Authentisierung muss der Zugang gesperrt werden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Kann im System als Regel hinterlegt werden (siehe Kapitel 5.2.15.2).

5.2.15.6 Anforderung 63

„Die Sitzung muss gesperrt oder beendet werden, wenn der Anwender eine definierte Zeitspanne in der Sitzung keine Aktivitäten durchführte (Sitzungs-Zeitlimit, Session Timeout).“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Nach der organisatorisch festgelegten Zeitspanne wird der Rechner automatisierte über den Aufruf einer Systemfunktion des Betriebssystems gesperrt.

5.2.15.7 Anforderung 64

„Ein Prozess zur Rücksetzung bzw. Entsperrung von gesperrten Zugangskennungen ist einzurichten, zu beschreiben und anzuwenden.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Hier muss organisatorisch festgelegt werden, wie das Procedere aussehen soll. Denkbar ist eine Entsperrung mittels hinterlegten benutzerspezifischen Frage-Antwort-Templates, von denen per Zufallsgenerator x (>1) Fragen ausgewählt werden. Oder eine Einbindung einer Hotline, die ein neues Passwort vergibt.

Dem Anwender kann eine Benachrichtigung bzgl. erfolgter Sperrung per SMS oder E-Mail gesandt werden, je nach organisatorischen Vorgaben.

5.2.15.8 Anforderung 65

„Die Anzahl der Fehlversuche, die zu einer Sperrung führt, ist schriftlich festzuhalten und den Anwendern gegenüber zu kommunizieren.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Kann als Regel hinterlegt werden (siehe Kapitel 5.2.15.2 und Kapitel 5.2.15.6).

5.2.15.9 Anforderung 66

„Benutzerkennungen, welche über einen definierten Zeitraum nicht benutzt wurden, sind zu sperren bzw. auf inaktiv zu setzen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Kann als Regel hinterlegt werden (siehe Kapitel 5.2.15.2).

5.2.15.10 Anforderung 67

„Sind in der Datenaustauschplattform Daten enthalten, die in einer medizinischen Notfallsituation zur Patientenbehandlung benötigt werden, so kann unter Berücksichtigung einer trotzdem erforderlichen Authentifizierung des Zugreifenden eine vereinfachte Form der Anmeldung genutzt werden. Hierbei sind der Zugreifende, eine Begründung des Notfallzugriffs sowie die gesichteten Daten zu protokollieren.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Siehe Kapitel 5.2.15.1

5.2.16 Zugriffskontrolle

5.2.16.1 Anforderung 68

„Es muss ein Berechtigungs- und Rollenkonzept erstellt und gepflegt werden, aus dem eindeutig abzulesen ist, wer welche Rolle (funktionell und strukturell) und damit verbundene Rechte bzgl. des Datenzugriffs hat.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.16.2 Anforderung 69

„Bzgl. der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept ist das Need-to-know-Prinzip anzuwenden.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.16.3 Anforderung 70

„Im Berechtigungs- und Rollenkonzept muss beschrieben sein, welche Funktionsrollen nicht miteinander vereinbar sind und somit nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Es sind technische und organisatorische Maßnahmen zu ergreifen, um diese Trennung sicherzustellen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

-

Beispiel(e) für Umsetzungsmöglichkeiten:

Das Berechtigungskonzept kann in ein Regelwerk überführt werden, welches beispielsweise mittels XACML abgebildet wird. Darauf greift eine regelbasierte Funktionalität der Plattform zu, überprüft die Berechtigungen und sorgt so für die Einhaltung der Regeln. Somit kann die Anforderung umgesetzt werden.

Allerdings muss man beachten, dass das Regelwerk umso komplexer wird, je differenzierter das Berechtigungs- und Rollenkonzept ausgearbeitet wird. Eine auf Anhieb von Menschen nachvollziehbare Abbildung des Regelwerks kann bei äußerst komplexen Berechtigungs- und Rollenkonzepten ggfs. nicht realisiert werden.

5.2.16.4 Anforderung 71

„Eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, ist zu verhindern. Es sind technische und organisatorische Maßnahmen zu ergreifen, um dies sicherzustellen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Das Berechtigungskonzept kann in ein Regelwerk überführt werden, welches beispielsweise mittels XACML für die Einhaltung der Regeln sorgt. Somit kann die Anforderung umgesetzt werden.

5.2.16.5 Anforderung 72

„Im Berechtigungskonzept ist festzulegen, wer auf Grund welcher Geschehnisse auf Protokolldaten zugreifen darf.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.16.6 Anforderung 73

„Protokolldaten sind gegen unbefugten Zugriff in geeigneter Weise entsprechend dem Stand der Technik zu schützen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Im Berechtigungskonzept bzw. im Protokollierungskonzept muss beschrieben werden, wer auf welche Daten aus welchen Gründen wann zugreifen darf. Dies kann in ein Regelwerk überführt, welches beispielsweise mittels XACML für die Einhaltung der Regeln sorgt. Somit kann die Anforderung umgesetzt werden.

5.2.16.7 Anforderung 74

„Die Aufbewahrungsdauer für Protolldaten ist schriftlich festzulegen."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.16.8 Anforderung 75

„Die Begründung für die Festlegung der Aufbewahrungsdauer ist schriftlich festzuhalten, sodass Dritte die Begründung nachvollziehen können."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17 Weitergabekontrolle

5.2.17.1 Anforderung 76

„Werden Daten an Dritte weitergegeben (z.B. durch die Weitergabe eines elektronischen Datenexports oder Ausdrucks der Daten), so muss entweder eine gesetzliche Grundlage hierfür vorhanden sein oder der Betroffene der Weitergabe zugestimmt haben."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.2 Anforderung 77

„Es ist festzulegen, welche Stellen/Personen an wen welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies zu geschehen hat.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Die Festlegung, welche Stellen/Personen an wen welche Daten übermitteln dürfen und auf welchem Übertragungsweg dies zu geschehen hat, ist eine rein organisatorische Maßnahme. Diese organisatorische Festlegung ist im Rahmen des Kontextes einer Datenaustauschplattform jedoch nur nutzbar, wenn diese Festlegung technisch adaptiert und geprüft werden kann. Die technische Unterstützung kann hierbei nicht bei der Festlegung bestehen (abgesehen von entsprechender Dokumentationssoftware, welche hilft den Überblick bzgl. der Regelungen zu behalten), sondern nur bei der Prüfung.

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.3 Anforderung 78

„Die Rechtmäßigkeit der Übermittlung von Daten ins Ausland ist vor der Übermittlung zu prüfen.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.4 Anforderung 79

„Erfolgt eine Übermittlung in ein Drittland, also außerhalb des EWR, so muss zwischen Daten exportierender Stelle und dem Datenimporteur eine vertragliche Regelung zum Datenschutz existieren, welche ein der EU angemessenes Datenschutzniveau beim Datenimporteur garantiert. D.h. es muss eine Verpflichtung der Parteien auf die Einhaltung der EU-Datenschutzregelungen sowie das Ergreifen ausreichender technisch-organisatorischer Maßnahmen vorhanden sein. Diese vertragliche Regelung schließt auch jegliche Zweckänderung inklusive der Verwendung der Daten für eigene Zwecke beim Datenimporteur aus.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.5 Anforderung 80

„Ist die Rechtmäßigkeit nicht eindeutig sichergestellt, ist die Übermittlung zu verhindern.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.6 Anforderung 81

„Die Übertragung personenbezogener oder personenbeziehbarer Gesundheitsdaten zwischen Clients und Servern wie auch zwischen Servern selbst muss entsprechend dem jeweiligen Stand der Technik generell verschlüsselt erfolgen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Auf Internettechnologie basierende Datenaustauschplattformen können prinzipiell TLS zur Verschlüsselung des Datentransfers verwenden. Ob der Plattformbetreiber diese Technologie nutzt und wenn ja, in welcher Stärke die Verschlüsselung erfolgt, liegt beim Betreiber.

5.2.17.7 Anforderung 82

„Sind Schnittstellen im System vorhanden, welche dem Datenimport oder -export dienen, so ist diese Schnittstelle zu dokumentieren.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

✍ **Hinweis:** die technische Dokumentation der Datenaustauschplattform, die selbstverständlich auch die Schnittstellenbeschreibung beinhaltet, liegt vor. Welche Schnittstellen in welcher Form im jeweiligen Szenario eingesetzt werden, muss der Betreiber dokumentieren.

5.2.17.8 Anforderung 83

„Es ist der Prozess zur Sammlung, Entsorgung/Vernichtung bzw. Löschung von Datenträgern festzulegen und schriftlich festzuhalten.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.17.9 Anforderung 84

„Dieser Prozess muss datenschutzgerechte Löschverfahren beinhalten.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Siehe Kapitel 5.2.13.4

5.2.17.10 Anforderung 85

„Die vollständige, datenschutzgerechte und dauerhafte Löschung von Datenträgern ist zu protokollieren.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Alle mit Methoden der Datenaustauschplattform initiierten Löschvorgänge werden protokolliert.

5.2.17.11 Anforderung 86

„Gesundheitsdaten sind entsprechend dem Stand der Technik verschlüsselt in der Datenbank zu speichern, so dass bei administrativen Zugriffen Wartungspersonal keinen unbefugten Zugriff auf die gespeicherten Daten erhalten kann.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die meisten Datenbanksysteme wie Oracle, MySQL usw. bieten die Möglichkeiten, Daten verschlüsselt in der Datenbank abzulegen, so dass die technische Umsetzung bei Nutzung dieser Mechanismen gewährleistet ist.

5.2.18 Eingabekontrolle

5.2.18.1 Anforderung 87

„Nur Personen, die laut Berechtigungskonzept zu einer Eingabe berechtigt sind, dürfen personenbezogene oder personenbeziehbare Daten in eine Datenaustauschplattform eingeben.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die Nutzung von Daten muss im Berechtigungskonzept hinterlegt werden. Die Vorgaben des Berechtigungskonzepts werden in ein Regelframework (z.B. durch Nutzung von XACML) überführt. D.h. wenn im Berechtigungskonzept die obige Forderung enthalten ist, wird dies auch im Regelwerk entsprechend berücksichtigt.

5.2.18.2 Anforderung 88

„Nur Personen, die laut Berechtigungskonzept zu einem Datenimport berechtigt sind, dürfen einen Import personenbezogener oder personenbeziehbarer Daten in eine Datenaustauschplattform durchführen oder veranlassen."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die Nutzung von Daten muss im Berechtigungskonzept hinterlegt werden. Die Vorgaben des Berechtigungskonzepts werden in ein Regelframework (z.B. durch Nutzung von XACML) überführt. D.h. wenn im Berechtigungskonzept die obige Forderung enthalten ist, wird dies auch im Regelwerk entsprechend berücksichtigt.

5.2.18.3 Anforderung 89

„Sowohl die Eingabe wie auch der Import personenbezogener oder personenbeziehbarer Daten muss protokolliert werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es existieren Frameworks zur Protokollierung wie beispielsweise log4j für Java, welche eine beliebige Detailtiefe bei der Protokollierung erlauben, so dass die obige Anforderung hinsichtlich der Protokollierung technisch durch diese Frameworks abgebildet werden kann.

Im Bereich IHE XDS erlaubt ATNA eine Protokollierung entsprechender Ereignisse.

5.2.19 Auftragskontrolle

5.2.19.1 Anforderung 90

„Der Auftraggeber überzeugt sich vor sowie in regelmäßigen Abständen auch nach Erteilung der Auftragsvergabe von der Einhaltung der vertraglich vereinbarten datenschutzrechtlichen Vorgaben, insbesondere der TOMs.."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.19.2 Anforderung 91

„Wenn personenbezogene oder personenbeziehbare Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, so ist ein ADV-Vertrag abzuschließen.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.19.3 Anforderung 92

„Der Auftragnehmer dokumentiert die Auftragsausführung dergestalt, dass der Auftraggeber die ordnungsgemäße Durchführung eines Auftrags, d.h. die Durchführung des Auftrags gemäß den Anweisungen des Auftraggebers, kontrollieren kann.“

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.20 Verfügbarkeitskontrolle

5.2.20.1 Anforderung 93

„Es muss ein Backup-Konzept vorhanden sein, welches gewährleistet, dass die Daten nach einem Vorfall in angemessener Zeit wieder zur Verfügung gestellt werden können. In diesem Backup-Konzept muss berücksichtigt werden, dass nur berechtigte Personen Zugriff auf Backup-Daten erlangen können.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Es besteht die Möglichkeit, regelbasiert nach bestimmten Ereignissen oder zu festgelegten Zeitpunkten alle oder einen definierten Teil der Daten zu exportieren. Die exportierten Daten stehen dann entweder einer externen Backup-Software zur Verfügung oder können in einem Netzwerk-Storage als Backup verbleiben.

5.2.20.2 Anforderung 94

„Es muss eine regelmäßige Prüfung stattfinden, ob mittels der gesicherten Daten eine Wiederherstellung möglich ist.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Das Zurückspielen der Daten kann getestet werden. Jedoch werden alle seit dem Backup erfassten Daten im Produktivsystem überschrieben. Daher empfiehlt es sich, zu Testzwecken ein Testsystem zur Verfügung zu haben, in welches testweise das Backup zurückgespielt wird.

5.2.20.3 Anforderung 95

„Entsprechend der festzulegenden Anforderung an die Verfügbarkeit der Datenaustauschplattform müssen Notfalleinrichtungen vorhanden sein."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Die internetbasierte Datenaustauschplattform kann im Cluster auf mehrere Server und dementsprechend mehrere verbundene Serverstandorte verteilt werden. IHE XDS könnte z.B. mehrere Repositories verwenden.

5.2.20.4 Anforderung 96

„Es muss ein Notfallplan vorhanden sein, dessen Befolgung eine Minimierung des Schadens bzw. eine Verhinderung des Eintretens eines Schadens zum Ziel hat."

Umsetzung:

X	Rein Organisatorisch
	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

-

5.2.21 Trennung

5.2.21.1 Anforderung 97

„Personenbezogene oder personenbeziehbare Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen getrennt verarbeitet werden."

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Ob eine Mandantentrennung durchgeführt wird, hängt vom Einsatzszenario der Datenaustauschplattform ab; generell sollte die Plattform mandantenfähig sein.

Ist die Datenaustauschplattform nicht mandantenfähig, so muss für jeden Zweck eine eigene Datenaustauschplattform genutzt werden.

5.2.21.2 Anforderung 98

„Die Verarbeitung personenbezogener Daten verschiedener Mandanten muss physisch oder logisch getrennt voneinander erfolgen.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Ob eine Mandantentrennung durchgeführt wird, hängt vom Einsatzszenario der Datenaustauschplattfom ab. Wird eine Mandantentrennung durchgeführt, so werden für jeden Mandanten physisch oder logisch getrennte Datenbanken angelegt, jedoch eine gemeinsame Datenbankmanagementlösung verwendet, sodass in diesen Fällen letztlich immer eine logische Trennung vorhanden ist.

5.2.21.3 Anforderung 99

„Die Aufbewahrung, Archivierung und Löschung von personenbezogenen Daten verschiedener Mandanten oder mit unterschiedlicher Zweckbindung muss getrennt voneinander möglich sein.“

Umsetzung:

	Rein Organisatorisch
X	Technische Unterstützung

Beispiel(e) für Umsetzungsmöglichkeiten:

Ob eine Mandantentrennung durchgeführt wird, hängt vom Einsatzszenario der Datenaustauschplattfom ab. Wird eine Mandantentrennung durchgeführt, so werden für jeden Mandanten separate Datenbanken angelegt, jedoch eine gemeinsame Datenbankmanagementlösung verwendet (logische Trennung). Von jeder Datenbank kann separat ein Backup angelegt werden.

6 Glossar

Abrufverfahren	Jedes Verfahren, mit dem personenbezogene Daten abgerufen werden können
Abrufverfahren, automatisiertes	Jedes Abrufverfahren, welches EDV nutzt
Betreiber	Jede natürliche oder juristische Person, die für den Betrieb verantwortlich ist, die erforderliche tatsächliche und rechtliche Verfügungsgewalt hat oder in dessen Namen das Unternehmen betrieben wird
Betroffener	Betroffener ist eine Bezeichnung eines Menschen, der betroffen ist von einer Sache. Im Sinne des Datenschutzes ist ein Betroffener eine bestimmte oder bestimmbare natürliche Person, zu welcher Daten über persönliche oder sachliche Verhältnisse beziehbar sind (§3 Abs. 1 BDSG)
Drittanbieter	Jede Person oder Stelle, welches Produkte und Produktfamilien anbietet, ohne dem Anbieter des Produkts („Erstanbieter“) anzugehören oder von ihm beauftragt zu sein („Zweitanbieter“).
Dritter	Jede Person oder Stelle außerhalb der verantwortlichen Stelle (§3 Abs. 8 BDSG). 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.
Empfänger	Jede Person oder Stelle, die Daten erhält (§3 Abs. 8 BDSG)
Empfängerland	Land, in welches Daten übermittelt und/oder gespeichert werden
Offline-Attacke	Offline Attacken sind Angriffe, die ihre schädliche Wirkung auch ohne eine bestehende Netzverbindung entfalten können. Zu den häufigsten Offline-Attacken zählen - Verbreitung von Viren - Übermittlung von Trojanischen Pferden - Manipulation von Daten - Brute Force Angriffe auf lokal gespeicherte, verschlüsselte Daten
Patient	Eine Person, die von einem Arzt, einer Ärztin oder einem Angehörigen anderer Heilberufe behandelt oder betreut wird
Plattformbetreiber	Betreiber einer Datenaustauschplattform (siehe auch Kapitel „Akteure“, Nr. 2)
Protokolldaten	Jedes Datum, welches im Rahmen einer Protokollierung erhoben wird.
Protokollierung	Eine Aufzeichnung, welche mindestens den Zeitpunkt, die ausgeführte Handlung und den Handelnden beinhaltet
Pseudonymisieren	Das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§3 Abs. 6a BDSG)

Stelle, speichernde	Jede Person oder Stelle, die personenbezogene Daten speichert
Stelle, übermittelnde	Jede Person oder Stelle, die personenbezogene Daten übermittelt
Stelle, verantwortliche	Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§3 Abs. 7 BDSG)

7 Abkürzungsverzeichnis

Abs.	Absatz
ADV	Auftragsdatenverarbeitung
Apps	Mobile Application Software
Art.	Artikel
ATNA	Audit Trail and Node Authentication
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BO	Berufsordnung
BPPC	Basic Patient Privacy Consents
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDA	Clinical Document Architecture
COCIR	European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry
DIN	Deutsches Institut für Normung
DSB	Datenschutzbeauftragter
EDV	Elektronische Datenverarbeitung
eEPA	Einrichtungsübergreifende elektronische Patientenakte
eFA	Fallbezogene einrichtungsübergreifende elektronische Patientenakte
EG	Europäische Gemeinschaft
EN	Europäische Norm
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GG	Grundgesetz
h.M.	Herrschende Meinung
HTML	Hypertext Markup Language
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IHE	Integrating the Healthcare Enterprise
IP	Internet protokoll
ISO	International Organization for Standardization
IT	Informationstechnik
ITK	Informations- und Telekommunikationstechnik
KIS	Krankenhaus-Informatzions—System
Lit.	Literal

MAC	Mandatory Access Control
Nr.	Nummer
OASIS	Organization for the Advancement of Structured Information Standards
PaaS	Platform as a Service
PACS	Picture Archiving and Communication System (Bildablage- und Kommunikationssystem)
pEPA	Persönliche einrichtungsübergreifende elektronische Patientenakte
RL	Richtlinie
SaaS	Software as a Service
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOMs	Technische und organisatorische Maßnahmen
TS	Technical Specification
UWG	Gesetz gegen den unlauteren Wettbewerb
XACML	eXtensible Access Control Markup Language
XDS	Cross-Enterprise Document Sharing
Ziff.	Ziffer