

Praxishilfe „Umgang mit Online-Terminmanagementsystemen“

Erarbeitet von Mitgliedern aus den nachfolgend genannten Verbänden:

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



Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.



Deutsche Vereinigung für Datenschutz DVD e.V.



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



Fachverband externe Datenschutzbeauftragte e.V.



Version 1

Stand: 9. November 2024

Autoren (alphabetisch)

Craezer, Stefan	Diözesan-Caritasverband für das Erzbistum Köln e.V.
Crookes, Jamie	Compliant Digital GmbH & Co. KG
Da Pont, Frank	B·A·D Gesundheitsvorsorge und Sicherheitstechnik GmbH
Knappe, Andreas	Klinikum Bad Salzungen GmbH
Koeppe, David	Vivantes - Netzwerk für Gesundheit GmbH
Letter, Michael	5medical management GmbH
Lotzkat, Sascha	Rechtsanwältin und Datenschutzbeauftragte
Möller, Georg	SK-Consulting Group GmbH
Mühlich, Regina	AdOrga Solutions GmbH
Rüdlin, Mark	Rechtsanwalt + Datenschutzbeauftragter
Schlütter, Johannes	net.ter GmbH
Schütze, Dr. Bernd	GMDS AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)
Weichert, Dr. Thilo	Deutschen Vereinigung für Datenschutz e. V.
Wunschel, Stefan	Sana Kliniken AG

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

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

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

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

Copyright

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

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



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

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

Die Nutzung ist unter den folgenden Bedingungen möglich:

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

Im Weiteren gilt:

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

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

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

bzw. für den vollständigen Lizenztext

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

Inhaltsverzeichnis

Zusammenfassung	1
1 Einführung ins Thema	3
1.1 Berufsrecht – Datenschutzrecht – Strafrecht: Was regelt was?	3
1.2 Stiftung Warentest: Online-Terminmanagementsysteme bieten bei Datenschutz „Optimierungspotenzial“	7
2 Abgrenzung/Klarstellung	8
3 Begriffsbestimmungen	9
3.1 Gesundheitsdaten	9
3.2 Geheimnisbetroffene	10
3.2.1 Berufsgeheimnisträger	10
3.2.2 Offenbarung	10
3.3 Leistungserbringer	12
3.4 Dienstleister, Anbieter, Lieferant, Hersteller	14
3.4.1 Hersteller	14
3.4.2 Anbieter/Lieferant	14
3.5 Patientendaten	14
3.6 Personenbezogene Daten	17
3.6.1 Pseudonyme Daten	18
3.6.2 Anonyme Daten	19
3.7 Sozialdaten	21
4 Rechtliche Rahmenbedingungen	23
4.1 Datenschutzrechtliche Anforderungen	23
4.1.1 Einhaltung der „Grundsätze für die Verarbeitung personenbezogener Daten“	23
4.1.2 Rechtsgrundlage der Verarbeitung	25
4.1.2.1 Einwilligung	25
4.1.2.2 Zweckänderung aufgrund einer Interessensabwägung	27
4.1.2.3 Behandlungsvertrag	28
4.1.2.4 Weitere Erlaubnistatbestände	31
4.1.3 Verschwiegenheitspflicht	32
4.1.4 Gewährleistung der Betroffenenrechte	32
4.1.4.1 Informationspflichten	33
4.1.4.2 Auskunftsrecht	33
4.1.4.3 Recht auf Berichtigung	33
4.1.4.4 Recht auf Einschränkung der Verarbeitung („Sperrung“)	33
4.1.4.5 Recht auf Löschung	34
4.1.4.6 Widerspruchsrecht	34
4.1.4.7 Recht auf Datenübertragbarkeit	34
4.1.4.8 Profilbildung / automatisierte Einzelfallentscheidung	35
4.1.5 Ort der Verarbeitung: Einsatz von Cloud-Dienstleistern	35

4.1.6	Auftragsverarbeitung: _____	38
4.1.6.1	Auftragnehmer muss Garantien zur Einhaltung DS-GVO vorweisen _____	38
4.1.6.2	Mandantentrennung muss zwingend beachtet werden _____	39
4.1.7	Gemeinsame für die Verarbeitung Verantwortliche _____	39
4.1.8	Sicherheit der Verarbeitung _____	40
4.1.9	Meldepflicht von Datenpannen _____	40
4.2	Ärztliche Schweigepflicht: Berufsrecht _____	41
4.3	Verschwiegenheits-/Schweigepflicht von anderen Berufsordnungen _____	44
4.4	Verbot der unbefugten Offenbarung: Strafrecht _____	44
4.5	Dokumentationspflicht der Patientenbehandlung _____	47
4.6	Behandlungspflicht: Dürfen Patienten, die eine Online-Terminvereinbarung nicht nutzen möchten, abgelehnt werden? _____	48
4.6.1	Versorgungspflicht bei Krankenhäusern _____	48
4.6.2	Versorgungspflicht von niedergelassene Vertragsärzten/Vertragszahnärzten _____	49
4.6.3	Betreuungspflicht durch Betriebsärzte _____	50
4.6.3.1	Rechte der Arbeitnehmer auf betriebsärztliche Betreuung _____	50
4.6.3.2	Übernahme der arbeitsmedizinischen Betreuung durch einen überbetrieblichen Dienst von Betriebsärzten _____	51
4.7	Pflicht zur Barrierefreiheit _____	52
4.7.1	Webseiten-Richtlinie der EU _____	53
4.8	Webportal: Ein digitaler Dienst _____	55
4.8.1	Anbieter von digitalen Diensten _____	55
4.8.2	Zu erfüllende Anforderungen _____	56
4.9	Beschlagnahmeschutz bei Dienstleistern _____	56
4.10	Eigenständige Datenerhebung durch den Dienstleister _____	57
4.10.1	Vom Leistungserbringer gegenüber dem Dienstleister zu erbringende Fachkundenachweise _____	58
4.10.2	Dienstleister fordert Versicherungsnachweis vom Leistungserbringer _____	58
4.10.3	Nutzung von Patientendaten zu statistischen Auswertungen des Dienstleisters _____	58
4.10.4	Patienten-Umfragen durch den Dienstleister _____	59
4.10.5	Rechteübertragung _____	59
4.10.6	Folgen einer eigenständigen Verarbeitung durch den Dienstleister _____	60
5	Anforderungen an Online-Terminbuchungssystemen _____	61
5.1	Anforderungen an Leistungserbringer, die IT-Lösungen nutzen _____	61
5.1.1	Rechtsgrundlage _____	61
5.1.2	Datenminimierung _____	61
5.1.3	Gewährleistung Betroffenenrechte _____	62
5.1.4	Barrierefreiheit _____	63
5.1.5	Privacy by Design _____	64
5.1.6	Sicherheit der Verarbeitung _____	64
5.1.7	Erinnerung an Termin _____	65
5.1.8	Anbieter eines digitalen Dienstes _____	66

5.2	Anforderungen, die Online-Terminmanagementsysteme erfüllen müssen	66
5.2.1	Mandantentrennung	66
5.2.2	Gewährleistung Betroffenenrechte	67
5.2.3	Barrierefreiheit	68
5.2.4	Privacy by Design	68
5.2.5	Sicherheit der Verarbeitung	69
5.2.6	Erinnerung an Termin	71
6	Abkürzungen	72
Anhang 1:	Beispielhafte Nennung von Leistungserbringern	74
Anhang 1.1	Leistungserbringer von Heilmitteln	74
Anhang 1.2	Leistungserbringer von Hilfsmitteln	74
Anhang 2:	Beispielhafte Aufzählung von Dienstleistern, die Online-Terminmanagementsysteme anbieten	76

Zusammenfassung

In Deutschland werden von verschiedenen Dienstleistern Terminverwaltungssysteme (Online-Terminmanagementsysteme oder auch Online-Terminbuchungslösungen) angeboten, welche die Suche und Buchung von Terminen bei niedergelassenen Ärzten und Zahnärzten sowie in Krankenhäusern ermöglichen. Mittlerweile werden auch im Rahmen der betriebsmedizinischen Betreuung durch einen arbeitsmedizinischen Dienstleister Termine online vergeben.

Dabei ist zu unterscheiden, ob die Patienten einen Account bei dem jeweiligen Dienstleister eingerichtet haben, sodass ein Vertragsverhältnis zwischen dem jeweiligen Patienten und dem Dienstleister des jeweiligen Online-Terminmanagementsystems besteht, oder ob das Vertragsverhältnis zwischen dem medizinischen Leistungserbringer (beispielsweise niedergelassene Ärzte, Krankenhäuser, Anbieter häuslicher Krankenpflege, Apotheker usw.) und dem Dienstleister des jeweiligen Online-Terminmanagementsystems besteht. In letzterem Fall muss der medizinische Leistungserbringer die gesetzlichen Rahmenbedingungen beachten, die für die Behandlung existieren. Dies sind beispielsweise die bei der Behandlung von gesetzlich versicherten Patienten zu beachtenden Vorgaben aus dem SGB V, aber natürlich auch Vorgaben aus dem Datenschutz- sowie dem Strafrecht.

Sowohl das Datenschutzrecht wie auch das Strafrecht verbieten eine unbefugte Offenbarung. Entsprechend der Rechtsprechung des EuGH ist der Begriff des Gesundheitsdatums sehr weit auszulegen, sodass bereits die Terminvereinbarung bei einem medizinischen Leistungserbringer unter diesen Begriff fällt. Insbesondere gelten strenge Verschwiegenheitspflichten. Dienstleister dürfen nur die für die Dienstleistung erforderlichen Daten verarbeiten, sodass selbstverständlich Zugriffe auf Daten abgeschlossener Behandlungsfälle wie auch auf Daten verstorbener Patienten unzulässig sind; ermöglicht ein medizinischer Leistungserbringer einen entsprechenden Zugriff, so verletzt er regelmäßig seine Verschwiegenheitspflicht und begeht nicht nur einen Datenschutzverstoß, sondern auch eine Straftat. Eine Ärztin oder ein Arzt verstößt damit zugleich gegen ärztliches Berufsrecht.

Die datenschutzrechtlichen Vorgaben verlangen bei der Einbindung von externen Dienstleistern u. a. einen Vertrag, wobei zwischen einem Vertrag zur Auftragsverarbeitung und einem Vertrag zur gemeinsamen Verantwortlichkeit unterschieden wird. Insbesondere dann, wenn der IT-Dienstleister die Daten (auch) für eigene Zwecke wie beispielsweise zur Qualitätssicherung nutzt, wird ein Vertrag zur Auftragsverarbeitung regelmäßig nicht ausreichen.

Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, wobei die Verarbeitung von Gesundheitsdaten, wie sie Patientendaten und damit auch Terminvereinbarungen von Patienten darstellen, besonders geschützt ist. Ein Behandlungsvertrag, den jeder Patient mit einem medizinischen Leistungserbringer beim Aufsuchen einer Arztpraxis, Apotheke oder Krankenhaus abschließt, erlaubt die Verarbeitung der für die medizinische Dienstleistung erforderlichen Patientendaten. Für die Behandlung kann auch eine Terminvereinbarung erforderlich sein, wobei eine Online-Terminvereinbarung in keinem Fall erforderlich ist; eine solche kann lediglich ein zusätzliches Angebot zur Terminvergabe in der Praxis – sei es vor Ort oder per Telefon – darstellen. Da eine entsprechende Online-Terminvereinbarung regelmäßig nicht erforderlich ist, ist der Behandlungsvertrag keine Legitimation für die Verarbeitung, d. h. es muss eine Einwilligung der betroffenen Patienten vorliegen, und zwar eine ausdrückliche Einwilligung, da es sich um Gesundheitsdaten handelt.

In diesem Zusammenhang ist es wichtig zu wissen, dass im Jahr 2023 rund 5 % der 16- bis 74-jährigen Personen in Deutschland sogenannte „Offliner“ waren,¹ also noch nie das Internet genutzt haben. In der Altersgruppe der 65- bis 74-Jährigen waren es sogar 15 %. Diese Menschen sind bei einer reinen Online-Terminvergabe von einer Behandlung ausgeschlossen. Ärzte mit Kassenzulassung haben gegenüber gesetzlich versicherten Bürgern eine Behandlungspflicht. Somit verstößt eine ausschließlich online angebotene Terminvergabe gegen die gesetzlichen Vorgaben aus dem SGB V.

Die beim Online-Dienstleister gespeicherten Daten sind i. d. R. kein Bestandteil der gesetzlichen Dokumentationspflicht bei der Patientenbehandlung. Daher sind die Daten nach Erreichen des Zweckes, dies ist die Terminvergabe, zu löschen. Eine unzulässige längere Speicherung der Daten stellt einen bußgeldbewehrten Verstoß gegen die Vorgaben der Datenschutz-Grundverordnung dar. Die Leistungserbringer müssen sich daher stets vergewissern, dass die eingesetzten Dienstleister die Daten der Online-Terminbuchung nach Erreichung des Verarbeitungszweckes regelmäßig löschen.

Viele Online-Terminmanagementsysteme besitzen die Funktionalität, Patienten an anstehende Termine zu erinnern. Auch dies ist regelmäßig nicht erforderlich und darf nur erfolgen, wenn eine ausdrückliche Einwilligung des jeweiligen Patienten zur Erinnerung per SMS oder E-Mail durch den Online-Dienst vorliegt.

¹ Statistisches Bundesamt: Zahl der Woche - Gut 5 % der Bevölkerung im Alter von 16 bis 74 Jahren in Deutschland sind offline. Online, verfügbar unter https://www.destatis.de/DE/Presse/Pressemitteilungen/Zahl-der-Woche/2024/PD24_15_p002.html

1 Einführung ins Thema

In Deutschland werden von verschiedenen Dienstleistern Terminverwaltungssysteme (Online-Terminmanagementsysteme oder auch Online-Terminbuchungslösungen) angeboten, welche die Suche und Buchung von Terminen bei niedergelassenen Ärzten bzw. Zahnärzten, und Krankenhäusern ermöglichen. Auch im Rahmen der betriebsmedizinischen Betreuung durch einen überbetrieblichen arbeitsmedizinischen Dienstleister werden Termine online vergeben. Diese Angebote richten sich an Probanden², aber auch an den Arbeitgeber der Betroffenen, die Termine z. B. für die gesetzlich vorgeschriebenen arbeitsmedizinischen Betreuungsvorgaben Ihrer Mitarbeitenden, festlegen wollen.

In der Regel richten sich die Angebote sowohl an Patienten als auch an Leistungserbringer als Kunden. D. h. Patienten können bei dem jeweiligen Dienstleister einen Account einrichten, sodass ein Vertragsverhältnis zwischen dem jeweiligen Patienten und dem Dienstleister des jeweiligen Online-Terminmanagementsystems besteht. Enthalten Webseiten von Leistungserbringern eigenständige Terminbuchungsangebote, so entstehen bei Nutzung durch Patienten keine neuen Vertragsverhältnisse; diese Fallkonstellationen sind aus Datenschutzsicht relativ unproblematisch und werden hier nicht vertieft untersucht.

Auf der anderen Seite richten sich die jeweiligen Angebote an die Leistungserbringer, die u. a. mit der Anzahl der Patienten, die einen Account beim Dienstleister haben, und dem Versprechen auf mehr Terminbuchungen umworben werden. Aber auch die Vereinfachung der eigenen Terminverwaltung wird Leistungserbringern in Aussicht gestellt. Schließt ein Leistungserbringer einen Vertrag mit einem Dienstleister eines Online-Terminmanagementsystems ab, so entsteht hierdurch ein Vertragsverhältnis zwischen den beiden Parteien. Hierbei ist zu beachten, dass ein Vertrag zu Lasten Dritter unzulässig ist, d. h. aus dem Vertragsverhältnis zwischen einem Leistungserbringer und dem Dienstleister eines Online-Terminmanagementsystems kann keine rechtliche Verpflichtung für einen Dritten, d. h. insbesondere auch nicht für einen Patienten des Leistungserbringers, entstehen.³

1.1 Berufsrecht – Datenschutzrecht – Strafrecht: Was regelt was?

Patientendaten werden nicht nur durch das Datenschutzrecht geschützt. Auch das ärztliche Berufsrecht sowie das strafrechtliche Verbot einer unbefugten Offenbarung schützen Patientendaten. Bei der Beurteilung, ob Daten durch einen externen Dienstleister verarbeitet werden dürfen, muss daher zwischen dem strafrechtlichen Offenbarungsverbot, der berufsrechtlichen Schweigepflicht und der datenschutzrechtlichen Verschwiegenheitspflicht unterschieden werden. Hierbei handelt es sich um drei unterschiedliche Rechtsgebiete, die unabhängig voneinander zu betrachten sind. Auch wenn eine Verarbeitung datenschutzrechtlich zulässig ist, kann diese berufsrechtlich und/oder strafrechtlich verboten sein.

Die **datenschutzrechtliche Verpflichtung zur Geheimhaltung** besteht sowohl für Verantwortliche als auch für Auftragsverarbeiter (siehe Kapitel 4.1.3). Im Kontext der Auftragsverarbeitung verlangt

² In der Arbeitsmedizin spricht man von Probanden und nicht von Patienten, da der Betroffene in der Regel gesund ist und nicht als Heilung suchender Patient den Arzt aufsucht.

³ BGH: Urt. v. 2004-06-29, Az. VI ZR 211/03, Rn. 16: „Ein unzulässiger Vertrag zu Lasten Dritter liegt nur dann vor, wenn durch ihn unmittelbar eine Rechtspflicht eines am Vertrag nicht beteiligten Dritten - ohne seine Autorisierung - entstehen soll.“ Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2004,1630>, Volltext unter <https://openjur.de/u/188926.html>

Art. 28 Abs. 3 S. 2 lit. b DS-GVO, dass eine Vereinbarung zur Auftragsverarbeitung stets eine Regelung enthält, wonach nur Personen, welche zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, zur Verarbeitung der personenbezogenen Daten befugt sind. Diese Verpflichtung trifft nach Ansicht der deutschen Datenschutzkonferenz auch Verantwortliche und deren Beschäftigte.⁴ Die datenschutzrechtliche Verschwiegenheitspflicht bezieht sich somit auf alle personenbezogenen oder personenbeziehbaren Informationen, die bei der Verarbeitung in irgendeiner Form bekannt werden. Verstöße gegen das Datenschutzrecht können zivilrechtlich verfolgt werden. Die datenschutzrechtlichen Pflichten ändern nichts an der Reichweite des Verbots der unbefugten Offenbarung in § 203 Abs. 1 und 2 StGB⁵: Die Offenbarung der durch § 203 StGB geschützten Daten wird weder erschwert noch erleichtert.⁶ Insbesondere reicht auch das Vorliegen einer Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag nach Art. 28 DS-GVO nicht aus, um eine unbefugte Offenbarung nach § 203 StGB auszuschließen.⁷

Die Unabhängigkeit der strafrechtlichen Vorschriften von den datenschutzrechtlichen Regelungen findet sich schon in den Regelungen selbst. Entsprechend Dritter Teil Titel V Kapitel 4 Art. 82, 83 des Vertrags über die Arbeitsweise der Europäischen Union⁸ (AEUV) besitzt die EU nur eine Regelungskompetenz hinsichtlich der gegenseitigen Anerkennung gerichtlicher Urteile und Entscheidungen und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen mit grenzüberschreitender Dimension, nationale Regelungen wie beispielsweise das Offenbarungsverbot in § 203 StGB fallen i. d. R. nicht in die Zuständigkeit der EU. Nach Art. 2 Abs. 2 lit. b, d DS-GVO fallen Verarbeitungen im Anwendungsbereich von Titel V Kapitel 2 des Vertrags über die Europäische Union (EUV) sowie Verarbeitungen zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung nicht unter die DS-GVO, sodass Regelungen der DS-GVO auch keine Offenbarung i. S. d. § 203 StGB legitimieren können. § 1 Abs. 2 S. 2 BDSG⁹ enthält die Regelung, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen von den Regelungen des BDSG unberührt bleibt, auch entsprechende datenschutzrechtliche Landesvorschriften enthalten regelmäßig Vorgaben, dass die Vorgaben des § 203 StGB zu beachten und einzuhalten sind.¹⁰ Gleiches gilt für Vorgaben zur

⁴ Datenschutzkonferenz: Kurzpapier Nr. 19 - Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO. Online, zitiert am 2024-08-24; verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

⁵ Schuster FP. (2015) Arztpraxen in der Cloud? - Strafbarkeitsrisiken nach § 203 StGB und weitere Fragestellungen. medstra: 280-284

⁶ Ulsenheimer K.: § 146, Rn. 30. In: Laufs/Kern/Rehborn (Hrsg.) Handbuch des Arztrechts. C. H. Beck Verlag, 5. Auflage 2019. ISBN 978-3-406-65614-9

⁷ Hartung: Teil 11.4.2 Datenschutz und Geheimnisschutz, Rn. 131. In Leupold/Wiebe/Glossner (Hrsg.) Münchener Anwaltshandbuch IT-Recht. C. H. Beck Verlag, 4. Auflage 2021. ISBN 978-3-406-74458-7
4. Auflage 2021

⁸ Vertrag über die Europäische Union (konsolidierte Fassung (AEUV)). Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012E/TXT>

⁹ Bundesdatenschutzgesetz (BDSG): § 1 Anwendungsbereich des Gesetzes Online, zitiert am 2024-08-24; verfügbar unter https://www.gesetze-im-internet.de/bdsg_2018/_1.html

¹⁰ So finden sich beispielsweise Regelungen bzgl. der Pflicht zur Einhaltung der Vorgaben von § 203 StGB in:

- § 46 Abs. 2, § 48 Abs. 2 Ziff. 2 Landeskrankenhausgesetz Baden-Württemberg
- § 24 Abs. 1 Landeskrankenhausgesetz Berlin
- § 41 Abs. 2 Bremisches Krankenhausgesetz
- § 38 Abs. 3 Landeskrankenhausgesetz Mecklenburg-Vorpommern
- § 27b Abs. 1 Ziff. 2 Thüringer Krankenhausgesetz

arbeitsmedizinischen Untersuchungen.¹¹ Datenschutzrechtliche und strafrechtliche Vorgaben sind daher unabhängig voneinander zu betrachten.^{12, 13, 14}

Die **berufsrechtliche Schweigepflicht** resultiert aus dem jeweiligen Berufsrecht wie beispielsweise:

- § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO);
- § 39a Abs. 2 Patentanwaltsordnung (PAO);
- § 57 Abs. 1 Steuerberatungsgesetz (StBerG) sowie § 5 Berufsordnung der Bundessteuerberaterkammer (BOSTB);
- § 43 Abs. 1 Wirtschaftsprüferordnung (WPO);
- § 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) bzw. deren Umsetzung im jeweiligen Landesrecht;
- Die Musterberufsordnung (MBO) der Bundeszahnärztekammer¹⁵ gilt für alle Mitglieder der (Landes-)Zahnärztekammern und für alle vorübergehend und gelegentlich im Geltungsbereich dieser Berufsordnung zahnärztlich tätigen Berufsangehörigen, rechtlich geltend ist jedoch nur die konkrete Berufsordnung des jeweiligen Bundeslandes; § 7 beinhaltet die Regelungen zur Verschwiegenheitspflicht, wobei die Regelungen den Regelungen der MBO-Ä entsprechen;
- § 8 (Muster-)Berufsordnung der Psychotherapeutinnen und -therapeuten¹⁶ (nach PsychThG) bzw. deren Umsetzung in den jeweiligen Psychotherapeuten Kammern;
- In jedem Bundesland existiert eine Berufsordnung für Apothekerinnen und Apotheker (allerdings gibt es keine Muster-Berufsordnung), in welcher sich eine Regelung zur Verschwiegenheit befindet, welche i. d. R. das in § 203 StGB enthaltene Offenbarungsverbot adressieren;¹⁷

¹¹ Siehe hierzu

- § 8 Abs. 1 ASiG
- § 6 Abs. 1 S. 6 ArbMedVV

¹² Hoeren T. (2018) Betriebsgeheimnisse im digitalen Zeitalter. Die Neuordnung von StGB und StPO. MMR: 12-18

¹³ Ein Beispiel bzgl. der unterschiedlichen Betrachtungsweise von datenschutzrechtlichen und strafrechtlichen Vorgaben findet sich in Kapitel „7.6 Broad consent: Keine Offenbarungsbefugnis i. S. d. § 203 StGB“ in der Praxishilfe von GMDS und GDD „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers“. Online, zitiert am 2024-08-24; verfügbar unter <https://gesundheitsdatenschutz.org/html/einwilligung.php>

¹⁴ Weichert, T.: Gutachten „Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung“, Kapitel 6.3 Materielles Verhältnis zum Datenschutzrecht. MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2022. ISBN 978-3-95466-700-0

¹⁵ Bundeszahnärztekammer: Musterberufsordnung (MBO). Online, zitiert am 2024-09-12; verfügbar unter <https://www.bzaek.de/recht/berufsrecht.html>

¹⁶ Bundespsychotherapeutenkammer (BPTK): Muster-Berufsordnung der Psychotherapeut*innen. Stand 14. Mai 2022. Online, zitiert am 2024-09-12; verfügbar unter <https://www.bptk.de/psychotherapeutinnen/#satzungen-and-ordnungen> bzw. pdf-Datei unter https://www.bptk.de/uploads/Muster_Berufsordnung_der_B_Pt_K_412a6bcb36.pdf

¹⁷ Beispielsweise:

- Berufsordnung für Apothekerinnen und Apotheker Bayerns, § 14. Online, zitiert am 2024-09-12; verfügbar unter <https://www.blak.de/berufsordnung>
- Berufsordnung der Apothekerkammer Niedersachsen, § 8. Online, zitiert am 2024-09-12; verfügbar unter <https://www.apothekerkammer-niedersachsen.de/rechtsvorschriften.php>
- Berufsordnung für Apothekerinnen und Apotheker der Apothekerkammer Nordrhein, § 14. Online, zitiert am 2024-09-12; verfügbar unter https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=75720170406111840737

- Einige Bundesländer – wenngleich nicht alle – haben eine Berufsordnung für Pflegefachkräfte,¹⁸ in denen jeweils auch Regelungen zur Verschwiegenheits- bzw. Schweigepflicht der Pflegekräfte regeln, welcher dieser Berufsordnung unterliegen.

Die ärztliche Schweigepflicht in den Berufs- und Standesvorschriften¹⁹ dient teilweise anderen Zwecken als § 203 StGB. Die berufsrechtliche Schweigepflicht richtet sich ausschließlich an die Angehörigen des jeweiligen Berufsstandes, beinhaltet aber nach § 9 Abs. 3 MBO-Ä (bzw. der jeweiligen Umsetzung in der jeweiligen Berufsordnung des betreffenden Landes) in der Regel die Verpflichtung, Beschäftigte und Dienstleister ebenfalls zur Schweigepflicht zu verpflichten.²⁰ Die Verschwiegenheits- und Schweigepflichten der anderen medizinischen Berufsordnungen sind der ärztlichen Berufsordnung in dieser Hinsicht vergleichbar. Die Verschwiegenheits- bzw. Schweigepflicht umfasst regelhaft alles, was den jeweiligen Personen in der Ausübung ihres Berufes anvertraut oder bekannt geworden ist. Verstöße gegen das jeweilige Berufsrecht können berufsrechtlich sanktioniert werden. Die in den Berufs- und Standesvorschriften enthaltenen Regelungen zur persönlichen Verschwiegenheit haben für die Strafnorm des § 203 StGB keine unmittelbare Bedeutung.²¹ Eine Verletzung der berufsrechtlichen Schweigepflicht kann jedoch mit den in den einzelnen Bundesländern gesetzlich festgelegten Sanktionen geahndet werden.²²

Die in § 203 Abs. 1, 2 StGB genannten Personen- und Berufsgruppen unterliegen dem **strafrechtlichen Offenbarungsverbot**, welches die unbefugte Offenbarung fremder Geheimnisse verbietet. Verstöße gegen dieses Offenbarungsverbot können strafrechtlich verfolgt werden. § 203 Abs. 1 StGB stellt den Geheimnisbruch durch Angehörige bestimmter Berufe, Beratungsstellen und Unternehmen unter Strafe, § 203 Abs. 2 StGB enthält die Pflicht zur Amtsverschwiegenheit, deren Verletzung durch Amtsträger und andere Personen, welche in amtlicher Eigenschaft auftreten oder

¹⁸ Beispielsweise

- Berufsordnung Land Berlin | Land Brandenburg. Online, zitiert am 2024-09-12; verfügbar unter https://deutscher-pflegerat.de/wp-content/uploads/2020/03/LPR-B_BB-Berufsordnung2010.pdf
- Pflegefachkräfte-Berufsordnung von Hamburg. Online, zitiert am 2024-09-12; verfügbar unter <https://www.landesrecht-hamburg.de/bsha/document/jlr-PflKrBerOHA2009rahmen>
- Berufsordnung für Pflegefachkräfte im Saarland. Online, zitiert am 2024-09-12; verfügbar unter <https://www.saarland.de/masfg/DE/portale/sozialesleben/leistungensoziales/pflege/pflegeausbildung/berufsordnung>
- Berufsordnung der Landespflegekammer Rheinland-Pfalz. Online, zitiert am 2024-09-12; verfügbar unter <https://pflegekammer-rlp.de/pflege-als-heilberuf/berufsordnung/>
- Sächsische Berufsordnung Pflegefachkräfte. Online, zitiert am 2024-09-12; verfügbar unter <https://www.revosax.sachsen.de/vorschrift/12628-Berufsordnung-Pflegefachkraefte>

¹⁹ Im juristischen Sprachgebrauch ist auch bis heute die Begrifflichkeit des „Standes- und Berufsrecht“ üblich. Das Standesrecht galt bis 1987, aufgrund der beiden „Bastille-Beschlüsse“ des Bundesverfassungsgerichtes (Urt. v. 1987-07-14, Az. 1 BvR 537/81) wurden die bis dahin geltenden Standesrichtlinien für Rechtsanwälte in Deutschland für unvereinbar mit dem Grundrecht auf Berufsfreiheit erklärt und seitdem etablierte sich für Anwälte ein modernes Berufsrecht. Einzelne Anwälte sind dagegen, dass in der heutigen Zeit weiterhin von Standesrecht gesprochen wird. Im medizinischen Umfeld fand eine Diskussion bzgl. der Nicht-Verwendung des Begriffs „Standesrecht“ bis heute nicht statt.

²⁰ Die entsprechende Regelung für Psychotherapeuten findet sich in § 8 Abs V der (Muster-)Berufsordnung

²¹ Ulsenheimer K.: § 139, Rn. 14. In: Laufs/Kern/Rehborn (Hrsg.) Handbuch des Arztrechts. C. H. Beck Verlag, 5. Auflage 2019. ISBN 978-3-406-65614-9

²² Eine Übersicht zu den in den jeweiligen Landesgesetzen enthaltenen für kammergerichtliche Verfahren findet sich z. B. in

- GMDS, BvD, DGU: „Landesrechtliche Anforderungen an medizinische Register: Was zu beachten ist“, Kapitel 3.3 „Ärztliche Schweigepflicht / Berufsrecht (§ 9 MBO-Ä)“. Stand: 2021-11-15. Online, zitiert am 2024-08-24; verfügbar unter https://gesundheitsdatenschutz.org/html/register_anforderungen.php

tätig werden, mit Strafe bedroht ist. Im Vordergrund von § 203 StGB steht das Individualinteresse an der Geheimhaltung bestimmter Tatsachen²³, d. h. der vom Geheimnis Betroffene kann über das Geheimnis verfügen. Aus dem in § 205 StGB enthaltenem Antragsfordernis ergibt sich, dass mit § 203 StGB ein Recht des Geheimnisbetroffenen, d. h. im Bereich der Gesundheitsversorgung des Patienten, geschützt werden soll. Daneben besteht ein Allgemeininteresse an der Verschwiegenheit von Amtsträgern. Es soll das Vertrauen der Bevölkerung gestärkt werden, dass Personen, welche in die Privatsphäre eindringen, diese Geheimnisse wahren.

Neben der strafrechtlichen Komponente ergibt sich aus § 203 StGB auch ein zivilrechtlicher Schutz. Entsprechend § 823 Abs. 2 BGB kann sich aus einem Verstoß gegen § 203 StGB eine zivilrechtliche Anspruchsgrundlage auf Schadensersatz ergeben, ggf. kann ein Verstoß gegen § 203 StGB, also eine unbefugte Offenbarung von Patientengeheimnissen, auch als Gesundheits- bzw. Freiheitsverletzung i. S. d. § 823 Abs. 1 BGB angesehen werden. Eine unbefugte Offenbarung von Patientengeheimnissen könnte eine Ursache für eine Psychose des Geheimnisbetroffenen, also des Patienten, darstellen und somit als „seelische Erschütterung“ eine pathologisch fassbare Beeinträchtigung der Gesundheit des Patienten auslösen.²⁴

1.2 Stiftung Warentest: Online-Terminmanagementsysteme bieten bei Datenschutz „Optimierungspotenzial“

Im Jahr 2020 testete Stiftung Warentest sieben Arzttermin Portale, die Ergebnisse wurden 2021 veröffentlicht.²⁵ Getestet wurden (in der Reihenfolge der Nennung bei Stiftung Warentest):

Arzttermin Portal	Bewertung „Basisschutz persönlicher Daten“
Kassenärztliche Bundesvereinigung eTerminservice (https://eterminservice.de/)	Sehr gut
Dr. Flex (https://dr-flex.de/)	Gut
jameda (https://www.jameda.de/)	Gut
ärzte.de MediService (https://www.arzttermine.de/)	Befriedigend
Doctena (https://www.doctena.de/)	Befriedigend
Doctolib (https://www.doctolib.de/)	Ausreichend
samedi (https://www.samedi.com/).	Ausreichend

²³ Hilgendorf E.: Einführung in das Medizinstrafrecht, 9. Kapitel. Die ärztliche Schweigepflicht, Rn. 4. C. H. Beck Verlag, 2. Auflage 2020. ISBN 978-3-406-74091-6

²⁴ So z. B. BGH Urt. v. 2019-05-21, AZVI ZR 299/17, Rn. 13: „Nach ständiger höchstrichterlicher Rechtsprechung können psychische Störungen von Krankheitswert eine Gesundheitsverletzung im Sinne des § 823 Abs. 1 BGB darstellen“. Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2019,17678> bzw. Volltext unter <https://openjur.de/u/2175633.html>

²⁵ Stiftung Warentest: Ganz schön unsensibel. test 1/2021: 92-95. Online, zitiert am 2024-08-24; verfügbar unter <https://www.test.de/Arzttermin-Portale-im-Test-Ganz-schoen-unsensibel-5692512-0/>

Dies zeigt, dass sowohl Patienten als auch Leistungserbringer, die Wert auf den Schutz der Gesundheitsdaten ihrer Kunden und Patienten legen, bei der Auswahl eines entsprechenden Dienstleisters sorgfältig vorgehen sollten und Werbeprospekten wenig Vertrauen schenken können.

Ziel dieser Praxishilfe ist es:

- a) Die wichtigsten rechtlichen Rahmenbedingungen für den Einsatz von Online-Terminmanagementsystemen zu besprechen,
- b) Leistungserbringern die wesentlichsten Aspekte aufzuzeigen, die bei der Auswahl und dem Einsatz einer entsprechenden Software-Lösung zu beachten sind,
- c) Dienstleistern von Online-Terminmanagementsystemen aufzuzeigen, was ihre Software aus datenschutzrechtlicher Sicht mindestens abbilden muss, sodass aus diesen Anforderungen ein Pflichtenheft abgeleitet werden kann, und
- d) Datenschutzbeauftragten eine Handreichung zum Thema zur Verfügung zu stellen, mit welcher sie ihre Arbeitgeber/Kunden noch besser beraten können.

2 Abgrenzung/Klarstellung

In dieser Praxishilfe geht es ausschließlich um eigenständige Online-Terminbuchungs-Software-Lösungen, die bei Leistungserbringern eingesetzt werden.

Die Verwendung entsprechender Online-Termin-Software durch Patienten, die sich bei entsprechenden Dienstleistern einen Account anlegen und darüber als Kunde des Dienstleisters des Online-Terminmanagementsystems Termine bei einem Leistungserbringer buchen, liegen nicht im Fokus dieser Praxishilfe. Gegebenenfalls kann es jedoch zu thematischen Überschneidungen kommen, bei denen einzelne Aspekte, die auch diese Szenarien betreffen, für den Einsatz entsprechender Tools bei einem Leistungserbringer relevant sind und daher ebenfalls besprochen werden.

3 Begriffsbestimmungen

3.1 Gesundheitsdaten

Der Begriff „Gesundheitsdaten“ wird in Art. 4 Nr. 15 DS-GVO europaweit legal definiert. Gesundheitsdaten sind „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Gesundheitsdaten gehören zu den in Art. 9 Abs. 1 DS-GVO genannten „besonderen Kategorien personenbezogener Daten“, deren Verarbeitung grundsätzlich verboten ist, ausgenommen ein in Art. 9 Abs. 2 DS-GVO genannter Ausnahmetatbestand erlaubt die Verarbeitung.²⁶ Entsprechend der Rechtsprechung des EuGH ist die Zuordnung eines Datums als „sensibles Datum“ i. S. d. Art. 9 Abs. 1 DS-GVO weit zu verstehen²⁷. Auch wenn ein Datum aufgrund der eigenen Bedeutung nach an sich kein sensibles Datum darstellt, ist entsprechend dem Urteil des EuGH zu prüfen, ob „mittels gedanklicher Kombination oder Ableitung“ auf diese in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien geschlossen werden kann. Werden in Art. 9 Abs. 1 DS-GVO genannte Datenkategorien mit anderen Daten verknüpft/in Beziehung gebracht, so gilt das Verarbeitungsverbot entsprechend der Rechtsprechung des EuGH für die Gesamtheit dieser Daten.²⁸

Aufgrund dieser Vorgaben des EuGH ist der Begriff „Gesundheitsdatum“ weit auszulegen²⁹. Insbesondere müssen auch indirekt mögliche Aussagen geprüft werden.

Beispiel: Eine Person besucht eine Arztpraxis. Die Standortdaten, also Straße, Postleitzahl und Ort, der Arztpraxis stellen eigentlich keine sensiblen Daten i. S. v. Art. 9 Abs. 1 DS-GVO dar. Da aber bekannt ist, dass eine Arztpraxis aufgesucht wird und dies i. d. R. für eine medizinische Betreuung erfolgt, ist diese Information als sensibles Datum zu bewerten.

Zur Klassifizierung als Gesundheitsdatum ist es unerheblich, ob die Daten zu dieser preisgebenden Person gehören oder zu einer dritten Person.³⁰ Sind Daten als Gesundheitsdaten i. S. v. Art. 4 Nr. 15 DS-GVO zu klassifizieren, ist der Anwendungsrahmen von Art. 9 DS-GVO eröffnet und eine Verarbeitung dieser Daten verboten, wenn nicht ein Ausnahmezustand von Art. 9 Abs. 2 DS-GVO i. V. m. mindestens einem der in Art. 6 Abs. 1 DS-GVO genannten Rechtfertigungstatbestände die Verarbeitung ausdrücklich erlaubt.

²⁶ EuGH Urt. v. 2023-01-26, Rechtssache C-205/21. Rn. 63. Online, zitiert am 2024-06-26; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0205>

²⁷ EuGH, Urt. v. 2022-08-01, Rechtssache C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2024-01-15; verfügbar unter <https://dejure.org/2010,236> bzw. Volltext abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184>

²⁸ EuGH Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 73. Online, zitiert am 2024-06-26; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

²⁹ Zu finden in verschiedenen Urteilen des EuGH, z. B.

- EuGH Urt. v. 2024-10-04, Rechtssache C-21/23. Rn. 81. Online, zitiert am 2024-10-06; verfügbar unter <https://curia.europa.eu/juris/document/document.jsf?text=&docid=290696&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4455161>

- EuGH Urt. v. 2004-01-10, Rechtssache C-101/01. Rn. 2, 50. Online, zitiert am 2024-10-06; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62001CJ0101>

³⁰ EuGH Urt. v. 2024-10-04, Rechtssache C-21/23. Rn. 85-90. Online, zitiert am 2024-10-06; verfügbar unter <https://curia.europa.eu/juris/document/document.jsf?text=&docid=290696&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4455161>

3.2 Geheimnisbetroffene

Der Betroffene ist diejenige Person, um dessen persönliches Geheimnis es sich handelt und auf dessen Geheimhaltungswillen und Geheimhaltungsinteresse es bei dem von § 203 StGB adressierten Schutz ankommt. Der Geheimnisbetroffene ist i. d. R. die Person, auf die sich die offenbarten Informationen beziehen und auch die Person, welche beispielsweise durch Erteilung einer Schweigepflichtentbindung eine Offenbarung legitimieren kann.

3.2.1 Berufsgeheimnisträger

Personen, welche zu den in § 203 Abs. 1 und 2 StGB aufgezählten Berufs- oder Personengruppen gehören, werden oftmals als „Berufsgeheimnisträger“ bezeichnet, teilweise wird der Begriff aber auch auf in § 203 Abs. 1 StGB genannten Berufs- oder Personengruppen beschränkt. Bei der Interpretation des Begriffs ist daher immer auch der Kontext zu beachten, d. h. wird nur § 203 Abs. 1 StGB von dem Begriff erfasst oder ist die umfassendere Bedeutung gemeint.

3.2.2 Offenbarung

Ein Offenbaren im Sinne des § 203 StGB ist jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten.³¹ Somit liegt eine Offenbarung immer dann vor, wenn das Geheimnis in irgendeiner Weise an einen anderen gelangt ist.³² Der Vorschrift liegt die Vorstellung zugrunde, dass nur der Geheimnisverpflichtete mit den Geheimnissen in Berührung kommen darf, denn nur der Geheimnisverpflichtete ist derjenige, den sich der Patient für die Offenbarung seines Geheimnisses ausgesucht hat.

Wenn ein Patient z. B. seinen Arzt aufsucht, geht § 203 StGB davon aus, dass lediglich dieser einen Einblick in den persönlichen Lebensbereich bekommen soll.³³

Grundvoraussetzung für eine Offenbarung ist, dass sowohl das Geheimnis selbst, als auch die Person des Geheimnisbetroffenen offenbart wird; Mitteilungen, aus denen die Person des Betroffenen nicht ersichtlich ist, erfüllen daher nicht den Tatbestand einer Offenbarung.³⁴

Weiterhin liegt ein Offenbaren nur dann vor, wenn das Geheimnis dem Empfänger noch unbekannt ist.³⁵ Für den Tatbestand einer Offenbarung ist es dabei nicht zwingend erforderlich, dass eine

³¹ So z. B.

- Cierniak/Niehaus § 203 Rn. 54. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8
- Eisele § 203 Rn. 20. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6
- Ehrmann, Outsourcing von medizinischen Daten – strafrechtlich betrachtet, 2008, S. 60
- Ulsenheimer K.: § 140, Rn. 12. In: Laufs/Kern/Rehborn (Hrsg.) Handbuch des Arztrechts. C. H. Beck Verlag, 5. Auflage 2019. ISBN 978-3-406-65614-9

³² Kargl W.: § 203 Rn. 19. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

³³ Bräutigam P. (2011) § 203 StGB und der funktionale Unternehmensbegriff - Ein Silberstreif am Horizont für konzerninternes IT-Outsourcing bei Versicherern. CR: 411-416

³⁴ So z. B.

- Cierniak/Niehaus § 203 Rn. 54. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8
- Eisele § 203 Rn. 20. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6
- Ulsenheimer K, Gaede K.: Teil 8 Die Verletzung der ärztlichen Schweigepflicht (§§ 203-205 StGB) und das Sanktionsregime der DSGVO, Rn. 1053. In Ulsenheimer/Gaede, Arztstrafrecht in der Praxis. C.F. Müller, 6. Auflage 2021. ISBN 978-3-8114-0637-7
- Weidemann M.: § 203, Rn. 33. In: Heintschel-Heinegg (Hrsg.) BeckOK StGB. C. H. Beck Verlag, 52. Edition Stand: 01.02.2022

Kenntnisnahme der geschützten Informationen durch eine unberechtigte Person erfolgt, sondern bereits eine bestehende Möglichkeit der Kenntnisnahme ist für den Tatbestand der Offenbarung ausreichend.³⁶ Bzgl. der Offenbarung wird zwischen drei verschiedenen Tatbeständen unterschieden:

- a. Mündliche Weitergabe/Mitteilung: Bei mündlichen Mitteilungen ist für den Tatbestand der Offenbarung erforderlich, dass ein Dritter das Geheimnis zur Kenntnis nimmt.³⁷
- b. Verkörpertes Geheimnis: Bei einem verkörperten Geheimnis wie beispielsweise einem Schriftstück in einer Patientenakte genügt für eine Offenbarung bereits die Möglichkeit, dass sich ein Dritter von dem Geheimnis Kenntnis verschaffen könnte.³⁸ Eine nachgewiesene Kenntnisnahme durch einen Unbefugten ist nicht erforderlich.³⁸ Insbesondere ist auch ein Offenbaren durch (aktives) Unterlassen möglich³⁹, z. B. wenn ein Arzt die Einsichtnahme in eine Patienten-/Krankenakte oder gar deren Mitnahme nicht verhindert.
- c. Digital gespeicherte Geheimnisse: Die Offenbarung digital gespeicherter Geheimnisse wird der Offenbarung von verkörperten Geheimnissen gleichgestellt.⁴⁰ So erfüllt bereits die Einräumung der Verfügungsgewalt über die Daten, z. B. durch die Weitergabe der Datei oder auch durch die Zugriffsmöglichkeit auf die Daten in einem Informationssystem, den Tatbestand der Offenbarung. Dementsprechend erfüllt auch bei digital gespeicherten Geheimnissen bereits die Möglichkeit der Kenntnisnahme den Tatbestand einer Offenbarung durch Unterlassen.

So reicht beispielsweise schon die Übermittlung der geschützten Daten durch den Berufsgeheimnisträger an einen Cloudanbieter aus, dass eine Offenbarung gegenüber dessen Mitarbeitern erfolgt.⁴¹ Nur wenn diese keine Möglichkeit zur Kenntnisnahme haben (z. B. durch Einsatz sicherer kryptografischer Methoden⁴²) erfolgt keine Offenbarung.⁴³

³⁵ So z. B.

- Cierniak/Niehaus § 203 Rn. 54. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8
- Eisele § 203 Rn. 21. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6
- Lenckner/Eisele § 203 Rn. 19a in Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 29. Auflage 2014. ISBN 978-3-406-65226-4

³⁶ So z. B.

- Dahns C. (2017) Rechtssicherheit beim Outsourcing von Dienstleistungen. NJW-Spezial: 766-767
- Eisele § 203 Rn. 20. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6
- Hackenberg: Teil 15.2 Big Data und Datenschutz, Rn. 47. In: Hoeren / Sieber / Holznagel (Hrsg.) Handbuch Multimedia-Recht. C. H. Beck Verlag, 57. Auflage 2022. ISBN 978-3-406-43668-0
- Hartung: Teil 11.4.2 Datenschutz und Geheimnisschutz, Rn. 117. In Leupold/Wiebe/Glossner (Hrsg.) Münchener Anwaltshandbuch IT-Recht. C. H. Beck Verlag, 4. Auflage 2021. ISBN 978-3-406-74458-7
- Hoeren T. (2018) Betriebsgeheimnisse im digitalen Zeitalter. Die Neuordnung von StGB und StPO. MMR: 12-18
- Kargl § 203 Rn. 19a. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

³⁷ So z. B. Eisele § 203 Rn. 20. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6

³⁸ So z. B. Kargl W.: § 203 Rn. 20. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

³⁹ So z. B. Kargl W.: § 203 Rn. 19a. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

⁴⁰ So z. B. Kargl W.: § 203 Rn. 21. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

⁴¹ So z. B.

Zu beachten sind im Rahmen des Tatbestands der Offenbarung die unterschiedlichen Regelungen in § 203 StGB bzgl. den die Berufsgeheimnisträger unterstützenden Personen:

- a. Werden Geheimnisse den bei Berufsgeheimnisträgern berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich gemacht, so liegt entsprechend § 203 Abs. 3 S. 1 StGB **kein** Offenbaren vor.
- b. Werden Geheimnisse hingegen sonstigen Personen, welche an der beruflichen oder dienstlichen Tätigkeit eines Berufsgeheimnisträgers mitwirken, zugänglich gemacht, so handelt es sich entsprechend § 203 Abs. 3 S. 2 StGB hingegen um ein Offenbaren, jedoch ein erlaubtes, also befugtes Offenbaren.

Diese Unterscheidung zwischen internem Personal, wie beispielsweise einer medizinischen Fachangestellten in einer niedergelassenen Arztpraxis, bei welcher kein Offenbaren vorliegt, und externem Personal, wie beispielsweise den Beschäftigten der die Praxisverwaltungssoftware betreuenden Firma, könnte strafrechtlich bei Irrtumsfragen Bedeutung erlangen. Dieses im Beispiel dargestellte Szenario gilt für alle Leistungserbringer, die von § 203 StGB erfasst werden, gleichermaßen.

Zu beachten ist weiterhin, dass eine analoge Anwendung des Rechtfertigungsgrundes des § 193 StGB („Wahrnehmung berechtigter Interessen“) auf § 203 StGB nicht anwendbar ist, d. h. der durch § 203 StGB gewährleistete Schutz von Privatgeheimnissen nicht contra legem relativiert werden kann.⁴⁴

3.3 Leistungserbringer

Der Begriff „Leistungserbringer“ ist in den Sozialgesetzbüchern nicht definiert. Allgemein werden unter „Leistungserbringer“ alle diejenigen Gruppierungen verstanden, die Leistungen für die Versicherten der Krankenkassen erbringen.

Leistungserbringer werden im SGB V insbesondere in nachfolgenden Regelungen angesprochen:

- §§ 72ff. SGB V (Vertragsärzte)

-
- Cierniak/Niehaus § 203 Rn. 60. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8
 - Pohle J, Ghaffari S. (2017) Die Neufassung des § 203 StGB – der Befreiungsschlag für IT-Outsourcing am Beispiel der Versicherungswirtschaft?! CR: 489-495

Aber auch die Bundesregierung führte aus, dass die Möglichkeit der Kenntnisnahme von geschützten Geheimnissen“ ausreicht (Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“. Drucksache 18/11936 vom 12.04.2017. Online, zitiert am 2024-08-24; verfügbar unter <https://dserver.bundestag.de/btd/18/119/1811936.pdf>)

⁴² So z. B.

- Heger M.: § 203 StGB, Rn. 25a. In: Lackner/Kühl (Hsrg.) Strafgesetzbuch: StGB. C. H. Beck Verlag, 29. Auflage 2018. ISBN 978-3-406-70029-3
- Grosskopf L, Momsen C. (2018) Outsourcing bei Berufsgeheimnisträgern – strafrechtliche Verpflichtung zur Compliance? CCZ: 98-108
- Holtorf ML (2013) Cloud Computing – Ein Überblick (Teil 2). MPR: 196-198

⁴³ So z. B.

- Hartung J.: Teil 11.4.2 Datenschutz und Geheimnisschutz, Rn. 120. In: Leupold / Wiebe / Glossner (Hsrg.) IT-Recht. C. H. Beck Verlag, 4. Auflage 2021. ISBN 978-3-406-74458-7
- Eisele § 203 Rn. 20. In Schönke / Schröder (Hsrg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6

⁴⁴ Neumann U: Probleme der Rechtfertigung bei der Offenbarung von ärztlichen Geheimnissen (§ 203 Abs. 1 Nr. 1 StGB). In: Engelhart/Kudlich/Vogel (Hsrg.) Digitalisierung, Globalisierung und Risikoprävention - Festschrift für Ulrich Sieber zum 70. Geburtstag. Duncker & Humblot Verlag, 2021. ISBN 978-3-428-15971-0. <https://doi.org/10.3790/978-3-428-55971-8>

- §§ 107ff. SGB V (Krankenhäuser)
- §§ 124ff. SGB V (Heilmittelerbringer)
- §§ 126 ff. SGB V (Hilfsmittelerbringer)
- §§ 129ff. SGB V (Apotheken und pharmazeutische Unternehmer)
- §§ 132ff. SGB V (sonstige Leistungserbringer).

Im allgemeinen Sprachgebrauch wird „Leistungserbringer“ sehr häufig mit „Ärzten“ gleichgesetzt, sei es im niedergelassenen oder im stationären Bereich. Leistungserbringer werden im Sozialgesetzbuch jedoch überwiegend über ihre Beziehung zu den Pflege- und Krankenkassen definiert. Entsprechend den Vorgaben des SGB V gehören viel mehr Personengruppen zu den Leistungserbringern. Nach dem Vierten Kapitel des SGB V sind zur Versorgung berechtigt:⁴⁵

- Viertes Kapitel Zweiter Abschnitt Siebter Titel: §§ 95ff SGB V, dies sind
 - o Zugelassene Ärzte, Zahnärzte, Psychotherapeuten
 - o Medizinische Versorgungszentren sowie
 - o Ermächtigte Ärzte, Zahnärzte, Psychotherapeuten und Einrichtungen;
- Viertes Kapitel Dritter Abschnitt; §§ 107 ff. SGB V, dies sind
 - o Krankenhäuser,
 - o Vorsorge- und Rehaeinrichtungen,
 - o Einrichtungen des Müttergenesungswerks oder gleichartige Einrichtungen;
- Viertes Kapitel Fünfter Abschnitt: §§ 124 ff. SGB V, d. h.
 - o Leistungserbringer von Heilmitteln (beispielhafte Darstellung siehe Anhang 1.1);
- Viertes Kapitel Sechster Abschnitt: §§ 126 SGB ff. V, d. h.
 - o Leistungserbringer von Hilfsmitteln (beispielhafte Darstellung siehe Anhang 1.2);
- Viertes Kapitel Siebter Abschnitt: §§ 129 ff. SGB V
 - o Apotheken,
 - o Krankenhausapotheken,
 - o Pharmazeutische Unternehmer⁴⁶;
- Viertes Kapitel Achter Abschnitt: §§ 132 ff. SGB V
 - o Sonstige Leistungserbringer, d. h. Erbringer von
 - Haushaltshilfe,
 - häuslicher Krankenpflege,
 - Soziotherapie,
 - sozialmedizinischen Nachsorgemaßnahmen,
 - spezialisierter ambulanter Palliativversorgung,
 - Schutzimpfungen,
 - Betriebsärzte,
 - Krankentransportleistungen und
 - Hebammenhilfe.

⁴⁵ Baumann C, Matthäus D.: § 140a SGB V, Rn. 83. In: Schlegel/Voelzke (Hrsg.) juris PraxisKommentar SGB V. Juris, 8. Auflage 2022. ISBN 978-3-86330-257-3

⁴⁶ Pharmazeutische Unternehmen sind Leistungserbringer im Sinne des SGB V, weil der 7. Abschnitt des Vierten Kapitels ihre Beziehungen zu den Apotheken regelt. So z. B. zu finden in:

- Sodan H. „Handbuch des Krankenversicherungsrechts“: § 13 Leistungserbringung durch Dritte als Folge des Sachleistungsprinzips, Rn. 37, 38. Verlag C. H. Beck, 3. Auflage 2018. ISBN 978-3-406-71288-3
- Zuck R.: § 36 Pharmazeutische Unternehmen, Rn. 2. In: Quaas/Zuck Clemens (Hrsg.) Medizinrecht. Verlag C. H. Beck, 4. Auflage 2018. ISBN 978-3-406-70773-5
- Krauskopf „Soziale Krankenversicherung, Pflegeversicherung“: § 128 SGB V, Rn. 26, 27. Verlag C. H. Beck, 121. Auflage 2024. ISBN 978-3-406-45832-3

Leistungserbringer i. S. d. § 393 SGB V sind daher diese zur Versorgung von gesetzlich versicherten Menschen berechtigten Einrichtungen bzw. Personengruppen.

3.4 Dienstleister, Anbieter, Lieferant, Hersteller

Anbietern (i. S. v. Lieferanten, bei denen Online-Terminmanagementsystem gekauft oder gemietet werden können) und Herstellern von Online-Terminmanagementsystemen kommen unterschiedliche Aufgaben zu, die Begrifflichkeiten können daher nicht beliebig ausgetauscht werden. Z. B. produziert/programmiert ein Hersteller Software und kann diese anpassen – was ein Anbieter nicht kann. Ein Anbieter wiederum schließt Verträge mit Auftraggebern, welche die Software einsetzen (wollen), ab und ist somit vertraglicher Ansprechpartner, welcher die vertraglich zugesicherten Verpflichtungen gewährleisten muss.

In vielen, aber nicht allen Fällen, sind Hersteller und Anbieter ein und dieselbe Person. Um diese Praxishilfe lesbarer zu gestalten, verwenden wir im Text überall den Begriff „Dienstleister“ als synonym für „Hersteller“ bzw. „Anbieter“; an welcher Stelle im Text welche Zuordnung erfolgen muss, wird i. d. R. durch den Kontext offenbar und die Zuordnung dürfte den Lesern dieser Praxishilfe leichtfallen.

Nachfolgend die Begriffsbestimmungen zu „Hersteller“ und „Anbieter“, wie sie innerhalb dieser Praxishilfe verwendet werden. Bei der Begriffsbestimmung wurde sich soweit wie möglich am europäischen Recht orientiert.

3.4.1 Hersteller

Art. 2 Ziff. 3 Verordnung (EG) Nr. 765/2008⁴⁷ versteht unter einem Hersteller „jede natürliche oder juristische Person, die ein Produkt herstellt bzw. entwickeln oder herstellen lässt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet.“

3.4.2 Anbieter/Lieferant

Analog zu Art. 2 Nr. 26 Verordnung (EG) Nr. 1272/2008⁴⁸ wird im Kontext dieser Praxishilfe unter einem Anbieter bzw. einem Lieferanten eine natürliche oder juristische Person verstanden, welche ein Produkt in Verkehr bringt. Dies schließt Hersteller mit ein, wenn diese die Aufgaben eines Anbieters/Lieferanten übernehmen.

3.5 Patientendaten

Der Begriff „Patientendaten“ wird im europäischen Recht nicht legal definiert und auch im Sozialrecht findet sich keine entsprechende Begriffsbestimmung. Umgangssprachlich werden als Patientendaten alle personenbezogenen Daten eines Patienten bezeichnet, die von einer Kranken- oder Pflegekasse bzw. einem Leistungserbringer verarbeitet werden.

⁴⁷ Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011. Online, zitiert am 2024-10-19; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32019R1020>

⁴⁸ Verordnung (EG) Nr. 1272/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über die Einstufung, Kennzeichnung und Verpackung von Stoffen und Gemischen, zur Änderung und Aufhebung der Richtlinien 67/548/EWG und 1999/45/EG und zur Änderung der Verordnung (EG) Nr. 1907/2006. Online, zitiert am 2024-10-19; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32008R1272&qid=172932877796>

In einigen Landeskrankenhausgesetzen finden sich allerdings Legaldefinitionen. Diese legen den Begriff „Patientendaten“ teilweise weit aus und beziehen in einigen Fällen auch Daten von Angehörigen oder sonstige Personen mit ein. Diese landesspezifischen Regelungen müssen im Anwendungsbereich des jeweiligen Gesetzes beachtet werden:

- § 43 Abs. 4 Landeskrankenhausgesetz Baden-Württemberg:
(<https://www.landesrecht-bw.de/bsbw/document/jlr-KHGBW2008V8P43>)
„Patientendaten sind einen Patienten, seine Angehörigen, Begleit- oder sonstige Bezugspersonen betreffende personenbezogene Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679, die im Krankenhaus im Zusammenhang mit der stationären Versorgung oder mit einer solchen ambulanten Behandlung des Patienten bekannt werden, die das Krankenhaus im Rahmen einer Institutsambulanz oder einer institutionellen Ermächtigung erbringt.“
- Art. 27 Abs. 1 Bayerisches Krankenhausgesetz
(<https://www.gesetze-bayern.de/Content/Document/BayKrG-27>)
„Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser.“
- § 27 Abs. 2 Brandenburgisches Krankenhausentwicklungsgesetz
(<https://bravors.brandenburg.de/gesetze/bbgkheg#27>)
„Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse
 1. bestimmter oder bestimmbarer Patientinnen oder Patienten aus dem Bereich der Krankenhäuser,
 2. von deren Angehörigen und anderen Bezugspersonen und
 3. sonstiger Dritter,die dem Krankenhaus im Zusammenhang mit einer stationären, teilstationären oder ambulanten Behandlung bekannt werden.“
- § 37 Abs. 1 Bremisches Krankenhausgesetz
(https://www.transparenz.bremen.de/metainformationen/bremisches-krankenhausgesetz-bremkrhg-vom-24-november-2020-159875?template=20_gp_ifg_meta_detail_d#jlr-KHGBR2020pP37)
„Patientendaten sind alle personenbezogenen Daten der Patientinnen und Patienten des Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von verstorbenen Patientinnen und Patienten, Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung des Patienten oder der Patientin bekannt werden. Patientendaten in diesem Sinne sind auch Daten, die im Zusammenhang mit einer ambulanten Behandlung stehen, die das Krankenhaus im Rahmen einer Ambulanz oder einer institutionellen Ermächtigung erbringt.“
- § 7 Abs. 1 S. 2 Hamburgisches Krankenhausgesetz
(<https://www.landesrecht-hamburg.de/bsha/document/jlr-KHGHAV7P7>)
„Zu den Patientendaten gehören auch die personenbezogenen Daten von Angehörigen einer Patientin oder eines Patienten oder von sonstigen Dritten, wenn die Daten dem Krankenhaus im Zusammenhang mit der Behandlung der Patientin oder des Patienten bekannt werden.“
- § 2 Abs. 1 Gesundheitsdatenschutzgesetz Nordrhein-Westfalen
(https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=1&bes_id=4283&anw_nr=2&aufgehoben=N&det_id=357746)
„Dieses Gesetz gilt für die Verarbeitung der personenbezogenen Daten

1. von Personen, die, auch aufgrund eines gesonderten ärztlichen Behandlungsvertrages, in einem zugelassenen Krankenhaus im Sinne von § 107 Abs. 1, § 108 und in einer Vorsorge- und Rehabilitationseinrichtung gemäß § 107 Abs. 2, § 111 des Sozialgesetzbuches, Fünftes Buch - Gesetzliche Krankenversicherung - (SGB V) vom 20. Dezember 1988 (BGBl. I S. 2477) in der jeweils geltenden Fassung, deren Träger nicht der Bund oder eine bundesunmittelbare Körperschaft gemäß Artikel 87 Abs. 2 des Grundgesetzes ist, (Einrichtung) ambulant oder stationär untersucht oder behandelt werden,
2. von Personen, für die Maßnahmen aufgrund des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG) vom 17. Dezember 1999 (GV. NW. S. 662) in der jeweils geltenden Fassung getroffen werden,
3. von Personen, die vom Gesundheitsamt untersucht oder von dessen Maßnahmen betroffen werden.

(Patientendaten). Den Patientendaten sind gleichgestellt personenbezogene Daten Dritter, die bei Tätigkeiten nach Satz 1 den dort genannten Stellen bekannt werden.“

- § 36 Abs. 1 S. 4 Landeskrankenhausgesetz Rheinland-Pfalz
<https://landesrecht.rlp.de/bsrp/document/jlr-KHGRP12P36>
 „Patientendaten im Sinne der folgenden Bestimmungen sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekanntwerden.“
- § 13 Abs. 1 Saarländisches Krankenhausgesetz
<https://recht.saarland.de/bssl/document/jlr-KHGSL2015V10P13>
 „Alle Daten von Patientinnen und Patienten (Patientendaten) im Krankenhaus unterliegen unabhängig von der Art ihrer Verarbeitung dem Datenschutz. Patientendaten sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patientin oder des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.“
- § 28 Abs. 2 Sächsisches Krankenhausgesetz
<https://www.revosax.sachsen.de/vorschrift/19826#p28>
 „Patientendaten sind personenbezogene Daten von Patientinnen und Patienten, deren Angehörigen und anderen Bezugspersonen sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.“
- § 16 Abs. 1 Krankenhausgesetz Sachsen-Anhalt
<https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-KHGST2005V9P16>
 „Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse
 1. bestimmter oder bestimmbarer Patienten aus dem Bereich des Krankenhauses sowie
 2. der Angehörigen des Patienten, anderer Bezugspersonen und sonstiger Dritter (Betroffene),
 die im Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden.“
- § 35 Abs. 2 Krankenhausgesetz für das Land Schleswig-Holstein
<https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-KHGSHpP35>
 „Patientendaten im Sinne dieses Gesetzes sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter und bestimmbarer Patientinnen und Patienten eines Krankenhauses. Als Patientendaten gelten auch personenbezogene Daten von Angehörigen

oder anderen Bezugspersonen der Patientinnen und Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit einer Behandlung bekannt werden.“

- § 27 Abs. 2 S. 2 Thüringer Krankenhausgesetz

(<https://landesrecht.thueringen.de/bsth/document/jlr-KHGTH2003V3P27>)

„Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer Patienten aus dem Bereich der Krankenhäuser. Patientendaten sind auch personenbezogene Daten von Angehörigen oder anderen Bezugspersonen der Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden.“

3.6 Personenbezogene Daten

Nach Art. 4 Ziff. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Die Begriffe „identifiziert“ und „identifizierbar“ werden dabei als gleichberechtigte Alternativen verwendet. Erfasst werden also nicht nur Informationen, welche eine Person direkt identifizieren, sondern auch alle Informationen, welche eine Person über Zwischenschritte identifizieren („identifizierbar machen“). Eine Identifizierung einer natürlichen Person liegt demnach bereits dann vor, wenn diese Person hinreichend individualisiert werden kann, weil sie sich aufgrund der vorhandenen Informationen ausreichend von anderen Personen in der vorhandenen Datenmenge hinreichend unterschieden werden kann⁴⁹. D. h. soweit und solange die Informationen aus sich heraus einen Rückschluss auf eine einzelne Person zulassen, handelt es sich um Daten einer bestimmten Person⁵⁰. (Beispiel: Bundeskanzlerin der BRD = Dr. Angela Merkel – schließlich gab es bisher nur eine Bundeskanzlerin.) Gleiches gilt, wenn weitere Informationen existieren, welche in Verbindung mit den vorhandenen Daten indirekt einen Rückschluss auf eine einzelne Person zulassen und diese somit als bestimmbar anzusehen ist. Da ErwGr. 26 DS-GVO auf die Mittel abstellt, die „nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person verwendet werden“, sind Mittel zu berücksichtigen, die von dem für die Verarbeitung Verantwortlichen oder auch von beliebigen „Dritten“ zur Identifizierung genutzt werden könnten. Für die Einstufung eines Datums als „personenbezogenes Datum“ ist es somit nicht erforderlich, dass sich alle zur Identifizierung der betreffenden (datenschutzrechtlich: „betroffenen“) Person erforderlichen Informationen in den Händen einer einzigen natürlichen oder juristischen Person befinden, sondern es muss auch das Wissen Dritter zu berücksichtigen.⁵¹

Der Begriff „identifizierbar“ ist somit im Sinne von „als Einzelperson wahrnehmbar“ oder einer „Einzelperson zuordenbar“ zu verstehen, wobei bei der Beurteilung auch evtl. vorhandenes

⁴⁹ Bzgl. indirekter Identifizierbarkeit siehe auch:

- EuGH, Urt. v. 19. Oktober 2016, Az. C-582/14, Rn. 41: „[...] dass es für die Einstufung einer Information als personenbezogenes Datum nicht erforderlich ist, dass die Information für sich genommen die Identifizierung der betreffenden Person ermöglicht.“ Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2016,33959> bzw. Urteil unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62014CJ0582>
- BGH, Urt. v. 16. Mai 2017, Az. VI ZR 135/13, Rn. 28: „[...] dass es für die Einstufung einer Information als personenbezogenes Datum nicht erforderlich sei, dass die Information für sich genommen die Identifizierung der betreffenden Person ermögliche.“ Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2017,15139> bzw. Volltext Urteil unter <https://openjur.de/u/2117724.html>

⁵⁰ Karg M. (2015) Anonymität, Pseudonyme und Personenbezug revisited. DuD: 520-526

⁵¹ EuGH, Urt. v. 19. Oktober 2016, Az. C-582/14, Rn. 43. Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2016,33959> bzw. Urteil unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62014CJ0582>

Zusatzwissen, über welches der Verantwortliche selbst oder ein beliebiger Dritter verfügt, berücksichtigt werden muss. Der Verantwortlichen muss berücksichtigen, dass es „Dritte“ gibt, welche über die notwendigen Kenntnisse und Mittel verfügen, um die betroffene Person zu identifizieren.⁵²

Die Möglichkeit der Identifizierbarkeit stellt folglich den entscheidenden Faktor bei der Beurteilung dar, ob Daten als anonym oder pseudonym zu bewerten sind.

In Bezug auf die in Art. 9 Abs. 1 DS-GVO benannten besonders sensiblen Daten ist dabei zu beachten, dass entsprechend der Rechtsprechung des EuGH die Zuordnung eines Datums als „sensibles Datum“ weit zu verstehen ist⁵³: Dies bedeutet, dass auch wenn ein Datum aufgrund der eigenen Bedeutung nach kein sensibles Datum darstellen würde, so ist zu prüfen, ob Daten, aus denen „mittels gedanklicher Kombination oder Ableitung“ auf in Art. 9 Abs. 1 DS-GVO genannte Datenkategorien geschlossen werden kann, und folglich als sensible Daten i. S. d. Art. 9 Abs. 1 DS-GVO anzusehen sind. Ist entsprechend dieser Vorgaben ein Datum als „personenbezogen oder personenbeziehbar“ zu klassifizieren, so muss bei der Prüfung, ob es sich um ein sensibles Datum i. S. d. Art. 9 Abs. 1 DS-GVO handelt, entsprechend vorgegangen werden. Auch indirekt mögliche Aussagen sind dabei prüfen.

Beispiel: Eine Person besucht eine Arztpraxis. Die Standortdaten, also Straße, Postleitzahl und Ort, der Arztpraxis werden üblicherweise nicht als sensible Daten i. S. v. Art. 9 Abs. 1 DS-GVO betrachtet. Da jedoch bekannt ist, dass eine Arztpraxis aufgesucht wird und dies i. d. R. für eine medizinische Betreuung erfolgt, ist diese Information als sensibles Datum aufzufassen.

Weiterhin urteilte der EuGH, dass ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, insgesamt als sensibles Datum i. S. v. Art. 9 Abs. 1 DS-GVO anzusehen ist.⁵⁴

3.6.1 Pseudonyme Daten⁵⁵

Der Begriff der Pseudonymisierung wird in Art. 4 Ziff. 5 DS-GVO definiert. Dort heißt es:

„Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Dieser Definition folgend charakterisiert eine Pseudonymisierung daher Nachfolgendes:

- Das Pseudonymisieren ist eine Verarbeitung personenbezogener Daten.
- Pseudonyme Daten sind Daten, die ohne weitere Informationen einer spezifischen Person nicht zuordenbar sind.

⁵² Schlussanträge des Generalanwalts M. Campos Sánchez-Bordona vom 12. Mai 2016, Rn. 64-68. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62014CC0582>

⁵³ EuGH, Urt. v. 2022-08-01, Az. C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2010,236> bzw. Volltext abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184>

⁵⁴ EuGH, Urt. v. 2023-07-04, Az. C-252/21, Rn. 89 sowie Leitsatz 2. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

⁵⁵ Weitergehende Informationen zum Thema „Pseudonymisierung“ findet man beispielsweise in der „Praxishilfe zur Pseudonymisierung/Anonymisierung“. Online, zitiert am 2024-09-09; verfügbar unter https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

- Die zur Zuordenbarkeit benötigten Informationen stehen keiner der an der Verarbeitung beteiligten natürlichen oder juristischen Personen zur Verfügung, sondern
 - werden gesondert aufbewahrt **und**
 - sind durch technische und organisatorische Maßnahmen vor jeglichem Zugriff durch die an der Verarbeitung beteiligten natürlichen oder juristischen Personen geschützt.
- Weder für den Verantwortlichen noch für einen Auftragsverarbeiter besteht bei der Verarbeitung von pseudonymisierten Daten eine Möglichkeit der Identifizierung der betroffenen Person, ansonsten handelt es sich nicht um pseudonymisierte Daten.

Hinweis: Gemäß ErwGr. 26 DS-GVO sind bei der Entscheidung, ob eine natürliche Person identifizierbar ist, alle Mittel zu berücksichtigen sind, die der Verantwortliche oder eine andere Person nach allgemeinem Ermessen wahrscheinlich einsetzen könnten, um die natürliche Person direkt oder indirekt zu bestimmen.

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden können, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Entsprechend der in der DS-GVO enthaltenen Definition von Pseudonymisierung sind – in Anlehnung an ErwGr. 26 S. 2 DS-GVO – pseudonyme Daten demnach solche Daten, welche in einem Verarbeitungszusammenhang einer spezifischen Person nicht zuzuordnen sind, jedoch durch die Einbeziehung weitergehender Informationen („Zuordnungsregeln“) die grundsätzliche Möglichkeit der Zuordnung besteht. Eine Re-Identifizierung der betroffenen Person durch Zuordnung zu ihrem bürgerlichen Namen ist hierfür nicht erforderlich.⁵⁰ Es reicht aus, wenn das Datum bzw. die Daten eine Individualisierung der betroffenen Person ermöglichen und Aussagen über deren sachliche und persönliche Verhältnisse ermöglichen; ein Name ist zur Einordnung als identifizierbare Person nicht erforderlich.⁵⁶

Maßstab für die Beurteilung, ob pseudonyme Daten vorliegen oder nicht, bilden die Anforderungen in Art. 4 Ziff. 5 DS-GVO i. V. m. ErwGr. 26 DS-GVO. Zu beachten ist, dass nach ErwGr. 28 S. 2 DS-GVO durch „die ausdrückliche Einführung der ‘Pseudonymisierung‘ in dieser Verordnung nicht beabsichtigt ist, andere Datenschutzmaßnahmen auszuschließen“. Pseudonymisierung ist folglich nur eine Schutzmaßnahme; sodass sämtliche Vorgaben der DS-GVO uneingeschränkt auch für pseudonyme Daten gewährleistet werden müssen.

3.6.2 Anonyme Daten⁵⁷

Anonymisierung wird in Art. 2 Ziff. 7 der Richtlinie (EU) 2019/1024⁵⁸ wie folgt definiert:

⁵⁶ Artikel-29-Datenschutzgruppe. WP 136 „Stellungnahme 4/2007 zum Begriff ‘personenbezogene Daten‘“, S. 16: [...] ein Name zur Identifizierung einer Person jedoch keineswegs immer notwendig ist“. Online, zitiert am 2024-08-24; verfügbar unter http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

⁵⁷ Weitergehende Informationen zum Thema „Anonymisierung“ findet man beispielsweise in der „Praxishilfe zur Pseudonymisierung/Anonymisierung“. Online, zitiert am 2024-09-09; verfügbar unter https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

⁵⁸ Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019L1024&qid=1697259421370>

„Anonymisierung“ den Prozess, in dessen Verlauf Dokumente in anonyme Dokumente umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten so anonym gemacht werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Diese Begriffsbestimmung entspricht der Definition der internationalen Norm ISO/IEC 29100⁵⁹:

„anonymity: characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly“.

Ins Deutsche übersetzt „Anonymität: Merkmale von Informationen, die eine direkte oder indirekte Identifizierung des Betroffenen nicht zulassen“.

Während die europäische Richtlinie den Prozess der Anonymisierung behandelt, definiert die internationale Norm ISO/IEC 29100 den Begriff der Anonymität; das eine ist das Ergebnis des anderen.

Europäische Richtlinien müssen durch nationale Rechtsakte umgesetzt werden.⁶⁰ Im Falle der Begriffsdefinition zur Anonymisierung erfolgte dies durch § 3 Ziff. 12 Datennutzungsgesetz:

„Anonymisierung“ ist der Prozess, in dessen Verlauf personenbezogene Daten in Daten umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder derart in Daten umgewandelt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Entsprechend ErwGr. 52 der Richtlinie (EU) 2019/1024 sind anonyme Informationen solche Informationen, welche

„sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, bzw. Informationen, die sich auf personenbezogene Daten beziehen, die so anonymisiert wurden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“

Daraus ergibt sich im Umkehrschluss, dass anonyme Daten weder direkt identifizierbare personenbezogene noch pseudonymisierte Daten i. S. d. DS-GVO sein können. D. h., anonyme Daten sind Daten, bei denen während des gesamten Lebenszyklus der Daten keine Zuordnungsmöglichkeit zu einer spezifischen betroffenen Person existiert⁶¹.

Am 26. April 2023 urteilte das EuG⁶², dass bei der Beurteilung der Frage, ob es sich bei an einen Dritten übermittelte Daten um personenbezogene Daten handelt oder nicht, auf das Verständnis abzustellen ist, das dieser Dritte bei der Bestimmung der Frage hat, ob die ihm übermittelten Informationen sich auf „identifizierbare Personen“ beziehen. Wenn nur der Absender, nicht jedoch

⁵⁹ ISO/IEC 29100:2011: „Information technology - Security techniques - Privacy framework. Online, zitiert am 2023-11-22; verfügbar unter <https://www.iso.org/standard/45123.html> bzw. download pdf-Datei kostenlos unter <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>

Deutsche Übersetzung der Norm von 2011 wurde 2020 vom Beuth-Verlag veröffentlicht: <https://www.beuth.de/de/norm/din-en-iso-iec-29100/325198919>

⁶⁰ Deutscher Bundestag, Wissenschaftliche Dienste: Kurzinformation – Umsetzung von EU-Richtlinien und Verfassungsrecht. Online, zitiert am 2024-08-24; verfügbar unter <https://www.bundestag.de/resource/blob/899872/33b2422d86eab34c741b67207ab1bda3/WD-3-045-22-pdf-data.pdf>

⁶¹ Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR) - A Practical Guide. Springer Verlag, 2017. ISBN 978-3-319-57958-0. PP 13-16, chapter „2.1.2.2 Anonymisation and Pseudonymisation“: „Anonymised data is either information that does not relate to an identified or identifiable individual or personal data that was rendered anonymous in such a manner that the person is not or no longer identifiable.“

⁶² EuG: Urt. v. 2023-04-26, AZ. T-557/20. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62020TJ0557>

der Empfänger eine Re-Identifizierung durchführen kann, seien diese Daten anonym. Gegen diese Entscheidung legte der Europäischen Datenschutzbeauftragte Rechtsmittel ein⁶³, das Verfahren ist zum Zeitpunkt der Erstellung dieser Praxishilfe beim EuGH noch anhängig.

3.7 Sozialdaten

Sozialdaten sind nicht durch europäisches Recht, sondern durch deutsches Recht definiert. Die Begriffsbestimmung findet sich in § 67 Abs. 2 SGB X:

„Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.“

Der Begriff Sozialdaten kann somit alle Formen personenbezogener Daten einbeziehen, einschließlich pseudonymer Daten (Art. 4 Nr. 5 DS-GVO), genetischer Daten (Art. 4 Nr. 13 DS-GVO), biometrischer Daten (Art. 4 Nr. 14 DS-GVO) und Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO).

Damit ein personenbezogenes Datum als Sozialdatum gilt, muss eine einzige Bedingung erfüllt werden: Die Verarbeitung muss von einer in § 35 SGB I genannten Stelle „im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch“ durchgeführt werden.

§ 35 SGB I benennt ausschließlich „Leistungsträger“. Die zum Sozialdatenschutz verpflichteten Leistungsträger ergeben sich aus § 12 i. V. m. §§ 18-29 SGB I, d. h. es handelt sich ausschließlich um die in den §§ 18-29 SGB I genannten Körperschaften, Anstalten und Behörden. Dies sind:

- Ämter und die Landesämter für Ausbildungsförderung (§ 18 SGB I);
- Agenturen für Arbeit und die sonstigen Dienststellen der Bundesagentur für Arbeit (§§ 19, 19a, 19b SGB I);
- Gesetzliche Krankenversicherung, d. h. Orts-, Betriebs- und Innungskrankenkassen, die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau als landwirtschaftliche Krankenkasse, die Deutsche Rentenversicherung Knappschaft-Bahn-See und die Ersatzkassen (§ 21, 21b SGB I);
- Pflegekassen (§ 21a SGB I);
- Gesetzliche Unfallversicherung, d. h. die gewerblichen Berufsgenossenschaften, die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau als landwirtschaftliche Berufsgenossenschaft, die Gemeindeunfallversicherungsverbände, die Feuerwehr-Unfallkassen, die Unfallkassen der Länder und Gemeinden, die gemeinsamen Unfallkassen für den Landes- und kommunalen Bereich und die Unfallversicherung Bund und Bahn (§ 22 SGB I);
- Gesetzliche Rentenversicherung (§ 23 SGB I);
- Die nach Bundesrecht oder Landesrecht bestimmten Träger der sozialen Entschädigung (§ 24 SGB I);
- Die nach § 7 des Bundeskindergeldgesetzes bestimmten Stellen sowie die für Bundeselterngeld- und Elternzeitgesetzes bestimmten Stellen (§ 25 SGB I);
- Die durch Landesrecht bestimmten für das Wohngeld zuständigen Behörden (§ 26 SGB I);
- Die für die Leistungen der Kinder- und Jugendhilfe zuständigen Kreise und die kreisfreien Städte, nach Maßgabe des Landesrechts auch kreisangehörige Gemeinden (§ 27 SGB I);

⁶³ EuGH: Rechtssache C-413/23 P. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62023CN0413&qid=1697259421370>

- Die für die Leistungen der Sozialhilfe zuständigen Kreise und kreisfreien Städte, die überörtlichen Träger der Sozialhilfe und für besondere Aufgaben die Gesundheitsämter (§ 28 SGB I);
- Die durch Landesrecht bestimmten für die Leistungen der Eingliederungshilfe zuständigen Behörden (§ 28a SGB I);
- Die für die Leistungen zur Rehabilitation und Teilhabe behinderter Menschen zuständigen und in den §§ 19 bis 24, 27 und 28g SGB I genannten Leistungsträger und die Integrationsämter (§ 29 SGB I).

Entsprechend § 35 Abs. 2 SGB I regeln die Vorschriften des 2. Kapitels des SGB X und der übrigen Bücher des Sozialgesetzbuches die Verarbeitung von Sozialdaten abschließend, soweit die DS-GVO als vorrangig geltendes Gesetz nicht unmittelbar anzuwenden ist. Daher können die in § 35 SGB I genannten Stellen personenbezogene Daten auch mit Einwilligung nur verarbeiten, wenn ihnen dies durch eine (ausdrückliche) Regelung des Sozialgesetzbuches erlaubt ist.

Leistungserbringer wie Krankenhäuser, niedergelassene Arztpraxen, Apotheken, häusliche Pflegedienste usw. verarbeiten daher **nie** Sozialdaten, da sie zu keiner der in § 35 SGB I genannten Stellen gehören. Erhält ein Leistungserbringer Daten von einem Leistungsträger, so sind die Daten nach Erhalt keine Sozialdaten mehr: Ab Erhalt der Daten verarbeitet ein Leistungserbringer die Daten und entsprechend der gesetzlichen Begriffsbestimmung können die Daten nicht mehr als Sozialdaten gelten, sobald sie unter der Verfügungsgewalt eines Leistungserbringers stehen und somit von diesem und nicht von einem Leistungsträger verarbeitet werden.

4 Rechtliche Rahmenbedingungen

4.1 Datenschutzrechtliche Anforderungen

4.1.1 Einhaltung der „Grundsätze für die Verarbeitung personenbezogener Daten“

Art. 5 Abs. 1 DS-GVO beinhaltet Grundsätze, die bei jeder Verarbeitung personenbezogener Daten immer gewährleistet sein müssen. Diese Grundsätze beinhalten:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz** (Art. 5 Abs. 1 lit. a DS-GVO):
Personenbezogene Daten dürfen ausschließlich auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies beinhaltet:
 1. Die Verarbeitung muss einem legitimen Zweck dienen und ein Erlaubnistatbestand zur Verarbeitung der Daten liegt vor. Desgleichen müssen im Falle der Verarbeitung der personenbezogenen Daten in einem Drittstaat die Vorgaben von Kapitel V DS-GVO erfüllt sein. Werden Auftragsverarbeiter eingesetzt, sind die Vorgaben zur Auftragsverarbeitung einzuhalten, bei Zusammenarbeit mit Partnern muss ggf. ein Vertrag zur gemeinsamen Verarbeitung abgeschlossen werden.
 2. Was genau der Ordnungsgeber unter der Regelung einer „Verarbeitung nach Treu und Glauben“ versteht, wird an keiner Stelle in der DS-GVO präzisiert. Jedoch findet sich in ErwGr. 38 RL 95/46⁶⁴ hierzu Folgendes:

„Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.“

D. h. die Verarbeitung muss „fair“ erfolgen.
 3. Die Verarbeitung der Daten muss für die betroffenen Personen transparent erfolgen. Dies erfordert insbesondere die Gewährleistung der in Kapitel II DS-GVO dargestellten Betroffenenrechte.
- **Zweckbindung** (Art. 5 Abs. 1 lit. b DS-GVO):
Die Verarbeitung personenbezogener Daten darf nur im Rahmen von festgelegten, eindeutigen und legitimen Zwecken erfolgen. Somit scheidet insbesondere eine Verarbeitung für noch unbekannte Zwecke aus, eine „Vorratsdatenspeicherung“ ist nicht mit den Vorgaben der DS-GVO vereinbar.
Eine Änderung des Zweckes bedarf wiederum eines eigenen Erlaubnistatbestandes. Dabei gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht als unvereinbar mit dem ursprünglichen Zweck, was ggf. für andere Zweckänderungen nachgewiesen werden muss.
- **Datenminimierung** (Art. 5 Abs. 1 lit. c DS-GVO):

⁶⁴ 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 am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A31995L0046>

Die Verarbeitung personenbezogener Daten muss für den verfolgten Zweck *erforderlich* und *angemessen* sein. Erforderlich ist die Verarbeitung personenbezogener Daten nur dann, wenn ohne diese Datenverarbeitung der verfolgte Zweck nicht erreicht werden kann. D. h. die Daten sind für die Erreichung der verfolgten Zwecke unverzichtbar.

Angemessenheit liegt vor, wenn es zu der Verarbeitung kein „milderes“ Mittel gibt, welches weniger in die Rechte und Freiheiten natürlicher Personen eingreift.

Datenminimierung beinhaltet daher nicht zwingend eine Beschränkung der absoluten Datenmenge, es kann durchaus die Verarbeitung einer sehr großen Menge personenbezogener Daten erforderlich und angemessen sein. Andererseits müssen ggf. Daten entfernt werden, wenn diese nicht benötigt werden wie beispielsweise GPS-Koordinaten aus Aufnahmen mit der Kamera eines mobilen Gerätes.

– **Richtigkeit** (Art. 5 Abs. 1 lit. d DS-GVO):

Die Daten müssen für die Dauer der Verarbeitung, die von der Erhebung der Daten bis zu deren Löschung andauert („Lebenszyklus“ der Daten), sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.

Es müssen alle „angemessenen“ Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Während eine Berichtigung falscher Daten immer erfolgen muss, muss eine Aktualisierung der vorhandenen Daten nur dann erfolgen, wenn die Aktualisierung für die Verarbeitung der Daten erforderlich ist. Wenn ein Patient beispielsweise vor zwei Jahren in Behandlung war und dieser Patient heute nach zwei Jahren umzieht, so liegt kein falsches Datum vor, denn zum Zeitpunkt der Behandlung stimmte die Adresse. Daher ist eine Korrektur nicht erforderlich und darf auch nicht erfolgen. Kommt dieser Patient jedoch zur erneuten Behandlung ins Krankenhaus, so muss die neue Adresse erfasst werden.

– **Speicherbegrenzung** (Art. 5 Abs. 1 lit. e DS-GVO):

Personenbezogene Daten dürfen nur so lange in einer die Identifizierung der betroffenen Personen erlaubenden Form gespeichert werden, wie es für die verfolgten Zwecke erforderlich ist.

Dabei erlauben auch pseudonymisierte Daten die Identifizierung einer Person. Art. 5 Abs. 1 lit. e DS-GVO verlangt also, dass personenbezogene Daten schnellstmöglich gelöscht oder anonymisiert werden. D. h. entweder direkt nach Zweckerreichung oder nach Ablauf der gesetzlichen Aufbewahrungspflichten, wenn diese für die Verarbeitung bestehen, muss eine Anonymisierung oder Löschung der vorhandenen Daten erfolgen.

Erfolgt die Verarbeitung **ausschließlich** für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke, so dürfen diese Daten länger gespeichert werden, wenn **geeignete** technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen durchgeführt werden. Dies beinhaltet insbesondere, dass das Verarbeitungsverfahren gemäß den Vorgaben von Art. 25 DS-GVO entwickelt und durchgeführt wird.

Dies setzt voraus, dass die Speicherdauer differenziert nach Zwecken festgelegt wird, damit der betroffenen Person gegenüber transparent dargestellt werden kann, wann welche Daten gelöscht werden.

– **Integrität und Vertraulichkeit** (Art. 5 Abs. 1 lit. f DS-GVO):

Bei jeder Verarbeitung muss die Integrität der Daten sowie der Schutz vor unbefugter Kenntnisnahme und Verarbeitung gewährleistet werden. Dies wird insbesondere durch die Umsetzung der Anforderungen von Art. 32 DS-GVO („Sicherheit personenbezogener Daten“) gewährleistet.

Art. 5 Abs. 2 DS-GVO verlangt, dass die Einhaltung dieser Grundsätze nachgewiesen werden muss. D. h. bei jeder Verarbeitung besteht eine Rechenschaftspflicht, welche die Erfüllung aller Anforderungen der DS-GVO umfasst.

4.1.2 Rechtsgrundlage der Verarbeitung⁶⁵

Die DS-GVO unterscheidet zwischen „normalen“ Daten und Daten, die zu den in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien gehören. Zu diesen Daten der besonderen Kategorien gehören:

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

Neben medizinischen Informationen gehören zu den besonderen Kategorien von Daten also auch biometrische Informationen wie Fingerprint oder Fotografien, wenn Letztere zur eindeutigen Identifikation genutzt werden können, wie es beispielsweise bei der Gesichtserkennung erfolgt.

Die Verarbeitung der besonderen Kategorien von Daten ist laut Art. 9 Abs. 1 DS-GVO grundsätzlich verboten! Die Verarbeitung ist nur statthaft, wenn ein gesetzlicher Erlaubnistatbestand vorhanden ist. Auch eine datenschutzrechtliche Einwilligung einer betroffenen Person ist ein gesetzlicher Erlaubnistatbestand.

4.1.2.1 Einwilligung

Gemäß Art. 9 Abs. 2 lit. a DS-GVO ist eine Verarbeitung besonderer Kategorien personenbezogener Daten gestattet, wenn

- a) die betroffene Person ausdrücklich für einen oder mehrere Zwecke einwilligt und
- b) Unionsrecht oder das Recht von Mitgliedstaaten die Verarbeitung nicht verbieten.

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden. Näheres zur rechtskonformen Einwilligung findet sich z. B. in der Praxishilfe „Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers“⁶⁶.

Auch für eine Einwilligung gilt die in Art. 5 Abs. 1 lit. a DS-GVO verankerte Transparenzpflicht, d. h. es muss u. a. über alle Verwendungszwecke aller Empfänger informiert werden.

⁶⁵ Der EuGH urteilte am 21. Dezember 2023 (Rechtssache C-667/21), dass neben einer Rechtsgrundlage nach Art. 9 DS-GVO auch immer ein Rechtfertigungsgrund nach Art. 6 DS-GVO erforderlich ist. Zu einer ausführlichen Darstellung von Rechtsgrundlagen auch im Kontext von nationalen gesetzlichen Regelungen siehe bspw. die Praxishilfe zum Umgang mit Erlaubnistatbeständen bei der Verarbeitung von Gesundheitsdaten und genetischen Daten. Online, zitiert am 2024-08-24; verfügbar unter <https://gesundheitsdatenschutz.org/html/erlaubnistatbestandgesundheitsdaten.php>

⁶⁶ GMDS, GDD: Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers. Stand der Bearbeitung: 30. April 2021. Online, zitiert am 2024-08-24; verfügbar unter <https://gesundheitsdatenschutz.org/html/einwilligung.php>

Die Beweislast, dass für die Verarbeitung der personenbezogenen Daten eine Einwilligung vorgelegen hat bzw. immer noch vorliegt, liegt beim Verantwortlichen. Ebenfalls muss nachgewiesen werden, dass alle Anforderungen an eine Einwilligung vorgelegen haben, insbesondere natürlich:

- Freiwilligkeit
D. h., die Einwilligung wurde ohne Zwang abgegeben, es existierte mindestens eine „echte“ Alternativmöglichkeit (ErwGr. 42 DS-GVO beachten: „[...] wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“)
- Für **den** bestimmten Fall (= Zweckbindung)
Entsprechend Art. 4 Nr. 11 DS-GVO muss eine Einwilligung für den bestimmten Fall abgegeben werden, was immer beinhaltet, dass der betroffenen Person der Zweck der Verarbeitung ihrer Daten vor Abgabe der Einwilligung bekannt sein muss.
- Informiertheit
Die Einwilligung muss in Kenntnis der Sachlage erteilt werden. Dies beinhaltet natürlich auch alle Informationen nach Art. 13 bzw. Art. 14 DS-GVO.
- Es muss sich um eine unmissverständlich abgegebene Willensbekundung handeln, also in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung geschehen.
- Bei Gesundheitsdaten zu beachten: Es ist eine ausdrückliche Willenserklärung erforderlich.
- Der Verantwortliche muss gemäß Art. 7 Abs. 1 DS-GVO nachweisen können, dass für die Verarbeitung eine rechts gültige Einwilligung vorgelegen hat bzw. immer noch vorliegt.

Hinweis 1: Man spricht von einem „Machtungleichgewicht“ zwischen Verantwortlichem und betroffener Person, wenn eine Abhängigkeit der betroffenen Person vom Verantwortlichen besteht, z. B. Arbeitgeber und Arbeitnehmer oder Arzt und Patient. Ein gewisses Ungleichgewicht zwischen Verantwortlichem und betroffenen Personen besteht natürlich immer, da nur der Verantwortliche über Zwecke und Mittel der Verarbeitung entscheidet. ErwGr. 43 DS-GVO hebt aber hervor, dass bei besonders klaren Ungleichgewichten ggf. eine Einwilligung keine Rechtsgrundlage darstellen kann, da die Einwilligung nicht als „freiwillig gegeben“ angesehen werden kann. Als Beispiel nennt ErwGr. 43 eine Behörde als Verantwortlichen. Aber auch im medizinischen Kontext kann dies eine Rolle spielen, da beispielsweise eine angebotene Heilung einer Krankheit (z. B. Krebs) immer eine starke Abhängigkeit des Patienten als betroffene Person erzeugt. Wird das Machtungleichgewicht missachtet, ist eine Einwilligung als Rechtsgrundlage der Verarbeitung daher ggf. nicht wirksam, eine darauf erfolgende Verarbeitung würde dann rechtswidrig erfolgen. Daher muss immer beachtet werden, wie dem Ungleichgewicht zwischen Verantwortlichem und betroffener Person begegnet werden kann, insbesondere durch eine transparente Verarbeitung, der Wahrung der Betroffenenrechte sowie der Gewährleistung der Sicherheit der Verarbeitung.

Hinweis 2: Grundsätzlich ist zu beachten: Auch eine Einwilligung kann keine übermäßige oder unverhältnismäßige Datenverarbeitung legitimieren.⁶⁷

⁶⁷ Artikel-29-Datenschutzgruppe: Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten vom 27. Februar 2013. Online, zitiert am 2024-08-24; verfügbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf

4.1.2.2 Zweckänderung aufgrund einer Interessensabwägung

Art. 6 Abs. 1 lit. f DS-GVO erlaubt eine Verarbeitung personenbezogener Daten, wenn

- a) dies „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich“ ist, und
- b) die überwiegenden „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“ stehen einer Verarbeitung nicht entgegen.

Grundsätzlich darf gemäß Art. 6 Abs. 1 lit. f DS-GVO also ein Verantwortlicher (bzw. ein Auftragsverarbeiter auf ausdrückliche Weisung des Verantwortlichen) oder ein Dritter (der dann selbst zum Verantwortlichen wird) personenbezogene Daten verarbeiten, wenn ein den Interessen der betroffenen Person überwiegendes Interesse an der Verarbeitung nachgewiesen werden kann. Auftragsverarbeiter, die in einem Auftrag Daten von einem Verantwortlichen erhielten und diese Daten ohne ausdrückliche Weisung des Verantwortlichen verarbeiten, agieren in diesen Fällen entsprechend Art. 28 Abs. 10 DS-GVO als Verantwortliche.

Aber: Die Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Datenkategorien wie Gesundheitsdaten, biometrischen oder genetischen Daten ist grundsätzlich verboten, außer ein in Art. 9 Abs. 2 DS-GVO genannter Erlaubnistatbestand liegt vor. Somit **stellt Art. 6 Abs. 1 lit. f DS-GVO alleine keinen Erlaubnistatbestand zur Verarbeitung** der in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien **dar**, eine zweckändernde Verarbeitung wie beispielsweise die Nutzung der personenbezogenen Daten zu Werbezwecken kann nicht alleine durch Art. 6 Abs. 1 lit. f DS-GVO legitimiert werden.

Entsprechend Art. 9 Abs. 4 DS-GVO können Mitgliedstaaten der EU zusätzliche Bedingungen für die Verarbeitung besonderer Kategorien von Daten betroffener Personen einführen oder aufrechterhalten, jedoch nur, „soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist“. Deutschland führte zusätzliche Regelungen für die Verarbeitung zu anderen Zwecken ein:

- 1) § 24 Abs. 1 Ziff. 1 BDSG erlaubt die Verarbeitung personenbezogener Daten zu anderen Zwecken, wenn diese Verarbeitung zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist; dies wird regelhaft für keine Verarbeitung durch natürliche oder juristische Personen, welche keine staatlichen Aufgaben wie beispielsweise die Bundeswehr oder Polizei wahrnehmen, anwendbar sein.
- 2) § 24 Abs. 1 Ziff. 2 BDSG erlaubt die Verarbeitung personenbezogener Daten zu anderen Zwecken, wenn diese zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Somit können ggf. personenbezogene Daten in Gerichtsprozessen, wenn Ansprüche gegenüber einer betroffenen Person durchgesetzt werden sollen, genutzt werden.
- 3) § 27 Abs. 1 BDSG erlaubt die Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken sowie zu statistischen Zwecken, wenn die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung **erheblich** überwiegen.

Eine **Nutzung personenbezogener Daten der besonderen Kategorie** durch Anwender **aufgrund einer Interessensabwägung ist** somit – ein nachgewiesenes **erhebliches überwiegendes Interesse vorausgesetzt – ausschließlich zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken** sowie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche **zulässig**. Jegliche Verarbeitung personenbezogener genetischer, biometrischer oder

Gesundheitsdaten zu anderen Zwecken, insbesondere zu Zwecken der Werbung, bedarf einer anderen Rechtsgrundlage als einer Interessensabwägung. In der Regel wird hierfür die ausdrückliche Einwilligung der jeweils betroffenen Person erforderlich sein.

4.1.2.3 Behandlungsvertrag

Im Zusammenhang mit der Behandlung von Patienten ist Art. 9 Abs. 2 lit. h DS-GVO i. V. m. Art. 6 Abs. 1 lit. b DS-GVO anwendbar: Die Verarbeitung ist erforderlich zur Vertragserfüllung, genauer des Behandlungsvertrages, welcher in den §§ 630a ff BGB geregelt wird.

Hinsichtlich der in Art. 9 Abs. 2 lit. h DS-GVO enthaltenen vertraglichen Rechtsgrundlage ist das Erfordernis zu beachten, dass der Vertrag mit „Angehörigen eines Gesundheitsberufs“ abgeschlossen werden muss. Der Begriff „Angehörige eines Gesundheitsberufs“ ist europarechtlich in Art. 3 lit. f Richtlinie 2011/24/EU⁶⁸ geregelt:

„Einen Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, einen Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG⁶⁹ vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt.“

In Deutschland stimmen „Angehörige eines Gesundheitsberufs“ weitgehend mit jenen Berufen überein, welche von § 203 Abs. 1 Ziff. 1 StGB adressiert werden: „Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert“.⁷⁰

Somit werden Verträge mit Ärzten, Krankenpflegepersonal usw. mit der Regelung in Art. 9 Abs. 2 lit. h DS-GVO adressiert, Verträge mit anderen Dienstleistern (z. B. zur Terminvermittlung zwischen einem Patienten und einem niedergelassenen Arzt, was entsprechend der weiten Auslegung^{71,72} des Art. 9 Abs. 1 DS-GVO ebenfalls eine Verarbeitung sensibler Daten darstellt) werden hierdurch wohl eher nicht legalisiert werden können. Ein Vertrag zwischen Verantwortlichen, die keine Angehörigen eines Gesundheitsberufes sind, und betroffenen Personen kann Art. 6 Abs. 1 lit. b DS-GVO genügen, jedoch nicht die Verarbeitung von Daten legitimieren, welche zu den in Art. 9 Abs. 1 DS-GVO

⁶⁸ Art. 3 lit. f Richtlinie 2011/24/EU. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02011L0024-20140101#tocId6>

⁶⁹ Art. 3 Abs. 1 lit. a der Richtlinie 2005/36/EG verweist auf „reglementierte Berufe“, bei welchen die Aufnahme oder Ausübung oder eine der Arten der Ausübung direkt oder indirekt durch Rechts- und Verwaltungsvorschriften an den Besitz bestimmter Berufsqualifikationen gebunden ist. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02005L0036-20231009#tocId25>

⁷⁰ Ein Hinweis hierzu findet sich z. B. in Schütze B, Spyrä G. (2018) Schweigepflicht und die Einbindung externer Kräfte: endlich geregelt. Online, zitiert am 2024-08-24; verfügbar unter https://gesundheitsdatenschutz.org/html/schweigepflicht_05.php

⁷¹ EuGH, Urt. v. 2022-08-01, Rechtssache C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2024-01-15; verfügbar unter <https://dejure.org/2010,236> bzw. Volltext abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184>

⁷² EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21, Rn. 89 sowie Leitsatz 2. Online, zitiert am 2024-01-15; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

genannten Kategorien zählen. I. d. R. wird hier nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO die Verarbeitung legalisieren können.⁷³

Zu beachten ist, dass Art. 9 Abs. 2 lit. h DS-GVO nur die Verarbeitung legitimiert, die für die Vertragserfüllung **erforderlich** sind. Somit muss bei Berufung auf dieser Rechtsgrundlage immer auch das Erfordernis nachgewiesen werden.

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

- der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder
- der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112).

D. h. damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte betroffener Personen weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht. Entsprechend urteilte der EuGH⁷⁴ verschiedentlich, dass die Voraussetzung der Erforderlichkeit der Verarbeitung personenbezogener Daten die Prüfung verlangt, ob die Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen.

Es kommt bei der Bewertung der „Erforderlichkeit“ also nicht darauf an, ob ein anderes Mittel beispielsweise aus betriebswirtschaftlicher Sicht geeigneter wäre (weil z. B. weniger Kosten anfallen), sondern darauf, ob ein anderes Mittel geeignet ist den Zweck bzw. die Zwecke zu erreichen und - wenn mehr als ein Mittel existiert – welches Mittel am wenigsten in die Grundrechte und Grundfreiheiten, zu denen mit und der EU-Grundrechtecharta auch die Rechte auf Achtung des Privatlebens (Art. 7) und auf Schutz personenbezogener Daten (Art. 8) gehören, der betroffenen Personen eingreift.

Um die Erforderlichkeit einer Verarbeitung personenbezogener Daten beurteilen zu können, müssen daher drei Fragen beantwortet werden:

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

Der EuGH verlangt in diesem Zusammenhang, dass die betreffende Verarbeitung objektiv unerlässlich sein muss, um einen Zweck zu verwirklichen, wobei dieser Zweck notwendiger

⁷³ Hierbei sollten die Ausführungen des EuGH bzgl. des Meta-Falles beachtet werden: EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 140ff, insbesondere Rn. 154. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

⁷⁴ So z. B.

- EuGH, Urt. v. 2024-09-12, verbundene Rechtssachen C-17/22 und C-18/22, Rn. 51. Online, zitiert am 2024-09-25; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1726468533308&uri=CELEX%3A62022CJ0017>
- EuGH, Urt. v. 2023-12-07, verbundene Rechtssachen C-26/22 und C-64/22, Rn. 77. Online, zitiert am 2024-09-25; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026>
- EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21, Rn. 108. Online, zitiert am 2024-09-25; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist: Die Verarbeitung der personenbezogenen Daten durch den Verantwortlichen muss für die ordnungsgemäße Erfüllung des zwischen dem Verantwortlichen und der betroffenen Person geschlossenen Vertrags wesentlich sein und es dürfen keine praktikablen und weniger einschneidenden Alternativen bestehen.⁷⁵ Im Kontext einer Terminvergabe muss beispielsweise u. a. beachtet werden:

- Für die Behandlung von Notfällen ist grundsätzlich keine Terminvereinbarung erforderlich. Notfälle sind nicht planbar. Somit fehlt es an dem Erfordernis, damit die im Kontext dieser Behandlungen an einen Dienstleister zu Online-Terminmanagementsystemen übermittelt werden.
- Zur Weiter- und Nachbehandlung auch von Notfällen kann eine Terminvergabe erforderlich sein.⁷⁶ Die Versorgung von Patienten durch Leistungserbringer erfordert in vielen Fällen eine Priorisierung, sodass eine Absprache bzgl. Behandlungsterminen unverzichtbar ist. Allerdings ist eine Online-Vereinbarung, egal ob durch einen Dienstleister oder durch den Leistungserbringer selbst, niemals⁷⁷ erforderlich, sondern dient ausschließlich der Vereinfachung von Prozessabläufen beim Leistungserbringer. Eine Terminvereinbarung vor Ort oder auch durch einen Telefonanruf bei einem Leistungserbringer mag aus dessen Sicht den Nachteil haben, dass eine Person einen Teil ihrer Arbeitszeit mit der Entgegennahme einer Terminanfrage ableistet. Eine Online-Terminvergabe verringert den Aufwand. Jedoch begründet eine organisatorische Entlastung eines Verantwortlichen – in diesem Falle eines Leistungserbringers – datenschutzrechtlich keine Erforderlichkeit. Daher ist zu berücksichtigen, dass eine Terminvereinbarung direkt vor Ort beim Leistungserbringer immer ein milderer Mittel, d. h. einen weniger invasiven Eingriff in das Recht der Selbstbestimmung als eine Online-Terminvergabe, welche zwingend die Nutzung des Internets mit allen damit verbundenen IT-Sicherheitsrisiken darstellt.
- Die Weitergabe von Patientendaten von abgeschlossenen Fällen ist grundsätzlich nie erforderlich; ob die Patienten den Leistungserbringer erneut aufsuchen oder nicht, liegt in einer ungewissen Zukunft und kann keine Erforderlichkeit begründen. Eine Weitergabe

⁷⁵ EUGH Urt. v. 2023-07-04, Rechtssache C252/21, Rn. 98 f. Online, zitiert am 2024-08-24; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252>

⁷⁶ Beispielhaft für einzelne Krankheitsbilder Vor- und Nachteile dargestellt in:

- Etingen B, Hogan TP, Martinez RN et al. (2019) How Do Patients with Mental Health Diagnoses Use Online Patient Portals? An Observational Analysis from the Veterans Health Administration. *Adm Policy Ment Health* 46: 596–608. <https://doi.org/10.1007/s10488-019-00938-x>
- Meade JG, Brown JS (2006) Improving access for patients – a practice manager questionnaire. *BMC Fam Pract* 7: 37. <https://doi.org/10.1186/1471-2296-7-37>
- Nuti L, Turkcan A, Lawley MA et al. (2015) The impact of interventions on appointment and clinical outcomes for individuals with diabetes: a systematic review. *BMC Health Services Research* 15:355. <https://doi.org/10.1186/s12913-015-0938-5>

⁷⁷ In sehr seltenen Fällen kann auch eine Terminerinnerung als Unterstützungsleistung medizinisch sinnvoll sein, aber in diesen Fällen ist immer ein ganzheitlicher Ansatz erforderlich, der Patientenaufklärung, verbesserte Kommunikation und maßgeschneiderte Strategien für die Gesundheitsversorgung umfasst; Terminerinnerung ist hier nur ein kleiner Teil des Ganzen. Siehe z. B.: Alturbag (2024) Factors and Reasons Associated With Appointment Non-attendance in Hospitals: A Narrative Review. *Cureus* 16(4):e58594. <https://doi.org/10.7759/cureus.58594>

Auch in diesen Fällen reicht i. d. R. eine telefonische Erinnerung ein oder zwei Tage vor dem Termin aus; Erinnerungen von Terminverwaltungssystemen konnten gegenüber den telefonischen Erinnerungen keinen Vorteil zeigen. Reda S, Makhoul S (2001) Prompts to encourage appointment attendance for people with serious mental illness. *Cochrane Database Syst Rev.* 2001(2):CD002085. <https://doi.org/10.1002/14651858.CD002085>

dieser Daten an Dienstleister von externen Online-Terminmanagementsystemen kann aufgrund der fehlenden Erforderlichkeit regelhaft nur durch eine datenschutzrechtliche Einwilligung legitimiert werden.

4.1.2.4 Weitere Erlaubnistatbestände

Art. 9 Abs. 2 DS-GVO kennt neben der Einwilligung noch weitere Erlaubnistatbestände, dazu gehören insbesondere:

- Ausübung von aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechten durch einen Verantwortlichen oder einer betroffenen Person (Art. 9 Abs. 2 lit. b DS-GVO)
- Verarbeitung ist zum Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben (Art. 9 Abs. 2 lit. c DS-GVO)
- Verarbeitung erfolgt durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten, wobei
 1. geeigneter Garantien zur Wahrung der Rechte und Freiheiten betroffener Personen sind vorhanden,
 2. es sind ausschließlich Informationen von Mitgliedern oder ehemaligen Mitgliedern der Organisation oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, betroffen
 3. und die personenbezogenen Daten werden nicht ohne Einwilligung nach außen offengelegt(Art. 9 Abs. 2 lit. d DS-GVO)
- Es werden ausschließlich Daten verarbeitet, welche die betroffene Person offensichtlich öffentlich gemacht hat (Art. 9 Abs. 2 lit. e DS-GVO)
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich (Art. 9 Abs. 2 lit. f DS-GVO)
- Verarbeitung ist für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich und
 1. die Verarbeitung beruht auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats
 2. oder erfolgt aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs.(Art. 9 Abs. 2 lit. h DS-GVO)
- Die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich und
 1. die Verarbeitung erfolgt auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, welches
 - a) in angemessenem Verhältnis zu dem verfolgten Ziel steht,
 - b) den Wesensgehalt des Rechts auf Datenschutz wahrt und
 - c) angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht(Art. 9 Abs. 2 lit. j DS-GVO).

4.1.3 Verschwiegenheitspflicht

Entsprechend Art. 9 Abs. 1 DS-GVO ist eine Verarbeitung sensibler Daten wie beispielsweise genetische oder Gesundheitsdaten verboten, wenn kein ausdrücklicher gesetzlicher Erlaubnistatbestand besteht (siehe auch Kapitel 4.1.2). Der Begriff der Verarbeitung ist in Art. 4 Ziff. 2 DS-GVO sehr weit gefasst und umfasst insbesondere auch jede Form der Übermittlung, Weitergabe oder Offenbarung personenbezogener Daten.

Somit müssen Verantwortliche und Auftragsverarbeiter personenbezogene Daten vor der Kenntnisnahme unbefugter Personen schützen, was auch eigene Beschäftigte umfasst, die für ihre Arbeit keine Kenntnis dieser Daten benötigen; die unberechtigte Kenntnisnahme durch Dritte i. S. v. Art. 4 Ziff. 10 DS-GVO ist zwingend zu verhindern.

Entsprechend weist Art. 28 Abs. 3 S. 2 lit. b DS-GVO Auftragsverarbeiter an, dass die mit der Verarbeitung personenbezogener Daten betrauten Personen zur Vertraulichkeit verpflichtet werden, wenn diese nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Art. 29 DS-GVO verlangt, dass jede einem Verantwortlichen (oder Auftragsverarbeiter) unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen; entsprechend Art. 32 Abs. 4 DS-GVO muss ein Verantwortlicher (auch der Auftragsverarbeiter) geeignete technische und organisatorische Maßnahmen die Anforderung von Art. 29 DS-GVO sicherstellen, entsprechend Art. 32 Abs. 1 durch geeignete technische und organisatorische Maßnahmen. Dem Wortlaut von Art. 28 Abs. 3 S. 2 lit. b DS-GVO nach müssen Auftragsverarbeiter alle an der Verarbeitung beteiligten Beschäftigten verpflichten. Aber letztlich trifft diese Pflicht zur Verpflichtung indirekt auch Verantwortliche: eine Verpflichtung stellt eine zumutbare und angemessene organisatorische Maßnahme dar, deren Nicht-Umsetzung vermutlich als ein Versäumnis der aus Art. 32 i. V. m. Art. 29 DS-GVO resultierenden Pflichten anzusehen ist.

Die deutschen Datenschutz-Aufsichtsbehörden bzw. die Datenschutzkonferenz stellt ein Muster für eine schriftliche Verpflichtung zur Verfügung.⁷⁸

4.1.4 Gewährleistung der Betroffenenrechte

Die Betroffenenrechte sind datenschutzrechtlich im Kapitel III der DS-GVO (Artikel 12 bis 22) festgelegt. Im Überblick handelt es sich um folgende Rechte des Betroffenen bzw. Pflichten gegenüber dem Betroffenen:

- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten, unterschieden nach:
 - Erhebung bei der betroffenen Person
 - Erhebung nicht bei der betroffenen Person („Dritterhebung“)
- Auskunftsrecht der betroffenen Person
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung

⁷⁸ Datenschutzkonferenz: Kurzpapier Nr. 19 - Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO. (Stand 2018-05-29). Online, zitiert am 2024-09-25; verfügbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall.

Entsprechend Art. 12 Abs. 1 DS-GVO muss der Verantwortliche geeignete Maßnahmen treffen, um diesen Pflichten nachzukommen,

4.1.4.1 Informationspflichten

Bei jeder Verarbeitung muss den aus Art. 13 und Art. 14 DS-GVO resultierenden Informationspflichten genügt werden, d. h. vor, spätestens bei Erhebung der personenbezogenen Daten sind den betroffenen Personen die notwendigen Angaben entsprechend Art. 13 bzw. Art. 14 DS-GVO zur Verfügung zu stellen. Die Informationen müssen dabei stets in einer klaren und einfachen Sprache vermittelt werden, wie es Art. 12 DS-GVO fordert.

4.1.4.2 Auskunftsrecht

Jede betroffene Person hat das Recht, Auskunft über die sie betreffenden verarbeiteten oder gespeicherten Daten zu erhalten. Auf dieses Recht ist im Rahmen der im Abschnitt 4.1.4.1 genannten Informationspflicht hinzuweisen. Idealerweise wird bei dieser Information der betroffenen Person auch eine Telefonnummer sowie eine spezielle nicht-personalisierte E-Mail-Adresse angegeben, damit Anfragen auch bei einem Personalwechsel richtig ankommen.

Nach Art. 15 Abs. 3 DS-GVO muss der Verantwortliche den betroffenen Personen auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Dabei darf ein Verantwortlicher eine Kopie nur dann in einem gängigen elektronischen Format zur Verfügung stellen, wenn die betroffene Person, d. h. der Patient, den Antrag elektronisch stellte: Der Patient hat also ein Wahlrecht, ob er die Daten elektronisch oder lieber in Papierform bekommen möchte.

4.1.4.3 Recht auf Berichtigung

Nach Art. 16 DS-GVO hat jede betroffene Person das Recht, dass unrichtige Daten berichtigt werden. Da Daten die Grundlage jeder medizinischen Behandlung und Forschung darstellen, liegt die Korrektur unrichtiger Daten selbstverständlich auch im ureigenen Interesse der die Daten verarbeitenden Stelle.

Allerdings hat nach Art. 16 DS-GVO jeder Patient auch das Recht, dass unvollständige Daten vervollständigt werden, ggf. auch mittels einer ergänzenden Erklärung. Hier kann es zu unterschiedlichen Interpretationen zwischen dem Verantwortlichen und der betroffenen Person bei der Auslegung des Begriffs „unvollständig“ kommen. Der europäische Gesetzgeber verlangt daher, dass dieses Recht „unter Berücksichtigung der Zwecke der Verarbeitung“ zu erfolgen hat. D. h. die Beurteilung bzgl. Unvollständigkeit muss aus Sicht des Verarbeitungszweckes erfolgen.

Jeder Patient muss im Rahmen der Informationspflicht (siehe Kapitel 4.1.4.1) darauf hingewiesen werden, dass für ihn diese Rechte bestehen.

4.1.4.4 Recht auf Einschränkung der Verarbeitung („Sperrung“)

Gemäß Art. 18 DS-GVO hat jeder Patient das Recht, unter den Voraussetzungen von Art. 18 Abs. 1 DS-GVO von dem Verantwortlichen die Einschränkung der Verarbeitung (= „Sperrung“) zu verlangen. Auch auf dieses Recht muss im Rahmen der Informationspflicht (siehe Kapitel 4.1.4.1) hingewiesen werden. Zugleich sollte er darauf hingewiesen werden, dass dieses Recht ggf. durch gesetzliche

Bestimmungen eingeschränkt werden kann und dann auch mitgeteilt werden, durch welche Gesetze welche Einschränkung dieses Rechts erfolgt.

Der Verantwortliche muss dabei beachten, dass gemäß Art. 18 Abs. 2 DS-GVO eine derartige Sperrung nur mit Einwilligung der betroffenen Person rückgängig gemacht werden darf. Ansonsten darf eine Verarbeitung, von einer Speicherung abgesehen, nur

- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
- zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
- aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats

erfolgen. Weiterhin muss der Verantwortliche entsprechend den Vorgaben von Art. 18 Abs. 3 DS-GVO die betroffene Person, die eine Sperrung erwirkte, unterrichten, bevor die Einschränkung aufgehoben wird.

4.1.4.5 Recht auf Löschung

Nach Art. 17 DS-GVO hat jede betroffene Person das Recht auf Löschung der sie betreffenden Daten, wenn die Voraussetzungen aus Art. 17 Abs. 1 DS-GVO vorliegen und die Ausnahmetatbestände aus Art. 17 Abs. 3 DS-GVO nicht anzuwenden sind. Auch über dieses Recht ist jede betroffene Person im Rahmen der Informationspflicht (siehe Kapitel 4.1.4.1) zu informieren. Gleichzeitig ist darauf hinzuweisen, dass dieses Recht ggf. durch gesetzliche Bestimmungen wie z. B. durch die Vorgabe gesetzlicher Aufbewahrungsfristen eingeschränkt werden kann und dann auch mitgeteilt werden, durch welche Gesetze welche Einschränkung dieses Rechts erfolgt.

4.1.4.6 Widerspruchsrecht

Nach Art. 21 Abs. 6 DS-GVO hat jede betroffene Person das Recht, aus Gründen, „die sich aus ihrer besonderen Situation ergeben“, einer Verarbeitung der sie betreffenden Daten zu widersprechen. Entsprechend Art. 21 Abs. 4 DS-GVO muss jede betroffene Person ausdrücklich auf dieses Recht hingewiesen werden, d. h. auch auf dieses Recht ist im Rahmen der Informationspflicht (siehe Kapitel 4.1.4.1) hinzuweisen.

Dabei ist zu berücksichtigen, dass auch darauf hingewiesen wird, dass ein Widerspruchsrecht ggf. durch gesetzliche Regelungen eingeschränkt sein kann, z. B. muss eine Speicherung aufgrund gesetzlicher Bestimmungen trotz eines des erfolgten Widerspruchs der betroffenen Person bei vorhandenen gesetzlichen Aufbewahrungsfristen erfolgen. Im Falle einer Beschränkung des Rechts sollte den betroffenen Personen dann auch mitgeteilt werden, durch welche Gesetze welche Einschränkung dieses Rechts erfolgt.

4.1.4.7 Recht auf Datenübertragbarkeit

Gemäß Art. 20 DS-GVO hat jeder Patient unter den Voraussetzungen von Art. 20 Abs. 1 lit. a, b DS-GVO das Recht, von ihm bereitgestellte Daten

- vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten
- sowie
- sie einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln bzw. übermitteln zu lassen.

Jede betroffene Person ist im Rahmen der Informationspflicht (siehe Kapitel 4.1.4.1) über dieses Recht zu informieren. Es sollte dabei aber auch darauf hingewiesen werden, dass kein Empfänger

dieser Daten gesetzlich dazu verpflichtet ist, diese Daten überhaupt oder in dem vom Verantwortlichen bereitgestellten Format anzunehmen.

4.1.4.8 Profilbildung / automatisierte Einzelfallentscheidung

Gemäß Art. 22 Abs. 1 DS-GVO dürfen betroffene Personen nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen werden, welche der betroffenen Person gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigen kann. Eine Ausnahme besteht entsprechend Art. 22 Abs. 2 DS-GVO, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

Bei der Verarbeitung von Daten der besonderen Kategorien wie Gesundheitsdaten, genetischen oder biometrischen Daten ist jedoch immer die ausdrückliche Einwilligung der betroffenen Person erforderlich; die zweite Möglichkeit (Art. 9 Abs. 2 lit. g DS-GVO) ist im Umfeld der hier besprochenen Szenarien regelhaft nicht anwendbar.

4.1.5 Ort der Verarbeitung: Einsatz von Cloud-Dienstleistern

Mit dem Digital-Gesetz⁷⁹ des Bundesministeriums für Gesundheit (BMG) wurde § 393 SGB V „Cloud-Einsatz im Gesundheitswesen“ eingeführt, der ab dem 1. Juli 2024 gilt. § 393 SGB V enthält Anforderungen, die alle gesetzlichen Pflege- und Krankenkassen sowie alle Leistungserbringer (also Arztpraxen, Krankenhäuser, Apotheken, häusliche Pflege usw.) bei Nutzung von Cloud-Computing Diensten⁸⁰ erbringen müssen.

§ 393 Abs. 2 SGB V beinhaltet Vorgaben für den Ort der Verarbeitung, wenn eine Verarbeitung von Gesundheits- oder Sozialdaten unter Einsatz einer Cloud erfolgt. So darf die Verarbeitung im Wege des Cloud-Computing-Dienstes nur im Inland oder in einem Mitgliedstaat der Europäischen Union erfolgen.

In einem Drittstaat wie den USA oder Japan darf eine Verarbeitung in einer Cloud hingegen nur erfolgen, **wenn für dieses Drittland ein Angemessenheitsbeschluss der EU-Kommission vorliegt.**⁸¹

Speziell in Bezug auf die USA ist zu beachten, dass kein Angemessenheitsbeschluss für die USA selbst vorliegt, sondern nur für dort zertifizierte Unternehmen.⁸² Beim Angemessenheitsbeschluss für die

⁷⁹ BMG: Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG). Online, zitiert am 2024-08-24; verfügbar unter <https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig>

⁸⁰ Bzgl. Cloud ist zu beachten, dass der Begriff „Cloud“ europarechtlich definiert ist. Mehr zu den Rahmenbedingungen beim Cloud-Einsatz und auch zu den Regelungen des SGB V finden sich z. B. in der Praxishilfe „Eine Cloud ist eine Cloud. Oder etwa doch nicht?“ Online, zitiert am 2024-08-24; verfügbar unter <https://gesundheitsdatenschutz.org/html/cloud-nis2-sgb-v.php>

⁸¹ Eine Liste der Angemessenheitsbeschlüsse der EU-Kommission findet man unter https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de (letzter Abruf der Webseite 2024-08-24)

⁸² Siehe Data Privacy Framework List. Online, zitiert am 2024-08-24; verfügbar unter <https://www.dataprivacyframework.gov/list>

USA (EU-US Data Privacy Framework) werden zwei Arten der Selbst-Zertifizierung unterschieden: „Non-HR-Data“ und „HR-Data“. Zum Stand dieser Ausarbeitung existierten bei den nachfolgend genannten amerikanischen Cloud-Anbietern folgende Zertifizierungen:

Cloud-Anbieter	Non-HR-Data	HR Data
Amazon.com, Inc.	Ja	Nein
Apple Inc.	Nein	Nein
Broadcom Inc. (VMWare)	Nein	Nein
Cisco Systems, Inc.	Nein	Nein
Dell Technologies Inc.	Nein	Nein
Dropbox Inc.	Nein	Nein
Google LLC	Ja	Ja
International Business Machines Corporation (IBM)	Ja	Nein
Microsoft Corporation	Ja	Ja
Oracle America Inc.	Ja	Nein
Oracle (Cerner Corporation)	Ja	Ja
Rackspace Inc.	Nein	Nein
Salesforce	Ja	Ja
ServiceNow, Inc.	Ja	Ja
Snowflake Inc.	Ja	Nein
Workday, Inc.	Ja	Ja

Werden im Rahmen der Cloud-Nutzung Beschäftigtendaten durch ein amerikanisches Unternehmen verarbeitet (z. B. durch personalisierte Anmeldung an den Cloud-Dienst), so muss nach Auffassung der EU-Kommission⁸³, des Europäischen Datenschutzausschusses sowie der deutschen Datenschutz-Konferenz⁸⁴ eine „HR-Data“-Zertifizierung vorliegen; die amerikanische US-Regierung wiederum geht davon aus, dass eine „HR-Data“-Zertifizierung nur dann erforderlich ist, wenn Daten von bei amerikanischen Unternehmen beschäftigten Personen Gegenstand der Verarbeitung durch europäische Unternehmen (im Falle der Cloud also durch den jeweiligen Cloud-Kunden) sind.⁸⁵

Diese unterschiedliche Sichtweise auf das EU-U.S. Data Privacy Framework führt dazu, dass diverse amerikanische Unternehmen keine Zertifizierung „HR-Data“ aufweisen und daher entsprechend den europäischen Vorgaben auch keine Daten von in der EU beschäftigten Personen verarbeiten

⁸³ Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA. Anhang I, III. Zusatzgrundsätze, Nr. 6 „Selbstzertifizierung“, lit. c. Online, zitiert am 2024-08-24; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj?locale=de

⁸⁴ Datenschutzkonferenz (DSK): Anwendungshinweis vom 4. September 2023 „Übermittlung personenbezogener Daten aus Europa an die USA“, S. 12 Kap. 1.2 „Welche Übermittlungen sind erfasst?“ Online, zitiert am 2024-08-24; verfügbar unter https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

⁸⁵ U.S. Department of Commerce: FAQs – Privacy Policy, Q7: Are there different requirements under the DPF Principles for non-human resources and human resources privacy policies? Online, zitiert am 2024-06-26; verfügbar unter [https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20Privacy-Policy-\(6%E2%80%9310\)](https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20Privacy-Policy-(6%E2%80%9310))

dürfen.⁸⁶ Für die Verarbeitung aller anderen Daten gilt das Erfordernis einer „Non-HR-Data“-Zertifizierung.

Ob jemand ergänzend zu einer „Non-HR-Data“-Zertifizierung“ zur Verarbeitung von Beschäftigendaten andere Garantien entsprechend der DS-GVO nutzen kann, ist rechtlich mindestens zweifelhaft. In Art. 46 Abs. 1 DS-GVO heißt es:

„**Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt**, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, [...]“.

Entsprechend Art. 45 Abs. 1 DS-GVO kann die EU-Kommission für „das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland“ die Angemessenheit beschließen. Für die USA liegt ein Angemessenheitsbeschluss vor, somit können entsprechend Art. 46 Abs. 1 DS-GVO andere in der DS-GVO genannten Garantien für einen Drittlandstransfer nicht angewendet werden.

Allein schon aufgrund von Authentisierungspflichten beim Zugriff auf Unternehmensdaten wird bei jeder elektronischen Verarbeitung auch HR-Daten der Unternehmen verarbeitet, insbesondere auch HR-Daten von europäischen Beschäftigten. Es gibt die Idee, dass bei einer Verarbeitung, wo sich der Angemessenheitsbeschluss nicht auf HR-Daten erstreckt, die Verarbeitung dieser Daten auf in Art. 46 Abs. 2 DS-GVO genannte Garantien zu stützen.

Somit würden zwei der in Kapitel V DS-GVO genannten Mechanismen bei ein und derselben Verarbeitung eingesetzt: Für Non-HR-Daten legitimiert der Angemessenheitsbeschluss die Übermittlung in ein Drittland, für HR-Daten hingegen eine der Art. 46 Abs. 2 DS-GVO dargestellten Garantien. Dabei wird argumentiert, dass Kapitel V die Übermittlung von Daten in ein Drittland behandelt, nicht jedoch eine Verarbeitung selbst.

Diese Argumentation berücksichtigt jedoch nicht, dass sowohl bei den verbindlichen internen Datenschutzvorschriften (Art. 47 DS-GVO, „Binding Corporate Rules“) als auch bei den von der EU-Kommission herausgegebenen Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DS-GVO, von der EU-Kommission „Standardvertragsklauseln“ genannt) immer auch die Verarbeitungen einbezogen sind, für welche die Verarbeitung der Daten erforderlich ist. Die Verarbeitung der HR-Daten ist nur erforderlich, weil Non-HR-Daten verarbeitet werden.

Daher wird eine Legitimation einer Übermittlung von personenbezogenen Daten in ein Drittland gestützt auf zwei Mechanismen, wovon ein Mechanismus ein Angemessenheitsbeschluss der EU-Kommission ist, vermutlich der Regelung in Art. 46 Abs. 1 DS-GVO widersprechen. Entsprechend der bisherigen Rechtsprechungspraxis des EuGH ist davon auszugehen, dass seitens des EuGH eine entsprechende Verwendung abgelehnt wird, sollte der EuGH sich im Rahmen einer Vorlage mit dieser Frage auseinandersetzen.

⁸⁶ Sie auch Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg „Tätigkeitsbericht 2023“, S. 103, Spalte 2: „Obwohl der Begriff „Beschäftigendaten“ durchaus nahelegt, dass darunter zumindest auch die Daten der Beschäftigten des jeweiligen Datenexporteurs – und gegebenenfalls auch anderer Stellen in der EU – fallen, sind damit nach dem Verständnis der US-Seite nur die Daten der Beschäftigten des jeweiligen Datenimporteurs in den USA gemeint.“ Online, zitiert am 2024-08-24; verfügbar unter <https://www.baden-wuerttemberg.datenschutz.de/taetigkeitsbericht-2023-zukunft-mit-datenschutz-gestalten/> bzw. pdf-Download unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

Insbesondere in Fällen, wo im deutschen Recht ausdrücklich ein Angemessenheitsbeschluss gefordert ist (wie beispielsweise in § 80 SGB X oder § 393 SGB V), stellt dies auf jeden Fall keine Lösung dar.

4.1.6 Auftragsverarbeitung:

4.1.6.1 Auftragnehmer muss Garantien zur Einhaltung DS-GVO vorweisen

Entsprechend Art. 28 Abs. 1 DS-GVO darf ein Verantwortlicher (= in den hier betrachteten Fällen der Leistungserbringer) nur Auftragsverarbeiter einsetzen, die **hinreichend Garantien** dafür **bieten**, dass geeignete **technische und organisatorische Maßnahmen so durchgeführt werden**, dass

- a) die Verarbeitung im Einklang mit allen Anforderungen der DS-GVO erfolgt und
- b) der Schutz der Rechte der betroffenen Person gewährleistet wird.

Diese Vorgabe muss über den gesamten Verarbeitungszeitraum erfüllt werden, d. h. eine alleinige Überprüfung vor Auftragsvergabe reicht nicht. Vielmehr muss regelmäßig überprüft werden, ob die Voraussetzungen für die Beauftragung des jeweiligen Dienstleisters auch weiterhin erfüllt sind. Sollten Vorkommnisse bekannt werden, die an der Erfüllung der Voraussetzungen zweifeln lassen, ist eine Überprüfung zwingend erforderlich. Im Kontext von Online-Terminmanagementsystemen wurde beispielsweise 2021 von diversen Presse-Verlagen über Sicherheitsprobleme beim Einsatz der Software Doctolib® berichtet,⁸⁷ was entsprechend den Vorgaben von Art. 28 Abs. 1 DS-GVO eine sofortige Überprüfung durch die Leistungserbringer, die diese Software einsetzen, zwingend verlangte.

Bescheinigungen von unabhängigen Dritten können den Anschein liefern, dass den Vorgaben genügt wird, zumindest, wenn die im Zertifikat bescheinigten Punkte auch tatsächlich die im Auftrag durchgeführte Verarbeitung betreffen. Dabei muss unbedingt die vorgelegte Bescheinigung betrachtet werden: Während Zertifikate i. d. R. Prozesse bewerten und somit auch eine gewisse Aussage über die nähere Zukunft nach der Zertifikatsbescheinigung erlauben, sind Testate von Wirtschaftsprüfern lediglich Bestandsaufnahmen zum testierten Zeitpunkt; schon einen Tag später können andere Voraussetzungen gelten. Testate haben zumeist unbegrenzt Gültigkeit, Zertifikate hingegen nur für einen begrenzten Zeitraum. Somit spielt die Art der Bescheinigung eines Dritten sowie die Aktualität eine Rolle bei der Bewertung der Geeignetheit eines Dienstleisters im Kontext der Auftragsvergabe.

Spätestens wenn Sicherheitsvorfälle bekannt werden, reichen Bescheinigungen von unabhängigen Dritten nicht mehr aus: Wenn der Sicherheitsvorfall trotz der Bescheinigung eintritt, kann die

⁸⁷ So z. B.

- Posteo: Chaos Computer Club findet Sicherheitslücken in Gesundheitsnetzwerken (2021-01-04) Online, zitiert am 2024-08-24; verfügbar unter <https://posteo.de/news/chaos-computer-club-findet-sicherheitsl%C3%BCcken-in-gesundheitsnetzwerken>
- Stuttgarter Nachrichten: Datenleck bei Patientenportal Doctolib (2021-07-08) Online, zitiert am 2024-08-24; verfügbar unter <https://www.stuttgarter-nachrichten.de/inhalt.doctolib-ist-die-patientenplattform-sicher-datenleck-bei-patientenportal-doctolib.144f6e1e-0e4e-407a-9a12-db34a84d69cb.html>
- Telepolis: Ist Doctolib ein Sicherheitsrisiko? (2021-08-23) Online, zitiert am 2024-08-24; verfügbar unter <https://www.telepolis.de/features/Ist-Doctolib-ein-Sicherheitsrisiko-6171673.html>
- Zeit Online: Ist Ihr Arzttermin sicher? (2021-06-23) Online, zitiert am 2024-08-24; verfügbar unter <https://www.zeit.de/digital/datenschutz/2021-06/doctolib-online-buchung-arzttermin-impftermin-datenschutz-sicherheitsluecke-patientendaten/komplettansicht>

Bescheinigung für die Bewertung, ob ein Dienstleister den Vorgaben von Art. 28 Abs. 1 DS-GVO genügt, allein wohl nicht als ausreichend angesehen werden.

Zu beachten: Bei einer Auftragsverarbeitung gilt i. d. R. für die Rechtsgrundlage der Verarbeitung des weisungsgebundenen Auftragsverarbeiters die des Verantwortlichen (= der jeweilige Leistungserbringer). Bei einer gemeinsamen Verantwortlichkeit (siehe Kapitel 4.1.7 sowie die Anmerkungen zur selbstständigen Verarbeitungstätigkeit durch einen Dienstleister in Kapitel 4.10) muss der ausgewählte Dienstleister einen vom Verantwortlichen unabhängigen Erlaubnistatbestand nach Art. 9 Abs. 2 DS-GVO vorweisen können.

4.1.6.2 Mandantentrennung muss zwingend beachtet werden

Leistungserbringer binden Dienstleister, d. h. externe Hersteller oder ggfs. auch einem Anbieter, deren Software sie nutzen, i. d. R. als Auftragsverarbeiter ein. Hierbei muss Art. 28 Abs. 10 DS-GVO beachtet werden:

„Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.“

Damit ein Auftragsverarbeitungsvertrag mit dem Dienstleister nicht zu einer Anwendung des Art. 28 Abs. 10 DS-GVO führt, müssen insbesondere folgende zwei Bedingungen erfüllt sein:

- 1) Im Auftragsverarbeitungsvertrag muss dem Dienstleister jegliche eigene Verarbeitung der Patientendaten verboten werden.
- 2) Der Dienstleister muss jegliche eigenverantwortliche Verarbeitung von Patientendaten unterlassen.

So **stellt die Zusammenführung von Patientendaten von verschiedenen Auftraggebern/Leistungserbringern**, z. B. um so einen Patienten übergreifend identifizieren zu können, **immer eine eigene Verarbeitung des Dienstleisters dar**, da der Auftraggeber nicht über die Daten anderer Auftraggeber verfügen darf. Eine entsprechende Zusammenführung darf somit nie auf Weisung eines Auftraggebers erfolgen. Sobald dies erfolgt, wird eine gemeinsame Verantwortlichkeit begründet, weshalb gemäß Art. 26 DS-GVO ein entsprechender Vertrag geschlossen werden muss.

Eine **Auftragsverarbeitung erfordert eine strenge Mandantentrennung**, sodass Patienten eines Leistungserbringers über einen gemeinsamen Auftragsverarbeiter nicht mit den Patientendaten anderer Leistungserbringer zusammengeführt werden dürfen.

4.1.7 Gemeinsame für die Verarbeitung Verantwortliche

Bietet der Dienstleister, welcher ein Online-Terminmanagementsystem Leistungserbringern zur Verfügung stellt, keine ausreichende Mandantentrennung an oder will er diese nicht einsetzen, so ist der Dienstleister nach Art. 28 Abs. 10 DS-GVO auch Verantwortlicher. In diesen Fällen muss zwischen dem Leistungserbringer und dem Dienstleister ein Vertrag gemäß Art. 26 DS-GVO ⁸⁸ geschlossen werden.

⁸⁸ Hinweise, wie ein entsprechender Vertrag aussehen könnte, finden sich z. B. in der Praxishilfe „Art. 26 DS-GVO: Gemeinsam Verantwortliche“ (Stand: 17. Juni 2018). Online, zitiert am 2024-08-24; verfügbar unter https://gesundheitsdatenschutz.org/html/gemeinsam_verantwortlich.php

Jeder Verantwortliche benötigt für seine eigene Verarbeitung jeweils eine eigene Rechtsgrundlage. D. h. sowohl der jeweilige Leistungserbringer als auch der Dienstleister müssen eine entsprechende Rechtsgrundlage nachweisen können.

4.1.8 Sicherheit der Verarbeitung

Art. 5 Abs. 1 lit. f DS-GVO verlangt, dass personenbezogene Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“. Um das angemessene Schutzniveau bestimmen und festlegen zu können, müssen der Schutzbedarf der Daten und das mit der Verarbeitung verbundene Risiko der Verarbeitung bestimmt werden, woraus sich dann die umzusetzenden technischen und organisatorischen Maßnahmen ableiten.

Hinsichtlich der Bewertung des Schutzbedarfs enthält ErwGr. 91 DS-GVO die Aussage, dass insbesondere die Sensibilität der Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt, sodass bei der Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien von Daten grundsätzlich von einem hohen oder sogar sehr hohen Schutzbedarf auszugehen ist. D. h. bei der Verarbeitung von sensiblen Daten wie Gesundheitsdaten, genetischen Daten oder auch biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist stets von einem hohen Risiko und damit auch von einem hohen Schutzbedarf auszugehen.

Jede Verarbeitung personenbezogener Daten beinhaltet grundsätzlich ein Risiko für die betroffene Person, deren Daten verarbeitet werden. Die Risiken müssen aus Sicht der betroffenen Person betrachtet werden: Relevant ist, welche Risiken für die betroffene Person existieren. In Deutschland werden häufig nur materielle Risiken (Finanzen, Gesundheit, ...) betrachtet, was u. a. an unserer zivilrechtlichen Rechtsprechung bzgl. Haftung liegt. Europarechtlich sind auch immaterielle Risiken zu betrachten, beispielsweise, wenn eine unbefugte Offenbarung von Geheimnissen bei der betroffenen Person Betroffenheit oder ein Schamgefühl auslöst oder zu einer Diskriminierung/Stigmatisierung führt. ErwGr. 75 und 83 DS-GVO führen beispielhaft verschiedene Risiken auf. Entsprechend ErwGr. 83 ist es unerheblich, ob die Risiken aus einer beabsichtigten, einer unbeabsichtigten oder auch einer unrechtmäßigen Handlung resultieren; daher müssen bei der Entwicklung einer Software-Lösung hinsichtlich der Verpflichtung zur Gewährleistung der IT-Sicherheit immer auch fehlerhafte oder unbeabsichtigte Handlungen berücksichtigt werden.

4.1.9 Meldepflicht von Datenpannen

Entsprechend Art. 33 DS-GVO sind Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an die Aufsichtsbehörde zu melden, „es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“ Der Begriff „Verletzung des Schutzes personenbezogener Daten“ wird dabei in Art. 4 Ziff. 12 DS-GVO definiert als

„eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Erläuternd findet sich in ErwGr. 75 DS-GVO dazu:

„Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem **Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten**, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann [...]“.

Auch in ErwGr. 85 DS-GVO wird auf diese Tatbestände verweisen:

„[...] wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, **Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten** oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile [...]“.

Es sollte bei einem Einsatz von Dienstleistern daher immer daran gedacht werden, dass ein Verstoß gegen

- die sich aus dem ärztlichen Berufsrecht resultierende Verschwiegenheitspflicht (siehe zur Vorschrift auch die Ausführungen in Kapitel 4.2) oder gegen
- das sich aus dem § 203 StGB (siehe zur Vorschrift auch die Ausführungen in Kapitel 4.3) resultierende Verbot der unbefugten Offenbarung (§ 203 Abs. 1 Ziff. 1 StGB adressiert medizinische Berufe, entspricht daher auch der Vorgabe aus den Erwägungsgründen der DS-GVO)

zu einem nach Art. 33 DS-GVO meldepflichtigen Tatbestand führen kann.

Analog kann sich eine Meldepflicht nach Art. 34 DS-GVO ergeben, sodass der Patient entsprechend informiert werden muss.

4.2 Ärztliche Schweigepflicht: Berufsrecht

Der in § 9 MBO-Ä geregelten ärztlichen Schweigepflicht unterliegt alles, was einer Ärztin oder einem Arzt in seiner/ihrer beruflichen Eigenschaft anvertraut wurde oder sonst bekannt geworden ist.⁸⁹ Dies umfasst nicht nur fremde Geheimnisse i. S. d. § 203 StGB, sondern alle nicht allgemein bekannten Tatsachen.⁹⁰ Nur Tatsachen, die beliebigen Dritten bekannt sind (z. B. weil ein Patient die Daten im Internet frei zugänglich veröffentlichte), unterliegen nicht der Schweigepflicht.⁹¹ Darüber hinaus gilt die ärztliche Schweigepflicht uneingeschränkt, d. h. gegenüber jedem, der nicht in das

⁸⁹ Wollersheim U.: § 6 Ärztliches Berufsrecht, Rn. 152. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. h. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9

⁹⁰ Scholz K.: § 9 MBO-Ä Rn. 2. In: Spickhoff (Hrsg.) Medizinrecht. C. H. Beck Verlag, 3. Auflage 2018. ISBN 978-3-406-72099-4

⁹¹ Lippert H-D: § 9 Rn. 4. in Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

Arzt-Patienten-Verhältnis einbezogen ist.⁹² Entsprechend § 9 Abs. 1 S. 1 MBO-Ä dauert die Schweigepflicht grundsätzlich über den Tod des Patienten hinaus.

Weiterhin geht § 9 MBO-Ä in gewisser Weise über den Schutz in § 203 StGB enthaltenen Schutz hinaus, da von § 9 MBO-Ä **auch fahrlässige Verstöße** erfasst werden.⁹³

Grundsätzlich muss ein Patient, dessen Behandlungsdaten für biomedizinische Forschung herangezogen werden sollen, hierin gesondert einwilligen und den Arzt von seiner beruflichen Schweigepflicht entbinden.⁹⁴ **Bleibt die Identität des Patienten hingegen anonym, kann die Einwilligung – analog zu § 203 StGB – entfallen.**⁹⁴

Hinweis: Verletzt ein Arzt oder eine Ärztin die Schweigepflicht, können hieraus berufs- und standesrechtliche Konsequenzen durch die kammerbezogene Berufsgerichtsbarkeit resultieren. Die Heilberufsgesetze bzw. die Kammergesetze für Heilberufe der Länder enthalten Vorgaben, wonach ein Pflichtverstoß beispielsweise durch nachfolgend aufgeführte Sanktionen geahndet werden kann:⁹⁵

- Verwarnung
- Verweis
- Entziehung des aktiven Berufswahlrechts
- Entziehung des passiven Berufswahlrechts
- Geldbuße
- Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten
- Feststellung der Unwürdigkeit zur Ausübung des Berufs

Genauerer regeln die Landesgesetze für kammergerichtliche Verfahren:

Bundesland	Mögliche Sanktionen
BW (§ 58 HBKG BW)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 50.000 Euro
BY (§ 67 HKaG BY)	<ul style="list-style-type: none"> • Verwarnung • Geldbuße bis zu 100.000 Euro
BE (§ 76 BlnHKG)	<ul style="list-style-type: none"> • Verwarnung • Geldbuße bis zu 100.000 Euro

⁹² Lippert H-D: § 9 Rn. 7. In Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

⁹³ So z. B.

- Wollersheim U.: § 6 Ärztliches Berufsrecht, Rn. 153. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. h. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9
- Sobotta D.: § 9 MBO-Ä Rn. 2. In Bergmann/Pauge/Steinmeyer (Hrsg.) Gesamtes Medizinrecht. Nomos, 3. Auflage 2018. ISBN 978-3-8487-2318-8
- Scholz K.: § 9 MBO-Ä Rn. 2. In: Spickhoff (Hrsg.) Medizinrecht. C. H. Beck Verlag, 3. Auflage 2018. ISBN 978-3-406-72099-4

⁹⁴ Lippert H-D: § 9 Rn. 40. In Ratzel R, Lippert H-D, Prütting J. (Hrsg.) Kommentar zur (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997. Springer Verlag, 7. Auflage 2018. ISBN 978-3-662-55165-3

⁹⁵ Katzenmeier C.: IX. Berufsgeheimnis und Dokumentation, Rn. 5. In: Laufs/Katzenmeier/Lipp - Arztrecht. C. h. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9

Bundesland	Mögliche Sanktionen
	<ul style="list-style-type: none"> • Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten • Feststellung der Unwürdigkeit zur Ausübung des Berufs
BB (§ 59 HeilBerG BB)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HB (§ 65 HeilBerG HB)	<ul style="list-style-type: none"> • Verwarnung • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 25.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HH (§ 3 HeilBerGerG HA)	<ul style="list-style-type: none"> • Verwarnung • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
HE (§ 50 HeilBerG HE)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 100.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
MV (§ 64 HeilBerG MV)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
NI (§ 63 HKG NI)	<ul style="list-style-type: none"> • Verweis • Geldbuße bis zu 100.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
NW (§ 60 HeilBerG NW)	<ul style="list-style-type: none"> • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 100.000 Euro • Teilnahme an einer bestimmten Fortbildung zur Qualitätssicherung auf eigene Kosten • Feststellung der Unwürdigkeit zur Ausübung des Berufs
RP (§ 52 HeilBG RP)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Geldbuße bis zu 200.000 Euro
SL (§ 33 SHKG)	<ul style="list-style-type: none"> • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts

Bundesland	Mögliche Sanktionen
	<ul style="list-style-type: none"> • Geldbuße bis zu 50.000 Euro
SN (§ 55 SächsHKaG)	<ul style="list-style-type: none"> • Verweis • Geldbuße bis zu 50.000 Euro
ST (§ 48 KGHB-LSA)	<ul style="list-style-type: none"> • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 25.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs
SH (§ 58 HBKG SH)	<ul style="list-style-type: none"> • Verweis • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro
TH (§ 48 ThürHeilBG)	<ul style="list-style-type: none"> • Verwarnung • Verweis • Entziehung des aktiven Berufswahlrechts • Entziehung des passiven Berufswahlrechts • Geldbuße bis zu 50.000 Euro • Feststellung der Unwürdigkeit zur Ausübung des Berufs

Weiterhin ist zu beachten, dass gemäß § 5 Abs. 2 i. V. m. § 3 Abs. 1 S. 1 Nr. 2 Bundesärzteordnung eine Approbation widerrufen werden kann, wenn sich eine Ärztin oder ein Arzt eines Verhaltens schuldig gemacht hat, aus dem sich seine Unwürdigkeit oder Unzuverlässigkeit zur Ausübung des ärztlichen Berufs ergibt. Insbesondere kann neben einer kammerbezogenen Berufsgerichtsbarkeit somit auch ein Verstoß gegen § 203 StGB und ein daraus resultierendes Urteil ebenfalls zum Widerruf einer Approbation führen; jedoch erfolgte bis heute bei keiner Ärztin und keinem Arzt in Deutschland (siehe Stand der Ausarbeitung) aufgrund eines Verstoßes gegen § 203 StGB ein Widerruf der Approbation.

4.3 Verschwiegenheits-/Schweigepflicht von anderen Berufsordnungen

Alle in Kapitel 1.1 aufgeführten enthalten Verschwiegenheits- bzw. Schweigepflichten ähneln oder entsprechen denen der ärztlichen Schweigepflicht. Daher können die in Kap. 4.2 enthalten Aussagen auch auf die Vorgaben dieser Berufsordnungen übertragen werden.

Zu diesen Berufsordnungen gibt es im Vergleich zur ärztlichen Berufsordnung nur wenig Rechtsprechung, jedoch existieren zu einigen Berufsordnungen Kommentare, die häufig vom Normersteller, z. B. der jeweiligen Kammer, herausgegeben werden.

4.4 Verbot der unbefugten Offenbarung: Strafrecht

§ 203 StGB schützt die Geheimnisse sowohl von natürlichen als auch von juristischen Personen⁹⁶ oder Personenverbänden⁹⁷, geht also über den aus dem Datenschutzrecht resultierendem Schutz der

⁹⁶ Cierniak/Niehaus § 203 Rn. 31. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8

⁹⁷ Kargl W.: § 203 Rn. 6. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

„personenbezogenen Daten“ hinaus. Allerdings müssen die Geheimnisse einer bestimmten oder bestimmbar natürlichen oder juristischen Person zuordenbar sein, damit die Geheimnisse unter den Schutz von § 203 StGB fallen.⁹⁸ Neben zu natürlichen Personen gehörenden Informationen wie beispielsweise Patientendaten können somit beispielsweise auch Betriebs- oder Geschäftsgeheimnisse zu den geschützten Geheimnissen gehören.⁹⁹ Auch wenn Dritte wie beispielsweise Ehepartner Geheimnisse eines Geheimnisbetroffenen wie z. B. eines Patienten oder Mandanten einem Arzt, Rechtsanwalt usw. anvertrauen, sind diese Geheimnisse geschützt – vorausgesetzt der jeweilige Patient oder Mandant, also der Geheimnisbetroffene selbst, hat ein eigenes Interesse an der Wahrung dieses Drittgeheimnisses.¹⁰⁰

Die Reichweite von § 203 StGB ist sehr weit: Geschützt sind fremde Geheimnisse, auch „Bagatellinformationen“ oder illegale Geheimnisse; auf einen moralisch billigen Inhalt kommt es bei dem Begriff des „Geheimnisses“ nicht an.¹⁰² Es muss sich bei den Geheimnissen um „Tatsachen“ handeln. Unter Tatsachen sind alle Informationen zu verstehen, die sich auf die Person des Betroffenen sowie seine Lebensverhältnisse beziehen. Werturteile sind damit zwar ausgeschlossen; allerdings kann als Tatsache der Umstand erfasst werden, dass eine Person eine bestimmte „Meinung“ vertritt.¹⁰¹ Auch Schlussfolgerungen fallen unter den Tatsachenbegriff, da hier Befundtatsache und Wertung untrennbar verbunden sind.¹⁰¹ Bei „Tatsachen“ kann es sich also um Informationen nahezu beliebiger Art handeln, die sich auf jeden denkbaren Lebensbereich beziehen.¹⁰²

Im Gesundheitsbereich handelt es sich bei den von § 203 StGB geschützten Geheimnissen allerdings überwiegend um Geheimnisse von natürlichen Personen, d. h. die bei der Patientenbetreuung oder -behandlung den von § 203 StGB adressierten Berufsgruppen wie Ärzten oder Pflegepersonal bekannt gewordenen (Patienten-)Informationen. Auch in diesem Umfeld ist die Reichweite des Schutzanspruches von § 203 StGB entsprechend der grundsätzlichen Ausrichtung der Regelung sehr weit¹⁰³: „Die ärztliche Schweigepflicht umfasst alle Erkenntnisse, die sich aus der ärztlichen

⁹⁸ Heger M.: § 203 StGB, Rn. 15. In: Lackner/Kühl (Hrsg.) Strafgesetzbuch: StGB. C. H. Beck Verlag, 29. Auflage 2018. ISBN 978-3-406-70029-3

⁹⁹ So z. B.

- Altenhain: § 203 StGB Rn. 19. In: Matt / Renzikowski (Hrsg.) Strafgesetzbuch: StGB. Vahlen Verlag, 2. Auflage 2020. ISBN 978-3-8006-4981-5
- Kargl W.: § 203 Rn. 6. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

¹⁰⁰ Eisele § 203 Rn. 8. In Schönke / Schröder (Hrsg.) Strafgesetzbuch: StGB. 30. Auflage 2019. ISBN 978-3-406-70383-6

¹⁰¹ Kargl W.: § 203 Rn. 6. In Kindhäuser / Neumann / Paeffgen (Hrsg.) Strafgesetzbuch. 5. Auflage 2017. ISBN 978-3-8487-3106-0

¹⁰² Weidemann M.: § 203, Rn. 6. In: Heintschel-Heinegg (Hrsg.) BeckOK StGB. C. H. Beck Verlag, 52. Edition Stand: 01.02.2022

¹⁰³ So z. B.

- Buckstegge: § 15 Datenschutz im Gesundheitswesen, Rn. 60. In: Saalfrank (Hrsg.) Handbuch des Medizin- und Gesundheitsrechts. Wissenschaftliche Verlagsgesellschaft, 9. EL August 2020. ISBN 978-3-8047-4126-3
- Hilgendorf E.: Einführung in das Medizinstrafrecht, 9. Kapitel. Die ärztliche Schweigepflicht, Rn. 20. C. H. Beck Verlag, 2. Auflage 2020. ISBN 978-3-406-74091-6
- Katzenmeier: IX. Berufsgeheimnis und Dokumentation, Rn. 12. In: Laufs / Katzenmeier / Lipp. Arztrecht. C. H. Beck Verlag, 8. Auflage 2021. ISBN 978-3-406-73675-9
- Sommer U, Tsambikakis M.: § 3 Strafrechtliche Arzthaftung, Rn. 110. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9

Behandlung ergeben und bezieht sich auf alle Umstände, die der Arzt im Rahmen der Behandlung in Erfahrung gebracht hat.¹⁰⁴ **Beispielsweise fällt schon die Anbahnung eines Behandlungsverhältnisses¹⁰⁵ wie eine Terminvereinbarung mit einem Arzt oder der Aufenthalt in einer Arztpraxis¹⁰⁶ oder einem Krankenhaus in den Schutzbereich von § 203 StGB**, ebenso die Ablehnung der Behandlung oder eine Bitte um ein falsches Gesundheitszeugnis¹⁰⁷. Ärzte sind grundsätzlich - unabhängig vom konkreten Rechtsverhältnis zum Patienten - zur Verschwiegenheit verpflichtet. Eine vertragliche Grundlage ist für das Anvertrauen nicht erforderlich,¹⁰⁸ relevant ist lediglich, ob ein Privatgeheimnis einer Person im Kontext eines der in § 203 Abs. 1 Nr. 1 StGB genannten Berufe anvertraut wurde („[...] ihm als [...]anvertraut worden oder sonst bekanntgeworden ist, [...]“).

Die strafrechtliche Schweigepflicht gilt nicht nur für die Ärzte: § 203 Abs. 1 StGB umfasst alle staatlich geregelten Berufe im Gesundheitsbereich,¹⁰⁹ wozu beispielsweise auch Krankenpflegepersonal, medizinisch-technische und pharmazeutisch-technische Assistenten, Hebammen oder auch medizinische Fachangestellte. Personen, die nicht direkt vom Gesetz selbst zur Verschwiegenheit adressiert werden wie beispielsweise IT-Dienstleister, dürfen nur eingesetzt werden, wenn diese Personen entsprechend § 203 Abs. 4 Nr. 1 StGB von der zur gesetzlichen Verschwiegenheit betroffenen beauftragenden Person zur gesetzlichen Verschwiegenheit verpflichtet wurden.

-
- Ulsenheimer K.: § 140 Der objektive Tatbestand der §§ 203, 204 StGB, Rn. 2. In: In: Laufs/Kern/Rehborn (Hrsg.) Handbuch des Arztrechts. C. H. Beck Verlag, 5. Auflage 2019. ISBN 978-3-406-65614-9
 - Ulsenheimer K, Gaede K.: Teil 8 Die Verletzung der ärztlichen Schweigepflicht (§§ 203-205 StGB) und das Sanktionsregime der DSGVO, Rn. 1045. In: Ulsenheimer/Gaede (Hrsg.) Arztstrafrecht in der Praxis. C. F. Müller Verlag, 6. Auflage 2021. ISBN 978-3-8114-0642-1
 - von Bar N: Gesetzlich nicht normierte ärztliche Auskunfts- und Offenbarungspflichten. In: § 3: Der Umfang der ärztlichen Schweigepflicht, B Strafrechtlicher Umfang, III.1.b)aa) Springer-Verlag, 1. Auflage 2017. ISBN 978-3-662-53798-5
 - Wollersheim U.: § 6 Ärztliches Berufsrecht, Rn. 152. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-72937-9

¹⁰⁴ So z. B.

- Weidemann M.: § 203, Rn. 6.2. In: Heintschel-Heinegg (Hrsg.) BeckOK StGB. C. H. Beck Verlag, 52. Edition Stand: 01.02.2022
- Götze C. Durchbrechung der ärztlichen und psychotherapeutischen Schweigepflicht bei in sicherheitsrelevanten Berufen tätigen Patienten. In: Teil 2: Umfang der ärztlichen bzw. psychotherapeutischen Schweigepflicht, C.I.2.a. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-5500-4

¹⁰⁵ Hansen C. (2020) Praxisveräußerung - Rechtssicherer Umgang mit Patientendaten im Rahmen der Praxisnachfolge. MedR: 663-669

¹⁰⁶ Cierniak/Niehaus § 203 Rn. 26. In Münchener Kommentar zum Strafgesetzbuch Band 4: §§ 185-262, 4. Aufl. 2021, ISBN 978-3-406-74604-8

¹⁰⁷ Ulsenheimer K.: § 140, Rn. 11. In: Laufs/Kern/Rehborn (Hrsg.) Handbuch des Arztrechts. C. H. Beck Verlag, 5. Auflage 2019. ISBN 978-3-406-65614-9

¹⁰⁸ Cierniak J, Niehaus H.: § 203 StGB, Rn. 51. In: Erb/Schäfer/Sander (Hrsg.) Münchener Kommentar zum Strafgesetzbuch: StGB, Band 4: §§ 185-262. C. H. Beck Verlag 4. Auflage, 2021. ISBN 978-3-406-74604-8

¹⁰⁹ Siehe z. B.

- Cierniak J, Niehaus H.: § 203 StGB, Rn. 37. In: Erb/Schäfer/Sander (Hrsg.) Münchener Kommentar zum Strafgesetzbuch: StGB, Band 4: §§ 185-262. C. H. Beck Verlag 4. Auflage, 2021. ISBN 978-3-406-74604-8
- Kargl W.: § 203 StGB, Rn. 48. In: Kindhäuser/Neumann/Paeffgen/Salige Hrsg.) Strafgesetzbuch: StGB. Nomos Verlag 6. Auflage, 2023. ISBN: 978-3-8487-7123-3
- Weidemann M.: § 203 StGB, Rn. 16-23. In: . Heintschel-Heinegg/Kudlich (Hrsg.) BeckOK StGB. 62. Edition, Stand: 2024-08-01

Der strafrechtliche Geheimnisschutz umfasst also deutlich mehr Informationen als Diagnosen und Therapien.

Nicht unter den Schutz von § 203 StGB fallen offenkundige Tatsachen. Eine Tatsache gilt so lange als nicht offenkundig und ist damit von § 203 StGB geschützt, wie diese Tatsache nur einem begrenzten Personenkreis bekannt ist und selbst fachkundige Dritte von dieser Tatsache nur schwer Kenntnis erlangen können.¹¹⁰ Solange die Kenntnis auf einen begrenzten Personenkreis beschränkt bleibt, führt die Mitteilung der Tatsache an weitere Dritte innerhalb dieses Kreises, selbst wenn dieser sehr groß ist, nicht zur Offenkundigkeit und der Schutz von § 203 StGB bleibt erhalten. Zum Inneren des Personenkreises zählen beispielsweise auch nicht-medizinische Personen wie Rechtsanwälte, die beim Vorwurf eines Behandlungsfehlers eingebunden werden, oder IT-Dienstleister des Berufsgeheimnisträgers, die entsprechend auf § 203 StGB verpflichtet wurden.

4.5 Dokumentationspflicht der Patientenbehandlung

Der Umfang der Dokumentationspflicht ergibt sich aus § 630f Abs. 2 BGB:

„Der Behandelnde ist verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen.“

Die Aufzählung in § 630f Abs. 2 S. 1 BGB ist keine abschließende, sondern eine beispielhafte Aufzählung („insbesondere“). In die Dokumentation müssen somit alle wesentlichen diagnostischen und therapeutischen Maßnahmen und Verlaufsdaten Eingang finden. Dazu können neben der in § 630f Abs. 2 S. 1 BGB aufgeführten Vorgaben beispielsweise Informationen wie ärztliche Anordnungen zur Pflege oder Namen von Operateuren gehören, desgleichen Behandlungsverweigerungen wie auch Beschwerden eines Patienten.¹¹¹

Die Einbeziehung von Aufklärungen und Einwilligungen in den Kreis der dokumentationspflichtigen Umstände durch § 630f Abs. 2 BGB zeigt, dass neben diagnostischen und therapeutischen Daten auch Umstände in die Dokumentation aufzunehmen sind, die für das Selbstbestimmungsrecht des Patienten von Bedeutung sind.¹¹²

Eine Dokumentation, die aus medizinischer Sicht nicht erforderlich ist, ist auch aus Rechtsgründen nicht geboten.¹¹³ Nicht dokumentarisch festgehalten zu werden brauchen medizinische

¹¹⁰ Altenhain: § 203 StGB, Rn. 15. In: Matt/Renzikowski (Hrsg.) Strafgesetzbuch. Verlag Franz Vahlen, 2. Auflage 2020. ISBN 978-3-8006-4981-5

¹¹¹ Katzenmeier C.: § 630f BGB, Rn. 13. In: Hau/Poseck (Hrsg.) BeckOK BGB. 70. Edition, Stand: 01.05.2024

¹¹² Wagner G.: § 630f BGB, Rn. 8. In: Henssler/ Krüger (Hrsg.) Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB, Band 5. C. H. Beck Verlag, 9. Auflage 2023. ISBN 978-3-406-76675-6

¹¹³ So zu finden bspw.:

- Spickhoff: § 630f BGB, Rn. 6. In: Spickhoff. Medizinrecht. C. H. Beck Verlag, 4. Auflage 2022. ISBN 978-3-406-78835-2
- Wagner G.: § 630f BGB, Rn. 10. In: Henssler/ Krüger (Hrsg.) Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB, Band 5. C. H. Beck Verlag, 9. Auflage 2023. ISBN 978-3-406-76675-6

Selbstverständlichkeiten sowie bloße ärztliche Vermutungen und ungesicherte Befunde, die nach allgemein anerkannten Regeln zum Dokumentationszeitpunkt irrelevant sind.¹¹⁴

Daher gehören Terminplanungen nicht zu der gesetzlich vorgeschriebenen Dokumentation der Patientenbehandlung. Zwar ist der Zeitpunkt einer Diagnosestellung oder Behandlung für derzeitige oder künftige Behandlungen relevant, jedoch nicht die Terminvereinbarung an sich. D. h. die Terminplanung unterliegt nicht der in § 630f BGB verankerten Dokumentationspflicht, insbesondere kann auch nicht der in § 630f Abs. 10 BGB angegebene Aufbewahrungszeitraum für diese Daten als Rechtsgrundlage für die Speicherung angesehen werden.

4.6 Behandlungspflicht: Dürfen Patienten, die eine Online-Terminvereinbarung nicht nutzen möchten, abgelehnt werden?

Die Ablehnung eines Patienten, welcher eine Online-Terminvereinbarung nicht nutzen möchte, durch ein zur Versorgung gesetzlicher versicherter Patienten berechtigtes Krankenhaus oder einem niedergelassenen Vertragsarzt wird regelhaft rechtswidrig erfolgen.

4.6.1 Versorgungspflicht bei Krankenhäusern

Erhalten Krankenhäuser entsprechend § 109 Abs. 4 S. 1 SGB V einen Versorgungsauftrag zur Krankenhausbehandlung gesetzlich versicherter Patienten, so besteht entsprechend § 109 Abs. 4 S. 2 SGB V eine Verpflichtung zur in § 39 SGB V definierten Krankenhausbehandlung, was eine vollstationäre, stationsäquivalente, tagesstationäre, teilstationäre, vor- und nachstationäre sowie ambulante Behandlung durch Krankenhäuser umfasst. Aus der Zulassung zur Krankenhausbehandlung ergibt sich gemäß § 109 Abs. 4 S. 2 SGB V daher eine gesetzlich verankerte Behandlungspflicht.¹¹⁵

Allerdings unterliegen Krankenhäuser bzgl. der Einhaltung des Versorgungsauftrags i. d. R. keiner Rechtsaufsicht. Vielmehr müssen auf die Einhaltung dieser sozialversicherungsrechtlich begründeten Pflicht die sozialversicherungsrechtlichen Partner des Krankenhauses achten, insbesondere also die gesetzlichen Krankenkassen.¹¹⁶

¹¹⁴ So zu finden bspw.:

- Glanzmann: § 630f BGB, Rn. 7. In: Bergmann/Paue/Steinmeyer (Hrsg.) *Gesamtes Medizinrecht*. Nomos Verlag, 4. Auflage 2024. ISBN 978-3-8487-7153-0
- Katzenmeier C.: § 630f BGB, Rn. 15. In: Hau/Poseck (Hrsg.) *BeckOK BGB*. 70. Edition, Stand: 01.05.2024

¹¹⁵ So zu finden bspw.:

- Penner A.: § 109 SGB V, Rn. 43. In: Rolfs/Giesen/Mießling/Udsching (Hrsg.) *BeckOK Sozialrecht*. 73. Edition, Stand: 01.06.2024
- Quaas M.: § 27 Die Rechtsbeziehungen zwischen den gesetzlichen Krankenkassen und den Krankenhäusern einschließlich Vorsorge- und Rehabilitationseinrichtungen nach dem SGB V, Rn. 88 ff. In: Quaas / Zuck / Clemens (Hrsg.) *Medizinrecht*. Verlag C. H. Beck, 4. Auflage 2018. ISBN 978-3-406-70773-5

¹¹⁶ Stollmann F, Wollschläger A.: § 79 Die Aufgaben der Krankenhäuser im gesundheitlichen Versorgungssystem, Rn. 64. In: Laufs/Kern/Rehborn (Hrsg.) *Handbuch des Arztrechts*. Verlag C. H. Beck, 5. Auflage 2019. ISBN 978-3-406-65614-9

4.6.2 Versorgungspflicht von niedergelassene Vertragsärzten/Vertragszahnärzten

Entsprechend § 95 Abs. 3 S. 1 SGB V ist ein Vertragsarzt Mitglied der für seinen Kassenarztsitz zuständigen Kassenärztlichen Vereinigung und zur Teilnahme an der vertragsärztlichen Versorgung berechtigt, aber auch verpflichtet.¹¹⁷

Mit der Zulassung zur Teilnahme an der vertrags- bzw. vertragszahnärztlichen Versorgung wird der Arzt also nicht nur berechtigt, sondern auch verpflichtet, gesetzlich Versicherte zu behandeln.¹¹⁸ Nicht nur eine vollständige Zurückweisung einer versicherten Person durch den aufgesuchten Arzt, sondern auch die nur teilweise erfolgende Verweigerung aller erforderlichen und wirtschaftlichen Leistungen begründen eine Pflichtverletzung.¹¹⁸

Jedoch besitzt ein Patient keinen Anspruch auf eine nicht wirtschaftliche oder nicht erforderliche Leistung. Auch kann ein Patient von einem Vertragsarzt nicht die Erbringung einer Nicht-Kassenleistung verlangen.

Entsprechend § 13 Abs. 7 S. 3 Bundesmantelvertrag-Ärzte¹¹⁹ (Fassung vom 12. Juni 2024, Inkrafttreten 2024-07-01) darf ein Vertragsarzt die Behandlung eines Versicherten nur in begründeten Fällen ablehnen. Entsprechend kann ein Vertragsarzt Besuche außerhalb seines üblichen Praxisbereiches ablehnen, es sei denn, dass es sich um einen dringenden Fall handelt und ein Vertragsarzt, in dessen Praxisbereich die Wohnung des Kranken liegt, nicht zu erreichen ist (§ 17 Abs. 4 BMV-Ä). Eine Ablehnung ist auch möglich, wenn ein Patient seine gültige elektronische Gesundheitskarte nicht vorlegt (§ 19 BMV-Ä).

Ansonsten kann ein Vertragsarzt nur in begründeten Fällen eine Behandlung ablehnen. Eine Ablehnung erfordert in diesen Fällen immer eine Abwägung, inwieweit dem aufgesuchten Arzt eine Behandlungsübernahme zumutbar ist oder einer Behandlung aner kennenswerte Gründe entgegenstehen.¹²⁰ Insbesondere muss die Dringlichkeit einer Behandlung und die Möglichkeit des Versicherten, ausreichend zeitnah eine Behandlung durch einen anderen Arzt erhalten zu können, bei der Abwägung berücksichtigt werden. Im Falle einer Behandlungsverweigerung muss der Arzt der zuständigen gesetzlichen Krankenkasse die Gründe der Ablehnung auf deren Nachfrage darlegen. In der Literatur finden sich als Beispiele für begründete Fälle einer Behandlungsverweigerung:¹²¹

¹¹⁷ Entsprechend urteilte bspw. LSG Nordrhein-Westfalen (11. Senat), Urteil vom 19.02.2014 - L 11 KA 42/12, Rn. 36: „Diese Behandlungspflicht resultiert gemäß § 95 Abs. 3 Satz 1 SGB V aus der Zulassung des Vertragsarztes und den Bestimmungen der Bundesmantelverträge, die für den Vertragsarzt verbindlich sind“. Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2014,8254>, Volltext unter <https://openjur.de/u/687706.html>

¹¹⁸ Siehe z. B.

- Hesral H.: Kap. 1. Disziplinarverfahren – materielles Recht, Rn. 91. In: Ehlers (Hsrg.) Disziplinarrecht für Ärzte und Zahnärzte. Verlag C. H. Beck, 2. Auflage 2013. ISBN 978-3-406-58905-8
- Wigge P.: § 2 Die Rechtsstellung des Vertragsarztes, Rn. 52. In: Schnapp/Wigge (Hsrg.) Handbuch des Vertragsarztrechts. Verlag C. H. Beck, 3. Auflage 2017. ISBN 978-3-406-70942-5

¹¹⁹ Kassenärztliche Bundesvereinigung KdöR: Bundesmantelvertrag (BMV). Online, zitiert am 2024-08-24; verfügbar unter <https://www.kbv.de/html/bundesmantelvertrag.php>

¹²⁰ Hesral H.: Kap. 1. Disziplinarverfahren – materielles Recht, Rn. 95. In: Ehlers (Hsrg.) Disziplinarrecht für Ärzte und Zahnärzte. Verlag C. H. Beck, 2. Auflage 2013. ISBN 978-3-406-58905-8

¹²¹ Z. B.:

- Hesral H.: Kap. 1. Disziplinarverfahren – materielles Recht, Rn. 96. In: Ehlers (Hsrg.) Disziplinarrecht für Ärzte und Zahnärzte. Verlag C. H. Beck, 2. Auflage 2013. ISBN 978-3-406-58905-8
- Wigge P.: § 2 Die Rechtsstellung des Vertragsarztes, Rn. 52. In: Schnapp/Wigge (Hsrg.) Handbuch des Vertragsarztrechts. Verlag C. H. Beck, 3. Auflage 2017. ISBN 978-3-406-70942-5

- Persönliche Umstände in der Arzt-Patientenbeziehung wie beispielsweise schwere Beleidigungen, Verleumdungen oder Strafanzeige wegen Körperverletzung nach früherer ärztlicher Behandlung;
- Erreichen der oberen Kapazitätsgrenze der Kassenpraxis, d.h. es wünschen mehr Kassenpatienten eine Behandlung als dem Arzt angesichts der Zahl der behandelten Kassenpatienten möglich ist; in Notfallsituationen kann eine Ablehnung aus diesem Grund jedoch auch pflichtwidrig erfolgen.

Grundsätzlich keine rechtfertigenden Gründe für die Ablehnung einer Behandlung stellen insbesondere folgende Umstände dar:¹²²

- Hinweis auf ein ausgeschöpftes Budget oder
- drohende Honorarkürzung nach Wirtschaftlichkeitsprüfung wegen Überschreitens des Arztgruppendurchschnitts.

4.6.3 Betreuungspflicht durch Betriebsärzte

4.6.3.1 Rechte der Arbeitnehmer auf betriebsärztliche Betreuung

Die arbeitsmedizinische Betreuung und Vorsorge gehören zu den Pflichten des Arbeitgebers. Der Arbeitgeber darf die Erbringung dieser Pflicht nicht durch technische oder organisatorische Maßnahmen erschweren. In der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) wird der Zugang zur arbeitsmedizinischen Betreuung weiter konkretisiert:

- § 3 Abs. 1 ArbMedVV: Arbeitgeber sind verpflichtet, den Arbeitnehmern eine arbeitsmedizinische Vorsorge anzubieten. Hierzu gehört auch, dass der Arbeitnehmer Zugang zu einem Betriebsarzt haben muss.
- § 3 Abs. 3 ArbMedVV: Die Vorsorge soll „während der Arbeitszeit stattfinden.“ Dies impliziert, dass dem Arbeitnehmer ein einfacher Zugang zur betriebsärztlichen Betreuung ermöglicht werden muss.

Diese Regelungen legen nahe, dass der Zugang zur arbeitsmedizinischen Betreuung für den Arbeitnehmer so niederschwellig wie möglich sein sollte und keine technischen Barrieren (wie die ausschließliche Nutzung eines Online-Terminvereinbarungssystems) errichtet werden dürfen, die den Zugang erschweren.

Neben den Pflichten des Arbeitgebers sind auch die Rechte der Arbeitnehmer zu berücksichtigen. Arbeitnehmer haben ein Anrecht auf regelmäßige Vorsorgeuntersuchungen und präventive Maßnahmen durch einen Betriebsarzt, die auf Grundlage der Gefährdungsbeurteilung des Arbeitgebers erfolgen. Diese Rechte ergeben sich insbesondere aus:

- § 3 Arbeitssicherheitsgesetz (ASiG), der die Aufgaben von Betriebsärzten und Fachkräften für Arbeitssicherheit regelt. Der Betriebsarzt hat die Aufgabe, „den Arbeitgeber bei allen Fragen

¹²² BSG, Urt. v. 2001-03-14 Az. B 6 KA 54/00: „Schon auf der Grundlage der bisherigen Rechtsprechung des Senats zum Recht der vertragsärztlichen Vergütung kann es keinem Zweifel unterliegen, daß finanzielle Aspekte wie die behauptete unzureichende Honorierung einer Einzelleistung einen Vertragsarzt nicht berechtigen, den Versicherten gesetzlich vorgesehene Leistungen nur außerhalb des Systems der vertragsärztlichen Versorgung zukommen zu lassen oder gänzlich zu verweigern. Auf die schon in der Vergangenheit wiederholt von Vertragsärzten vorgetragene Behauptung der nicht kostendeckenden Honorierung bestimmter Leistungen kann es schon deshalb nicht ankommen [...]“. Online, zitiert am 2024-08-24; verfügbar unter <https://dejure.org/2001,121>, Volltext unter <https://www.sozialgerichtsbarkeit.de/legacy/1496?modul=esgb&id=1496>

des Gesundheitsschutzes zu unterstützen“ und „die Arbeitnehmer zu untersuchen und zu beraten“.

Es gibt keine ausdrückliche Regelung im Arbeitsschutzgesetz, der Arbeitsmedizin-Verordnung oder im Arbeitssicherheitsgesetz, die den Zugang zur arbeitsmedizinischen Betreuung über ein bestimmtes technisches Medium, wie ein Online-Terminmanagementsystem, verbietet oder vorschreibt. Dennoch lassen sich aus den oben dargestellten Verpflichtungen des Arbeitgebers und der Rechte der Arbeitnehmer folgende rechtliche Anforderungen ableiten:

- a) **Zugangsrecht zur arbeitsmedizinischen Betreuung**
Der Arbeitgeber hat die Pflicht, den Zugang zur arbeitsmedizinischen Betreuung so zu gestalten, dass dieser für die Arbeitnehmer barrierefrei und niederschwellig zugänglich ist. Dies bedeutet, dass Arbeitnehmer nicht gezwungen werden dürfen, ein bestimmtes technisches System wie ein Online-Terminvereinbarungstool zu verwenden, insbesondere dann, wenn dies für einzelne Arbeitnehmer eine Barriere darstellt (z. B. aufgrund von technischen Unkenntnissen, fehlendem Zugang zu Internet oder mangelnden Sprachkenntnissen).
- b) **Keine Abhängigkeit von einer bestimmten technischen Infrastruktur**
Ähnlich wie bei der medizinischen Versorgung von Patienten (§ 109 SGB V für Krankenhäuser und § 95 SGB V für Vertragsärzte) sollte auch im arbeitsmedizinischen Kontext kein Ausschluss der Betreuung erfolgen, nur weil der Arbeitnehmer nicht auf ein bestimmtes Tool zugreifen kann. Eine solche Einschränkung würde der Betreuungspflicht widersprechen, die sich aus den oben genannten arbeitsschutzrechtlichen Vorschriften ergeben. Es ist daher davon auszugehen, dass ein Betriebsarzt nicht ausschließlich auf die Nutzung eines Online-Terminmanagementsystems bestehen darf.
- c) **Alternativen zur Online-Terminvereinbarung**
Für den Fall, dass ein Online-Terminvereinbarungstool eingesetzt wird, sollte der Arbeitgeber oder der Betriebsarzt sicherstellen, dass alternative Möglichkeiten der Terminbuchung bestehen, beispielsweise durch telefonische Vereinbarung oder persönliche Anmeldung. Dies stellt sicher, dass auch Arbeitnehmer ohne Internetzugang oder solche, die mit der Technik nicht vertraut sind, einen Termin wahrnehmen können.

Die Ausschließlichkeit einer Online-Terminbuchung würde somit gegen die allgemeinen arbeitsschutzrechtlichen Vorschriften zur Sicherstellung des Zugangs zur arbeitsmedizinischen Betreuung verstoßen.

4.6.3.2 Übernahme der arbeitsmedizinischen Betreuung durch einen überbetrieblichen Dienst von Betriebsärzten

Gemäß § 19 Abs. 1 ASiG kann ein Arbeitgeber, der nicht über eigene Betriebsärzte oder Fachkräfte für Arbeitssicherheit verfügt, die arbeitsmedizinische Betreuung und sicherheitstechnische Beratung an einen überbetrieblichen Dienst vergeben. Dies erfolgt per Betreuungsvertrag, der den externen Dienstleister zur Wahrnehmung der Aufgaben verpflichtet, die ansonsten dem Arbeitgeber im Rahmen des Arbeitsschutzes und der Gesundheitsvorsorge obliegen. Dazu zählen insbesondere die Pflichten aus:

- § 2 ASiG: Hierbei geht es um die Bestellung von Betriebsärzten, die den Arbeitgeber in Fragen der mit der Tätigkeit verbundenen Unfall- und Gesundheitsgefahren einhergehenden Risiken unterstützen.

- § 3 ASiG: Diese Regelung beschreibt die Aufgaben der Betriebsärzte, zu denen die arbeitsmedizinische Vorsorge, die Durchführung von Untersuchungen sowie die Beratung der Arbeitgeber und Arbeitnehmer gehört.

Der überbetriebliche Dienstleister wird durch den Vertrag mit dem Arbeitgeber zur Erfüllung der Aufgaben nach § 3 ASiG verpflichtet. Das bedeutet, dass der Dienstleister die gleichen Aufgaben zu erfüllen hat wie ein intern beschäftigter Betriebsarzt. Dazu zählen insbesondere:

- Beratung und Unterstützung des Arbeitgebers in allen Fragen des Gesundheitsschutzes und der Arbeitsmedizin.
- Durchführung arbeitsmedizinischer Vorsorgeuntersuchungen und Überwachung der Gesundheit der Arbeitnehmer.
- Unterstützung bei der Gefährdungsbeurteilung und bei der Implementierung von Maßnahmen des betrieblichen Gesundheitsschutzes.

Der überbetriebliche Dienst als Vertragspartner des Arbeitgebers wird in die Rolle des Betriebsarztes eingesetzt und übernimmt dessen Pflichten vollständig. Der Betreuungsvertrag ist somit die Grundlage und bildet in Verbindung mit § 19 ASiG die Basis für die Übernahme der Aufgaben.

Trotz der Beauftragung eines externen Dienstes bleibt der Arbeitgeber für die ordnungsgemäße arbeitsmedizinische Betreuung seiner Beschäftigten verantwortlich. Auch wenn ein überbetrieblicher Dienst diese Aufgabe übernimmt, bleiben die Pflichten des Arbeitgebers, insbesondere nach dem Arbeitsschutzgesetz (ArbSchG) und der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV), in vollem Umfang bestehen.

Daraus ergibt sich eine Konsequenz für die Frage, ob die Terminvereinbarung ausschließlich über ein Online-Terminmanagementsystem erfolgen darf. Der Arbeitgeber ist nach den arbeitsmedizinischen Vorschriften verpflichtet, sicherzustellen, dass alle Beschäftigten Zugang zur arbeitsmedizinischen Betreuung haben. Diese Pflicht wird auf den überbetrieblichen Dienstleister übertragen, was bedeutet:

- **Barrierefreier Zugang zur arbeitsmedizinischen Betreuung:** Der überbetriebliche Dienstleister, der per Vertrag die Aufgaben des Arbeitgebers übernimmt, muss den Zugang zur arbeitsmedizinischen Betreuung sicherstellen. Das heißt, die Nutzung eines Online-Terminmanagementsystems darf nicht die einzige Möglichkeit sein, einen Termin zu vereinbaren. Es müssen alternative Wege zur Verfügung stehen (z. B. telefonische Terminvereinbarung).
- **Verantwortung für ordnungsgemäße Umsetzung:** Der überbetriebliche Dienstleister muss dafür sorgen, dass die arbeitsmedizinischen Vorsorgeuntersuchungen für alle Arbeitnehmer erreichbar sind, unabhängig von deren technischen Möglichkeiten oder Kenntnissen.

4.7 Pflicht zur Barrierefreiheit

Die UN-Behindertenrechtskonvention¹²³ (UN-BRK) ist in Deutschland seit dem 26. März 2009 in Kraft¹²⁴, Europa trat 2010 bei. Darin findet sich u. a.:¹²⁵

¹²³ 15. Convention on the Rights of Persons with Disabilities. Online, zitiert am 2024-09-12; verfügbar unter https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtmsg_no=IV-15&chapter=4&clang=en

¹²⁴ Bundesministerium für Arbeit und Soziales (BMAS): Behindertenrechtskonvention der Vereinten Nationen. Online, zitiert am 2024-09-12; verfügbar unter <https://www.bmas.de/DE/Soziales/Teilhabe-und-Inklusion/Politik-fuer-Menschen-mit-Behinderungen/Behindertenrechtskonvention-der-Vereinten-Nationen/behindertenrechtskonvention-der-vereinten-nationen.html>

Art. 25 Gesundheit UN-BRK

„Die Vertragsstaaten anerkennen das Recht von Menschen mit Behinderungen auf das erreichbare Höchstmaß an Gesundheit ohne Diskriminierung aufgrund von Behinderung. Die Vertragsstaaten treffen alle geeigneten Maßnahmen, um zu gewährleisten, dass Menschen mit Behinderungen Zugang zu geschlechtsspezifischen Gesundheitsdiensten, einschließlich gesundheitlicher Rehabilitation, haben. Insbesondere:

- a. [...]
- d. erlegen die Vertragsstaaten den Angehörigen der Gesundheitsberufe die Verpflichtung auf, Menschen mit Behinderungen eine Versorgung von gleicher Qualität wie anderen Menschen angedeihen zu lassen, namentlich auf der Grundlage der freien Einwilligung nach vorheriger Aufklärung, indem sie unter anderem durch Schulungen und den Erlass ethischer Normen für die staatliche und private Gesundheitsversorgung das Bewusstsein für die Menschenrechte, die Würde, die Autonomie und die Bedürfnisse von Menschen mit Behinderungen schärfen;
- e. [...]
- f. verhindern die Vertragsstaaten die diskriminierende Vorenthaltung von Gesundheitsversorgung oder -leistungen oder von Nahrungsmitteln und Flüssigkeiten aufgrund von Behinderung.

Menschen mit Behinderungen dürfen bei der medizinischen Versorgung gegenüber Menschen ohne Behinderungen nicht benachteiligt werden. Dies bedeutet insbesondere auch, dass Leistungserbringer bei der Bereitstellung eines Online-Terminmanagementsystems darauf zu achten haben, dass Menschen mit Behinderung nicht benachteiligt werden.

Im Zuge der nationalen Umsetzung wurden entsprechend Art. 33 UN-BRK drei Anlaufstellen eingerichtet: die staatliche Anlaufstelle (Focal Point), die unabhängige Stelle (Monitoring-Stelle) und die staatliche Koordinierungsstelle. Als Monitoring-Stelle wurde das Deutsche Institut für Menschenrechte (DIMR) benannt und ist somit für die Einhaltung der Rechte von Menschen mit Behinderungen verantwortlich, muss die Umsetzung der UN-Behindertenrechtskonvention in Deutschland überwachen, Stellungnahmen und Empfehlungen zu politischen, behördlichen oder gerichtlichen Entscheidungen abgeben und – sofern erforderlich – auch die Einhaltung der UN-Behindertenrechtskonvention anmahnen.¹²⁶

Menschen mit Behinderungen haben die Möglichkeit, im Zweifelsfall auch den Rechtsweg zu beschreiten und die aus der UN-BRK resultierenden Rechte einzuklagen.

4.7.1 Webseiten-Richtlinie der EU

Die Richtlinie (EU) 2016/2102¹²⁷ über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen ist am 2. Dezember 2016 im Amtsblatt der Europäischen Union

¹²⁵ Fedlex Die Publikationsplattform des Bundesrechts der Schweiz: Übereinkommen über die Rechte von Menschen mit Behinderungen. Online, zitiert am 2024-09-12; verfügbar unter <https://www.fedlex.admin.ch/eli/cc/2014/245/de>

¹²⁶ Deutsches Institut für Menschenrechte e. V.: Über die Monitoring-Stelle. Online, zitiert am 2024-09-12; verfügbar unter <https://www.institut-fuer-menschenrechte.de/das-institut/abteilungen/monitoring-stelle-un-behindertenrechtskonvention/ueber-die-monitoring-stelle>

¹²⁷ Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates vom 26. Oktober 2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen. Online, zitiert am 2024-09-12; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L2102>

veröffentlicht worden. Die Durchführungsbeschlüsse der EU-Kommission erläutern einzelne, in der Richtlinie angekündigte Pflichten und legen die weitere inhaltliche Ausgestaltung dieser Verpflichtungen dar:

1. Durchführungsbeschluss Mustererklärung zur Barrierefreiheit¹²⁸
2. Durchführungsbeschluss Überwachungsmethodik¹²⁹
3. Durchführungsbeschluss maßgebender Standard¹³⁰

Die Richtlinie (EU) 2016/2102 wurde in Deutschland durch das Behindertengleichstellungsgesetz¹³¹ (BGG) und der Barrierefreien-Informationstechnik-Verordnung¹³² (BITV) umgesetzt. Entsprechend § 1 Abs. 3 BGG sollen Träger öffentlicher Gewalt darauf hinwirken, dass Einrichtungen, Vereinigungen und juristische Personen des Privatrechts, an denen die Träger öffentlicher Gewalt unmittelbar oder mittelbar ganz oder überwiegend beteiligt sind, die Ziele dieses Gesetzes in angemessener Weise berücksichtigen.

Das BGG adressiert somit nicht jede natürliche oder juristische Person. ErwGr. 34 Richtlinie (EU) 2016/2102 beinhaltet die Aufforderung an die Mitgliedstaaten, die Anwendung dieser Richtlinie auf private Stellen auszuweiten, die Einrichtungen und Dienstleistungen anbieten, die der Öffentlichkeit offenstehen bzw. bereitgestellt werden, unter anderem in den Bereichen Gesundheitswesen, Kinderbetreuung, soziale Integration und soziale Sicherheit. Deutschland griff diese Anregung jedoch nicht auf und adressierte in seiner Gesetzgebung private natürliche und juristische Personen nur eingeschränkt. Unabhängig von der Richtlinie (EU) 2016/2102 und deren deutscher Umsetzung sind die Vorgaben der UN-BRK aufgrund deren Anerkennung Deutschlands ggf. aber auch auf anderen Rechtswegen einklagbar.

Fällt eine natürliche und/oder juristische Person unter den Wirkungsbereich der Richtlinie (EU) 2016/2102 bzw. der jeweiligen nationalen Umsetzung, so ist entsprechend des Anhangs des Durchführungsbeschlusses (EU) 2018/2048 der EU-Kommission die Norm EN 301 549 in Version 3.2.1 (Stand: 2021-03) verpflichtend anzuwenden.

¹²⁸ Durchführungsbeschluss (EU) 2018/1523 der Kommission vom 11. Oktober 2018 zur Festlegung einer Mustererklärung zur Barrierefreiheit gemäß der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen. Online, zitiert am 2024-09-12; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32018D1523>

¹²⁹ Durchführungsbeschluss (EU) 2018/1524 der Kommission vom 11. Oktober 2018 zur Festlegung einer Überwachungsmethodik und der Modalitäten für die Berichterstattung der Mitgliedstaaten gemäß der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen. Online, zitiert am 2024-09-12; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=uriserv:OJ.L_.2018.256.01.0108.01.DEU

¹³⁰ Durchführungsbeschluss (EU) 2018/2048 der Kommission vom 20. Dezember 2018 über die harmonisierte Norm für Websites und mobile Anwendungen zur Unterstützung der Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates. Online, zitiert am 2024-09-12; verfügbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02018D2048-20220212>

¹³¹ Gesetz zur Gleichstellung von Menschen mit Behinderungen. Online, zitiert am 2024-09-12; verfügbar unter <https://www.gesetze-im-internet.de/bgg/index.html>

¹³² Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz. Online, zitiert am 2024-09-12; verfügbar unter https://www.gesetze-im-internet.de/bitv_2_0/index.html

Die Norm EN 301 549 wurde von CEN, CENELEC und ETSI entwickelt und wird in englischer Sprache kostenlos zum Download angeboten.¹³³ Die Norm EN 301 549 adressiert für Web-basierte Angebote ein Kapitel 9.0 die W3C Web Content Accessibility Guidelines¹³⁴ und fordert in Kapitel 9.5 und 9.6 die Umsetzung der entsprechenden Anforderungen.

4.8 Webportal: Ein digitaler Dienst¹³⁵

§ 1 Abs. 4 Ziff. 1 DDG verweist bzgl. der Begriffsbestimmung eines digitalen Dienstes auf Art. 1 Abs. 1 lit. b Ziff. 2 Richtlinie (EU) 2015/1535, wonach eine „elektronisch erbrachte Dienstleistung“ eine Dienstleistung ist, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird.

Zu den digitalen Diensten i. S. d. DDG zählen insbesondere

- Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit, z. B. Angebot von Verkehrs-, Wetter-, Umwelt- oder Börsendaten, Newsgroups, Chatrooms, elektronische Presse, Fernseh-/Radiotext, Teleshopping
- Video auf Abruf („Video on Demand“), soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst im Sinne der Richtlinie 89/552/EWG handelt
- Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen, also Internetsuchmaschinen
- die kommerzielle Verbreitung von Informationen über Waren-/ Dienstleistungsangebote mit elektronischer Post wie beispielsweise z. B. Werbe-Mails
- geschäftsmäßige Online-Dienste wie z. B. Internetangebote („Homepages“).

Online-Terminmanagementsysteme stellen auch immer einen digitalen Dienst dar.

4.8.1 Anbieter von digitalen Diensten

Entsprechend § 2 Abs. 2 Ziff. 1 TDDDG wird unter „Anbieter von digitalen Diensten“ jede natürliche oder juristische Person verstanden, welche

- eigene oder fremde digitale Dienste erbringt,
- an der Erbringung mitwirkt oder
- den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt.

Es ist dabei nicht entscheidend, ob eigene oder fremde digitale Dienste Gegenstand des Angebots sind, sondern allein die Funktion des Anbietens. Es genügt zur Einordnung als Diensteanbieter, dem Kunden die Nutzung von digitalen Diensten zu ermöglichen.

Somit gelten Leistungserbringer, welche ein Online-Terminmanagementsystem anbieten, als „Diensteanbieter“ i. S. d. DDG und müssen die entsprechenden Vorgaben erfüllen.

¹³³ EN 301 549 V3.2.1 (2021-03). Accessibility requirements for ICT products and services. In englischer Sprache kostenlos abrufbar bei ETSI. Online, zitiert am 2024-09-12; verfügbar unter <https://www.etsi.org/standards#page=1&search=EN%20301%20549&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&withdrawn=1&historical=1&isCurrent=1&superseded=1&startDate=1988-01-15&endDate=2024-09-12&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1> bzw. pdf-Datei unter https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf

¹³⁴ W3C: Web Content Accessibility Guidelines (WCAG) 2.1. Online, zitiert am 2024-09-12; verfügbar unter <https://www.w3.org/TR/WCAG21/>

¹³⁵ Eine Einführung in das Thema findet sich z. B. in der „Praxishilfe zur Beachtung des TDDDG im Bereich der Telemedizin“. Online, zitiert am 2024-08-24; verfügbar unter <https://gesundheitsdatenschutz.org/html/ttdsg.php>

4.8.2 Zu erfüllende Anforderungen

In Art. 4 Abs. 1a RL 2002/58/EG heißt es: „Unbeschadet der Richtlinie 95/46/EG ist durch die in Absatz 1 genannten Maßnahmen zumindest Folgendes zu erreichen“. D. h., bei den Anforderungen hinsichtlich technischer und organisatorischer Vorkehrungen im TDDDG handelt es sich um die RL 95/46/EG *ergänzende* Maßnahmen, es erfolgt insbesondere keine Verdrängung der Anforderungen der Datenschutz-Richtlinie 95/46/EG, bzw. der DS-GVO als Nachfolger der Datenschutz-Richtlinie. Damit muss allen Anforderungen der DS-GVO genügt werden, insbesondere auch den Anforderungen aus

- Art. 25 DS-GVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy by Design/Default“),
- Art. 32 DS-GVO Sicherheit der Verarbeitung und
- Art. 35 DS-GVO Datenschutz-Folgenabschätzung.

Somit müssen Anbieter von digitalen Diensten – wozu auch Leistungserbringer gehören können – bei der Einbindung eines Online-Terminmanagementsystems von Anfang an Datenschutz mit beachten und dieses Softwareangebot datenschutzfreundlich ausgestalten.

Gemäß § 19 Abs. 3 TDDDG ist die Weitervermittlung zu einem anderen Anbieter von digitalen Diensten dem Nutzer anzuzeigen. Bei internetbasierten Diensten ist dies beispielsweise regelmäßig der Fall, wenn ein Nutzer mittels eines Hyperlinks zu einem anderen Dienst, also einer anderen Internetpräsenz geführt wird. Leitet ein Leistungserbringer einen Patienten bei einer Terminanfrage von seinem eigenen Internetauftritt zu einem Dienstleister weiter, so muss dies dem Benutzer zuvor mitgeteilt werden.

Anbieter von geschäftsmäßig angebotenen digitalen Diensten müssen gemäß § 19 Abs. 4 TDDDG

- soweit dies technisch möglich und wirtschaftlich zumutbar ist
- unter Berücksichtigung des Stands der Technik
- durch technische und organisatorische Vorkehrungen sicherstellen, dass
 - o kein unerlaubter Zugriff auf die für ihre digitalen Dienste genutzten technischen Einrichtungen möglich ist und
 - o diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

Leistungserbringer als Anbieter von digitalen Diensten sind somit auch dafür verantwortlich, dass ein externer Dienst zur Terminbuchung erreichbar ist. Vertraglich sollten sich die Leistungserbringer von einem Dienstleister zusichern lassen, dass Wartungsarbeiten und die damit verbundene Nicht-Erreichbarkeit zuvor dem Leistungserbringer angekündigt werden und dass Störungen der Erreichbarkeit dem Leistungserbringer unverzüglich angezeigt werden, damit der Leistungserbringer die Patienten über seinen Internetauftritt entsprechend informieren kann.

4.9 Beschlagnahmeschutz bei Dienstleistern

Analog dem Recht des Berufsgeheimnisträgers zur Zeugnisverweigerung („Aussageverweigerung“, § 53 StPO) haben alle entsprechend § 203 Abs. 4 S. 2 StGB zur Verschwiegenheit verpflichteten Personen ein Schweigerecht. In § 53a StPO heißt es:

„Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen

- eines Vertragsverhältnisses,
- einer berufsvorbereitenden Tätigkeit oder
- einer sonstigen Hilfstätigkeit

an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.“

Das aus § 97 StPO resultierende Beschlagnahmeverbot wurde entsprechend angepasst. Das Beschlagnahmeverbot richtet sich nach dem Recht zur Zeugnisverweigerung. In § 97 Abs. 4 StPO heißt es: „Dieser Beschlagnahmeschutz erstreckt sich auch auf Gegenstände, die von den in § 53 Abs. 1 Satz 1 Nr. 4 genannten Personen den an ihrer Berufstätigkeit nach § 53a Absatz 1 Satz 1 mitwirkenden Personen anvertraut sind.“ D. h., dass solange das Recht zur Zeugnisverweigerung besteht, besteht auch ein Beschlagnahmeverbot, z. B. im Rechenzentrum eines Dienstleisters, solange die Verpflichtung nach § 203 StGB ordnungsgemäß erfolgte.

Dabei ist zu beachten, dass der Dienstleister Daten mit strikter Mandantentrennung verarbeiten muss, da ansonsten der Schutz durch eine Vermischung von geschützten und ungeschützten Daten aufgehoben werden könnte. Beispiel:

Der Dienstleister hat Vertragsverhältnisse sowohl mit Patienten selbst wie auch mit Leistungserbringern. D. h. ein Patient kann über den Dienstleister selbst Termine suchen und bei einem ausgewählten Leistungserbringer buchen. Der Dienstleister bietet zugleich gegenüber dem Leistungserbringer den Service eines Terminbuchungssystems an.

Bucht ein Patient jetzt Daten beim Leistungserbringer, so muss zwischen den Daten des Patienten als Kunden des Dienstleisters und Daten des Patienten als Kunden des Leistungserbringers unterschieden werden. Je nach Art der Speicherung resultiert daraus:

- a) Werden die Daten nur an einer Stelle gespeichert, unterliegen die Daten ggf. nicht mehr dem Recht zur Aussageverweigerung und ebenfalls nicht einem Beschlagnahmeschutz.
- b) Werden die Daten getrennt entsprechend den Vorgaben einer Mandantentrennung gespeichert – was zu einer redundanten Speicherung führt –, können die Patientendaten, die im Kontext des Patienten als Kunden des Dienstleisters gewonnen werden, ggf. beschlagnahmt werden, die Patientendaten, die im Kontext als Patient des Leistungserbringers stehen, hingegen nicht.

Erfolgt keine entsprechende Mandantentrennung, sind betroffene Patientendaten also nicht bzgl. Aussageverweigerung oder beschlagnahme geschützt, was zu einer unbefugten Offenlegung beim Leistungserbringer führen kann. Um eine Aufhebung der Mandantentrennung zu legitimieren, bedarf es einer strafrechtlichen Einwilligung („Schweigepflichtentbindung“) des jeweiligen Patienten. Aufgrund der Anforderungen hinsichtlich des Bestimmtheitsgebots muss jedoch beachtet werden, dass diese für jede einzelne Terminabsprache erforderlich sein kann und in diesen Fällen regelmäßig wiederholt werden müsste. Erfolgt hingegen durch fehlende Mandantentrennung eine Offenbarung von Patientengeheimnissen über den Dienstleister, kann dies eine unbefugte Offenbarung von Patientengeheimnissen des Leistungserbringers beinhalten, was für den Leistungserbringer sowohl strafrechtliche wie auch berufsrechtliche Folgen haben kann.

4.10 Eigenständige Datenerhebung durch den Dienstleister

Eine eigenständige Datenerhebung seitens des Dienstleisters ist im Rahmen einer Auftragsverarbeitung unzulässig, da Auftragsverarbeiter nur auf Weisung des Verantwortlichen handeln dürfen.

4.10.1 Vom Leistungserbringer gegenüber dem Dienstleister zu erbringende Fachkundenachweise

Sehen vertragliche Regelungen vor, dass ein Dienstleister, welcher ein Online-Terminmanagementsystem anbietet, Termine nur vermittelt, wenn der Auftraggeber dem Dienstleister zuvor Nachweise des Behandlers (Approbationsurkunde, Fotografien des Personals, Personalausweiskopie, Spezialisierungsnachweise wie beispielsweise Fachkundenachweise, beruflicher Werdegang oder dergleichen) bereitstellt, so begründet diese Datenerhebung des Dienstleisters eines Online-Terminmanagementsystems immer auch eine eigene Verantwortlichkeit, da bei einer Auftragsverarbeitung derartige Bewertungen ausschließlich vom Verantwortlichen vorzunehmen sind, niemals jedoch von einem Dienstleister. Der Dienstleister eines Online-Terminmanagementsystems sieht sich in diesen Fällen selbst in der Verantwortung, dass Termine nur mit qualifizierten Leistungserbringern vereinbart werden können.

4.10.2 Dienstleister fordert Versicherungsnachweis vom Leistungserbringer

Es gibt Dienstleister, die vom Leistungserbringer eine Haftpflichtversicherung fordern.¹³⁶ Hier ist zu beachten, für welche Schäden eine Versicherung verlangt wird: Eine Versicherung wegen vom Vertragspartner dem Dienstleister zugefügten Schäden gibt i. d. R. keinen Hinweis auf eine selbstständige Verarbeitung.

Verlangt der Dienstleister aber eine Versicherung gegenüber Dritten, so übernimmt der Dienstleister Sorgfaltspflichten über das Maß eines Auftragsverarbeiters hinaus: Er gibt Rahmenbedingungen für die Verarbeitung vor, die ein Auftraggeber, d. h. der datenschutzrechtlich Verantwortliche, nicht beeinflussen kann und wird hierdurch regelhaft zu einer natürlichen oder juristischen Person, welche über Mittel der Verarbeitung von personenbezogenen Daten entscheidet; laut Rechtsprechung des EuGH beinhaltet dies eine gemeinsame Verantwortlichkeit.¹³⁷

4.10.3 Nutzung von Patientendaten zu statistischen Auswertungen des Dienstleisters

Einige Dienstleister behalten sich das Recht vor, eigene Statistiken zur Nutzung des Online-Terminmanagementsystems zu erstellen und damit auch die Patientendaten des jeweiligen Leistungserbringers zu nutzen.

¹³⁶ So z. B. die Doctolib GmbH in ihren AGB vom März 2024, Abschnitt 19 „Versicherung: „Sie verpflichten sich, bei einer vertrauenswürdigen und solventen Versicherungsgesellschaft Ihrer Wahl eine marktübliche Haftpflichtversicherung abzuschließen, um alle materiellen, körperlichen und/oder immateriellen Schäden, die Sie Doctolib und/oder Dritten zufügen können, sowie alle besonderen Risiken im Zusammenhang mit Ihrer Tätigkeit während der gesamten Laufzeit des Vertrags abzudecken.“ Online, zitiert am 2024-10-04; verfügbar unter <https://info.doctolib.de/allgemeine-geschäftsbedingungen/#article-h2-abonnement-fuer-die-doctolib-dienste>

¹³⁷ Siehe z. B.

- EuGH, Urt. v. 2024-01-11, Rechtssache C-231/22, Rn. 48: „Damit eine Person gemeinsam für die Verarbeitung verantwortlich gemacht werden kann, reicht es aus, wenn diese Person zu ihren eigenen Zwecken auf die Verarbeitung personenbezogener Daten Einfluss nimmt und daher an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung beteiligt ist.“ Online, zitiert am 2024-10-04; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0231>
- EuGH, Urt. v. 2018-07-10, Rechtssache C-25/17, Rn. 68: „Hingegen kann eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als für die Verarbeitung Verantwortlicher im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden.“ Online, zitiert am 2024-10-04; verfügbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62017CJ0025>

Auch in diesen Fällen werden Daten zu eigenen Interessen des Dienstleisters verarbeitet, nicht jedoch auf Weisung des Verantwortlichen. Die Erstellung entsprechender Statistiken ist bei der Beurteilung, ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit vorliegt, somit immer zu berücksichtigen.

Hiergegen wird argumentiert, dass die Daten vom Dienstleister nur anonym genutzt würden. Die Daten sind jedoch zunächst immer einem Patienten zuordenbar, sonst könnte der jeweilige Leistungserbringer nicht feststellen, welcher Patient welchen Termin vereinbarte. Im Kontext einer Auftragsverarbeitung zählt der Auftragsverarbeiter zur Sphäre des Verantwortlichen und somit muss das Wissen des Verantwortlichen immer auch dem Auftragsverarbeiter zugerechnet werden. Diese Sphäre des Verantwortlichen wird vom Auftragnehmer verlassen, wenn eine Anonymisierung im Interesse des Auftragnehmers erfolgt.

Ob außerhalb der Sphäre des Verantwortlichen agierende Dienstleister – also Nicht-Auftragsverarbeiter – anonymisierte Daten vorliegen haben, wenn der ursprüngliche Verantwortliche die Daten betroffenen Personen zuordnen kann, der Dienstleister aber nicht, liegt aktuell dem EuGH zur Entscheidung vor.¹³⁸

4.10.4 Patienten-Umfragen durch den Dienstleister

Auch vom Software-Dienstleister durchgeführte Patienten-Umfragen wie beispielsweise eine Umfrage zur Zufriedenheit mit dem angebotenen Terminvergabe-Dienst dienen i. d. R. dem Software-Dienstleister, welcher damit die Qualität der Dienstleistungen messen will. Sie sind regelhaft keine für den Leistungserbringer durchgeführte Leistung, insbesondere, wenn die Umfragen nicht auf die Patienten des Leistungserbringers beschränkt bleiben, sondern Aussagen von Patienten mehrerer Leistungserbringer vom Software-Dienstleister gemeinsam ausgewertet werden.

4.10.5 Rechteübertragung

In einigen Fällen behalten sich Dienstleister, dass der Dienstleister sich aus dem Vertrag zwischen Leistungsvertreter und Dienstleister ergebenden Rechte und Pflichten an Dritte übertragen darf, regelhaft auch ohne Zustimmung durch den Leistungserbringer.

Hier sind verschiedene Aspekte zu beachten:

- 1) Entsprechend Art. 28 DS-GVO darf nur ein Verantwortlicher, d. h. in diesen Fällen der jeweilige Leistungserbringer, entscheiden, wer als Auftragsverarbeiter eingesetzt werden darf. Somit widerspricht eine solche Regelung grundsätzlich den Vorgaben einer Auftragsverarbeitung.
- 2) Beinhaltet der zwischen Dienstleister und Leistungserbringer geschlossene Vertrag auch die Rechteübertragung zu Daten von Patienten, so werden Rechte Dritter (= der Patienten) ggfs. beeinträchtigt. Dies kann einen Vertrag zu Lasten Dritter darstellen, der unzulässig wäre.¹³⁹

¹³⁸ EuGH, Vorlagefrage vom 2023-08-04, Rechtssache C-413/23. Verfahrensdokumentation online verfügbar unter <https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C%2D413%2F23> (zitiert am 2024-10-04)

¹³⁹ Analog BVerfG, Urt. v. 2016-03-24, Az. 2 BvR 1546/13, Rn. 6. Online, zitiert am 2024-10-04; verfügbar unter <https://dejure.org/2016,6490>, Volltext unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/03/rk20160324_2bvr154613.html

4.10.6 Folgen einer eigenständigen Verarbeitung durch den Dienstleister

In den oben genannten Fällen liegt i. d. R. keine Auftragsverarbeitung vor, sondern eine gemeinsame Verantwortlichkeit entsprechend Art. 26 DS-GVO. Es muss daher kein Vertrag zur Auftragsverarbeitung abgeschlossen werden, sondern einen Vertrag nach Art. 26 DS-GVO.

Der Software-Dienstleister benötigt in diesen Fällen unabhängig vom Leistungserbringer eine eigene Rechtsgrundlage zur Verarbeitung der Daten. Hierbei ist zu beachten, dass in diesen Fällen regelhaft Gesundheitsdaten i. S. v. Art. 9 Abs. 1 DS-GVO verarbeitet werden. Der Software-Dienstleister muss daher neben einem der in Art. 6 Abs. 1 DS-GVO aufgeführten (eng auszulegenden) Rechtfertigungsgründe somit immer auch einen der in Art. 9 Abs. 2 DS-GVO aufgeführten Erlaubnistatbestände nachweisen.

In Frage stehen könnte auch, ob in diesen Fällen für den Leistungserbringer der Behandlungsvertrag eine Rechtsgrundlage bildet: Entsprechend Art. 9 Abs. 3 DS-GVO muss das Fachpersonal, welches die Daten gemäß Art. 9 Abs. 2 lit. h DS-GVO verarbeitet, einem Berufsgeheimnis oder einer gleichgestellten gesetzlichen Geheimhaltungspflicht unterliegen. Bei gemeinsam Verantwortlichen unterliegen die Daten, die der Software-Anbieter/-Hersteller für eigene Zwecke nutzt und die zugleich Daten eines Leistungserbringers, die unter die in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien fallen, nicht dem aus dem Berufsrecht resultierendem Berufsgeheimnis und auch nicht dem in § 203 StGB verankertem Verbot der unbefugten Offenbarung. In diesen Fällen wird daher ggfs. auch ein Leistungserbringer eine Einwilligung des Patienten für eine Online-Terminvergabe als Rechtsgrundlage benötigen.

5 Anforderungen an Online-Terminbuchungssystemen

5.1 Anforderungen an Leistungserbringer, die IT-Lösungen nutzen

5.1.1 Rechtsgrundlage

Entsprechend Art. 5 Abs. 1 DS-GVO muss ein Erlaubnistatbestand zur Verarbeitung der Patientendaten vorliegen. Eine Terminvergabe kann zwar für eine Behandlung erforderlich i. S. v. Art. 9 Abs. 2 lit. h DS-GVO sein, dies gilt jedoch nicht für eine Online-Terminvergabe. Somit ist für eine Online-Terminvergabe eine Einwilligung der jeweiligen Patienten erforderlich.

Damit die Einwilligung als freiwillig gegeben angesehen werden kann, muss auf jeden Fall auch eine Alternative zur Online-Terminvergabe angeboten werden, z. B. die Terminvergabe in der Arztpraxis bzw. im Krankenhaus vor Ort und/oder telefonisch.

Anforderung 1: Für eine Online-Terminvergabe ist immer das Vorliegen einer ausdrücklichen Einwilligung i. S. v. Art. 9 Abs. 2 lit. a DS-GVO i. V. m. Art. 6 Abs. 1 lit. a DS-GVO erforderlich.

Anforderung 2: Der Leistungserbringer ist als der Behandler des Patienten Verantwortlicher i. S. v. Art. 4 Ziff. 7 DS-GVO und muss somit nachweisen, dass eine datenschutzrechtliche Einwilligung vor Beginn der Verarbeitung vorlag.

Anforderung 3: Vor der Erteilung der Einwilligung zur Verarbeitung der personenbezogenen Daten müssen den betroffenen Patienten alle erforderlichen Informationen bereitgestellt werden. Dazu gehören insbesondere auch alle Informationen nach Art. 13 bzw. Art. 14 DS-GVO.

Anforderung 4: Eine Einwilligung muss für den Patienten jederzeit mit Wirkung für die Zukunft temporär oder permanent widerrufbar sein.

Anforderung 5: Der Widerruf muss mindestens so einfach sein wie die Erteilung der Einwilligung.

5.1.2 Datenminimierung

Gemäß Art. 5 Abs. 1 lit. c DS-GVO muss die Verarbeitung personenbezogener Daten für den verfolgten Zweck erforderlich und angemessen sein. Insbesondere dürfen an einen Dienstleister bzw. dessen Softwarelösung zur Terminbuchung auf keinen Fall Daten übermittelt werden, die nicht auch bei einer Terminvereinbarung beim Leistungserbringer selbst oder bei einem Telefongespräch zwischen Patienten und Leistungserbringer abgefragt werden. Zu beachten ist weiterhin, dass entsprechend Art. 5 Abs. 2 DS-GVO der Leistungserbringer als Verantwortlicher i. S. v. Art. 4 Ziff. 7 DS-GVO nachweispflichtig ist, d. h. die einzelnen Datenkategorien wie z. B. der Name des Patienten oder dessen Versicherungsart (gesetzlich/privat) müssen in einer Dokumentation inklusive der Begründung für die Dokumentation beschrieben sein (Art. 30 DS-GVO).

Für eine Terminvergabe ist die Weitergabe aller jemals behandelten Patienten-Stammdaten an einen Dienstleister grundsätzlich nicht erforderlich; diese ist damit stets rechtswidrig. Die Weitergabe von Patientendaten verstorbener Patienten wie auch von Patienten, deren Behandlung abgeschlossen ist, kann nicht mit einer möglichen Terminvergabe in der Zukunft legitimiert werden, da hierfür keine Erforderlichkeit besteht. Somit verstößt eine entsprechende Weitergabe **ohne ausdrückliche Einwilligung** (siehe Kapitel 4.1.2.1) der Patienten gegen

- a) Vorgaben der DS-GVO,
- b) § 203 StGB sowie gegen
- c) die aus dem Berufsrecht resultierende ärztliche Schweigepflicht.

Anforderung 6: Es dürfen nur Stammdaten an einen Dienstleister zum Zwecke einer Online-Terminvergabe übermittelt werden, die für diese Zwecke erforderlich sind.

Anforderung 7: Der zwingend einzuhaltende Grundsatz der Erforderlichkeit beinhaltet insbesondere, dass nur Stammdaten von Patienten übermittelt werden dürfen, von denen sicher ist, dass sie künftig online Termine vereinbaren werden.

Anforderung 8: In einer Dokumentation muss jede übermittelte Datenkategorie wie beispielsweise Patientennamen aufgelistet werden. Zu jeder Datenkategorie ist die Erforderlichkeit der Übermittlung zu begründen.

5.1.3 Gewährleistung Betroffenenrechte

Alle in Kap. III DS-GVO genannten Betroffenenrechte müssen von Verantwortlichen erfüllt werden. Dies umfasst:

- Informationspflicht bei Erhebung bzw. Zweckänderung von personenbezogenen Daten
- Auskunftsrecht der betroffenen Person
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Beschränkung der Zulässigkeit automatisierter Entscheidungen im Einzelfall.

Leistungserbringer müssen bei einem Online-Terminmanagementsystem sicherstellen, dass allen Anforderungen genügt wird.

Der Informationspflicht wird i. d. R. durch Bereitstellung entsprechender Datenschutzhinweise genügt; für alle anderen Anforderungen müssen entsprechende Funktionalitäten in der Software vorhanden sein. Zu beachten ist dabei, dass der betroffene Patient auch über Besonderheiten wie beispielsweise einer Cloud-Verarbeitung oder Drittland-Verarbeitung durch den für die Verarbeitung Verantwortlichen informiert werden muss.

Terminbuchungen sind kein Bestandteil der Dokumentation entsprechend § 630f BGB (siehe Kapitel 4.5). Daher ist die dort vorgesehene gesetzliche Aufbewahrungspflicht nicht anwendbar. Auch andere gesetzliche Pflichten schreiben keine Aufbewahrung von Terminbuchungen vor. Daher dürfen die Daten gemäß Art. 5 Abs. 1 lit. e DS-GVO nicht länger gespeichert werden, als es für den Zweck der Datenverarbeitung, dies ist die Terminbuchung, unbedingt erforderlich ist;¹⁴⁰ in ErwGr. 39 DS-GVO findet sich die Aussage, dass „die Speicherfrist für personenbezogene Daten auf das unbedingt

¹⁴⁰ So zu finden z. B. in

- Heberlein H.: Art. 5 DS-GVO, Rn. 34. In: Ehmann/Selmayr (Hrsg.) Datenschutz-Grundverordnung: DS-GVO. Verlag C. H. Beck, 3. Auflage 2024. ISBN 978-3-406-79777-4
- Herbst: Art. 5, Rn. 64. In: Kühling/Buchner (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. Verlag C. H. Beck, 3. Auflage 2020. ISBN: 978-3-406-74994-0
- Roßnagel A.: Art. 5, Rn. 154. In: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7
- Schantz P.: Art. 5, Rn. 32, 33. In: Wolff/Brink/v. Ungern-Sternberg (Hrsg.) BeckOK Datenschutzrecht. 48. Edition, Stand: 01.05.2024

erforderliche Mindestmaß beschränkt bleibt“. D. h., spätestens nach Beendigung des Termins sind die Daten zu löschen.

Anforderung 9: Leistungserbringer müssen Patienten über alle Empfänger informieren, dies schließt auch den Dienstleister, der das Online-Terminmanagementsystem im Auftrag des Leistungserbringers betreibt, mit ein.

Anforderung 10: Werden bei dem eingesetzten Online-Terminmanagementsystem IT-Systeme von Dienstleistern aus Drittstaaten wie beispielsweise den USA eingesetzt, müssen Patienten darüber sowie über alle daraus resultierenden Risiken informiert werden.

Anforderung 11: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, welches das Recht auf Auskunft gewährleistet.

Anforderung 12: Insbesondere muss das Online-Terminmanagementsystem auch eine Möglichkeit zum Export aller Daten eines Patienten bieten, sowohl als physischen Papiausdruck als auch einen Export in einem gängigen elektronischen Format.

Anforderung 13: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, bei welchem Patientendaten auf Wunsch eines Patienten berichtigt werden können.

Anforderung 14: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, bei welchem die Daten nach Erreichung des konkreten Verarbeitungszweckes **gelöscht** werden.

Anforderung 15: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, bei welchem die Daten eines Patienten auf dessen Wunsch gelöscht werden können.

Anforderung 16: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, bei welchem Zugriffe auf die Daten eingeschränkt werden können. Hierbei muss beachtet werden, dass auch der Dienstleister der Software selbst keinen Zugriff auf die Patientendaten hat.

Anforderung 17: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, welches die Möglichkeit bietet, dem Patienten alle ihn betreffenden Daten in einer strukturierten, gängigen und maschinenlesbaren Form bereitzustellen.

Anforderung 18: Leistungserbringer sollten nur ein Online-Terminmanagementsystem einsetzen, welches die Möglichkeit bietet, alle einen Patienten betreffenden Daten auf Wunsch des Patienten einem anderen Verantwortlichen in einer strukturierten, gängigen und maschinenlesbaren Form zu übermitteln.

Anforderung 19: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, welches den Widerspruch eines Patienten zur Verarbeitung seiner Daten berücksichtigt. Insbesondere muss bei einem Widerspruch zur Verarbeitung die Löschung der vom Widerspruch betroffenen Daten entsprechend Art. 17 Abs. 1 lit. b DS-GVO erfolgen.

Anforderung 20: Leistungserbringer dürfen nur ein Online-Terminmanagementsystem einsetzen, bei dem sichergestellt ist, dass dieses keine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung wie beispielsweise Terminvergabe oder -ablehnung trifft. Eine Terminvergabe oder -ablehnung kann im medizinischen Kontext terminsuchende Patienten erheblich in ihrer Gesundheit beeinträchtigen.

5.1.4 Barrierefreiheit

Menschen mit Behinderungen dürfen entsprechend Art. 25 UN-BRK¹⁴¹ bei der Gesundheitsversorgung gegenüber Menschen ohne Behinderung nicht benachteiligt werden. Daher

¹⁴¹ In Deutschland umgesetzt durch

- Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz - BGG)
- Gesetz zur Umsetzung der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (Barrierefreiheitsstärkungsgesetz - BFSG)

sollte ein Online-Terminmanagementsystem nur eingesetzt werden, wenn diese Software-Lösung eine digitale Barrierefreiheit gewährleistet.

Anforderung 21: Leistungserbringer sollten nur ein Online-Terminmanagementsystem einsetzen, wenn diese Softwarelösung eine digitale Barrierefreiheit gewährleistet.

Es stehen auch Testangebote bzgl. Einhaltung der Barrierefreiheit zur Verfügung, sodass Leistungserbringer prüfen können, ob eine Software den gesetzlichen Anforderungen genügt.¹⁴²

5.1.5 Privacy by Design

Art. 25 DS-GVO verlangt „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, was in der Öffentlichkeit meistens als „Privacy by Design/Default“ bezeichnet wird. Während Privacy by Design bereits in der konzeptionellen Phase beginnt, verlangt Privacy by Default, dass zu Beginn der Datenverarbeitung eine datenschutzfreundliche Grundeinstellung existiert. Grundlegendes zum Thema Privacy by Design/Default findet man in der Praxishilfe von bvitg, GDD und GMDS¹⁴³. Der europäische Datenschutzausschuss veröffentlichte im Oktober 2020 Leitlinien zum Thema.¹⁴⁴ Es empfiehlt sich, den Text zu lesen, um die Sicht der europäischen Aufsichtsbehörden zum Thema kennenzulernen.

Art. 25 DS-GVO verlangt das Treffen geeigneter technisch-organisatorischer Maßnahmen, sowohl zur Umsetzung der in Art. 5 DS-GVO genannten Datenschutzgrundsätze wie auch zur Durchsetzung der Betroffenenrechte. Die Maßnahmen müssen dabei dafür ausgelegt sein,

- die in Art. 5 DS-GVO genannten Datenschutzgrundsätze wirksam umzusetzen,
- die Rechte der betroffenen Personen zu schützen sowie
- die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen.

Dabei enthält Art. 25 DS-GVO im Gegensatz zu Art. 32 DS-GVO keine Beschränkung bzgl. der „Angemessenheit“ der Maßnahmen: Die getroffenen Maßnahmen müssen die Anforderungen von Art. 25 vollumfänglich umsetzen.

Anforderung 22: Bei der Einführung eines Online-Terminmanagementsystems sind von Anfang an die Anforderungen der Datenschutz-Grundverordnung zu berücksichtigen. Der Anforderungskatalog zur Beschaffung einer entsprechenden Software-Lösung muss dies abbilden.

Anforderung 23: Datenschutz und IT-Sicherheit müssen für den gesamten Lebenszyklus des Online-Terminmanagementsystems berücksichtigt werden, angefangen bei der Anforderungsanalyse und Einführung der Anwendung bis hin zur Abkündigung/Abschaffung der IT-Lösung.

5.1.6 Sicherheit der Verarbeitung

Art. 5 Abs. 1 lit. f DS-GVO verlangt, dass personenbezogene Daten nur „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem

¹⁴² DIAS GmbH - Daten, Informationssysteme und Analysen im Sozialen: Wir unterstützen Sie mit dem BIK BITV-Test. Online, zitiert am 2024-09-12; verfügbar unter <https://bitvtest.de/>

¹⁴³ bvitg, GDD, GMDS: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO). Online, zitiert am 2024-08-24; verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/privacy_design_default.php

¹⁴⁴ EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Online, zitiert am 2024-08-24; verfügbar unter <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and-de>

Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“. Um den angemessenen Schutz festlegen zu können, müssen der Schutzbedarf der Daten und das Risiko der Verarbeitung bestimmt werden.

Hinsichtlich der Bewertung des Schutzbedarfs enthält ErwGr. 91 DS-GVO die Aussage, dass insbesondere die Sensibilität der Daten die Wahrscheinlichkeit eines „hohen“ Risikos vermuten lässt, sodass bei einer Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien von Daten grundsätzlich von einem hohen oder sogar sehr hohen Schutzbedarf auszugehen ist. D. h. bei der Verarbeitung sensibler Daten wie Gesundheitsdaten, genetischen Daten wie auch biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist immer von einem hohen Risiko und dementsprechend von einem hohen Schutzbedarf auszugehen.

Dementsprechend müssen die technischen und organisatorischen Maßnahmen ein sehr hohes Sicherheitsniveau gewährleisten. Diese Maßnahmen schließen u. a. Folgendes ein (Art. 32 Abs. 1 DS-GVO):

- Pseudonymisierung personenbezogener Daten;
- Verschlüsselung personenbezogener Daten;
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Aufgrund dieser Vorgabe in Art. 32 DS-GVO muss nachvollziehbar begründet werden, wenn eine der in Art. 32 DS-GVO genannten Maßnahmen wie beispielsweise Verschlüsselung nicht genutzt wird.

Anforderung 24: Es muss ein dem bei Gesundheitsdaten vorliegendem hohen Risiko angemessenes Schutzniveau gewährleistet werden. Hierzu muss ein Risikomanagementsystem vorhanden sein, in welchem u. a. alle betrachteten sowie aufgetretenen Risiken sowie die Maßnahmen zur Risikobehandlung dokumentiert sind.

Anforderung 25: Die Dokumentation muss insbesondere Begründungen beinhalten, wenn einzelne der in Art. 32 Abs. li. a-d DS-GVO genannten Maßnahmen nicht eingesetzt werden.

Anforderung 26: 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.

Anforderung 27: 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 28: Bzgl. der Rollen- und Rechtevergabe im Berechtigungs- und Rollenkonzept muss das Need-to-know-Prinzip angewendet werden.

5.1.7 Erinnerung an Termin

Eine Erinnerung an einen Termin ist grundsätzlich aus medizinischer und damit auch aus datenschutzrechtlicher Sicht nicht erforderlich, wenngleich diese seitens eines Leistungserbringers vielleicht wünschenswert ist. Daher ist eine Terminerinnerung grundsätzlich nur mit Einwilligung des jeweiligen Patienten rechtlich zulässig.

Anforderung 29: Der Leistungserbringer ist dafür verantwortlich, dass nur Patienten eine Terminerinnerung erhalten, die dieser mit einer ausdrücklichen, den Anforderungen der DS-GVO genügenden Einwilligung zustimmen. Dabei ist zu unterscheiden, ob ein Patient einer postalischen Erinnerung, dem Erhalt einer E-Mail zur Erinnerung oder einer Erinnerung mittels SMS zustimmte.

5.1.8 Anbieter eines digitalen Dienstes

Leistungserbringer, die ein Online-Terminmanagementsystem einsetzen, gelten als „Diensteanbieter“ i. S. d. DDG und müssen die entsprechenden Anforderungen erfüllen. Da Leistungserbringer einen entsprechenden Dienst i. d. R. von einem externen Dienstleister einkaufen, muss darauf geachtet werden, dass sich Leistungserbringer entsprechende Zusagen zur Erfüllung der gesetzlichen Vorgaben von ihrem Dienstleister vertraglich bestätigen lassen. Hierzu wird auf die entsprechende Literatur verwiesen, nachfolgend werden einige grundlegende Anforderungen in Kürze dargestellt.

Anforderung 30: Leistungserbringer müssen sich vertraglich bestätigen lassen, dass beim ausgewählten Dienstleister, welcher ein Online-Terminmanagementsystem im Auftrag des Leistungserbringers betreibt, kein unerlaubter Zugriff auf die für ihre digitalen Dienste genutzten technischen Einrichtungen möglich ist.

Anforderung 31: Leistungserbringer müssen sich vertraglich bestätigen lassen, dass der ausgewählte Dienstleister sich gegen Störungen, auch soweit sie durch Angriffe von außen verursacht werden, abgesichert hat.

Anforderung 32: Leistungserbringer sollten sich vom ausgewählten Dienstleister vertraglich zusichern lassen, dass Wartungsarbeiten und damit verbundene Nicht-Erreichbarkeit zuvor dem Leistungserbringer angekündigt werden und Störungen der Erreichbarkeit dem Leistungserbringer unverzüglich angezeigt werden. Erfolgt eine entsprechende Information, müssen Leistungserbringer Patienten über den eigenen Internetauftritt bzgl. der Nicht-Erreichbarkeit informieren.

Anforderung 33: Leistungserbringer müssen sich vom ausgewählten Dienstleister vertraglich zusichern lassen, dass gesetzlich verpflichtende Auskünfte sowie Datenweitergaben an Dritte nur nach vorheriger Rücksprache mit und Freigabe durch den Leistungserbringer erfolgen.

Anforderung 34: Leistungserbringer müssen prüfen, ob die vertraglichen Zusagen auch im laufenden Vertragsverhältnis eingehalten werden.

Anforderung 35: Links oder Weiterleitungen vom eigenen Internetauftritt des Leistungserbringers auf externe Online-Terminmanagementsysteme beim Dienstleister, welcher die Software im Auftrag des Leistungserbringers betreibt, müssen mit einem Abgrenzungshinweis versehen werden. Der Patient muss erkennen können, dass ein Link zu einem Dritten führt, oder, dass er an einen Dritten weitergeleitet wird.

5.2 Anforderungen, die Online-Terminmanagementsysteme erfüllen müssen

5.2.1 Mandantentrennung

Die Zusammenführung von Patientendaten von verschiedenen Leistungserbringern, z. B. um so Patienten mandantenübergreifend identifizieren zu können, stellt immer eine eigene Verarbeitung des Dienstleisters dar, denn der den Dienstleister beauftragende Leistungserbringer kann nicht über die Patientendaten anderer Leistungserbringer verfügen.

Anforderung 1: Im Rahmen einer Auftragsverarbeitung muss ein Online-Terminmanagementsystem zwingend eine strikte Mandantentrennung gewährleisten, sodass Patientendaten verschiedener Leistungserbringer nicht leistungserbringerübergreifend zusammengeführt werden können.

Anforderung 2: Ohne strikte Mandantentrennung liegt keine Auftragsverarbeitung vor. Vielmehr muss ein Vertrag zur gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO abgeschlossen werden.

5.2.2 Gewährleistung Betroffenenrechte

Ein Online-Terminmanagementsystem muss einem Leistungserbringer die Wahrnehmung der in Kap. III DS-GVO genannten Betroffenenrechte ermöglichen.

Anforderung 3: Die Software muss die Möglichkeit bieten, dass der jeweilige von der Verarbeitung betroffene Patient die Möglichkeit hat, jederzeit Einblick in alle zu seiner Person gespeicherten Daten zu erhalten. Dies umfasst auch die Möglichkeit, Änderungen seiner gespeicherten Daten nachzuvollziehen.

Anforderung 4: Die Software muss die Möglichkeit bieten, dass der jeweilige von der Verarbeitung betroffene Patient die Möglichkeit hat, eine Kopie seiner Daten zu erhalten. Dies muss sowohl als Ausdruck wie auch als ein für die jeweilige betroffene Person verwertbarer elektronischer Export in einem gängigen elektronischen Format erfolgen, welcher aller zu seiner Person gespeicherten Daten umgesetzt werden. Die Entscheidung, ob ein Ausdruck oder Export in elektronischer Form erfolgen muss, liegt beim Patienten.

Anforderung 5: Die Software muss die Möglichkeit bieten, dass der jeweilige von der Verarbeitung betroffene Patient die Möglichkeit hat, Daten zu seiner Person zu korrigieren.

Anforderung 6: Die Software muss die Möglichkeit bieten, dass der jeweilige von der Verarbeitung betroffene Patient die Möglichkeit hat, die zu seiner Person erhobenen und/oder verarbeiteten personenbezogenen Daten zu aktualisieren oder zu ergänzen.

Anforderung 7: Es muss protokolliert werden, wer wann welche Daten eines Betroffenen auf dessen Wunsch änderte. Die Protokollierung muss einen Zeitstempel, eindeutige ID der ändernden Person sowie die geänderten Daten umfassen. Es sollte die Eingabe der Begründung „Änderung erfolgte auf Wunsch des Betroffenen“ möglich sein.

Anforderung 8: Wurden Daten vom Betreiber des Online-Terminmanagementsystems an andere Stellen übermittelt, so sollten, sofern zumutbar, diese Stellen über erfolgte Berichtigungen informiert werden, sofern diese Benachrichtigung im Interesse des betroffenen Patienten liegt.

Anforderung 9: In dem Online-Terminmanagementsystem muss eine Möglichkeit vorhanden sein, um personenbezogene Daten mit dem Merkmal „gesperrt“ zu kennzeichnen. Eine weitere Verarbeitung von als gesperrt gekennzeichneten Daten darf nicht erfolgen.

Anforderung 10: Eine Sperrung darf nicht aufgehoben werden, ohne die betroffene Person zuvor zu informieren.

Anforderung 11: Ein Online-Terminmanagementsystem muss eine Möglichkeit bieten, dass ein Widerspruch zur Verarbeitung der eigenen Daten eines Patienten erfasst wird.

Anforderung 12: Ein Online-Terminmanagementsystem muss eine Möglichkeit bieten, dass Daten eines Patienten bei einem in der Software eingetragenen Widerspruch nicht weiter verarbeitet werden.

Anforderung 13: Bei einem Widerspruch sollte die Software einen Verantwortlichen darüber informieren, dass bei einem Widerspruch zur Verarbeitung die Löschung der vom Widerspruch betroffenen Daten entsprechend Art. 17 Abs. 1 lit. b DS-GVO erfolgen muss, wenn keine andere Rechtsgrundlage für die Verarbeitung, auf die der betroffene Patient vor Verarbeitungsbeginn hingewiesen wurde, existiert.

Anforderung 14: Ein Online-Terminmanagementsystem muss einem Verantwortlichen eine Möglichkeit bzw. Funktion bieten, mit welcher der Verantwortliche nicht mehr benötigte Daten bzw. zu löschende Daten identifizieren kann.

Anforderung 15: Ein Online-Terminmanagementsystem muss eine **Löschfunktion** implementiert haben, welche eine Rekonstruktion gelöschter Informationen ausschließt.

Anforderung 16: Ein Online-Terminmanagementsystem muss dem von der Verarbeitung betroffenen Patienten die Möglichkeit bieten, alle ihn betreffenden Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu exportieren.

Anforderung 17: Ein Online-Terminmanagementsystem sollte einem von der Verarbeitung betroffenen Patienten die Möglichkeit bieten, alle ihn betreffenden Daten zu einem anderen Verantwortlichen zu übertragen, z. B. an die für gesetzlich versicherte Personen bereitgestellte elektronische Patientenakte.

Anforderung 18: Eine automatisierte Einzelfallentscheidung mit rechtlichen oder ähnlichen Auswirkungen für die betroffene Person darf in dem Online-Terminmanagementsystem nicht erfolgen. Jede entsprechende Entscheidung muss durch einen Menschen erfolgen. Dies betrifft i. d. R. auch alle automatisiert vergebenen Termine, insbesondere Terminablehnungen, da eine abgelehnte oder zu spät erfolgende medizinische Betreuung die Gesundheit des betreffenden Patienten erheblich beeinträchtigen kann.

Anforderung 19: Eine Profilbildung darf in einem Online-Terminmanagementsystem nicht erfolgen.

5.2.3 Barrierefreiheit

Menschen mit Behinderungen dürfen entsprechend Art. 25 UN-BRK bei der Gesundheitsversorgung gegenüber Menschen ohne Behinderung nicht benachteiligt werden. Leistungserbringer als Kunden eines Dienstleisters eines Online-Terminmanagementsystems dürfen eine Software nur einsetzen, wenn diese Software-Lösung eine digitale Barrierefreiheit gewährleistet.

Die BITV¹⁴⁵ enthalten Vorgaben, die durch die Einhaltung der Web Content Accessibility Guidelines¹⁴⁶ (WCAG) eingehalten werden können. Es stehen auch Testangebote bzgl. Einhaltung der Barrierefreiheit zur Verfügung.¹⁴⁷

Anforderung 20: Online-Terminmanagementsysteme sollten schon bei der Anforderungsanalyse die Pflicht aus Art. 25 UN-BRK berücksichtigen und eine digitale Barrierefreiheit als Anforderung aufnehmen.

Anforderung 21: Online-Terminmanagementsysteme sollten ein barrierefreies Webdesign umgesetzt haben.

5.2.4 Privacy by Design

Online-Terminmanagementsysteme müssen den Anforderungen von Art. 25 DS-GVO genügen, d. h. „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ gewährleisten.

¹⁴⁵ Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz. Online, zitiert am 2024-09-12; verfügbar unter https://www.gesetze-im-internet.de/bitv_2_0/index.html

¹⁴⁶ World Wide Web Consortium: Web Content Accessibility Guidelines (WCAG). Online, zitiert am 2024-09-12; verfügbar unter <https://www.w3.org/TR/WCAG21/>

¹⁴⁷ DIAS GmbH - Daten, Informationssysteme und Analysen im Sozialen: Wir unterstützen Sie mit dem BIK BITV-Test. Online, zitiert am 2024-09-12; verfügbar unter <https://bitvtest.de/>

Anforderung 22: Datenschutz und IT-Sicherheit müssen für den gesamten Lebenszyklus des Systems berücksichtigt werden, angefangen bei Anforderungsanalyse und Design der Anwendung bis hin zur Abkündigung der IT-Anwendung, d. h. der Beendigung der Weiterentwicklung und Pflege der App sowie der Beendigung der Bereitstellung des Online-Terminmanagementsystems.

Anforderung 23: Bei der Planung von Online-Terminmanagementsystemen müssen von Anfang an die Anforderungen der DS-GVO berücksichtigt werden, insbesondere, dass in der Anwendung besonders sensible Gesundheitsinformationen verarbeitet werden. Die Dokumentation der Software-Entwicklung muss dies abbilden.

Anforderung 24: In der Design-Phase muss berücksichtigt werden, dass ein Online-Terminmanagementsystem besonders sensible Daten aus dem Gesundheitsbereich verarbeitet. Die Architektur muss dementsprechend das besonders hohe Schutzniveau bei der Verarbeitung, beginnend mit der Erhebung bis hin zur Löschung der Daten, gewährleisten.

Anforderung 25: Online-Terminmanagementsysteme müssen die in Art. 5 DS-GVO beschriebenen „Grundsätze für die Verarbeitung personenbezogener Daten“ einhalten, d. h. insbesondere auf die Einhaltung der Anforderungen bzgl. Datenminimierung, Zweckbindung, Speicherbegrenzung sowie Integrität und Vertraulichkeit entwickelt werden. In der Dokumentation des Online-Terminmanagementsystems muss die Einhaltung der Vorgaben nachvollziehbar dargestellt sein.

Anforderung 26: In einem Online-Terminmanagementsystem muss die Grundeinstellung der Software den maximal möglichen Datenschutz der Anwendung darstellen. Ein Leistungserbringer kann den Datenschutz durch Änderung der Einstellungen aktiv herabsenken.

Anforderung 27: Es dürfen in dem Online-Terminmanagementsystem keine personenbezogenen Daten verarbeitet werden, welche zur Erreichung des Zweckes einer Terminvergabe nicht zwingend erforderlich sind.

5.2.5 Sicherheit der Verarbeitung

Die personenbezogenen Gesundheitsdaten, welche in einem Online-Terminmanagementsystem erfasst und ggf. an andere IT-Systeme bei Leistungserbringern übermittelt werden, beinhalten stets ein hohes Risiko für die Patienten und erfordern entsprechend ein hohes Schutzniveau. Daher müssen Online-Terminmanagementsysteme insbesondere den nachfolgend dargestellten Anforderungen genügen.

Anforderung 28: Online-Terminmanagementsysteme müssen ein Rechte- und Rollenkonzept umgesetzt haben, welches nach dem Need-to-Know-Prinzip ausgelegt ist.

Anforderung 29: Eine Kombination von Rollen bzw. Zugriffsrechten für eine Person, welche der Person mehr Rechte auf Datenzugriffe erteilt, als für ihre Aufgabe nötig ist, muss durch technische und organisatorische Maßnahmen verhindert werden.

Anforderung 30: Von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte müssen vor ihrer Verwendung hinsichtlich der Gewährleistung einer sicheren Verarbeitung geprüft werden. Die Prüfung und das Ergebnis müssen dokumentiert und einem Kunden auf dessen Verlangen bereitgestellt werden.

Anforderung 31: Nutzt die Anwendung von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, müssen ungenutzte Funktionen von eingesetzter Drittanbieter-Software deaktiviert werden. Es muss sichergestellt sein, dass diese ungenutzten Funktionen durch Dritte nicht aktiviert werden können.

Anforderung 32: Nutzt die Anwendung von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, müssen diese von Drittanbietern bereitgestellte und genutzte Software in der aktuell verfügbaren stabilen („stable“) Version verwendet werden, experimentelle Versionen dürfen nicht genutzt werden.

Anforderung 33: Nutzt die Anwendung von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte, müssen diese Software-Produkte durch den Dienstleister regelmäßig auf Schwachstellen überprüft und bzgl. der Sicherheit bei der weiteren Nutzung beurteilt werden. Die Prüfung und die Beurteilung müssen dokumentiert werden. Drittanbieter-Software mit bekannten Sicherheitslücken darf nicht eingesetzt werden, ggf. muss sogar ein Produktrückruf durchgeführt werden, wenn anders die Sicherheit der sensiblen Gesundheitsdaten nicht gewährleistet werden kann.

Anforderung 34: Zur Gewährleistung der Verfügbarkeit der Daten muss die Anwendung die Möglichkeit der Erstellung von Backups sowie die Wiederherstellung von Daten aus den Backup-Daten anbieten.

Anforderung 35: Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems müssen behoben oder gegen Missbrauch abgesichert werden. Dies gilt auch für von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte.

Anforderung 36: Ungeplante Programmabbrüche (Exceptions) müssen abgefangen und kontrolliert werden. Das Online-Terminmanagementsystem muss insbesondere bei einer Exception jegliche Zugriffe auf sensible Daten abbrechen und entsprechende Daten im Speicher löschen.

Anforderung 37: Software-Komponenten inklusive virtueller Infrastrukturangebote wie beispielsweise eine Cloud, für die es keine Wartung oder Pflege durch den Dienstleister gibt, dürfen nicht verwendet werden. Dies gilt auch für von Dritten bereitgestellte Infrastrukturangebote wie beispielsweise eine Cloud, Softwarebibliotheken, Frameworks oder ähnliche Softwareprodukte.

Anforderung 38: Das System muss robust gegen unerwartete Eingaben sein. Insbesondere müssen alle Eingaben validiert werden. Weiterhin darf durch einen Austausch von Informationen in einer aufrufenden URL kein unberechtigter Zugriff auf Informationen möglich sein.

Anforderung 39: Der Dienstleister, der ein Online-Terminmanagementsystem für den Leistungserbringer betreibt, muss eine deutschsprachige Bedienungsanleitung bereitstellen, die so detailliert und so verständlich ist, dass durch Lesen der Bedienungsanleitung durch Anwender des Online-Terminmanagementsystems Fehler in deren Nutzung weitestgehend verhindert werden können. Die Bedienungsanleitung sollte eine Best-Practice-Anleitung beinhalten, mit welchen Einstellungen in dem Online-Terminmanagementsystem ein Maximum an Datenschutz und IT-Sicherheit erzielt werden kann. Das Online-Terminmanagementsystem kann durch eine Einführung in die Bedienung den Umgang mit dem Online-Terminmanagementsystem zusätzlich erleichtern.

Anforderung 40: Leistungserbringer müssen die Möglichkeit haben, in einem Online-Terminmanagementsystem aufgetretene Fehler einer Stelle zu melden, welche die Fehler in angemessener Zeit beseitigt. Es muss mindestens eine Hotline-Telefonnummer oder eine E-Mail-Adresse existieren, über die man eine entsprechende Meldung abgeben kann.

Anforderung 41: Für Protokolldaten wie auch für Crash Reports müssen dem geltenden Recht entsprechende Aufbewahrungszeiträume und Löschfristen festgelegt und eingehalten werden.

Anforderung 42: Protokolldaten wie auch für Crash Reports dürfen nicht sensible Daten, insbesondere keine Gesundheitsdaten enthalten.

Anforderung 43: In den Versand und die Auswertung von Protokolldaten und/oder Crash Reports muss der jeweilige Leistungserbringer ausdrücklich einwilligen, ansonsten darf ein Versand oder eine Auswertung nicht erfolgen.

Anforderung 44: Der Dienstleister muss alle Datenpannen dokumentieren. Dies muss in einem entsprechenden Verzeichnis der Datenpannen erfolgen.

Anforderung 45: Der Dienstleister muss bei Vorliegen einer Datenpanne unverzüglich alle Leistungserbringer informieren, deren Daten von der Datenpanne betroffen sind oder betroffen sein könnten.

5.2.6 Erinnerung an Termin

Viele Online-Terminmanagementsysteme besitzen eine Funktionalität, mit der Patienten an anstehende Termine erinnert werden. Das Online-Terminmanagementsystem darf jedoch nur an die Patienten, die dem zustimmten, eine Nachricht zur Erinnerung zusenden.

Anforderung 46: Bietet ein Online-Terminmanagementsystem die Funktionalität, Patienten an anstehende Termine zu erinnern, an, so muss auch die Funktionalität bestehen, dass eine Erinnerung nur an Patienten versendet wird, die einer entsprechenden Erinnerung ausdrücklich zustimmten. Daher muss das Online-Terminmanagementsystem zwischen Patienten, welche zustimmten, und Patienten, die dem nicht zustimmten, unterscheiden. Die Software muss dies für jeden einzelnen Fall jeweils neu beachten.

Anforderung 47: Bietet ein Online-Terminmanagementsystem die Funktionalität, Patienten an anstehende Termine mittels des Versands einer E-Mail zu erinnern, so dürfen nur Patienten eine Erinnerung-E-Mail erhalten, die dem Erhalt einer E-Mail ausdrücklich zustimmten. Daher muss das Online-Terminmanagementsystem zwischen Patienten, welche zustimmten, und Patienten, die dem nicht zustimmten, unterscheiden. Die Software muss dies für jeden einzelnen Fall jeweils neu beachten.

Anforderung 48: Bietet ein Online-Terminmanagementsystem die Funktionalität, Patienten an anstehende Termine mittels des Versands einer SMS zu erinnern, so dürfen nur Patienten eine Erinnerung-SMS erhalten, die dem Erhalt einer SMS ausdrücklich zustimmten. Daher muss das Online-Terminmanagementsystem zwischen Patienten, welche zustimmten, und Patienten, die dem nicht zustimmten, unterscheiden. Die Software muss dies für jeden einzelnen Fall jeweils neu beachten.

6 Abkürzungen

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
ArbMedVV	Verordnung zur arbeitsmedizinischen Vorsorge
ArbSchG	Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit (Arbeitsschutzgesetz)
ASiG	Gesetz über Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit (Arbeitssicherheitsgesetz)
Art.	Artikel
BGB	Bürgerliches Gesetzbuch
BGG	Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz)
BITV	Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung)
BMV	Bundsmantelvertrag
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
BVerfG	Bundesverfassungsgericht
CEN	Europäische Komitee für Normung (CEN aus dem französischen Comité Européen de Normalisation)
CENELEC	Europäische Komitee für elektrotechnische Normung (CENELEC aus dem französischen Comité Européen de Normalisation Électrotechnique),
DDG	Digitale-Dienste-Gesetz
DSG	Datenschutzgesetz
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DSK	Datenschutzkonferenz
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
EN	Europäische Norm
ErwGr.	Erwägungsgrund/Erwägungsgründe
ETSI	Europäische Institut für Telekommunikationsnormen (ETSI aus dem englischen European Telecommunications Standards Institute)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
GDD	Gesellschaft für Datenschutz und Datensicherheit (GDD) e. V.
GG	Grundgesetz
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Hs.	Halbsatz
i. d. R.	in der Regel
i. S.	im Sinne
i. S. d.	im Sinne des/der

i. S. d.	im Sinne der/des
i. V. m.	in Verbindung mit
i. S. v.	im Sinne von
IT	Informationstechnik, informationstechnisches...
Kap.	Kapitel
KHG	Krankenhausgesetz
LDSG	Landesdatenschutzgesetz
LKHG	Landeskrankenhausgesetz
LKG	Landeskrankenhausgesetz
lit.	littera (lat. „Buchstabe“)
MBO	Muster-Berufsordnung
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
Nr.	Nummer
OLG	Oberlandesgericht
RL	Richtlinie
Rn.	Randnummer
S.	Satz
SG	Sozialgericht
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz)
UN-BRK	Übereinkommen über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention)
Unterabs.	Unterabsatz
Urt.	Urteil
u. U.	unter Umständen
vgl.	vergleiche
vs.	versus (lat. „gegen“), wird häufig i. S. v. „Objekt/Begriff 1 gegenüber / im Vergleich zu Objekt/Begriff 2“ verwendet
VO	Verordnung
Ziff.	Ziffer

Anhang 1: Beispielhafte Nennung von Leistungserbringern

Anhang 1.1 Leistungserbringer von Heilmitteln

Heilmittel, die als Dienstleistung abgegeben werden und nicht entsprechend § 34 SGB ausgeschlossen wurden (beispielsweise Arzneimittel zur Anwendung bei Erkältungskrankheiten und grippalen Infekten), dienen entsprechend § 124 SGB V insbesondere folgenden Leistungen:

- der Physiotherapie,
- der Stimm-, Sprech- und Sprachtherapie,
- der Ergotherapie,
- der Podologie oder
- der Ernährungstherapie.

Dies kann den ambulanten Sektor betreffen, aber auch stationäre Erbringer von entsprechenden Dienstleistungen werden von der Regelung erfasst (§ 124 Abs. 5 SGB V). Die Versorgung mit Heilmitteln darf entsprechend § 32 Abs. 1 SGB V auch telemedizinisch erbracht werden.

Erbringer von entsprechenden Dienstleistungen sind z. B.:

- Ergotherapeuten
- Ernährungstherapeuten wie beispielsweise Diätassistent(-in)
- Masseur, z. B. Masseur (-in) und medizinische Bademeister(-in)
- Physiotherapeuten
- Podologen wie beispielsweise
 - o Medizinische(r) Fußpfleger(-in)
 - o Podologe/-in
- Stimm-, Sprech-, Sprach- und Schlucktherapeuten, somit können beispielsweise folgende Berufsgruppen erfasst sein:
 - o Akademische(r) Sprachtherapeut(-in)
 - o Atem-, Sprech- und Stimmlehrer(-in)
 - o Logopäde/-in
 - o Medizinische(r) Sprachheilpädagoge(-in)
 - o Staatlich anerkannter Sprachtherapeut(-in)

Anhang 1.2 Leistungserbringer von Hilfsmitteln

Dies umfasst alle Dienstleister, die als Vertragspartner mit Kranken- bzw. Pflegekassen (Pflegehilfsmittel nach § 40 SGB XI werden von den Pflegekassen finanziert) Hilfsmittel, die nicht entsprechend § 34 Abs. 4 SGB durch Rechtsverordnung des Bundesministeriums für Gesundheit von der gesetzlichen Leistung ausgeschlossen wurden, an gesetzlich Versicherte abgeben dürfen. Der Begriff „Hilfsmittel“ ist sehr weitgehend zu verstehen und umfasst beispielsweise:

- Gehhilfen,
- Hörhilfen,
- Inkontinenzhilfen,
- Kompressionsstrümpfe,
- Orthopädische Hilfsmittel,
- Mobilitätshilfen,
- Prothesen,
- Rollstühle,
- Schuheinlagen,
- Sehhilfen,
- Verbandmaterial.

Auch eine digitale Gesundheits- oder Pflegeanwendung (§ 33a SGB V bzw. § 40a SGB XI) stellt i. d. R. ein Hilfsmittel dar.

Im Hilfsmittelverzeichnis¹⁴⁸ der GKV werden alle zugelassenen Hilfsmittelarten aufgeführt. Dienstleister, die entsprechend Verträgen mit Krankenkassen zur Abgabe dieser Hilfsmittel berechtigt sind, fallen unter dem Begriff „Leistungserbringer“.

Leistungserbringer, die Hilfsmittel an Versicherte abgeben, sind beispielsweise:

- Apotheken,
- Augenoptiker(-in),
- Hörgeräteakustiker(-in),
- Orthopädietechniker(in),
- Orthopädieschuhmacher (-in),
- Sanitätshäuser.

¹⁴⁸ GKV-Spitzenverband: Hilfsmittelverzeichnis. Online, zitiert am 2024-07-14; verfügbar unter <https://www.gkv-spitzenverband.de/krankenversicherung/hilfsmittel/hilfsmittelverzeichnis/hilfsmittelverzeichnis.jsp> bzw. Online-Katalog unter <https://hilfsmittel.gkv-spitzenverband.de/home>

Anhang 2: Beispielhafte Aufzählung von Dienstleistern, die Online-Terminmanagementsysteme anbieten

Nachfolgend angeführte Dienstleister, welche Online- Terminmanagementsysteme anbieten, ist eine Sammlung von Software-Lösungen, welche den Autoren bekannt sind. Die Nennung ist daher als beispielhaft aufzufassen, da die Autoren nicht davon ausgehen, dass ihnen alle auf dem Markt erhältlichen Lösungen bekannt sind. Die Nennung enthält keine Wertung, insbesondere kann von einer Nicht-Nennung nicht davon ausgegangen werden, dass eine andere Software-Lösung besser oder schlechter ist; sie war den Autoren bei der Erstellung dieser Praxishilfe nur unbekannt.

Die Nennung erfolgt in alphabetischer Reihenfolge:

- 116117 (eTerminservice der Kassenärztliche Bundesvereinigung)
(<https://praxis.116117-termine.de/>)
- 321 MED
<https://321med.com/de>
- ärzte.de MediService
(<https://www.arzttermine.de/>)
- Arzttermine.de
<https://www.arzttermine.de/>
- Betty24
<https://www.betty24.de/>
- DMRZ
<https://www.dmrz.de/software/therapeutensoftware/online-terminbuchung>
- Doctena
(<https://www.doctena.de>)
- Doctolib
(<https://www.doctolib.de/>)
- Dr. Flex
(<https://dr-flex.de/>)Dubidoc
<https://www.dubidoc.de/>
- Dr.wait
<https://www.drwait.de/kalender>
- eTermin
<https://www.etermin.net/online-terminplaner-arzt>
- Etermio
<https://www.etermio.com/>
- jameda
(<https://www.jameda.de/>)
- samedi
(<https://www.samedi.com/>)
- TerMed
<https://www.termed.de/start>
- Terminiko
<https://www.terminiko.de/>
- Terminland
<https://www.terminland.de/>

- TimeControl
<https://arztpraxis-termine.de/>
- Timify
<https://www.timify.com/de/solutions/praxis-online-terminvereinbarung/>
- tomedo
<https://tomedo.de/praxissoftware/>