universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Rechts- bzw datenschutzkonforme sowie technisch sichere Datenverarbeitung in einer Arztpraxis sowie die damit verbundene Patientenkommunikation“

verfasst von / submitted by

Mag[a]. iur. Lea Strasser

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	Univ.-Prof. Dr. Dietmar Jahnel

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl	Amtsblatt
Abs	Absatz
AG	Amtsgericht
AGBs	Allgemeinen Geschäftsbedingungen
Art	Artikel
ÄrzteG	Ärztegesetz
BGBl	Bundesgesetzblätter
BNetzA	Bundesnetzagentur
bPK	bereichsspezifischen Personenkennzeichen
bzw	beziehungsweise
bspw	beispielsweise
CR	Computer und Recht
Dako	Datenschutz Konkret
dh	das heißt
DSB	Datenschutzbehörde
DSG 2000	Datenschutzgesetz 2000
DS-GVO	Datenschutzgrundverordnung
DuD	Datenschutz und Datensicherheit
E-GovG	E-Government-Gesetz
eHVD	eHealth-Verzeichnisdienst
EMRK	Europäische Menschenrechtskonvention
ErlRV	Erläuterungen zur Regierungsvorlage
ErwGr	Erwägungsgrund
etc	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FinStrG	Finanzstrafgesetz
GDA	Gesundheitsdiensteanbieter
gem	gemäß
GTelG	Gesundheitstelematikgesetz 2012
hL	herrschende Lehre
idF	in der Fassung
ieS	im engeren Sinne
iSd	im Sinne des
IP	Internet Protocol
IT	Informationstechnologie
iVm	in Verbindung mit
iZm	im Zusammenhang mit
JMG	Journal für Medizin- und Gesundheitsrecht
lit	litera
OTT	Over-the-top
RL	Richtlinie
RTR	Rundfunk und Telekom Regulierungs-GmbH
Rz	Randziffer
sog	sogenannte
StGB	Strafgesetzbuch

StGG	Staatsgrundgesetz
StPO	Strafprozeßordnung
SVG	Signatur- und Vertrauensdienstegesetz
TKG	Telekommunikationsgesetz 2003
TK-Kodex	Europäischer Kodex für die elektronische Kommunikation
VO	Verordnung
WBL	Wirtschaftsrechtliche Blätter
Z	Ziffer
zB	zum Beispiel

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Diplomarbeit die Sprachform des generischen Maskulinums angewendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

1. Einleitung

Das Thema eines Arztbesuches begegnet jedem Menschen im alltäglichen Leben. Es beginnt mit der telefonischen Terminvereinbarung, setzt sich mit der Aufnahme in der Ordination fort, und aufgrund der fortschreitenden digitalen Entwicklung ist darüber hinaus eine schriftliche elektronische Erkundung der Patienten über etwaige Befunde oder Untersuchungsergebnisse weit verbreitet. Da die ärztliche Kommunikation stets mit sehr persönlichen, den Gesundheitszustand der Patienten betreffenden Informationen verbunden ist, wird eine datenschutz- bzw datensicherheitsrechtliche Begutachtung dieser digitalen Kommunikationskanäle zum Schutz der betroffenen Personen unumgänglich.

Um nun auf die Frage der rechts- bzw datenschutzkonformen sowie technisch sicheren Kommunikation zwischen Ärzten und ihren Patienten eingehen zu können, soll in dieser Master Thesis zuerst herausgearbeitet werden, auf welcher rechtlichen Grundlage ein Arzt personenbezogene Daten in seiner Praxis bzw Ordination grundsätzlich erfasst und (automationsunterstützt) verarbeitet. Geht man in diesem Zusammenhang von einem niedergelassenen Arzt in seiner eigenen Praxis aus, so gibt es laut einer Studien-Erhebung aus der Zeitung "der Standard" im Jahr 2018 7029 Ärzte in Österreich, welche einen Kassenvertrag halten. In dieser Studie sind Allgemeinmediziner und Fachärzte, ausgenommen der Zahnärzte erfasst.[1] Gegenstand einer Datenverarbeitung von personenbezogenen Daten in einer Arztpraxis können sowohl Patientendaten als auch Mitarbeiterdaten und Daten etwaiger Lieferanten sein, wobei hier ausschließlich auf die Verarbeitung von Patientendaten eingegangen wird.

Diese Arbeit weist in ihrer rechtlichen Begutachtung weiters auf die Unterschiede hinsichtlich der datensicherheitsrechtlichen Anforderungen einer lokalen Speicherung und einer Cloud Computing Lösung durch den niedergelassenen Arzt hin. Die ärztlichen Kommunikationsarten im Einzelnen werden im Anschluss auf der Grundlage einer rechtmäßigen Datenverarbeitung im Hinblick auf die Datensicherheit beleuchtet. Insbesondere stellt die Kommunikation über die „Over the top-Dienste" (wie bspw der Messenger-Dienst WhatsApp) den Gesetzgeber für die datenschutz- bzw telekommunikationsrechtliche Einordnung vor große Herausforderungen und gilt es sich

[1] <https://www.derstandard.at/story/2000079701899/weniger-kassenaerzte-mehr-wahlaerzte-in-oesterreich> (16.11.2019)

in diesem Zusammenhang mit der datenschutzrechtlichen Verantwortlichkeit genauer zu beschäftigen.

2. Begriffsbestimmungen

2.1 Personenbezogene Daten Art 4 Z 1

"Unter personenbezogenen Daten versteht Art 4 Z 1 alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."[2]

2.2 Besondere Kategorien personenbezogener Daten Art 9

Personenbezogene Daten, durch die sich die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit ergeben, gehören zu den besonderen Kategorien personenbezogener Daten. Gleichermaßen ist davon auch die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person erfasst.[3]

2.3 Gesundheitsdaten Art 4 Z 15

Spricht man von „Gesundheitsdaten", so sind darunter personenbezogene Daten zu verstehen, die mit der körperlichen oder geistigen Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, in Zusammenhang stehen und aus denen sich Informationen über deren Gesundheitszustand ableiten lassen.[4]

[2] *Heißl* in Knyrim (Hrsg), DatKomm Art 2 DS-GVO Rz 46 (Stand 1.12.2018).
[3] Art 9 Abs 1 VO (EU) 2016/679.
[4] Art 4 Z 15 VO (EU) 2016/679.

2.4 Verarbeitung Art 4 Z 2

Eine Verarbeitung im Sinne der Datenschutzgrundverordnung bezeichnet "*jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*".[5]

Obwohl der Terminus "automatisierte Verfahren" in Art 4 Z 2 DS-GVO gebraucht wird, fehlt eine diesbezügliche Definition. Ausschlaggebend sind in diesem Zusammenhang die erleichterte Zugänglichkeit und Auswertung der Daten in einer großen Datenmenge.

Für *Jahnel/Bergauer* fließt in die Beurteilung ein, ob „*sämtliche Verarbeitungsschritte ohne menschlich-manuelle Interaktion (zB Tastatureingaben) programmgesteuert bzw elektronisch vorgenommen"* werden.[6]

2.5 Dateisystem Art 4 Z 6

Werden personenbezogene Daten nicht automatisiert verarbeitet, findet die DS-GVO nur dann Anwendung, wenn diese Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Als Dateisystem wird in der DS-GVO "*jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird*", bezeichnet.[7]

3. Allgemeine Zulässigkeit

3.1 Sachlicher und räumlicher Anwendungsbereich

Die Datenschutzgrundverordnung (DS-GVO) "*gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte*

[5] Art 4 Z 2 VO (EU) 2016/679.
[6] *Heißl in* DatKomm Art 2 Rz 49.
[7] *Heißl* in DatKomm Art 2 Rz 51.

Verarbeitung personenbezogener Daten [natürlicher Personen], die in einem Dateisystem gespeichert sind oder gespeichert werden sollen."[8]

Gemäß dem Erwägungsgrund 15 (zu Art 2 Abs 1 DS-GVO) soll das ernsthafte Risiko einer Umgehung der Vorschriften dadurch vermieden werden, dass der Schutz natürlicher Personen technologieneutral gestaltet und nicht von den verwendeten Techniken abhängig gemacht wird. Natürliche Personen sind folglich sowohl bei einer automatisierten Verarbeitung, als auch bei einer manuellen Verarbeitung von personenbezogenen Daten, wenn die personenbezogenen Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen, geschützt. Sind hingegen Akten oder Aktensammlungen sowie ihre Deckblätter nicht nach bestimmten Kriterien geordnet, sollten sie nicht in den Anwendungsbereich der Datenschutzgrundverordnung fallen.[9] Nicht unter den sachlichen Anwendungsbereich der DS-GVO fallen bloß mündlich, akustisch oder visuell erlangte Daten, unter der Voraussetzung, dass keine Speicherabsicht besteht.[10]

Sofern personenbezogene Daten im Rahmen von Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Europäischen Union verarbeitet werden, ungeachtet dessen, ob die Verarbeitung selbst in der Union erfolgt, ist auch der räumliche Anwendungsbereich der DS-GVO zu bejahen.[11]

Der räumliche Anwendungsbereich der DS-GVO ist unter anderem auch bei einer Verarbeitung außerhalb der Europäischen Union gegeben, wenn diese personenbezogenen Daten dazu dienen, Personen innerhalb der Europäischen Union Waren oder Dienstleistungen anzubieten, auch wenn keine Zahlung oder Gegenleistung erwartet wird.[12]

Geht man davon aus, dass jeder niedergelassene Arzt ein (automationsunterstütztes) Patientenverzeichnis führt, da das ärztliche Berufsrecht in § 51 Abs 1 und 3 Ärztegesetz (ÄrzteG) eine Dokumentations- und Aufbewahrungspflicht vorschreibt, dann kann der sachliche Anwendungsbereich der Datenschutzgrundverordnung bejaht werden. Eine Ausnahme aus dem sachlichen Anwendungsbereich, insbesondere die Verarbeitung

[8] Art 1 und Art 2 Abs 1 VO (EU) 2016/679.
[9] *Heißl* in DatKomm Art 2; ErwGr 15 VO (EU) 2016/679.
[10] *Heißl* in DatKomm Art 2 Rz 55.
[11] Art 3 Abs 1 VO (EU) 2016/679.
[12] Art 3 Abs 2 lit a VO (EU) 2016/679.

personenbezogener Daten für den persönlichen Gebrauch ("Haushaltsausnahme"), liegt jedenfalls nicht vor.[13] Weiters handelt es sich in dem vorliegenden Sachverhalt um inländische Arztpraxen, in welchen die Datenverarbeitung in der Union erfolgt, daher ist auch der räumliche Anwendungsbereich der DS-GVO zu bejahen.

3.2 Verarbeitung von Personenbezogenen Daten und Gesundheitsdaten in einer Arztpraxis

Unbestritten ist, dass ein niedergelassener Arzt in seiner Praxis nicht nur personenbezogene Daten, sondern darüber hinaus besondere Kategorien personenbezogener Daten und insbesondere Gesundheitsdaten verarbeitet.[14] Diese umfassen alle Daten, aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person ableitbar sind. Von personenbezogenen Gesundheitsdaten kann weiters dann gesprochen werden, wenn es um Informationen natürlicher Personen im Zusammenhang mit einer Anmeldung für oder der Erbringung von Gesundheitsdienstleistungen geht sowie bei jeglichen Daten, die Rückschlüsse auf Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand einer betroffenen Person ermöglichen, ungeachtet der Herkunft dieser Daten. Auch Kennzeichen, die einer natürlichen Person zu ihrer Identifizierung für gesundheitliche Zwecke zugeteilt wurden und schließlich die Informationen, deren Ableitung durch eine Untersuchung eines Körperteils oder einer körpereigenen Substanz, aus genetischen Daten und biologischen Proben ermöglicht wurde, werden von der Definition der personenbezogenen Gesundheitsdaten eingeschlossen.[15]

Der Arzt führt Aufzeichnungen über seine durchgeführten Beratungen und medizinischen Behandlungen, vermerkt im Besonderen auch den Gesundheitszustand der Patienten bei Übernahme der Beratung oder Behandlung, die Entstehung bzw Vorgeschichte einer Erkrankung, den Diagnose- und Krankheitsverlauf sowie die Art und den Umfang der bereits erfolgten beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Verschreibung und Anwendung von Arzneispezialitäten.[16] Damit

[13] Art 2 Abs 2 lit c VO (EU) 2016/679.
[14] <https://www.aekwien.at/datenschutzgrundverordnung> (16.11.2019); Art 4 Z 1 und Z 15 VO (EU) 2016/679.
[15] ErwGr 35 VO (EU) 2016/679.
[16] § 51 Abs 1 ÄrzteG.

einhergehend werden bei Patientenaufnahme des Weiteren der Name, die Adresse, die Kontaktdaten, das Geburtsdatum, die Sozialversicherungsnummer und gegebenenfalls der Arbeitgeber erfasst und gespeichert.

3.3 Rollenverteilung

Der Verantwortliche ist jene Person oder Einrichtung, die dafür Sorge zu tragen hat, dass die Datenschutzbestimmungen der DS-GVO eingehalten werden, dies als Konsequenz seiner Rolle in der DS-GVO. Als Adressat der Pflichten aus der DS-GVO, werden dem Verantwortlichen auch begrifflich alle Verantwortlichkeiten zugewiesen (Art 24 Rz 1). Ansprüche der betroffenen Personen und Maßnahmen der Aufsichtsbehörde sind ebenso an den Verantwortlichen zu richten. Im Vordergrund für die Frage, ob jemand als Verantwortlicher iSd Art 4 Z 7 DS-GVO qualifiziert wird und damit die Verpflichtungen erfüllen muss, steht, wer die Entscheidung über den Zweck und die Mittel der Verarbeitung von personenbezogenen Daten trifft.[17] Nicht erforderlich für die Zuschreibung der Eigenschaft des Verantwortlichen ist es, dass der Verantwortliche persönlich diese Daten verarbeitet oder die Daten selbst besitzt. Sobald er jedoch die Datenverarbeitung verfügt, werden ihm alle unter seiner Aufsicht und Anweisung tätigen Personen und Stellen als Hilfsorgane zugerechnet.[18] Jeder niedergelassene Arzt übernimmt definitionsgemäß aufgrund seiner Entscheidungsmacht über den Zweck und die Mittel die datenschutzrechtliche Rolle des Verantwortlichen bei der Verarbeitung von personenbezogenen Daten seiner Patienten. Bei diesen Patienten, deren Daten verarbeitet werden, handelt es sich um die "betroffenen Personen".[19]

An der Verantwortlichen-Eigenschaft des niedergelassenen Arztes würde sich auch nichts ändern, wenn er einen externen Dienstleister (als Auftragsverarbeiter) mit der lokalen Datenverarbeitung beauftragt, da dieser die Daten nicht zu eigenen, sondern vielmehr zu fremden Zwecken und auf Weisung des Arztes erhoben und gespeichert hat.[20] Ein Auftragsverarbeiter ist nach Definition der DS-GVO "*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*".[21] Neben dem Verantwortlichen, werden auch

[17] Art 24 VO (EU) 2016/679; ErwGr 74 VO (EU) 2016/679.
[18] *Hödl* in Knyrim (Hrsg), DatKomm Art 4 DS-GVO Rz 83 (Stand 1.12.2018).
[19] <https://www.aekwien.at/datenschutzgrundverordnung> (16.11.2019).
[20] *Hödl* in DatKomm Art 4 Rz 84.
[21] Art 4 Z 8 VO (EU) 2016/679.

dem Auftragsverarbeiter einige datenschutzrechtliche Verpflichtungen auferlegt, so zB das Führen eines Verzeichnisses seiner Verarbeitungstätigkeiten.

Beauftragt ein niedergelassener Arzt daher für seine Praxis einen externen IT-Dienstleister für einen Softwarewartungsvertrag, handelt es sich bei diesem um den Auftragsverarbeiter. Neben der Weisung des Verantwortlichen ist für eine auftragsgemäße Datenverarbeitung durch den Auftragsverarbeiter ein Auftragsverarbeitungsvertrag (Art 28 DS-GVO) erforderlich.

Als Abgrenzungskriterium wird immer die Entscheidung über die Verarbeitungszwecke und -mittel herangezogen, welche der Auftragsverarbeiter nicht definieren darf. Verstößt der Auftragsverarbeiter gegen die Bestimmungen der DS-GVO und verarbeitet die personenbezogenen Daten für eigene Zwecke, nimmt er selbst die Rolle des Verantwortlichen ein.[22]

3.4 Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten

Grundsätzlich ist die Verarbeitung personenbezogener Daten gemäß Art 6 DS-GVO nur dann rechtmäßig, wenn zumindest einer der sechs taxativ aufgezählten Zulässigkeitstatbestände (oder auch Erlaubnistatbestände genannt) erfüllt ist.[23]

Für den gegenständlichen Fall einer Praxis eines niedergelassenen Kassenarztes, wären mehrere der in Art 6 aufgezählten Erlaubnistatbestände denkbar. Zunächst ist in diesem Zusammenhang an die Erfüllung einer rechtlichen Verpflichtung zu denken, da § 51 Abs 1 des Ärztegesetzes eine Dokumentationspflicht für Ärzte vorsieht (Art 6 Abs 1 lit c DS-GVO iVm § 51 Abs 1 ÄrzteG). Im Hinblick auf den Behandlungsvertrag zwischen dem Arzt und seinen Patienten wäre weiters auch die Grundlage der Vertragserfüllung heranzuziehen (Art 6 Abs 1 lit b DS-GVO). Schließlich ist auch auf den möglichen Tatbestand der Einwilligung hinzuweisen (Art 6 Abs 1 lit a DS-GVO).[24]

Aus dem in der Verordnung neu eingeführten Wort "mindestens", könnte entnommen werden, dass eine Datenverarbeitung auch auf mehr als eine Rechtsgrundlage aus Art 6 DS-GVO gestützt werden kann. Ob allerdings der Erlaubnistatbestand der Einwilligung auch als Absicherung neben einem anderen Tatbestand genutzt werden kann, ist bislang

[22] *Hödl* in DatKomm Art 4 Rz 91 ff.
[23] Art 6 VO (EU) 2016/679
[24] *Engel Jun.*, Digitalisierung in der Medizin: Praxismanagement und Datenschutz, J Ästhet Chir 2018/11, 146 (149)

nicht abschließend geklärt. Man könnte diese Interpretationsmöglichkeit jedenfalls durch das Recht auf Löschung unterstrichen sehen, denn Art 17 Abs 1 lit b DS-GVO verlangt eine unverzügliche Löschung der Daten bei Widerruf der Einwilligung durch die betroffene Person, wenn keine "anderweitigen Rechtsgrundlagen" gegeben sind. Durch das bestehende "Rückgriffsverbot", gilt es jedoch zu beachten, dass bei Widerruf der Einwilligung und sofern die Datenverarbeitung bisher stets ausschließlich darauf gestützt wurde, nur in eingeschränktem Umfang auf einen gesetzlichen Erlaubnistatbestand zurückgegriffen werden darf. Es darf dadurch keinesfalls eine Irreführung der betroffenen Personen verursacht werden. Eine solche Irreführung könnte bewirkt werden, in dem einem Patient ein Einwilligungsformular ausgehändigt und damit gleichzeitig der Anschein erweckt wird, die Daten dürfen nur aufgrund der Einwilligung verarbeitet werden, wenngleich die Datenverarbeitung rechtmäßig auf einen anderen Tatbestand gestützt werden kann.[25]

Eine Rangordnung der sechs abschließend aufgezählten gesetzlichen Grundlagen für eine Datenverarbeitung personenbezogener Daten besteht darüber hinaus nach Meinung der Literatur nicht, sie stehen alternativ nebeneinander und/oder gemeinsam.[26]

3.4.1 Die Erfüllung einer rechtlichen Verpflichtung (Art 6 Abs 1 lit c DS-GVO)

Der Rechtfertigungsgrund des Art 6 Abs 1 lit c dient als Rechtsgrundlage für jene Sachverhalte, für die eine Datenverarbeitung *"zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt."*[27] Die Voraussetzung ist jedenfalls, dass der Verantwortliche einer bestimmten Rechtsvorschrift auch tatsächlich unterliegt, die dem Unionsrecht oder dem Recht des jeweiligen Mitgliedstaates entspringt.[28] Das Gesetz eines fremden Mitgliedstaates kann in diesem Zusammenhang lediglich ein "berechtigtes Interesse" nach Art 6 Abs 1 lit f begründen, nicht jedoch als datenschutzrechtliche Grundlage zur Erfüllung einer rechtlichen Verpflichtung herangezogen werden. Darüber hinaus hat die rechtliche Verpflichtung ausdrücklich und unmittelbar die Datenverarbeitung zu betreffen.[29] Jeder Arzt unterliegt dem Ärztegesetz, welches in seinem § 51 Abs 1 eine zehnjährige Dokumentationspflicht statuiert. Dadurch hat ein Arzt unter anderem Aufzeichnungen über die Beratung und

[25] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim (Hrsg), DatKomm Art 6 DS-GVO Rz 15 ff (Stand 1.10.2018).
[26] *Kastelitz/Hötzendorfer/Tschohl* in DatKomm Art 6 Rz 14.
[27] Art 6 Abs 1 lit c VO (EU) 2016/679.
[28] Art 6 Abs 3 VO (EU) 2016/679.
[29] *Kastelitz/Hötzendorfer/Tschohl* in DatKomm Art 6 Rz 39 ff.

Behandlung seiner übernommenen Patienten sowie deren Gesundheitszustand bei Patientenaufnahme zu führen. Weiters bezieht sich der Absatz 2 desselben Paragraphen unmittelbar auf die Datenverarbeitung, in dem er den Ärzten ausdrücklich die "automationsunterstützten Verarbeitung personenbezogener Daten gemäß Abs. 1 (...)" gestattet.[30] Aufgrund der Tatsache, dass die Verarbeitung der Patientendaten durch die rechtliche Verpflichtung der Ärzte erforderlich ist, ist der Rechtfertigungstatbestand des Art 6 Abs 1 lit c DS-GVO primär einschlägig.

3.4.2 Die Erfüllung eines Vertrages (Art 6 Abs 1 lit b DS-GVO)

Erfolgt die Datenverarbeitung, um einen Vertrag, dessen Vertragspartei die betroffene Person ist, zu erfüllen, oder um vorvertragliche Maßnahmen auf Anfrage der betroffenen Person durchzuführen, dient als Rechtsgrundlage Art 6 Abs 1 lit b DS-GVO.

Diese Definition bedarf einer Konkretisierung, da vorher zu prüfen ist, ob die Verarbeitung der Daten zur Erfüllung des gemeinsamen Vertrages auch erforderlich ist. Nur wenn die Erforderlichkeit bejaht werden kann, ist die Datenverarbeitung auf dieser Rechtsgrundlage rechtmäßig. Genauer gesagt wird das Kriterium der Erforderlichkeit danach beurteilt, ob die vollständige Vertragserfüllung nur durch die Verarbeitung der Daten gewährleistet werden kann. Wichtig dazu ist demnach die Beurteilung der Gründe für den Vertragsabschluss. Der Verantwortliche hat die Inhalte und Intentionen des Vertrages zu beleuchten und für alle Daten gesondert zu entscheiden, ob deren Erhebung also für die Vertragserfüllung erforderlich und zweckmäßig ist.[31] Da zwischen einem behandelnden Arzt und seinem Patienten zweifelsohne ein Behandlungsvertrag abgeschlossen wird, wird auf die Definition des Wortes "Vertrag" in diesem Zusammenhang verzichtet.[32]

Relevant ist vielmehr die genaue Betrachtung der einzelnen Daten, die ein niedergelassener Arzt von seinen Patienten verarbeitet, da jedes Datum für sich zur Vertragserfüllung oder zur Vorbereitung eines Vertragsschlusses erforderlich sein muss, um die Rechtsgrundlage für die Datenverarbeitung in Art 6 Abs 1 lit b DS-GVO zu finden. Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Telefonnummer und

[30] § 51 Abs 1 und 2 ÄrzteG.
[31] *Braun/Hasenauer,* Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DS-GVO, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht (2018) 9 (23).
[32] *Pletzer,* Die Haftung des Arztes für Behandlungsfehler und Aufklärungsmängel, in Kierein/Lanske/Wenda (Hrsg), Jahrbuch Gesundheitsrecht (2007) 199 (203).

möglicherweise der Arbeitgeber - diese Daten werden einerseits für die Identifizierung der Patienten und andererseits für eine Kontaktaufnahme mit den diesen aufgenommen. Die Erhebung erscheint zur Vertragserfüllung sohin erforderlich. Die Verarbeitung von Gesundheitsdaten wird gesondert behandelt.[33]

3.4.3 Die Einwilligung (Art 6 Abs 1 lit a DS-GVO)

Nachdem in Hinblick auf Art 5 Abs 1 lit a DS-GVO eine Datenverarbeitung nach Treu und Glauben nicht zu einer Irreführung des Betroffenen führen darf, sollte der Erlaubnistatbestand der Einwilligung subsidiär und nur dann herangezogen werden, wenn keine andere Möglichkeit zur rechtmäßigen Datenverarbeitung besteht.[34]

Für einen niedergelassenen Arzt wird daher die Rechtmäßigkeit der Datenverarbeitung primär auf die Erfüllung einer rechtlichen Verpflichtung bzw auf die Vertragserfüllung gestützt.[35]

3.5 Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten

Nachdem die Daten, die ein niedergelassener Arzt in seiner Praxis bei Patientenaufnahme und Behandlung verarbeitet und speichert, über die personenbezogenen Daten gemäß Art 6 DS-GVO hinausgehen und unter die besonderen Kategorien personenbezogener Daten nach Art 9 DS-GVO fallen, bedarf es dafür der Heranziehung einer anderen Rechtsgrundlage für die rechtmäßige Datenverarbeitung der erhobenen Gesundheitsdaten.[36]

Art 9 DS-GVO normiert ein Verarbeitungsverbot der besonderen Kategorien personenbezogener Daten, die auch die Gesundheitsdaten mit einschließen, und gewährt nur durch Ausnahmen vom Verarbeitungsverbot die Möglichkeit der zulässigen Datenverarbeitung. Die Tatbestände der zulässigen Datenverarbeitung sind in Art 9 Abs 2 lit a-j DS-GVO taxativ aufgezählt. Die strengen Anforderungen lassen sich schlicht und ergreifend mit der höheren Schutzwürdigkeit der besonderen Kategorien personenbezogener Daten erklären. Dies deshalb, da ansonsten erhebliche Risiken für die

[33] *Kastelitz/Hötzendorfer/Tschohl* in DatKomm Art 6 Rz 36 ff.
[34] Art 5 Abs 1 lit a VO (EU) 2016/679.
[35] *Engel Jun.*, J Ästhet Chir 2018/11, 149
[36] Ebd.

Grundrechte und Grundfreiheiten bestehen.[37] Der neuen Literatur zufolge sowie nach Ansicht des Europäischen Datenschutzausschusses bedarf es für die Zulässigkeit der Datenverarbeitung besonderer Kategorien neben einem Ausnahmetatbestand des Art 9 Abs 2 DS-GVO ergänzend eines Erlaubnistatbestandes nach Art 6 Abs 1 DS-GVO.[38]

3.5.1 Gesundheitsdaten (Art 9 Abs 2 lit h iVm Abs 3 iVm Art 6 Abs 1 lit c DS-GVO iVm § 51 ÄrzteG)

Art 9 Abs 2 lit h DS-GVO schafft die Rechtsgrundlage für die Verarbeitung von "besonderen Kategorien personenbezogener Daten" (insbesondere von Gesundheitsdaten), wenn diese zu Zwecken der "*Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien*" erforderlich ist.[39] Von den Gesundheitsdienstleistungen sollen daher sowohl die diagnostischen und kurativen, als auch die präventiven sowie nachsorgenden erfasst sein.

Art 9 Abs 3, welcher im Gegenzug wechselseitig auf Abs 2 Bezug nimmt und daher nur gemeinsam mit diesem gelesen werden kann, führt weiters dazu aus, dass die "*in Absatz 1 genannten personenbezogenen Daten (...) zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden (dürfen), wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal (...) (einem) Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls (...) einer Geheimhaltungspflicht unterliegt.*"[40] Für Ärzte wird - neben der in § 51 ÄrzteG geregelten Dokumentationspflicht - in seinem § 54 eine berufliche Verschwiegenheitspflicht normiert.[41] Diese gesetzlichen Grundlagen ermöglichen einem niedergelassenen Arzt die Erfüllung der datenschutzrechtlichen Anforderungen für eine Datenverarbeitung der Gesundheitsdaten seiner Patienten.

---

[37] *Kastelitz/Hötzendorfer/Tschohl* in DatKomm Art 6 Rz 1 ff. ErwGr 51 VO (EU) 2016/679.
[38] *Pfandlsteiner/Gabauer/Trieb*, Rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten - Zum Anwendungsbereich des GTelG 2012, RdM 2019/5, 171 (175).
[39] Art 9 Abs 2 lit h VO (EU) 2016/679
[40] Art 9 Abs 3 VO (EU) 2016/679
[41] § 51 und § 54 ÄrzteG; *Raabe-Stuppnig/Bisset,* To delete or not to delete: Lösch- und Aufbewahrungspflichten in der Medizin, JMG 2019/2, 100 (102).

3.6 Administrative Pflichten

3.6.1 Verzeichnis von Verarbeitungstätigkeiten (Art 30 DS-GVO)

Jeder Verantwortliche (und gegebenenfalls auch sein Vertreter) hat ein Verzeichnis über die in seiner Zuständigkeit befindlichen Verabeitungstätigkeiten (Verarbeitungsverzeichnis) zu führen. Die genau zu dokumentierenden Informationen für den Verantwortlichen sind in Art 30 Abs 1 DS-GVO (und in Abs 2 für den Auftragsverarbeiter) genannt. ErwGr 82 führt dazu näher aus, dass ein Verarbeitungsverzeichnis "zum Nachweis der Einhaltung dieser Verordnung" dient und damit die Kontrolle der Erfüllung und eine Zusammenarbeit mit der Datenschutzbehörde zu gewährleisten.[42] Über die Intention des ErwGr 82 hinaus, dient ein Verarbeitungsverzeichnis auch dem Überblick des Verantwortlichen und/oder des Auftragsverarbeiters selbst. Weiters kann dadurch auch die Umsetzung der durch die DS-GVO gebotenen technischen und organisatorischen Sicherheitsmaßnahmen sichergestellt werden. Schließlich erleichtert die Führung eines Verarbeitungsverzeichnisses zusätzlich andere Funktionen wie bspw die der Beweisführung, der Hilfestellung des Datenschutzbeauftragten oder die Auskunftserteilung bei Betroffenenanfragen (Art 13, 14 und 15 DS-GVO).[43] Ausgenommen von der Pflicht zur Führung eines Verzeichnisses über die Verarbeitungstätigkeiten sind Unternehmen bzw Einrichtungen mit einer Mitarbeiterzahl von weniger als 250 Personen unter der Voraussetzung, dass durch die von ihnen vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der Betroffenen geschaffen wird, die Verarbeitung über keine gelegentliche Tätigkeit hinausgeht oder davon weder die Verarbeitung besonderer Kategorien personenbezogener Daten, noch die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen erfasst ist.[44] Für den gegenständlichen Sachverhalt eines niedergelassenen Arztes, ist festzustellen, dass in Hinblick auf die Verarbeitung der Gesundheitsdaten seiner Patienten iSd Art 9 DS-GVO in seiner Praxis jedenfalls ein Verarbeitungsverzeichnis nach Art 30 Abs 1 DS-GVO erstellt und geführt werden muss.[45]

[42] ErwGr 82 VO (EU) 2016/679; *Gerhartl,* Verarbeitungsverzeichnis nach DS-GVO: Alles klar?, ecolex 2019/8, 719 (719 ff)
[43] *Bogendorfer* in Knyrim (Hrsg), DatKomm Art 30 DS GVO Rz 1 ff (Stand 1.10.2018).
[44] Art 30 Abs 5 VO (EU) 2016/679
[45] *Engel Jun.*, J Ästhet Chir 2018/11, 146 (148 f)

3.6.2 Datenschutz-Folgenabschätzung (Art 35 DS-GVO)

Grundsätzlich wird einem Verantwortlichen durch Art 35 Abs 1 DS-GVO die Pflicht auferlegt, bei einer risikoreichen Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, bspw durch Heranziehung neuer Technologien oder "*aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung*", eine Datenschutz-Folgenabschätzung der beabsichtigten Verarbeitungsvorgänge zum Schutz personenbezogener Daten durchzuführen. Sind mehrere ähnliche Verarbeitungsvorgänge mit vergleichbarem Risiko vorgesehen, ist eine einzige Abschätzung ausreichend.[46] Neben Absatz 4 dieses Artikels, welcher der Datenschutzbehörde vorschreibt, eine Liste für Vorgänge zu erstellen, die zwingend eine Datenschutz-Folgenabschätzung erfordern (DSFA-V), sieht Absatz 5 eine Möglichkeit für eine Listen-Erstellung durch die Datenschutzbehörde vor, in der die Arten der Vorgänge aufgezählt sind, für die es keiner Abschätzung bedarf.[47] Dem folgend ergriff die Datenschutzbehörde die genannte Möglichkeit und legte die Ausnahmen der Notwendigkeit für eine Datenschutz-Folgenabschätzung in der "Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV)" auf Grundlage des Art 35 Abs 5 DS-GVO fest.

Danach ist "die Patientenverwaltung und Honorarabrechnung" einzelner Ärzte anläßlich der Datenverarbeitung von der Verfassung einer Datenschutz-Folgenabschätzung ausgenommen.[48]

Bedauerlicherweise bleibt dadurch eine von der DS-GVO nicht abschließend beantwortete Frage auch weiterhin ungeklärt: ErwGr 91 zur DS-GVO führt dazu unter anderem aus, dass eine Verarbeitung von personenbezogenen Daten nicht als umfangreich iSd Art 35 Abs 1 gelten und damit nicht zwingend eine Datenschutz-Folgenabschätzung vorgeschrieben werden soll, wenn die Verarbeitung der Patientendaten durch einen einzelnen Arzt erfolgt.[49]

„Dies wurde im Schrifttum als unsachlich kritisiert, zumal etwa einzelne niedergelassene Allgemeinmediziner oder Pathologen im Rahmen von Gewebeuntersuchungen, eine

[46] Art 35 Abs 1 VO (EU) 2016/679; DSB 16.11.2018, DSB-D213.692/0001-DSB/2018, ecolex 2019/241, 553 (*Knyrim*)
[47] Art 35 Abs 4, 5 VO (EU) 2016/679.
[48] Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl I 165/1999 idF BGBl I 120/2017 (DSFA-A12).
[49] ErwGr 91 VO (EU) 2016/679.

deutlich größere Anzahl von personenbezogenen Daten verarbeiten können als etwa hochspezialisierte Gruppenpraxen von Privatärzten. Damit erweist sich die Anzahl der Verantwortlichen (allein) als ein untaugliches Kriterium für die konkrete Auslegung des Begriffs „umfangreich". "[50]

Im Umkehrschluss würde diese Ausführung des ErwGr bedeuten, dass Ärztezentren oder Gemeinschaftspraxen bei Patientenverwaltung bzw Honorarabrechnung nicht von der Pflicht zur Führung einer Datenschutz-Folgenabschätzung ausgenommen sind, da sie Gesundheitsdaten in großem Umfang verarbeiten. Hinzuweisen ist in diesem Zusammenhang auf die unterschiedliche Wortwahl der DSFA-A12 "einzelner Ärzte" einerseits und dem ErwGr 91 "durch einen einzelnen Arzt" andererseits. Nach wie vor ungeklärt ist, ob die DSFA-A12 darüber hinaus Ärzte-Gemeinschaften mit einschließen wollte. Jedenfalls bleibt die Auflösung der Abgrenzungsfragen, ab welcher Zahl an Ärzten eine DSFA durchzuführen ist, nach wie vor abzuwarten.[51]

3.6.3 Benennung eines Datenschutzbeauftragten (Art 37 DS-GVO)

Die Vorgaben über die (verpflichtende) Benennung eines Datenschutzbeauftragten, der die Aufgabe hat, bei der Gewährleistung sowohl des in Art 8 Abs 1 Grundrechtecharta (GRC), als auch des in Art 16 Abs 1 AEUV geregelten Grundrechts auf Datenschutz mitzuwirken, befinden sich in Art 37 DS-GVO.[52] Obgleich zu den Kerntätigkeiten eines Arztes, die Verarbeitung besonderer Kategorien personenbezogener Daten, insbesondere von Gesundheitsdaten, zuzurechnen ist, wie dies in Art 37 Abs 1 lit c DS-GVO aufgegriffen wurde, fehlt bei einem einzelnen niedergelassenen Arzt dennoch die zusätzliche Komponente der "umfangreichen" Verarbeitung. Denn auch für Art 37 Abs 1 lit c DS-GVO ist ErwGr 91 einschlägig, der eine Verarbeitungstätigkeit durch einen einzelnen Arzt nicht als umfangreich qualifiziert.[53] Ist ein Verantwortlicher (oder Auftragsverarbeiter) nach der Datenschutzgrundverordnung nicht verpflichtet einen Datenschutzbeauftragten zu bestellen, besteht dessen ungeachtet die Möglichkeit, auf freiwilliger Basis einen zu ernennen. Von grundlegender Bedeutung ist hierbei, dass dennoch die Grundsätze und Vorgaben für die Bestellung der verpflichtenden Fälle eingehalten werden. Widrigenfalls kann dieser nicht die Rolle des formellen gesetzlichen

[50] *Jahnel,* „Whitelist" und „Blacklist" zur Datenschutz-Folgenabschätzung, jusIT 2019/12, 36 (37).
[51] *Pollirer/Weiss/Knyrim/Haidinger,* DSG[4] Anlage DSFA-AV (Stand 1.4.2019).
[52] *König* in Knyrim (Hrsg), DatKomm Art 37 DS-GVO Rz 1 ff (Stand 1.12.2018).
[53] Art 37 Abs 1 lit c VO (EU) 2016/679, ErwGr 91 VO (EU) 2016/679; DSB 16.11.2018, DSB-D213.692/0001-DSB/2018.

Datenschutzbeauftragten einnehmen, sondern hat lediglich eine Datenschutzverantwortung inne.[54]

3.7 Informationspflichten (Art 13, 14, 18 und 21 DS-GVO)

Im Sinne der Transparenz verpflichtet die Datenschutzgrundverordnung die Verantwortlichen, bei der Verarbeitung personenbezogener Daten grundsätzlich eine Vielzahl an Informationen den betroffenen Personen gegenüber offenzulegen. Diese Offenlegungs- und Informationspflichten sind in Art 13 und 14 DS-GVO konkretisiert und differenzieren zwischen den Informationspflichten bei Datenerhebung unmittelbar bei der betroffenen Person und der Datenerhebung, die nicht bei der betroffenen Person selbst erfolgt ist.[55]

Diesen Grundsätzen der Informationspflichten in Hinblick auf die Datenverarbeitung folgt das Ärztegesetz nicht und weicht ausdrücklich in seinem § 3b Abs 2 davon ab. Obgleich die Verarbeitung personenbezogener Daten nach dem Ärztegesetz neben seinen eigenen Zwecken in § 3b Abs 1 auch die Einhaltung der Normen aus der Datenschutzgrundverordnung vorsieht, schließt Abs 2 "*hinsichtlich der Verarbeitung personenbezogener Daten gemäß Abs. 1 (...) die Rechte und Pflichten gemäß Art. 13, 14, 18 und 21 Datenschutz-Grundverordnung aus (...).*"[56] Damit sieht das Ärztegesetz zwar die Einhaltung der Datenschutzgrundverordnung als solche jedenfalls vor, nimmt aber genau vier einzelne Bestimmungen aus. Konkret sind davon - neben den Informationspflichten (Art 13 und 14) - das Recht auf Einschränkung der Verarbeitung (Art 18) und das Widerspruchsrecht (Art 21) umfasst.[57]

Das Recht auf Einschränkung der Verarbeitung ist formal als eigenständiger Rechtsanspruch in Art 18 DS-GVO geregelt und kann dennoch nicht allein für sich gelesen und interpretiert werden. Vielmehr handelt es sich dabei systematisch um einen Anspruch, der nur in Zusammenhang mit dem Recht auf Berichtigung (Art 16), dem Recht auf Löschung (Art 17) und/oder dem Widerspruchsrecht (Art 21) eine Rechtsfolge

[54] Art-29-Datenschutzgruppe, Stellungnahme 12/2016 idF 04/2017 Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), WP 243 rev.01, 16/DE, 24. <https://www.dsb.gv.at/documents/22758/112500/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf/d241f0fd-6908-44fd-a12a-0f861e7a1dfb> (16.11.2019).

[55] *Illibauer* in Knyrim (Hrsg), DatKomm Art 13 DS-GVO (Stand 1.10.2018); *Pollirer,* Checkliste Erfüllung der Informationspflichten gem Art 13 und 14 DS-GVO, Dako 2018 H 4, 86 (87).

[56] § 3b ÄrzteG.

[57] § 3b ÄrzteG; Art 13, 14, 18 und 21 VO (EU) 2016/679.

auslöst. Die Einschränkung der Verarbeitung zielt darauf ab, dass die Daten - bis auf die Speicherung - nicht mehr verarbeitet werden dürfen. Die übrigen Verarbeitungsvorgänge unterliegen strengen Vorgaben (Art 4 Z 3, Art 18 Abs 2).[58]

Das Widerspruchsrecht nach Art 21 DS-GVO ermöglicht betroffenen Personen "*aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen*". Ob die Datenverarbeitung demzufolge im Einzelfall untersagt wird, bleibt in dieser Arbeit außer Betracht. Vielmehr ist an dieser Stelle darauf hinzuweisen, dass eine Datenverarbeitung durch einen Arzt jedenfalls nicht auf die Rechtfertigungsgründe des Art 6 Abs 1 lit e und f - zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten - gestützt werden würde und dennoch schließt das Ärztegesetz die Anwendung dieser Bestimmung ausdrücklich aus. Dieser Vorgang bedeutet einen Ausschluss einer Rechtsnorm, welche ohnehin keine Anwendung gefunden hätte.[59]

Begründet wurde der Ausschluss der Anwendbarkeit des Rechts auf Einschränkung und auf Widerspruch damit, dass ohne diese Maßnahme die Besorgung der Aufgaben des Ärztegesetzes "*von vornherein wesentlich beeinträchtigt und eine geordnete Durchführung der gesetzlich geregelten Aufgaben nicht mehr möglich*" wäre. Zudem hätte die Ausübung dieser Rechte und Pflichten einen "*beträchtlichen und unverhältnismäßigen Aufwand*" zur Folge.[60]

Das Recht auf Löschung, das in Art 17 Abs 1 und 2 DS-GVO ein weiteres Betroffenenrecht gewährleistet, wird vom Ärztegesetz nur deshalb nicht eigens ausgeschlossen, da Art 17 Abs 3 lit b bereits einen eigenen Ausschlusstatbestand für jene Datenverarbeitung vorsieht, die der Erfüllung einer rechtlichen Verpflichtung nach dem nationalen Recht dient. In diesem Zusammenhang ist auf die einschlägige gesetzliche ärztliche Dokumentations- und Aufbewahrungspflicht hinzuweisen, die die Speicherung der Daten für zehn Jahre vorsieht.[61]

[58] *Haidinger* in Knyrim (Hrsg), DatKomm Art 18 DS-GVO Rz 1 (Stand 1.10.2018).
[59] *Haidinger* in DatKomm Art 21 DS-GVO.
[60] ErlRV 108 BlgNr XXVI.GP, 52 ff.
[61] § 51 Abs 3 ÄrzteG.

Das Auskunftsrecht der betroffenen Person (Art 15 DS-GVO) und das Recht auf Berichtigung (Art 16 DS-GVO) werden nicht beschränkt oder ausgeschlossen und bleiben demnach auch für Patienten aller Ärzte aufrecht.

Ein interessanter Aspekt in diesem Zusammenhang ist, dass der Ausschluss der Informationspflichten gemäß Art 13 und 14 DS-GVO hingegen in den Erläuterungen zum 2. Materien-Datenschutz-Anpassungsgesetz 2018 mit keinem Wort begründet wird.

Nachdem sich die Verpflichtung zur Einhaltung der Datenschutzgrundverordnung zweifelsfrei bereits aus ihrer unmittelbaren Anwendbarkeit ergibt, ist die Grundlage für eine Durchbrechung der von ihr geregelten Rechte und Pflichten gleichermaßen nur durch ihre eigenen Artikel und die darin normierten Ausnahmebestimmungen möglich.[62] Der österreichische Gesetzgeber stützt daher die Regelung des Ärztegesetzes (§ 3b) auf die Öffnungsklausel in Art 23 DS-GVO, die den Mitgliedstaaten unter anderem die Schaffung oder Beibehaltung weitreichender Ausnahmen von den Betroffenenrechten ermöglicht. Ausnahmen gemäß Art 23 DS-GVO dürfen ausschließlich im Wege von Gesetzgebungsmaßnahmen in Kraft gesetzt werden, sofern die im Einzelfall angedachte Beschränkung "*den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt*"[63], die darüber hinaus eines oder mehrere der abschließend aufgezählten Ziele (Art 23 Abs 1 lit a-j) verfolgt und "*insbesondere gegebenenfalls*" einen Mindestinhalt umschließt.[64] Wenngleich die möglichen Ziele in Art 23 Abs 1 DS-GVO unzweifelhaft durch seine Wortwahl taxativ aufgezählt sind, einhält lit e im Gegensatz dazu eine Generalklausel zur Erreichung des Schutzes sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats und geht dabei im Besonderen auf die wichtigen wirtschaftlichen oder finanziellen Interessen sowie auf den Bereich der öffentlichen Gesundheit und der sozialen Sicherheit ein. Durch die Generalklausel wird die taxative Aufzählung in der praktischen Durchführung umgangen. Für die gesetzliche Bestimmung des § 3b Abs 2 ÄrzteG kann zusätzlich zur Generalklausel auch das Ziel des Art 23 Abs 1 lit g DS-GVO als Schutz der berufsständischen Regeln reglementierter

[62] ErlRV 108 BlgNr XXVI.GP, 52 ff.
[63] Art 23 Abs 1 VO (EU) 2016/679.
[64] *Haidinger* in DatKomm Art 23 Rz 7.

Berufe herangezogen werden.[65] Wenngleich der letztgenannten Rechtfertigung durch Art 23 Abs 1 lit g DS-GVO hier mE nicht zuzustimmen ist.

3.8 Sicherheit der Verarbeitung (Art 32 DS-GVO, GTelG)

Neben den Anforderungen an die Rechtmäßigkeit der Datenverarbeitung, die dem Verantwortlichen in Art 24 DS-GVO dafür die Ergreifung von "geeigneten technischen und organisatorischen Maßnahmen" auferlegt, ist überdies die Sicherheit der Datenverarbeitung von immenser Bedeutung und daher uneingeschränkt zu garantieren.[66] Art 32 DS-GVO, der die wesentliche Rechtsvorschrift für die Sicherheit der Datenverarbeitung ist und darüber hinaus die Umsetzung eines Sicherheitskonzepts vorsieht, richtet sich sowohl an den Verantwortlichen, als auch an den Auftragsverarbeiter. Ergänzend dazu regelt die DS-GVO in ihrem Art 28 Abs 3 lit c, dass die verpflichtende Ergreifung der Sicherheitsmaßnahmen nach Art 32 durch den Auftragsverarbeiter sogar im Auftragsverarbeitungsvertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter zu besiegeln ist.[67] Die davon abzuleitende "*doppelte Verantwortlichkeit für die Einhaltung der Informationssicherheit*" hat durchaus ihre Sinnhaftigkeit, da nicht davon ausgegangen werden kann, dass der Verantwortliche ausreichend Einblick sowie die Kontrollmöglichkeit der Vertragserfüllung iSd Art 28 Abs 3 lit c DS-GVO hat. Durch Art 32 DS-GVO ist sohin die eigenständige Verantwortlichkeit über die ordnungsgemäße Umsetzung der Sicherheitsmaßnahmen bei Datenverarbeitung des Auftragsverarbeiters gesichert.[68] Der Grund für den hohen Grad an Bedeutung der Datensicherheit, ist die Weiterentwicklung der Informations- und Kommunikationstechnologie. Wenngleich diese unbestrittenermaßen viele Vorteile mit sich bringt, birgt sie dennoch einige Risiken, die es zu verhindern gilt. Als Anforderung an den Verantwortlichen (und Auftragsverarbeiter) im Zusammenhang mit der Informationssicherheit legt die DS-GVO in Art 32 Abs 1 die Verpflichtung fest, "*unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen,* (...) *geeignete technische und organisatorische Maßnahmen*"[69] zu

[65] *Ebd.* Rz 17; ErlRV 108 BlgNr XXVI.GP, 52 ff.
[66] Art 24 Abs 1 VO (EU) 2016/679.
[67] Art 32 und 28 Abs 3 lit c VO (EU) 2016/679.
[68] *Pollirer* in Knyrim (Hrsg), DatKomm Art 32 DS-GVO Rz 19 (Stand 1.10.2018).
[69] Art 32 Abs 1 VO (EU) 2016/679.

ergreifen, damit ausreichend und angemessenen für Schutz des jeweils vorliegenden Risikos gesorgt ist.[70]

Eigens in der Verordnung als geeignete Maßnahmen angeführt, werden die Pseudonymisierung und Verschlüsselung der Daten, weiters die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung sowie die Fähigkeit zur zeitnahen Wiederherstellung der *"Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall"* und ein regelmäßiges Überprüfungs-, Bewertungs- und Evaluierungsverfahren über die Wirksamkeit der gewählten Sicherheitsmaßnahmen. Diese vier genannten möglichen Maßnahmen zur Gewährleistung der Datensicherheit werden in der Verordnung jedenfalls nur demonstrativ genannt und gelten nicht als abschließend. Dies wird durch die gewählte Wortwahl "*unter anderem*" verdeutlicht.[71] Für das gebührende Schutzniveau und die Wahl der passenden Sicherheitsmaßnahmen einer Datenverarbeitung, sind die entsprechenden Risiken, insbesondere "*Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden*", zu beachten.[72] Schließlich soll Art 32 Abs 4 DS-GVO sicherstellen, dass auch Mitarbeiter der Verantwortlichen bzw Auftragsverarbeiter sowie diesen anderweitig unterstellte natürliche Personen ihnen zugängliche Daten grundsätzlich nur auf Anweisung der Verantwortlichen verarbeiten. Sind diese Personen hingegen "*nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet*", können die Daten ohne Anweisung der Verantwortlichen, aber auf der einschlägigen rechtlichen Grundlage verarbeitet werden.[73]

Neben den generellen Anforderungen des Art 32 DS-GVO sind auch die Sicherheitsanforderungen des Gesundheitstelematikgesetzes (GTelG) zu berücksichtigen. In seinen 31 Paragrafen hat das Gesundheitstelematikgesetz die Verarbeitung (Art. 4 Z 2 DS-GVO) personenbezogener elektronischer Gesundheitsdaten und genetischer Daten (Art. 4 Z 15 und Z 13 DS-GVO) durch die Gesundheitsdiensteanbieter (GDA) gemäß § 2 Z 2 zum Gegenstand. Nachdem ein Arzt in der Rolle des Verantwortlichen (§ 28 Abs 1 Z 1 GTelG) regelmäßig Gesundheitsdaten oder genetische Daten in elektronischer Form zu

[70] *Pollirer* in DatKomm Art 32 Rz 1 ff.
[71] Art 32 Abs 1 VO (EU) 2016/679.
[72] Art 32 Abs 2 VO (EU) 2016/679.
[73] Art 32 Abs 4 VO (EU) 2016/679.

Zwecken der medizinischen Behandlung oder Versorgung verarbeitet, ist er damit nach den Begriffsbestimmungen des § 2 Z 2 lit a GTelG als Gesundheitsdiensteanbieter zu qualifizieren. Ziel des Gesundheitstelematikgesetzes ist unter anderem die Schaffung von bundeseinheitlichen Mindeststandards, um die Datensicherheit zu erweitern, einen Datenmissbrauch zu verhindern sowie die Informationsgrundlagen für die Entwicklung und Steuerung der Gesundheitstelematik zu schaffen und diese auszubauen.[74]

Die Paragraphen 3 bis 7 GTelG bleiben für die Betrachtung der rechtmäßigen lokalen Datenverarbeitung eines einzelnen niedergelassenen Arztes in seiner Praxis außer Acht, da es diesbezüglich zu keiner elektronischen Übermittlung kommt.

Zu beachten ist jedenfalls § 8 GTelG, wonach Gesundheitsdiensteanbieter alle im Rahmen eines IT-Sicherheitskonzepts nach Art 32 DS-GVO und dem Gesundheitstelematikgesetzes vorgesehenen Datensicherheitsmaßnahmen dokumentieren und aufzeichnen müssen. Dadurch soll sichergestellt werden, dass der Datenzugriff und gegebenenfalls eine Datenübermittlung ordnungsgemäß erfolgt und Unbefugte keinen Zugriff erhalten. Definitionsgemäß handelt es sich bei dem "IT-Sicherheitskonzept" iSd § 8 Abs 1 GTelG um die "*Summe aller Datensicherheitsmaßnahmen eines Gesundheitsdiensteanbieters, die zum Schutz von personenbezogenen Daten, insbesondere von besonderen Kategorien personenbezogener Daten, notwendig und angemessen im Sinne des Art 32 DS-GVO sind.*"[75]

3.9 Wahrung der Betroffenenrechte (Art 15, 16, 17, 19 und 20 DS-GVO)

3.9.1 Auskunftsrecht der betroffenen Person (Art 15 DS-GVO)

Die Datenschutzgrundverordnung ermöglicht es betroffenen Personen, Auskunft hinsichtlich der sie betreffenden und bereits erhobenen personenbezogenen Daten einzuholen. Zur Gewährleistung bzw eigenen Überprüfbarkeit der rechtmäßigen Datenverarbeitung soll dieses Auskunftsrecht ohne Hindernisse und in angemessenen Abständen ausgeübt werden dürfen. Dieses Recht soll auch eine Klärung ermöglichen, ob überhaupt Daten der betroffenen Person erhoben wurden. Erwägungsgrund 63 erwähnt ausdrücklich, dass dieses Recht auch die Einholung der Auskünfte über die eigenen

[74] Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelT 2012), BGBl 111/2012 idF 100/2018.
[75] § 2 Z 3 GTelG

bereits verarbeiteten Gesundheitsdaten umfasst. Betroffene Personen können sich demnach über die "*Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten*" erkundigen.[76] Insbesondere soll das Auskunftsrecht der Aufklärung über die Verarbeitungszwecke, die Art der Kategorien personenbezogener Daten, die Speicherdauer, die Datenempfänger sowie unter anderem über die Art der Logik der automatischen Datenverarbeitung und die Folgen einer solchen Datenverarbeitung, sofern sie auf Profiling beruht, dienen.[77]

Nach Art 15 Abs 3 DS-GVO hat der Verantwortliche dem Betroffenen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Erst für alle weiteren beantragten Kopien, kann ihm der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten vorschreiben. Bei elektronischer Antragstellung sind die Informationen dem Betroffenen in einem allgemein bekannten elektronischen Format zur Verfügung zu stellen, falls kein spezielles Format gewünscht wird.[78]

Interessant an dieser Stelle sei zu erwähnen, dass § 51 Abs 1 ÄrzteG zwar eine Auskunftspflicht der Ärzte gegenüber den Patienten vorsieht und darüber hinaus diese veranlasst, den Patienten Einsicht in die ärztliche Dokumentation zu gewähren, jedoch kann bei Wunsch auf Herstellung einer Abschrift bereits bei der ersten Ausfertigung ein Kostenersatz verlangt werden.[79] Im Gegensatz dazu ist die erste Kopie der gegenständlichen Daten nach der DS-GVO kostenlos auszustellen. Es bleibt abzuwarten, ob eine Klarstellung im oder Gesetzesänderung des Ärztegesetzes erfolgt. Bis zu einer allfälligen Gesetzesänderung findet mE die Bestimmung des Ärztegesetzes aufgrund der Generalklausel des Art 23 Abs 1 lit e DS-GVO Anwendung.

3.9.2 Recht auf Berichtigung (Art 16 DS-GVO) und Recht auf Löschung („Recht auf Vergessenwerden") (Art 17 DS-GVO)

Art 16 DS-GVO gewährt dem Betroffenen zwei Rechtsansprüche gegenüber dem Verantwortlichen. Einerseits besteht dadurch das Recht, von diesem die Berichtigung

[76] ErwGr 63 VO (EU) 2016/679.
[77] ErwGr 63 VO (EU) 2016/679; *Pollirer,* Checkliste Auskunftsrecht nach Art 15 DS-GVO, Dako 2017/3, 66 (66 ff).
[78] *Haidinger*, in DatKomm Art 15 Rz 35.
[79] § 51 Abs 1 ÄrzteG.

unrichtiger personenbezogener Daten, welche die betroffene Person betrifft, zu verlangen (Recht auf Berichtigung ieS), andererseits kann die betroffene Person, sofern der Zweck der Verarbeitung diesem nicht entgegenspricht, die Vervollständigung unvollständiger personenbezogener Daten begehren (Recht auf Vervollständigung).[80] Unbestritten ist, dass das Recht auf Berichtigung ieS nur dann besteht, wenn eine Unrichtigkeit personenbezogener Daten vorliegt. Nachdem die DS-GVO keine nähere Definition über das Wort "Unrichtigkeit" zur Verfügung stellt, muss auf den allgemeinen Sprachgebrauch zurückgegriffen werden, der als Synonyme ua die Termini "inkorrekt", "unzutreffend" oder "falsch" kennt. Als Beispiele können etwa eine Adressänderung auf Grund eines Wohnortwechsels oder eine Namensänderung nach einer Heirat herangezogen werden. Der Verantwortliche, der nach wie vor eine alte Adresse oder den Mädchennamen speichert, verarbeitet Daten, die schlichtweg nicht mehr mit der Realität übereinstimmen. Rechtliche Einordnungen können ebenso zu einer Verarbeitung unrichtiger Daten führen, wenn der Status einer betroffenen Person als ledig geführt wird, die bereits verheiratet ist. Geringfügige Unrichtigkeiten sind nicht erfasst, sofern diese nicht Folgefehler oder gar Verwechslungen auslösen können. Wie es zu der Verarbeitung der unrichtigen Daten gekommen ist, ist jedenfalls unbedeutend für diesen Rechtsanspruch. Primär handelt es sich bei dem Berichtigungsanspruch dem Inhalt nach ausschließlich um personenbezogene Daten des Antragstellers, auch wenn unter Umständen Daten anderer Personen für den Antragsteller von Bedeutung sein können. Im Vergleich zu Tatsachen, können Werturteile nicht bewiesen werden und sind daher dem Anspruch auf Berichtigung nicht zugänglich.

Die Beweislast hat betreffend den Anspruch auf Berichtigung - mangels eindeutiger Bestimmung in der DS-GVO - zwei Blickwinkel zu beachten. Vorerst obliegt dem Antragsteller die Beweislast, demnach muss der Antrag auf Berichtigung umfangreich und verständlich die Begründung für die Unrichtigkeit darlegen und damit einhergehend die korrekten Daten präsentieren. Dennoch schreibt Art 5 der DS-GVO dem Verantwortlichen nicht nur eine sachlich richtige Datenverarbeitung vor, die auf dem neuesten Stand zu sein hat und legt diesem damit die Verpflichtung auf, alle Maßnahmen zur unverzüglichen Berichtigung unrichtiger Daten zu treffen, sondern verlangt darüber hinaus auch den Nachweis der Einhaltung von dem Verantwortlichen. Daraus ist

[80] Art 16 VO (EU) 2016/679.

abzuleiten, dass beide Parteien eine Mitwirkungspflicht trifft und der Verantwortliche einen Antrag auf Berichtigung jedenfalls prüfen muss.[81]

Betrachtet man demgegenüber den Anspruch auf Vervollständigung, so muss die angestrebte Vervollständigung für den Zweck der Datenverarbeitung wesentlich sein. Erst dann kann dieser Anspruch mittels ergänzender Erklärung begehrt werden. Dem Zweck der Verarbeitung gegenüber unverhältnismäßig weitreichende Vervollständigungsbegehren müssen nicht umgesetzt werden, da diese unrechtmäßig Einfluss auf Eigentumsrechte des Verantwortlichen nehmen würden. Da die DS-GVO auch den Terminus "unvollständig" nicht weiter ausführt, geht man in diesem Zusammenhang davon aus, dass die Gesamtheit an Daten "lückenhaft" ist, wenn bspw einzelne Daten für sich zwar stimmig sind, dennoch aber gesamt ein falsches oder unklares Bild vermittelt.

Obgleich § 27 Abs 3 DSG 2000 aufgehoben wurde, wonach die Richtigstellung der Daten bei Vorliegen eines Dokumentationszwecks in gewissen Fällen ausgeschlossen war und nachträgliche Änderungen nur durch ergänzende Anmerkungen vorgenommen werden konnten, wurde dennoch keine Änderung der Rechtslage und dadurch auch keine Abkehr der praktischen Umsetzung bewirkt. Von Bedeutung könnten vergangene Ereignisse sein, die auf Basis der dokumentierten Daten nachvollziehbar und überprüfbar gehalten werden sollen. Das bedeutet weiterhin, dass sofern der Dokumentationszweck einer Datenanwendung spätere Änderungen nicht erlaubt, kann nur eine nachträgliche Ergänzung Abhilfe leisten. Der Zweck der Dokumentation kann sich aus gesetzlichen Bestimmungen ergeben, wie sich dies auch im gegenständlichen Sachverhalt eines Arztes durch die gesetzliche Bestimmung im Ärztegesetz ergibt, nach welchem Krankengeschichten zehn Jahre aufbewahrt werden müssen.[82] Begehrt ein Patient bspw die Richtigstellung seines Namens, wird auch ein Arzt diesem Begehren nachkommen können.

Eine grundlegende Ablehnung eines Antrages auf Vervollständigung oder Berichtigung kann von dem Verantwortlichen nur mangels Vorliegen der Voraussetzungen, somit wenn falsche oder unvollständige Daten nicht vorliegen, argumentiert werden. Andere allgemeine - für diesen Sachverhalt unbedeutende - Ablehnungsgründe sehen die Art 23,

[81] *Haidinger* in DatKomm Art 17 Rz 21 ff.
[82] § 51 Abs 3 ÄrzteG.

85 und 89 DS-GVO vor, spezifische Ablehnungsgründe werden in Art 16 DS-GVO nicht normiert.[83]

Das "Recht auf Vergessenwerden" gemäß Art 17 DS-GVO gewährt den betroffenen Personen gegenüber dem Verantwortlichen einen Löschungsanspruch der sie betreffenden personenbezogene Daten, sofern einer der in Art 17 Abs 1 lit a - f vorliegenden Gründe zu bejahen ist. Genannt werden als Gründe für die Löschung der Wegfall der Notwendigkeit der Datenverarbeitung, der Widerruf der Einwilligung, die Einlegung eines Widerspruchs, die unrechtmäßige Datenverarbeitung, die rechtliche Verpflichtung zur Löschung und der Widerruf der Einwilligung eines Kindes iZm einem Dienst der Informationsgesellschaft. Zu beachten ist allerdings, dass Abs 3 lit a - e spezifische Ausnahmen dieser Löschungsverpflichtung des Verantwortlichen vorsieht. Durch lit b, "*zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert*", oder lit c, "*aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3*", iVm § 51 Abs 3 ÄrzteG wird die rechtliche Ausnahmeregelung des Löschungsanspruches ua für Ärzte normiert. Diese Ausnahme umfasst die Verarbeitung jener besonderen Kategorien personenbezogener Daten, die aufgrund der Aufbewahrungspflicht und für die vorgegebene Frist gespeichert werden müssen. Werden hingegen darüber hinaus Daten verarbeitet, sind die Vorgaben über die Löschung dieser Daten nach der DS-GVO gesondert zu prüfen.[84]

3.9.3 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art 19 DS-GVO)

Für den Verantwortlichen besteht nach Art 19 DS-GVO die Mitteilungspflicht, allen Empfängern, deren personenbezogene Daten offengelegt wurden, die Information über eine etwaige Berichtigung oder Löschung der Daten sowie gegebenenfalls über eine Einschränkung der Verarbeitung nach Art 16, 17 Abs 1 und 18 DS-GVO zu übermitteln, sofern sich dieser Vorgang nicht als unmöglich erweist oder zu einem unverhältnismäßigen Aufwand führen würde. Weiters ist die betroffene Person auf ihren

[83] *Haidinger* in DatKomm Art 17 Rz 32 ff.
[84] *Haidinger* in DatKomm Art 17 Rz 47 ff; DSB 15.11.2018, DSB-D122.944/0007-DSB/2018 Dako 2019/3, 67 (*Haidinger/Weiss*).

Wunsch auch über diese Empfänger in Kenntnis zu setzen.[85] Die Mitteilungspflicht für einen Arzt ist in diesem Zusammenhang wohl sehr eingeschränkt, da die Anwendung von Art 18 DS-GVO (Recht auf Einschränkung der Verarbeitung) ohnehin durch das Ärztegesetz ausgeschlossen wurde und Art 17 DS-GVO ("Recht auf Vergessenwerden") nur bei den von § 51 Abs 3 ÄrzteG nicht erfassten personenbezogenen Daten oder jenen, die bereits über zehn Jahre aufbewahrt wurden, zur Anwendung gelangen kann.[86]

3.9.4 Recht auf Datenübertragbarkeit (Art 20 DS-GVO)

ErwG 68 führt zum Recht auf Datenübertragbarkeit aus, dass der betroffenen Person "*im Fall der Verarbeitung personenbezogener Daten mit automatischen Mitteln eine bessere Kontrolle über die eigenen Daten*" ermöglicht werden soll, indem sie berechtigt wird, "*die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zu erhalten und sie einem anderen Verantwortlichen zu übermitteln*".[87] Dieses Kontrollwerkzeug der DS-GVO steht der betroffenen Person nur dann zur Verfügung, wenn die gegenständlichen Daten entweder auf Grundlage einer Einwilligung (Art 6 Abs 1lit a, Art 9 Abs 2 lit a) oder eines Vertrages (Art 6 Abs 1 lit b) erhoben bzw verarbeitet werden. Die Daten müssen außerdem von der betroffenen Person selbst bereit gestellt worden sein, wobei darunter nicht nur die aktiv und wissentlich übermittelten Daten zu verstehen sind, sondern auch jene, die durch Nutzung des Dienstes des Verantwortlichen oder durch die Beobachtung entstanden sind.[88] Die betroffene Person hat durch Art 20 DS-GVO nicht nur ein Recht auf Übertragung an Dritte, vielmehr kann sie auch die Herausgabe an sich selbst verlangen. Das Recht auf Datenübertragbarkeit und das Auskunftsrecht unterscheiden sich in elementaren Grundsätzen: zum einen ist der Verantwortliche beim Auskunftsrecht an kein Format gebunden und zum anderen ermöglicht es die Auskunft über alle Daten, nicht nur über jene, die von der betroffenen Person selbst bereitgestellt wurden. Geht man davon aus, dass die Verarbeitung der Gesundheitsdaten (zB die Krankengeschichte) vorrangig auf dem Rechtmäßigkeitstatbestand der rechtlichen Verpflichtung fußen, so können von dem Recht auf Datenübertragbarkeit nur die übrigen personenbezogenen Daten betroffen sein.

[85] Art 19 VO (EU) 2016/679.
[86] § 51 Abs 3 ÄrzteG.
[87] ErwG 68 VO (EU) 2016/679.
[88] Art-29-Datenschutzgruppe, Stellungnahme 12/2016 Leitlinien zum Recht auf Datenübertragbarkeit („DSB"), WP 242 rev.01, 16/EN. <https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP242de_Art_29-Gruppe_Datenubertragbarkeit.pdf> (16.11.2019).

Wichtig zu erwähnen sei an dieser Stelle auch, dass das Recht auf Löschung (Art 17) durch die Anwendung der Datenübertragbarkeit nicht berührt wird.[89] ErwGr 68 erwähnt hiezu auch, dass die Ausübung des Rechts auf Datenübertragbarkeit nicht die Löschung der Daten zur Folge hat, die betroffene Personen betreffen und zur Erfüllung eines Vertrages zur Verfügung gestellt worden sind, und zwar für den Zeitraum, in dem die Daten zur Vertragserfüllung noch notwendig sind.[90]

4. Cloud Computing

4.1 Definition

In einigen Fällen wird ein niedergelassener Kassenarzt seine Patientendaten nicht lokal verarbeiten bzw speichern, da ihm dazu womöglich die Ressourcen und das fachliche Wissen fehlen. Vielmehr kommt es in der Praxis oftmals zu "Cloud Computing" Lösungen der Ärzte. Bei den sogenannten Cloud Computing Lösungen werden dem Arzt die IT-Infrastruktur und/oder die IT-Leistungen wie beispielsweise der Speicherplatz, die Rechenleistung oder auch die Anwendungssoftware als Leistungen über das Internet angeboten und bereitgestellt. Durch die Auslagerung dieser Leistungen an spezialisierte Anbieter, müssen keine eigenen Mitarbeiter beschäftigt, keine Investitionen in besondere Hardware getätigt sowie keine eigenen Prozesse dafür geschaffen werden. Da die Bereitstellung, Installation und Betreuung eigener Rechensysteme sehr kostenintensiv ist und breites Fachwissen erfordert, bewirkt die diesbezügliche Auslagerung für Ärzte eine große Erleichterung, da dadurch die Kosten, Aufwendungen und Verfügbarkeit der Anwendungen planbar werden.[91] Cloud Computing ist kein im Vorhinein entworfenes Gesamtprodukt, vielmehr können diese Dienste individuell und bedarfsorientiert in Anspruch genommen und entsprechend den genutzten Services abgerechnet werden. Das Prinzip, welches hinter der jeweiligen Cloud Computing Lösung steht, entspricht einer Vernetzung von mehreren, verschiedenen Rechnern, die über das Internet verbunden und deren Services für Kunden gleichermaßen über das Internet abrufbar sind.

Im Hinblick auf die Verarbeitung von Patientendaten unterscheiden sich die datenschutzrechtlichen Sicherheitsanforderungen einer Cloud Lösung in hohem Ausmaß von einer lokalen Speicherung. Insbesondere muss bereits bei der Wahl des Cloud

[89] *Haidinger* in DatKomm Art 20 Rz 20 ff.
[90] ErwGr 68 VO (EU) 2016/679.
[91] *Völkel,* Neue Vorgaben für IT-Sicherheit in Banken, Die Presse 2019/38/02.

Computing Anbieters auf die datenschutzrechtlichen Anforderungen Bedacht genommen werden. Darüber hinaus muss in diesem Zusammenhang auch die Rollenverteilung und das Rechtsverhältnis zwischen den involvierten Personen erneut betrachtet werden.[92]

4.2 Unterschiede bei Datenspeicherung in einem externen System/Übermittlung

Aufbauend auf den allgemeinen Anforderungen an die Sicherheit der Datenverarbeitung nach der DS-GVO (Art 32) normiert das Gesundheitstelematikgesetz in seinen Paragraphen 3-8 die speziellen Vorgaben an die Datensicherheit bei der elektronischen Übermittlung von Gesundheits- und genetischen Daten (Art. 4 Z 15 und Z 13 DS-GVO). Paragraph 3 Abs 1 GTelG bestätigt, dass der zweite Abschnitt dieses Gesetzes "*für alle Formen der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten (gerichtete und ungerichtete Kommunikation) durch Gesundheitsdiensteanbieter (§ 2 Z 2)*" gilt.

4.2.1 Elektronische Übermittlung

Nach dem Erlass der Datenschutzgrundverordnung wurde durch das 2. Materien-Datenschutz-Anpassungsgesetz 2018 den neuen Begrifflichkeiten entsprechend auch das Gesundheitstelematikgesetz novelliert. Im Zuge dessen, war unter anderem das in § 3 Abs 1 angeführte Wort „Weitergabe" durch das Wort "Übermittlung" zu ersetzen.[93] Bislang fehlt es allerdings an der Definition des Wortes "Übermittlung". Der Begriff „Weitergabe" betitelte die Überlassung und Übermittlung im Sinne des § 4 DSG 2000, nicht jedoch die anderen dort genannten Verwendungsarten (§ 4 Z 8 DSG 2000).[94] Davon umfasst war daher einerseits die „*Weitergabe von Daten zwischen Auftraggeber* [Verantwortlichem] *und Dienstleister* [Auftragsverarbeiter] *im Rahmen des Auftragsverhältnisses*" (Überlassen iSd § 4 Z 11 DSG 2000) und andererseits „*die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber* [Verantwortlichen] *oder einen Dienstleister* [Auftragsverarbeiter]*, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers*" (Übermitteln iSd § 4 Z 12 DSG 2000). Ungeklärt bleibt dadurch weiterhin, ob der Gesetzgeber bewusst den Begriff

[92] <https://novadex.com/de/glossar-artikel/definition-cloud-computing-was-ist-cloud-computing> (16.11.2019)
[93] 2. Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I 37/2018.
[94] ErlRV 1936 BlgNr XXIV. GP, 20 ff.

"Übermitteln" gewählt und damit ausschließlich diesen alten Bedeutungsgehalt übernehmen und die Definition einschränken wollte oder, ob die Begriffsanpassung keine inhaltliche Veränderung bewirken sollte. Würde man der ersten Annahme folgen, unterläge nunmehr die Weitergabe von Daten innerhalb eines Auftragsverarbeitungsvertrages nicht mehr erhöhten datenschutzrechtlichen Sicherheitsanforderungen. Diese Annahme erscheint jedoch nicht richtig, da insbesondere auf Grund der digitalen Weiterentwicklung eher mit erhöhten Sicherheitsanforderungen zu rechnen ist, um den Schutz der betroffenen Personen garantieren zu können.

4.2.2 Gesundheitsdiensteanbieter (§ 2 Z 2 GTelG)

Die Tatsache, dass Ärzte als Gesundheitsdiensteanbieter iSd § 2 Z 2 GTelG qualifiziert werden können, wurde bereits unter dem Punkt „3.8 Sicherheit der Verarbeitung (Art 32 DS-GVO, GTelG)" behandelt und festgestellt. Ebenso gleichbleibend verhält sich die Rolle des Arztes als Verantwortlicher bei Nutzung einer Cloud Lösung, da die Entscheidung über die Zwecke und Mittel der Datenverarbeitung nach wie vor allein der Arzt trägt.[95] Das Gesundheitstelematikgesetz erfasst gemäß § 2 Z 2 neben den Verantwortlichen aber auch die Auftragsverarbeiter als Gesundheitsdiensteanbieter, sofern diese regelmäßig Gesundheitsdaten oder genetische Daten zu den unter lit a bis e genannten Zwecken verarbeiten. Geht man weiterhin davon aus, dass der Arzt sich bei der Datenverarbeitung seiner Patienten (bspw zu Zwecken der medizinischen Behandlung oder Versorgung gem lit a) und unter Nutzung einer Cloud Lösung eines externen Dienstleisters bedient, ist dieser als Auftragsverarbeiter (gegebenenfalls auch als Subauftragsverarbeiter) jedenfalls Gesundheitsdiensteanbieter iSd § 2 Z 2 GTelG.[96]

4.2.3 Heranziehung eines Auftragsverarbeiters (Art 28 DS-GVO)

Ein Auftrag für eine Datenverarbeitung darf von dem Verantwortlichen grundsätzlich nur an Auftragsverarbeiter vergeben werden, "*die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen [der DS-GVO] erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet*".[97] Auftragsverarbeiter trifft zudem die Pflicht vor Heranziehung weiterer Auftragsverarbeiter als Subauftragsverarbeiter eine gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen einzuholen.

[95] Art 4 Z 7 VO (EU) 2016/679.
[96] § 2 Z 2 GTelG
[97] Art 28 Abs 1 VO (EU) 2016/679.

Wird auf eine allgemeine Genehmigung zurückgegriffen, so hat der Verantwortliche dennoch im Einzelfall über jede Änderung zumindest informiert zu werden und verfügt somit in diesem Zusammenhang über ein Einspruchsrecht.[98] Die Grundlage für eine Datenverarbeitung durch einen Auftragsverarbeiter schafft ein Vertrag mit dem Verantwortlichen oder ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten. Darin erfolgt die Vereinbarung über den Gegenstand und die Dauer, sowie die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und schließlich die Rechte und Pflichten des Verantwortlichen. Ferner werden den Vertragsparteien eines Auftragsverarbeitungsvertrages in Abs 3 lit a bis h weitere zu regelnde Aspekte auferlegt. Insbesondere muss ausdrücklich festgehalten werden, dass der Auftragsverarbeiter die genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält oder wie bereits in dieser Arbeit ausgeführt, muss mit dem Auftragsverarbeiter bereits im Vertrag seine Pflicht bedungen werden, alle gemäß Art 32 DS-GVO für die Sicherheit der Verarbeitung erforderlichen Maßnahmen zu ergreifen.[99]

Entscheidet sich der Auftragsverarbeiter für die Hinzuziehung eines Subauftragsverarbeiters und damit für die Abgabe bestimmter Verarbeitungstätigkeiten an diesen, führt die DS-GVO dazu aus, dass dem Subauftragsverarbeiter durch einen zu schließenden Vertrag mit dem ersten Auftragsverarbeiter (oder einem anderen Rechtsinstrument nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats) dieselben Datenschutzpflichten übertragen werden müssen, die zwischen dem Auftragsverarbeiter und dem Verantwortlichen bereits in deren Vertrag vereinbart wurden. Besonderes Augenmerk muss auf das Vorliegen hinreichender Garantien für geeignete technische und organisatorische Maßnahmen zur rechtskonformen Datenverarbeitung iSd DS-GVO gelegt werden. Gesetzt den Fall, dass der Subauftragsverarbeiter die ihn treffenden Datenschutzpflichten nicht erfüllt, trifft die diesbezügliche Haftung dem Verantwortlichen gegenüber den ersten Auftragsverarbeiter.[100]

Einen äußerst wichtigen und heiklen Aspekt bei der Auswahl eines Auftragsverarbeiters (oder Subauftragsverarbeiters) stellen für einen Arzt als Verantwortlichen die

[98] Art 28 Abs 2 VO (EU) 2016/679.
[99] Art 28 Abs 3 VO (EU) 2016/679.
[100] Art 28 Abs 4 VO (EU) 2016/679.

Rahmenbedingungen der Datenübermittlung in ein Drittland dar. Im Gegensatz zu einem Sachverhalt mit lokaler Speicherung, besteht bei einer Cloud Lösung jedenfalls die Gefahr des "Transports" der Daten in ein Drittland. Art 44 DS-GVO normiert als allgemeine Grundsätze einer Datenübermittlung personenbezogener Daten, dass eine solche an ein Drittland oder eine internationale Organisation (oder auch eine Weiterübermittlung von einem Drittland in ein weiteres) nur unter Einhaltung der Regelungen des 5. Kapitels der DS-GVO durchgeführt werden darf. Diese Vorgaben dienen der Gewährleistung bzw dem Erhalt des uneingeschränkten Schutzniveaus der Datenschutzgrundverordnung.[101] Den Vorgaben des 5. Kapitels folgend, ist eine Datenübermittlung in jene Drittländer zulässig, für die die Kommission einen Angemessenheitsbeschluss gefasst und im Amtsblatt der Europäischen Union und auf ihrer Website veröffentlicht hat, wonach ein angemessenes Schutzniveau für die Datenverarbeitung für gegeben befunden wurde. Dieser Angemessenheitsbeschluss kann auch nur bestimmte Gebiete und spezifische Sektoren in einem Drittland und einzelne internationalen Organisationen benennen.[102] Liegt hingegen für ein Drittland kein Angemessenheitsbeschluss der Kommission iSd Art 45 Abs 3 DS-GVO vor, ist eine Datenübermittlung an ein Drittland nur rechtmäßig, sofern entweder der Verantwortliche oder der Auftragsverarbeiter bzw Subauftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zustatten kommen. Die Wahl der Rechtsinstrumente zur Gewährleistung der sogenannten "geeigneten Garantieren" ist eingeschränkt und diese sind taxativ in Art 46 Abs 2 und 3 DS-GVO aufgezählt, wobei auf die beiden in Abs 3 angeführten Instrumente nur vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde zurückgegriffen werden kann.[103] Sowohl der Arzt in der Rolle des Verantwortlichen (Art 4 Z 7), als auch der externe Dienstleister in der Rolle des Auftragsverarbeiters (Art 4 Z 8) haben sicherzustellen, dass die genutzte IT-Infrastruktur ein angemessenes Schutzniveau gewährleistet und den Anforderungen des GTelG entspricht.

4.2.4 Grundsätze der Datensicherheit (§§ 3-8 GTelG)

Zu beachten ist vorab, dass die Verarbeitung der Gesundheitsdaten oder der genetischen Daten nur in den dafür zulässigen Rollen abzubilden ist. In diesem Zusammenhang trifft

[101] Art 44 VO (EU) 2016/679.
[102] Art 45 Abs 8 VO (EU) 2016/679.
[103] Art 46 VO (EU) 2016/679.

die Gesundheitsdiensteanbieter die Verantwortung über die Sicherstellung, dass die Verarbeitung der Gesundheitsdaten oder genetischen Daten nur in diesen Rollen erfolgt.[104]

Gesundheitsdiensteanbieter dürfen eine Übermittlung von Gesundheitsdaten und genetischen Daten nur bewirken, sofern die in § 3 Abs 4 Z 1 bis 6 GTelG kumulativ aufgezählten Voraussetzungen erfüllt sind. Dazu gehört (a) die rechtliche Zulässigkeit gemäß Art 9 DS-GVO (Z 1), bei der an dieser Stelle auf die Ausführungen unter Punkt „3.5. Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten" verwiesen werden dürfen, wonach die Rechtmäßigkeit zweifelsfrei gegeben ist. Als weitere Voraussetzung für die Zulässigkeit der Übermittlung wird gefordert, dass sowohl (b) die Identität (§ 4 GTelG) jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen (Z 2), als auch (c) die Identität der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen ist (Z 3).[105]

Die Art der Identitätsprüfung der Betroffenen richtet sich nach der Kommunikationsform. Es ist daher in einem ersten Schritt diese zu evaluieren. Wenngleich das GTelG keine exakte Definition der Begriffe "gerichtete" und "ungerichtete" Kommunikation enthält, so ergibt sich aus den Erläuterungen zur Regierungsvorlage, dass unter gerichteter Kommunikation die Weitergabe an im Vorhinein bestimmte Empfänger/innen zu verstehen ist. Eine klare Einordnung erfolgt lediglich in § 2 Z 6 GTelG und wird darin festgehalten, dass ELGA jedenfalls als ungerichtete Kommunikation zu qualifizieren ist.[106]

In diesem gegenständlichen Fall ist die gerichtete Kommunikationsform ganz offensichtlich erfüllt, denn der niedergelassene Kassenarzt verarbeitet bzw speichert seine Patientendaten in einer Cloud, in der ausschließlich der Vertragspartner bzw Auftragsverarbeiter, welcher diese zur Verfügung stellt, Zugriff hat und einsehen kann. Die Übermittlung erfolgt daher an einen konkreten und im Vorhinein bestimmten Empfänger.

Paragraph 4 Abs 1 und Abs 2 GTelG legen anhand des E-Government-Gesetzes die qualitativen Anforderungen für die Identifikation der Betroffenen fest, wobei eine höhere

[104] § 3 Abs 3 GTelG.
[105] § 3 Abs 4 GTelG.
[106] ErlRV 1936 BlgNr XXIV. GP, 5 ff.

Qualität - nämlich die eindeutige Identität - ausschließlich für die Identifikation im Rahmen der ungerichteten Kommunikation vorgesehen ist. Da der vorliegende Sachverhalt eine gerichtete Kommunikation darstellt, ist die Identität des Betroffenen gemäß § 2 Z 1 E-Government-Gesetz festzustellen. Es müssen dafür Merkmale vorhanden sein, die geeignet sind, ihre Unterscheidbarkeit zu anderen zu ermöglichen. Solche Merkmale sind bspw der Name, das Geburtsdatum oder der Arbeitgeber.[107]

Das Gesundheitstelematikgesetz sieht bei der Art der Identitätsprüfung der Gesundheitsdiensteanbieter (zB Ärzte) hingegen drei Alternativmöglichkeiten für die Identifikation - unabhängig davon, ob eine gerichtete oder ungerichtete Kommunikation vorliegt - vor. Die Identifikation kann entweder (i) durch Verwendung von elektronischen Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen, in Kombination mit bereichsspezifischen Personenkennzeichen (bPK, § 9 E-GovG), (ii) durch elektronischen Abgleich mit dem eHealth-Verzeichnisdienst (eHVD, § 9 GTelG) oder (iii) durch elektronischen Abgleich mit dem GDA-Index festgestellt werden. Da aber die in Anspruch genommenen Cloud Lösungen bzw Services von Ärzten variieren, sollen Spekulationen betreffend den zu wählenden Identifikationsnachweis außer Acht bleiben und nur die Möglichkeiten dargelegt werden.[108]

Weiters fordert das GTelG für die Übermittlung von Gesundheitsdaten und genetischen Daten, (d) dass die Rollen (§ 5) der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen sind. Dieser Nachweis und die Prüfung der Rolle der Gesundheitsdiensteanbieter hat auf dieselbe Weise wie die Identitätsprüfung zu erfolgen, dies bedeutet, durch Verwendung von elektronischen Signaturen in Kombination mit bPKs, durch elektronischen Abgleich mit dem eHVD oder durch elektronischen Abgleich mit dem GDA-Index. Dazu ist anzumerken, dass die Gesundheitsdiensteanbieter nicht selbst Rollen definieren dürfen, sondern nur die auf Grundlage von § 28 Abs 1 Z 1 GTelG mit Verordnung festgelegten Rollen zu verwenden haben.[109]

Im Hinblick auf die Vertraulichkeit (e) der Daten verlangt § 6 GTelG, dass die elektronische Übermittlung mit entsprechenden technischen Maßnahmen vor unbefugten

[107] § 4 Abs 1 GTelG; § 2 Z 1 E-GovG.
[108] § 4 Abs 4 GTelG.
[109] § 5 GTelG.

Zugriffen abgesichert sein muss und, dass dafür entsprechende Protokolle und Verfahren verwendet werden. Es müssen demnach adäquate kryptographische und bauliche Maßnahmen, ein beschränkter Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzergruppe sowie die Authentifizierung durch die Benutzer vorgesehen sein. Bei der Sicherstellung der Vertraulichkeit durch geeignete Protokolle und Verfahren, haben diese die vollständige Verschlüsselung der Gesundheitsdaten und genetischen Daten zu bewirken. Überdies haben deren kryptographische Algorithmen in der nach § 28 Abs 1 Z 2 GTelG zu erlassenden Verordnung aufzuscheinen. Dieser Verordnung obliegt, nach Einbeziehung einer Bestätigungsstelle gemäß § 7 Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016, die Beurteilung der Eignung spezieller kryptographischer Algorithmen nach dem jeweiligen Stand der Netzwerksicherheit zur Verschlüsselung gemäß § 6 GTelG.[110]

Stützt sich ein Arzt bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten auf § 6 Abs 1 Z 2 GTelG, darf keine Möglichkeit bestehen, den unter Umständen von der Verschlüsselung ausgenommenen Informationen Hinweise auf die [111]betroffenen Personen (Art 4 Z 1 DS-GVO), deren Gesundheitsdaten oder genetische Daten zu entnehmen oder auf allfällige Authentifizierungsdaten zuzugreifen.

In diesem Zusammenhang ist auch ausdrücklich gesetzlich normiert, "*dass die Speicherung von Gesundheitsdaten und genetischen Daten in Datenspeichern, die einem Verantwortlichen (Art. 4 Z 7 DSGVO) bedarfsorientiert von einem Auftragsverarbeiter (Art. 4 Z 8 DSGVO) bereitgestellt werden („Cloud Computing")*", nur unter Anwendung der Verschlüsselung mittels eines dem aktuellen Stand der Technik entsprechenden Verfahrens (Abs 1 Z 2) erfolgen darf.[112]

Um schließlich die Integrität (f) elektronischer Gesundheitsdaten und genetischer Daten zu gewährleisten, ist der Nachweis und die Prüfung durch den Einsatz entsprechender Signaturen oder Siegel beizubringen. Wenn § 7 GTelG von Integrität spricht, wird damit die „Unverfälschtheit" oder „Echtheit" der weitergegebenen Gesundheitsdaten bezeichnet (lat. integritas „unversehrt", „intakt" bzw „vollständig"). Ein Absehen von der Verwendung elektronischer Signaturen der in Abs 1 festgelegten Qualität ist lediglich für

[110] § 6 GTelG.
[111] § 6 Abs 2 GTelG.
[112] § 6 Abs 3 GTelG.

die Weitergabe in besonders abgesicherten Netzwerken (§ 6 Abs 1 Z 1) und nur insofern zulässig, als "*der Zugang zu diesem Netzwerk ausschließlich für im Vorhinein bekannte Gesundheitsdiensteanbietern möglich ist*".[113]

Für die Vorgaben an bzw das Vorsehen eines IT-Sicherheitskonzepts gemäß § 8 GTelG darf an dieser Stelle auf Punkt „3.8 Sicherheit der Verarbeitung (Art 32 DS-GVO, GTelG)" verwiesen werden.

5 Kommunikationsmittel bzw Kommunikationsarten zwischen Arzt und Patient

5.1 Mündliche Kommunikation (im Warteraum der Ordination)

Die Ärztliche Kommunikation beginnt bereits bei der Patientenaufnahme im Empfangsbereich, in manchen Fällen sogar vor persönlicher Aufnahme bei Terminvereinbarung am Telefon. Oftmals befinden sich der Empfangs- und Wartebereich einer Praxis in demselben Raum oder aneinander anschließend ohne Tür bzw Trennmöglichkeit. Dazu kommt, dass die Organisation der Praxisräume häufig so gestaltet ist, dass die einzelnen Ordinations- bzw Behandlungsräume nicht eigens verschließbar sind, sondern tatsächlich nur durch einen Sichtschutz einer halboffenen Schiebewand voneinander getrennt sind. Diese Komponenten führen in der Praxis dazu, dass wartende Patienten die Gespräche oder Telefonate des Praxispersonals mitanhören können sowie Patienten untereinander die Behandlungen miterleben und diese Daten anderer zur Kenntnis nehmen können. Dabei ist ausdrücklich hinzuzufügen, dass die Patienten überwiegend namentlich aufgerufen werden und eine Anonymisierung der Daten dadurch ausgeschlossen ist.[114]

Geht man weiter in der Annahme, dass der gegenständliche niedergelassene Kassenarzt seine Patientendaten grundsätzlich in einem automationsunterstützten System speichert, wird hier die Ansicht vertreten, dass damit auch bei einem mündlichen Erheben, Erfassen, Auslesen und Abfragen sowie bei der Organisation, Anpassung oder Veränderung der Daten iSd Art 4 Z 2 DS-GVO eine (wenn auch nur teilweise) automatisierte Verarbeitung

[113] § 7 GTelG; ErlRV 1936 BlgNr XXIV. GP, 24.
[114] *Vedder*, Datenschutz in Arztpraxen, DuD 2014/38, 821 (821 ff).

personenbezogener Daten vorgenommen und die Anwendbarkeit der DS-GVO angenommen wird. [115]

Betrachtet man die einzelnen Vorgänge, wie bspw das Vorlesen seiner Daten im Empfangsbereich sowie die persönlichen Gespräche mit dem Arzt oder seinem Personal, für sich, muss festgestellt werden, dass es sich hierbei jedenfalls um keine elektronische Übermittlung dieser Patientendaten iSd GTelG handelt. Demnach können die Datensicherheitsanforderungen des Gesundheitstelematikgesetzes nicht greifen. Aus Art 32 DS-GVO, der unter Berücksichtigung ua des Stands der Technik, der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der Risiken für die Rechte und Freiheiten der Patienten den Verantwortlichen und Auftragsverarbeitern die Pflicht zur Umsetzung geeigneter (technischer und) organisatorischer Maßnahmen zur Hintanhaltung der Risiken und Gewährleistung des angemessenen Schutzes auferlegt, könnten Hinweise für eine datenschutzkonforme Lösung der persönlichen Aufnahme- und Behandlungsgespräche in einer Arztpraxis abgeleitet werden.[116]

Hinzu kommt, dass § 1 des Datenschutzgesetzes (DSG) jedermann als Grundrecht das Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gewährt, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, soweit daran ein schutzwürdiges Interesse besteht.[117] Dieses Grundrecht als Verfassungsbestimmung wird einerseits als Kontrollinstanz für einfache Gesetze herangezogen, die aufgrund des von der DS-GVO ermöglichten Ausgestaltungsspielraums grundrechtsbeschränkend ausgerichtet sind (sog doppelte Bindung), und andererseits bewirkt jede Datenverarbeitung einen Eingriff in das Grundrecht auf Datenschutz und muss neben der Erfüllung der Zulässigkeitsvoraussetzungen der DS-GVO darüber hinaus einer Zulässigkeitsprüfung der Grundrechtsbeschränkung gemäß § 1 Abs 2 DSG standhalten.

Unbestritten bleibt allerdings, dass eine Datenverarbeitung der Patientendaten durch den Arzt (und seine Mitarbeiter) rechtmäßig erfolgt (siehe „Punkt 3. Allgemeine Zulässigkeit“). Es gilt in diesem Zusammenhang ausschließlich den Datenschutz und die Datensicherheit in Bezug auf die mündliche Kommunikation in einer Ordination zu

[115] Art 2 Abs 1 VO (EU) 2016/679.
[116] Art 32 Abs 1 VO (EU) 2016/679.
[117] § 1 DSG.

beleuchten und nur gegenüber anderen anwesenden Patienten. Das Schutzgut des Grundrechts auf Geheimhaltung umfasst nach hL eine weit gefasste Definition und schließt nicht nur den Schutz vor schlichter Weitergabe, sondern auch vor Ermittlung bzw Sammlung der Daten mit ein. Im Gegensatz zur DS-GVO verfolgt das Grundrecht auf Datenschutz einen weiter gefassten sachlichen Anwendungsbereich. Es wird nicht auf die ganz oder teilweise automatisierte Datenverarbeitung sowie nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, beschränkt. Vielmehr kommt es auf die Art des Datenträgers, auf dem Daten verarbeitet werden sollen, nicht an und sind auch unstrukturierte Dateisysteme von dem Grundrecht auf Geheimhaltung umfasst.

Gelangt man nach den Ausführungen dennoch zu der Auffassung, dass eine mündliche Kommunikation in einer Arztpraxis nicht der automatisierten Datenverarbeitung (mittels Arztsoftware) der Patientendaten iSd DS-GVO zuzurechnen ist, ist der Sachverhalt gleichwohl von § 1 DSG erfasst, da ein Geheimhaltungsinteresse der Patienten an ihren personenbezogenen (Gesundheits-)Daten gegenüber anderen anwesenden Personen - ausgenommen des Arztes und seiner Mitarbeiter - jedenfalls zu bejahen ist. Von Bedeutung ist allerdings die Betrachtung der Drittwirkung eines Grundrechts, da diese im Allgemeinen an den Staat adressiert sind und demnach nur für diesen bindend sind. Eine Drittwirkung würde sodann für den Einzelnen einen Anspruch aus dem Grundrecht ableitbar machen und eine Rechtsbeziehung zwischen Privatpersonen schaffen, die wechselseitig auch geltend gemacht werden können. Ist eine Drittwirkung für ein Grundrecht beabsichtigt, muss dies ausdrücklich gesetzlich vorgesehen werden und war eine solche Drittwirkung bisher in § 5 Abs 4 DSG normiert. Obwohl die alte Bestimmung des § 5 Abs 4 DSG mit Umsetzung der DS-GVO ersatzlos gestrichen wurde, ist den Erläuterungen der Erhalt der unmittelbaren Drittwirkung des Grundrechts auf Geheimhaltung zu entnehmen und wird diese Meinung auch von der hL trotz fehlender Rechtssicherheit vertreten.[118]

Mangels konkreter gesetzlicher Vorgaben in der Umsetzung des Datenschutzes bei mündlicher Kommunikation in Ordinationen, sieht *Vedder* diesbezüglich nur die Möglichkeit Empfehlungen an Ärzte auszusprechen. Angeraten wird die Organisation der Praxisräume derart zu gestalten, dass unbefugtes Mitlesen und Mithören unterbunden

[118] *Kriegner,* Anmerkungen zu § 1 DSG nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO), WBL 2019/2, 79 (83 f).

werden kann. Empfangs- und Wartebereich sollten entweder mittels verschließbarer Tür trennbar oder nicht aneinander anschließend angeordnet sein. Ratsam wäre des Weiteren auch die Behandlungsräume mit jeweils einzeln ausgestatteter Türen zu versehen, damit überdies Behandlungsgespräche von anderen Patienten nicht mit angehört werden können. Ist eine räumliche Trennung bspw zwischen Empfangs- und Wartebereich räumlich nicht möglich, wäre von einer mündlichen Patientenaufnahme abzuraten und anstelle der mündlichen Datenerhebung, eine schriftliche vorzulegen. Patientenunterlagen oder erste Fragebögen sollten dann unmittelbar in die digitalen Verarbeitungssysteme eingespielt und im Anschluss vernichtet oder sicher aufbewahrt und verstaut werden. Abschließend ist auch Vorsicht bei der Zugänglichkeit zu Ordinationsgeräten geboten, die personenbezogene bzw medizinische Daten preisgeben. Eine Einsehbarkeit in Bildschirme von Computern oder medizinische Geräte soll unterbunden werden, indem entweder Sichtschutz eingesetzt oder eine andere Positionierung gewählt wird. Mitarbeiter haben diese Maßnahmen zu unterstützen und an einer datenschutzkonformen Umgebung mitzuwirken, indem sie Türen verschließen, Unterlagen nicht an für andere Personen zugänglichen Orten platzieren sowie die PCs passwortgeschützt halten, wenn sie ihren Arbeitsplatz verlassen.[119]

5.2 Kommunikation via WhatsApp oder E-Mail

Statistiken zeigen, dass über eine Milliarde Menschen zum Stichtag Juli 2017 zu den regelmäßigen Nutzern des Messenger-Dienst WhatsApp zählen und diesen zum Versenden und Empfangen von Kurznachrichten sowohl in Text, als auch in Bild und Ton verwenden. An dieser Stelle muss zunächst festgehalten werden, dass der Besitz eines Smartphones für die Nutzung des Online-Messenger-Dienstes WhatsApp unumgänglich ist. Darüber hinaus werden die User von WhatsApp (teilweise bereits vor Installation dieser App) aufgefordert in deren Zugriff auf diverse Informationen auf dem Smartphone einzuwilligen. Beispielsweise fordert WhatsApp Zugriff auf alle Kontakte des Smartphones (nicht nur jene darunter, die WhatsApp User sind), die Identität und den Standort des Handybesitzers, die Fotos, Medien und andere Dateien sowie weiters Zugriff auf die Kamera des Geräts und das Mikrofon. Willigt der User in die Zugriffsgewährung ein, erscheint in weiterer Folge die Aufforderung zur Zustimmung in die Allgemeinen Geschäftsbedingungen (AGBs), die zwar in der deutschen Sprache (neben 56 anderen

[119] *Vedder*, Datenschutz in Arztpraxen, DuD 2014/38, 821 (821 ff).

Sprachen) verfügbar, jedoch äußerst umfangreich sind und nicht den konsumentenschutzrechtlichen Bestimmungen in Europa entsprechen. Anzumerken ist überdies, dass WhatsApp in seinen AGB eine Nutzung für Kinder unter sechzehn Jahren nicht gestattet.[120] In einem Beschluss des Amtsgerichts Bad Hersfeld in Deutschland wurde 2017 festgehalten, dass Eltern, die "*ihrem minderjährigen Kind ein digitales "smartes" Gerät (zB Smartphone) zur dauernden eigenen Nutzung*" überlassen, die Pflicht trifft, "*die Nutzung dieses Geräts durch das Kind bis zu dessen Volljährigkeit ordentlich zu begleiten und zu beaufsichtigen*". In diesem Zusammenhang erkannte das Amtsgericht weiters, dass die Nutzung des Messenger-Dienstes WhatsApp fortlaufend eine Übermittlung in Klardaten-Form aller in dem eigenen Smartphone-Adressbuch eingetragener Personen an das hinter dem Dienst stehende Unternehmen bewirkt. Hat ein User seine im Adressbuch eingetragenen Kontaktpersonen zuvor nicht um Erlaubnis ersucht und unterstützt er durch seine WhatsApp Nutzung eine andauernde Datenweitergabe, könnte diese deliktische Handlung eine kostenpflichtige Abmahnung nach sich ziehen.[121]

Zunächst wurde das Unternehmen WhatsApp Inc. 2009 in Kalifornien, USA gegründet und 2014 von Facebook übernommen. Dieses bietet weder eine Gewähr für eine vertrauliche und sichere Übermittlung der Inhalte, noch wird die Einhaltung des Grundsatzes der Datenminimierung (Art 5 Abs 1 lit c DS-GVO) angestrebt. Als Teil der Facebook-Unternehmensgruppe behält sich WhatsApp vor, Informationen von anderen Facebook-Unternehmen zu erhalten und gleichzeitig eigene Informationen mit diesen zu teilen. Den Ausführungen von WhatsApp zufolge dient dieser Informationsaustausch der Absicherung, Unterstützung, Bereitstellung, Pflege und Verbesserung ihrer Services und im Übrigen auch der Bekämpfung von Bedrohungen, Missbrauch und Verletzungsaktivitäten.[122] Zur Speicherdauer betont WhatsApp selbst, dass diese Daten nur bis zu dem Zeitpunkt des Empfangs beim Empfänger aufbewahrt werden, jedenfalls nicht länger als dreißig Tage. Es wird dem User nebenbei die Möglichkeit gewährt, sein WhatsApp Konto bei Bedarf selbst zu löschen oder unter den vorgesehenen Datenschutzeinstellungen eigene vorzunehmen. Beispielsweise kann von einem User selbst entschieden werden, ob der Absender durch blau markierte Häkchen erfahren soll,

[120] *Thiele,* Der Multimediale Helpdesk – Datenschutzrechtliche Grundlagen des Einsatzes von WhatsApp zur digitalen Kundenkommunikation, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht (2017), 231 (234).
[121] AG Bad Hersfeld 15.05.2017, F 120/17 EASO.
[122] <www.whatsapp.com> (16.11.2019)

dass und wann der adressierte Empfänger seine übertragene Übermittlung erhalten bzw geöffnet und gelesen hat. Ferner kann die Entscheidung über die Offenlegung des "zuletzt online"-Status aktiviert oder auch deaktiviert werden. Nicht zuletzt schafft WhatsApp für seine User neben der internetbasierten Datenübermittlung auch das internetbasierte Telefonieren. Nach Aussagen des Unternehmens, wird seit Anfang 2016 für die gesamte Übertragung und Kommunikation über WhatsApp eine "end-to-end-Verschlüsselung" angewandt. Es soll dadurch das Entschlüsseln und absaugen der übertragenen Inhalte nur dem Sender und Empfänger ermöglicht werden, dennoch kann dadurch eine unbefugte Datenweitergabe an Dritte nicht zweifelsfrei verhindert werden. WhatsApp verfügt hingegen - im Vergleich zu dem Kommunikationsdienst "Threema" bspw - über keine Datensicherheits-ISO-Zertifizierung.[123]

5.2.1 Telekommunikationsrechtliche Einordnung von WhatsApp/E-Mail

Bevor eine datenschutzrechtliche Prüfung zB des Messenger-Dienstes WhatsApp erfolgen kann, muss die telekommunikationsrechtliche Einordnung beleuchtet werden. Das erscheint zweckmäßig, da dies ua Unterschiede für die datenschutzrechtliche Rollenverteilung nach sich zieht.

Folgt man dem telekommunikationsrechtlichen Blickwinkel, ist der Messenger-Dienst WhatsApp - im Gegensatz zu Festnetz- und Mobiltelefonie - kein Telekommunikationsdienst. Vielmehr spricht man dabei von einem "Over-The-Top"-Kommunikationsdienst (OTT-Dienst). OTT-Dienste bezeichnen Dienste, die über das offene Internet angeboten werden, die Netze anderer Netzbetreiber nutzen ohne zwingend selbst ein Signalübertragungsdienst sein zu müssen und zunehmend die klassischen Telekommunikationsdienste ablösen. Zu nennen sind an dieser Stelle neben WhatsApp auch Facebook Messenger, E-Maildienste wie bspw Google Mail und GMX sowie Videotelefoniedienste wie ua Skype.[124] Bisher definierte der Gesetzgeber den Begriff "Kommunikationsdienst" als gewerbliche Dienstleistung, "*die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht*".[125] Dies übernahm das TKG aus der Richtlinie 2002/21/EG (sog Rahmenrichtlinie), die bislang als eine von insgesamt vier Richtlinien den Rechtsrahmen zum Telekommunikationsrecht der

[123] *Thiele* in Jahnel, Jahrbuch Datenschutzrecht, 231 (235).
[124] <https://www.rtr.at/de/inf/Konkurrenz_aus_dem_Netz_OTT/Die_Konkurrenz_aus_dem_Netz_OTT-Dienste.pdf> (16.11.2019).
[125] Art 2 lit c RL 2002/21/EG; § 3 Z 9 TKG.

Europäischen Union (EU) bildete. Dieser Definition folgend, waren die OTT-Dienste bis dato überwiegend nicht als Kommunikationsdienste iSd TKG einzuordnen, wobei sich die telekommunikationsrechtliche Einordnung dieser Dienste, die zum Teil gleichartige Funktionalitäten auszeichnen, wie klassische Telekommunikationsdienste, darunter auch der Messenger-Dienst WhatsApp, nach derzeit in Geltung stehendem österreichischen Telekommunikationsrecht schwierig verhielt. Dies geht insbesondere aus den Vorabentscheidungs-Gesuchen mehrerer nationaler Gerichte der Mitgliedstaaten an den EuGH hervor.[126]

Die für die telekommunikationsrechtliche Einordnung des WhatsApp Dienstes sowie webbasierte E-Maildienste bedeutendste Vorlagefrage erging aus Deutschland. Bei dieser vertrat die deutsche Bundesnetzagentur (BNetzA) die Ansicht, dass es sich bei OTT-Anbietern, als Anbieter von Substitutsprodukten der klassischen Telekommunikationsdiensten, die dabei gewisse Vermittlungsleistungen selbst erbringen, um Anbieter von Telekommunikationsdiensten iSd deutschen Telekommunikationsgesetzes handle. Darüber hinaus befand die BNetzA, dass solche OTT-Anbieter meldepflichtig seien und schrieb Google eine Registrierungspflicht als Telekommunikationsanbieter für den webbasierten E-Maildienst Gmail vor. Google teilte diese Ansicht nicht.

Rechtlich oblag dem EuGH die Begutachtung der Frage nach der Funktion des Gmail-Dienstes. Insbesondere galt es festzustellen, ob der Gmail-Dienst tatsächlich ganz oder überwiegend in der Übertragung von Signalen oder elektronischen Kommunikationsnetzen besteht. Wie bereits eindeutig festgestellt, nutzen OTT-Dienste, so auch Gmail, elektronische Kommunikationsdienste anderer Telekommunikationsnetzbetreiber und führen selbst keine maßgebende Signalübertragung aus.

Zu klären blieb in diesem Zusammenhang, welche Dimension ein OTT-Diensteanbieter an eigener Netzinfrastruktur oder vertraglicher Verfügungsgewalt über ein Netz bzw Netzdienst vorweisen muss, damit eine Zurechnung der Signalübertragung an ihn und

[126] <https://diercks-digital-recht.de/2019/07/eugh-c-193-18-gmail-ist-kein-telekommunikationsdienst-i-auswirkung-auf-ott-dienste-nebst-ausblick-auf-eu-richtlinie-ueber-den-kodex-fuer-die-elektronische-kommunikation-2018-1972/> (16.11.2019)

seine Qualifizierung als elektronischer Kommunikationsdienst vorgenommen werden kann.

Schon im Jahr 2013 strich der EuGH in seiner UPC-Entscheidung das Überwiegen der Verantwortlichkeit gegenüber den Endnutzern als Merkmal der Signalübertragung hervor und betonte, dass die Eigenschaft als Eigentümer der Netzinfrastruktur nicht überwiege für diese Einordnung. In einer dieser vorangehenden Entscheidung über die telekommunikationsrechtliche Einordnung des Dienstes SkypeOut, stützte sich der EuGH auf die Zuführungsvereinbarung der Telefonanrufe zwischen Skype und den zuständigen Telekommunikationsnetzbetreibern in Belgien, aus der eine Verantwortung der Firma Skype seinen Nutzern gegenüber für die Weiterleitung dieser Telefonanrufe erwächst. Folglich qualifizierte der EuGH diesen Dienst als elektronischen Kommunikationsdienst.

Seiner Argumentation folgend entschied sich der EuGH im Fall Gmail gegen die Qualifikation als elektronischen Kommunikationsdienst, da er befand, dieser E-Maildienst bestehe nicht ganz oder überwiegend in der Signalübertragung über elektronische Kommunikationsnetze. Bei dem E-Maildienst Gmail werden den E-Mail Adressen IP-Adressen von Google zugewiesen und aus Teilen der Nachrichten Datenpakete erzeugt, die durch Standard-Protokolle übermittelt werden. Die E-Mail Zustellung erfolgt über eigene Server der Firma Google über das offene Internet, die für die Identifizierung der Ziel-Server und die Versendung der Datenpakete die informationstechnischen Verarbeitungsprozesse durchführen. Für die Vornahme des Routings bzw der Leitung dieser Datenpakete zum Ziel-Server trifft Google keine Verantwortung und ist dies von ihnen auch nicht beeinflussbar. Nach Ansicht des EuGH ist die beschriebene Tätigkeit demnach allein nicht ausreichend für eine Eignung zur gänzlichen oder überwiegenden Übertragung von Signalen über elektronische Kommunikationsnetze.

Letztlich bemerkte der EuGH an dieser Stelle, dass auch die Tatsache des eigenständigen Betreibens elektronischer Kommunikationsnetze Googles in Deutschland nicht die Eigenschaft eines elektronischen Kommunikationsdienstes aller Dienste von Google herbeiführen kann, sondern nur jener, die in der Tat über die eigenen Netze fungieren. Einerseits unterbindet der EuGH mit seiner Entscheidung eine weite Auslegung der Definition der ganz oder überwiegenden Signalübertragung und andererseits bevorzugt er

eine rein technische Auslegung, mit der die OTT-Dienste, so auch der Messenger-Dienst WhatsApp, keine elektronischen Kommunikationsdienste sind.[127]

5.2.2 Datenschutzrechtliche Einordnung von WhatsApp/E-Mail

Legt man der datenschutzrechtlichen Prüfung vorab zugrunde, dass es sich nach derzeit geltender Rechtslage bei dem Messenger-Dienst WhatsApp (bzw dem E-Maildienst Gmail) nicht um einen elektronischen Kommunikationsdienst iSd § 3 Z 9 TKG handelt, kann angemerkt werden, dass auch den datenschutzrechtlichen Sonderbestimmungen des TKGs keine Beachtung geschenkt werden muss. Viel mehr fällt die ärztliche Kommunikation über den Messenger-Dienst WhatsApp, bei welcher bspw Termine mit Patienten vereinbart oder Informationen zu Befunden erteilt werden, unter die elektronische Übermittlung von Gesundheitsdaten und genetischen Daten im Sinne des § 3 GTelG (siehe Punkt „4.2.1 Elektronische Übermittlung“). Hinsichtlich der datenschutzrechtlichen Sicherheitsanforderungen sind als Grundlage die entsprechenden Bestimmungen der Datenschutzgrundverordnung gemeinsam mit dem Gesundheitstelematikgesetz heranzuziehen und kann diesbezüglich auf die allgemeinen Ausführungen dieser Arbeit verwiesen werden. Des Weiteren kommt es zu keiner datenschutzrechtlichen Rollenverschiebung, der Arzt behält seine Rolle als Verantwortlicher und die Firma WhatsApp wäre in einer solchen Konstellation als Auftragsverarbeiter des Arztes zu sehen. Unter Bezugnahme auf ein mögliches Auftragsverarbeitungsverhältnis ist jedenfalls auf eine Reihe heikler Aspekte hinzuweisen. Die DS-GVO gibt den Verantwortlichen die Vorgabe nur Auftragsverarbeiter heranzuziehen, die hinreichend Garantien für geeignete technische und organisatorische Maßnahmen bieten, um den Anforderungen dieser Verordnung an eine Datenverarbeitung gerecht zu werden und die Rechte der betroffenen Personen zu schützen.[128] Wie in Kapitel „4.2 Unterschiede bei Datenspeicherung in einem externen System/Übermittlung“ beschrieben, bemüht sich WhatsApp nicht vollends um diese Garantien. Hinzu kommt, dass WhatsApp zwar die Rechte, die die DS-GVO betroffenen Personen gewährt und anerkennt, dennoch in ihrer Datenschutzrichtlinie ausdrücklich festhält, dass “*die [ihnen] zur Verfügung stehenden Daten [verwendet werden], um diese Dienste bereitzustellen. Wenn [sich eine Person] gegen die Bereitstellung bestimmter*

[127] *Kiparski,* Der EuGH schafft Klarheit: OTT-Dienste sind in der Regel keine Telekommunikationsdienste, CR 2019/35, 460 (460 ff).
[128] Art 28 Abs 1 VO (EU) 2016/679.

Daten [entscheidet], wird möglicherweise die Qualität [des] Erlebnisses bei der Nutzung von WhatsApp beeinträchtigt".[129] Überdies müsste der Arzt, um der DS-GVO zu entsprechen, für die Datenverarbeitung einen Auftragsverarbeitungsvertrag mit der Firma WhatsApp schließen.[130] Das bedeutet, dass eine reine Nutzung des Messenger-Dienstes WhatsApp für eine datenschutzkonforme Nutzung der ärztlichen Kommunikation ausgeschlossen ist. Außerdem ist nicht anzunehmen, dass WhatsApp dem Versuch eines Arztes, einen solchen Vertrag zu schließen, nachkäme, da dies ihrem Unternehmenskonzept widersprechen würde. Abschließend muss daher von der ärztlichen Nutzung des Messenger-Dienstes WhatsApp (und der webbasierten E-Maildienste) dringend abgeraten werden, zumal dies den österreichischen und europäischen Datenschutzvorschriften widersprechen würde und eine erhebliche Gefahr für die Datensicherheit der Patienten bewirken zur Folge hätte.

5.2.3 Aussicht auf die kommende Gesetzesnovelle - der TK-Kodex

Nach einem zweijährigen Gesetzgebungsprozess veröffentlichte die Europäische Kommission im Dezember 2018 den Europäischen Kodex für die elektronische Kommunikation (TK-Kodex)[131] im Amtsblatt der EU, welcher in Zukunft die vier bestehenden Richtlinien (RL 2002/19/EG sog Zugangs-RL, RL 2002/20/EG sog Genehmigungs-RL, RL 2002/21/EG sog Rahmen-RL und RL 2002/22/EG sog Universaldienste-RL) ersetzen soll. Den Mitgliedstaaten wurde eine Umsetzungsfrist von zwei Jahren zugestanden. Künftig soll eine Einbeziehung der OTT-Dienste in den Rechtsrahmen des Telekommunikationsrechts erfolgen, welche durch eine Ergänzung der Legaldefinition des Kommunikationsdienstes geschieht. Im Gegensatz zur bisherigen Legaldefinition, umfasst der TK-Kodex in seinem Art 2 Z 4 ergänzend auch Internetzugangsdienste und interpersonelle Kommunikationsdienste. Art 2 Z 5 des TK-Kodex beschreibt die interpersonellen Kommunikationsdienste als gegen Entgelt erbrachte Dienste, "*die einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglichen*".[132] Damit sind unter dem Begriff des interpersonellen Kommunikationsdienstes ab dem Zeitpunkt der Umsetzung der

[129] <https://www.whatsapp.com/legal/?eea=1#how-we-process-your-information> (16.11.2019)
[130] Art 28 Abs 3 VO (EU) 2016/679.
[131] Richtlinie 2018/1972/EU des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), ABl L 321/36.
[132] Art 2 Z 5 RL 2018/1972/EU.

Bestimmungen des TK-Kodex in nationales österreichisches Recht neben den klassischen Telekommunikationsdiensten wie zB die Sprachtelefonie darüber hinaus auch die OTT-Dienste, wie bspw E-Maildienste oder andere Mitteilungsdienste, zu subsumieren. Mit dieser Erweiterung wird eine Anknüpfung des Telekommunikationsrechts fortan an der Funktion des Dienstes und nicht mehr ausschließlich an dem Merkmal der Signalübertragung vorgenommen.[133] Dessen ungeachtet wird die Frage der Abgrenzung von Signalübertragungsdiensten und OTT-Diensten weiterhin von Bedeutung bleiben, da sich die Anforderungen an interpersonelle Kommunikationsdienste von jenen der Signalübertragungsdienste nach wie vor unterscheiden.[134]

Sobald eine Umsetzung der Vorgaben des TK-Kodex in nationales österreichisches Recht vorliegt, wird dies eine Neubeurteilung der datenschutzrechtlichen Einordnung und damit verbunden der Vorgaben an die OTT-Dienste erfordern und mit sich bringen. Die neue Rechtslage wird auch eine dem Kapitel 3.3 angepasste Rollenverteilung und datenschutzrechtliche Verantwortung nach sich ziehen, die es künftig zu beachten gilt.

5.3 Sprachtelefonie bzw SMS/MMS

Unbestritten ist, dass es sich bei der Sprachtelefonie und SMS um einen klassischen Kommunikationsdienst iSd § 3 Z 9 TKG handelt und, dass das Telekommunikationsrecht eigene Datenschutzvorgaben vorsieht. Bei dem Verständnis des Verhältnisses zwischen der DS-GVO und dem Telekommunikationsgesetz (bzw der ePrivacyRL, RL 2002/58/EG) ist Art 95 DS-GVO behilflich, welcher "*natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf[erlegt], soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.*"[135] Wenngleich diese Bestimmung nicht konkret und ausdrücklich das Konkurrenzverhältnis benennt, geht dennoch aus Erwägungsgrund 173 zur DS-GVO hervor, dass damit jedenfalls ein Anwendungsvorrang der ePrivacyRL erzielt werden sollte. Diesen Anwendungsvorrang strich bereits die ePrivacyRL selbst in ihrem Art 1 Abs 2 hervor, indem sie sich selbst als Detaillierung der Datenschutzrichtlinie (Richtlinie

[133] ErwGr 15 RL 2018/1972/EU.
[134] *Kiparski,* Der Europäische Telekommunikations-Kodex – Ein neuer Rechtsrahmen für die elektronische Kommunikation, CR 2019/35, 179 (179).
[135] Art 95 VO (EU) 2016/679.

95/46/EG) sah und ihren Regelungen den Stellenwert der lex specialis für die elektronische Kommunikation einräumte. Als Nachfolgeregelung der Datenschutzrichtlinie, übernimmt die DS-GVO dieses Verhältnis. Es ist sohin festzustellen, dass den datenschutzrechtlichen Vorgaben des Telekommunikationsgesetzes, als Umsetzung der ePrivacyRL in nationales österreichisches Recht, ebenso als lex specialis Vorrang gegenüber der DS-GVO zukommt.[136]

Möchte man nun eine datenschutzrechtliche Prüfung des Mediums der Sprachtelefonie oder SMS beginnen, finden sich die diesbezüglichen Auflagen in den §§ 95 ff TKG. Die Pflicht zur Erlassung von Datensicherheitsmaßnahmen im Sinne der Art 24, 25 und 32 DS-GVO betreffend die Erbringung eines öffentlichen Kommunikationsdienstes wird durch § 95 TKG dem Betreiber auferlegt, der diese Maßnahmen jeweils für alle von ihm erbrachten öffentlichen Kommunikationsdienste sicherzustellen hat.[137] Dabei wird eine Verschiebung der datenschutzrechtlichen Rollenverteilung im Gegensatz zur DS-GVO sichtbar. Während die DS-GVO und das Gesundheitstelematikgesetz in der gegenständlichen Prüfung bisher den Arzt als Verantwortlichen bei der Verarbeitung seiner Patientendaten verankert haben und dieser auch die Verantwortung für eine Nichtumsetzung zu tragen hatte, obliegt diese Sicherheitsgarantie nach dem TKG hingegen dem Betreiber des öffentlichen Kommunikationsdienstes. Ein Unternehmen ist dann Betreiber eines Kommunikationsdienstes iSd § 3 Z 3 TKG, sofern es "*die rechtliche Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Kommunikationsdienstes notwendig sind ausübt und diese Dienste anderen anbietet*".[138] In diesem Zusammenhang kommt sowohl den Patienten, als auch dem niedergelassenen Kassenarzt lediglich eine teilnehmende Stellung in der datenschutzrechtlichen Prüfung zu. Neben den Datensicherheitsmaßnahmen, die von dem Betreiber jedenfalls zu treffen sind, hat dieser die Teilnehmer, sohin ua den Arzt und seine Patienten, gegebenenfalls bei Bestehen eines besonders hohen Risikos der Verletzung der Vertraulichkeit über diese Tatsache zu informieren und - selbst bei Vorliegen eines Risikos außerhalb seines Anwendungsbereichs - ihnen mögliche Abhilfen sowie deren Kosten aufzuzeigen.[139]

[136] DSB 31.10.2018, DSB-D123.076/0003-DSB/2018; ErwGr 173 VO (EU) 2016/679; *Kiparski/Sassenberg,* DSGVO und TK-Datenschutz – Ein komplexes europarechtliches Geflecht, CR 2018/34, 324 (324 ff).
[137] § 95 Abs 1 TKG
[138] § 3 Z 3 TKG
[139] § 95 Abs 2 TKG

Unbeschadet der vorgegebenen Regelungen der DS-GVO, haben Betreiber eines öffentlichen Kommunikationsdienstes nach dem TKG unter Anwendung zielgerichteter Datensicherheitsmaßnahmen konkret drei Aspekte als Mindestanforderung sicherzustellen: Einerseits (i) dürfen nur "*ermächtigte Personen für rechtlich zulässige Zwecke Zugang zu personenbezogenen Daten erhalten*". Andererseits (ii) muss für ausreichend Schutz der gespeicherten oder bereits übermittelten personenbezogenen Daten vor unbeabsichtigter bzw unrechtmäßiger Zerstörung, Verlust oder Veränderung sowie vor unbefugter bzw unrechtmäßiger Speicherung, Verarbeitung, Zugang zu oder Weitergabe der Daten gesorgt werden. Und schließlich (iii) verlangt das TKG eigens die Ausarbeitung und Durchführung eines Sicherheitskonzepts für die Datenverarbeitung. Um das vorgesehene Sicherheitsniveau tatsächlich garantieren zu können, legitimiert das TKG die Regulierungsbehörde sich die getroffenen Maßnahmen vorlegen und präsentieren zu lassen und kann diese weiters prüfen und Empfehlungen abgeben.[140] Angesichts der in §§ 95 ff TKG normierten Datenschutz-Regelungen, kann durchaus eine Empfehlung der Nutzung des Mediums der Sprachtelefonie und SMS an Ärzte gerichtet und diese auch vertreten werden.

5.4 Kommunikation via Post (durch einen Brief)

In Österreich ist das Briefgeheimnis ein Grundrecht, das grundsätzlich jedem Bürger zusteht. Das im Dezember 1867 beschlossene Staatsgrundgesetz legt in seinem Art 10 gemeinsam mit Art 8 der Europäischen Menschenrechtskonvention (EMRK) den Grundstein für das besagte Grundrecht. Demnach hat jedermann Anspruch auf Achtung [...] seines Briefverkehrs und darf dieses Briefgeheimnis nicht verletzt werden, es sei denn ein Eingriff ist gesetzlich vorgesehen und stellt eine Maßnahme dar, "*die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist*".[141] Aus diesem Blickwinkel kann bspw auf die Bestimmungen der Strafprozessordnung (StPO) oder des Finanzstrafgesetzes (FinStrG) verwiesen werden.[142] Wie zuvor in Kapitel „5.1 Mündliche Kommunikation (im Warteraum der Ordination)" behandelt, ist Adressat eines

[140] § 95 Abs 3 TKG.
[141] Art 8 Abs 2 EMRK.
[142] §§ 135 ff StPO; §§ 93 ff FinStrG.

Grundrechts ausschließlich der Staat und entfaltet dieses nur dann eine Drittwirkung, wenn der Gesetzgeber dies ausdrücklich normiert. Dem Vorhaben, das Grundrecht auf sein Briefgeheimnis auch zwischen Privatpersonen durchsetzbar zu machen, wurde mit § 118 Strafgesetzbuch (StGB) Rechnung getragen. Darin ist die Strafbarkeit für eine Verletzung des Briefgeheimnisses und die Unterdrückung von Briefen geregelt. Das Öffnen eines nicht zu seiner Kenntnisnahme bestimmten verschlossenen Briefes oder anderes solches Schriftstücks wird mit einer Freiheitsstrafe bis zu drei Monaten oder Geldstrafe bis zu 180 Tagessätzen bestraft, wenn auch nur auf Verlangen des Verletzten, ausgenommen bei Begehung durch einen Beamten.[143]

Mit dieser rechtlichen Absicherung, kann den Ärzten eine Kommunikation mit ihren Patienten durch Briefverkehr ohne Probleme empfohlen werden.

5.5 Besonderheit: Telefax

Das GTelG gestattet eine Übermittlung von Gesundheitsdaten und genetischen Daten per Fax in § 27 Abs 12 in Form einer Ausnahmeregelung. Dies nur insofern, als ein Nachweis oder die Prüfung von Identität, Rollen oder Integrität gemäß dem 2. Abschnitt unzumutbar sind und wenigstens die Identitäten und bedeutenden Rollen der betroffenen Gesundheitsdiensteanbieter wechselseitig durch entweder persönlichen oder telefonischen Kontakt oder durch Festlegung gewisser vertraglicher Bestimmungen nachgewiesen sind.[144]

Neben den genannten Voraussetzungen des § 27 Abs 10 Z 1 bis 3 GTelG, erfordert eine Übertragung per Fax darüber hinaus das Vorliegen von (i) Faxanschlüssen, die ausreichend vor unbefugtem Zugang und Gebrauch geschützt sind, (ii) Rufnummern, die nachweislich und regelmäßig auf ihre Aktualität geprüft werden, (iii) Deaktivierungen automatischer Weiterleitungen, wenn es sich dabei nicht um die jeweiligen Gesundheitsdiensteanbieter selbst handelt, (iv) der Nutzung der vom Gerät unterstützten Sicherheitsmechanismen sowie (v) der ausschließlich eingeschränkten Aktivierung der Fernwartungsfunktion nur für die vereinbarte Dauer der Fernwartung.[145]

[143] § 118 Abs 1 StGB.
[144] § 27 Abs 12 iVm Abs 10 Z 1-3 GTelG
[145] § 27 Abs 12 GTelG

6 Resümee

Zusammenfassend kann festgestellt werden, dass ein einzelner niedergelassener Kassenarzt neben allgemeinen personenbezogenen Daten seiner Patienten auch besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, in seiner Ordination rechtmäßig verarbeitet. Diese Rechtmäßigkeit schafft die DS-GVO für die Verarbeitung personenbezogener Daten mit den in Art 6 taxativ aufgezählten Erlaubnistatbeständen, für Gesundheitsdaten hingegen durch die in Art 9 iVm Art 6 abschließend genannten Ausnahmetatbestände. Die ärztliche Datenverarbeitung kann sowohl auf die Erfüllung einer rechtlichen Verpflichtung aufgrund der Bestimmung über die Dokumentationspflicht des § 51 Abs 1 ÄrzteG (Art 6 lit c), als auch auf eine Vertragserfüllung wegen des Behandlungsvertrages (Art 6 lit b) sowie auf eine Einwilligung (Art 6 lit a) gestützt werden, wobei für die Verarbeitung der Gesundheitsdaten ausschließlich der Rechtfertigungstatbestand des Art 9 Abs 2 lit h herangezogen werden kann, welcher ua auf die Gesundheitsvorsorge und medizinische Diagnostik Bezug nimmt. Entscheidende Bedeutung kommt neben der Rechtmäßigkeit, auch der Sicherheit der Datenverarbeitung zu, für die die DS-GVO und das GTelG jedoch unterschiedlich strenge Vorgaben bei lokaler Datenspeicherung und einer Cloud Computing Lösung vorsehen. In jedem Fall hat der Arzt, in der Rolle des Verantwortlichen, die Datensicherheit durch Umsetzung eines in Art 32 DS-GVO normierten Sicherheitskonzeptes zu garantieren und die Maßnahmen des GTelG zu beachten, indessen ist bei Nutzung einer Cloud Computing Lösung auch der externe Dienstleister als Auftragsverarbeiter und aufbauend auf einem Auftragsverarbeitungsvertrag daran gebunden. Darüber hinaus stellt die Cloud Computing Lösung eine elektronische Übermittlung iSd GTelG dar, die angesichts des erhöhten Eingriffsrisikos zusätzliche Datensicherheitsmaßnahmen erfordert.

Für die Beurteilung der Frage nach der Existenz rechts- bzw datenschutzkonformer sowie technisch sicherer Datenübertragungsarten bzw Kommunikationsmittel zwischen Ärzten und anderen Parteien bzw ihren Patienten, wurden in dieser Arbeit vier unterschiedliche Kommunikationsmedien genauer betrachtet und deren Garantie für die Datensicherheit anhand der gesetzlichen Vorgaben geprüft. Die mündliche Kommunikation zwischen dem Arzt und seinen Patienten in der Ordination kann unter Anwendung ausreichender praktischer Schutz- und Sicherheitsmaßnahmen grundsätzlich durchgeführt werden, es gilt jedoch neben Art 32 DS-GVO, auch das Grundrecht auf Datenschutz zu beachten.

Die Kommunikation via Post und jene über Sprachtelefonie und SMS kann jedem Arzt ohne weiteres empfohlen werden. Ausführend ist zu bemerken, dass das Briefgeheimnis zu den Grundrechten in Österreich gehört, welches in weiterer Folge eine strafrechtliche Verantwortung nach sich zieht, um eine Drittwirkung des Grundrechts zu ermöglichen. Die Sprachtelefonie hingegen ist als klassischer elektronischer Kommunikationsdienst dem Telekommunikationsgesetz zuzuordnen, welches als lex specialis Vorrang gegenüber den Bestimmungen der DS-GVO genießt und durch eine datenschutzrechtliche Rollenverschiebung dem Netzbetreiber die Verantwortung der Datensicherheit auferlegt. Anders verhält es sich mit der Kommunikation über sogenannte OTT-Dienste, von deren Nutzung dem Arzt nach derzeit in Geltung stehender Rechtslage abgeraten werden muss. OTT-Dienste, wie bspw der Messenger-Dienst WhatsApp oder der E-Maildienst Gmail, werden nach der Judikatur des EuGH nicht als elektronische Kommunikationsdienste iSd TKG subsumiert, wodurch die Rolle des Arztes als Verantwortlicher aufrecht erhalten bleibt und diesem zur Nutzung des WhatsApp-Dienstes die Pflicht zum Abschluss eines Auftragsverarbeitungsvertrages mit der Firma WhatsApp auferlegt werden würde. Ein solcher Kompromiss erscheint seitens WhatsApp aber aussichtslos. Nach Umsetzung der neuen EU-Richtlinie, dem TK-Kodex, in nationales österreichisches Recht wird infolge Einbeziehung der OTT-Dienste unter das Telekommunikationsrecht die Legitimität der Nutzung neu zu beurteilen sein. Ergänzend wurde auch die Übertragung per Telefax angeführt, die dem GTelG als Ausnahmeregelung entnommen werden kann.

7 Literaturverzeichnis

- Art-29-Datenschutzgruppe, Stellungnahme 12/2016 idF 04/2017 Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), WP 243 rev.01, 16/DE
- Art-29-Datenschutzgruppe, Stellungnahme 12/2016 Leitlinien zum Recht auf Datenübertragbarkeit („DSB“), WP 242 rev.01, 16/EN
- Ärztekammer Wien, FAQs DS-GVO <https://www.aekwien.at/datenschutzgrundverordnung> (16.11.2019).
- *Bergauer Christian/Jahnel Dietmar* (Hrsg), Teilkommentar zur DS-GVO, Datenschutz-Grundverordnung, Teil-Kommentar (Jan Sramek 2018)
- *Braun Ingo/Hasenauer Stefan,* Die Rechtmäßigkeit der Verarbeitung gemäß Art 6 DS-GVO, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht 2018, (NWV Verlag)
- Die Konkurrenz aus dem Netz, OTT-Dienste in Medien und Telekommunikation, RTR <https://www.rtr.at/de/inf/Konkurrenz_aus_dem_Netz_OTT/Die_Konkurrenz_aus_dem_Netz_OTT-Dienste.pdf> (16.11.2019).
- *Engel Jun. Harald*, Digitalisierung in der Medizin: Praxismanagement und Datenschutz, Journal für Ästhetische Chirurgie 2018, Vol 11/3
- EuGH Entscheidung: Gmail ist kein Telekommunikationsdienst <https://diercks-digital-recht.de/2019/07/eugh-c-193-18-gmail-ist-kein-telekommunikationsdienst-i-auswirkung-auf-ott-dienste-nebst-ausblick-auf-eu-richtlinie-ueber-den-kodex-fuer-die-elektronische-kommunikation-2018-1972/> (16.11.2019)
- *Gerhartl Andreas,* Verarbeitungsverzeichnis nach DS-GVO: Alles klar?, ecolex: Fachzeitschrift für Wirtschaftsrecht 2019/Heft 8
- *Jahnel Dietmar*, „Whitelist“ und „Blacklist“ zur Datenschutz-Folgenabschätzung, jusIT 2019/12
- *Kiparski Gerd,* Der EuGH schafft Klarheit: OTT-Dienste sind in der Regel keine Telekommunikationsdienste, Computer und Recht 2019, Band 35/Heft 7
- *Kiparski Gerd,* Der Europäische Telekommunikations-Kodex – Ein neuer Rechtsrahmen für die elektronische Kommunikation, Computer und Recht 2019, Band 35/Heft 7
- *Kiparski Gerd/Sassenberg Thomas,* DSGVO und TK-Datenschutz – Ein komplexes europarechtliches Geflecht, Computer und Recht 2018, Band 34/Heft 5
- *Knyrim Rainer (Hrsg), Der DatKomm: Praxiskommentar zum Datenschutzrecht – DS-GVO und DSG (Manz 2018)*

- *Kriegner Johann,* Anmerkungen zu § 1 DSG nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO), Wirtschaftsrechtliche Blätter 2019, Vol 33/2
- Novadex, Definition Cloud Cumputing <https://novadex.com/de/glossar-artikel/definition-cloud-computing-was-ist-cloud-computing> (16.11.2019)
- *Pfandlsteiner Eva-Maria/Gabauer Claudia/Trieb Gerald,* Rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten - Zum Anwendungsbereich des GTelG 2012, Recht der Medizin 2019/5
- *Pletzer Renate,* Die Haftung des Arztes für Behandlungsfehler und Aufklärungsmängel, in Kierein/Lanske/Wenda (Hrsg), Jahrbuch Gesundheitsrecht 2007, (NWV Verlag)
- *Pollirer Hans-Jürgen,* Checkliste Auskunftsrecht nach Art 15 DS-GVO, Datenschutz Konkret 2017/Heft 3
- *Pollirer Hans-Jürgen,* Checkliste Erfüllung der Informationspflichten gem Art 13 und 14 DS-GVO, Datenschutz Konkret 2018/Heft 4
- *Pollirer Hans-Jürgen/Weiss Ernst M./Knyrim Rainer/Haidinger Viktoria (Hrsg),* DSG Online – Sonderausgabe zum Datenschutzgesetz (Manz 2019)
- *Raabe-Stuppnig Katharina/Bisset Katharina,* To delete or not to delete: Lösch- und Aufbewahrungspflichten in der Medizin, Journal für Medizin- und Gesundheitsrecht 2019/Heft 2
- *Thiele Clemens,* Der Multimediale Helpdesk – Datenschutzrechtliche Grundlagen des Einsatzes von WhatsApp zur digitalen Kundenkommunikation, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht 2017, (NWV Verlag)
- *Vedder Karin*, Datenschutz in Arztpraxen, Datenschutz und Datensicherheit 2014, Vol 38/12
- Völkel Oliver, Neue Vorgaben für IT-Sicherheit in Banken, Die Presse 2019/38/02
- Weniger Kassenärzte, mehr Wahlärzte in Österreich<https://www.derstandard.at/story/2000079701899/weniger-kassenaerzte-mehr-wahlaerzte-in-oesterreich> (16.11.2019)
- WhatsApp Datenschutzrichtlinie <www.whatsapp.com> (16.11.2019) <https://www.whatsapp.com/legal/?eea=1#how-we-process-your-information> (16.11.2019)

8 Judikaturverzeichnis

- AG Bad Hersfeld 15.05.2017, F 120/17 EASO
- DSB 15.11.2018, DSB-D122.944/0007-DSB/2018 Datenschutz Konkret 2019/Heft 3 (*Haidinger/Weiss*)
- DSB 16.11.2018, DSB-D213.692/0001-DSB/2018
- DSB 16.11.2018, DSB-D213.692/0001-DSB/2018, ecolex: Fachzeitschrift für Wirtschaftsrecht 2019/Heft 6 (*Knyrim*)
- DSB 31.10.2018, DSB-D123.076/0003-DSB/2018
- EuGH 13.06.2019, C 193/18

9 Rechtsquellenverzeichnis

- 2. Materien-Datenschutz-Anpassungsgesetz 2018, BGBl. I 37/2018.
- Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GtelG 2012), BGBl I 111/2012 idF 100/2018
- Bundesgesetz über die Ausübung des Ärztlichen Berufs und die Standesvertretung der Ärzte (Ärztegesetz 1998 – ÄrzteG 1998), BGBl I 169/1998 idF 105/2019
- Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl I 10/2004 idF 104/2018
- Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB), BGBl 60/1974 idF BGBl I 105/2019
- Bundesgesetz vom 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (Finanzstrafgesetz – FinStrG.), BGBl 129/1958 idF BGBl I 91/2019
- Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF 14/2019
- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 70/2003 idF 111/2018
- Erläuterungen zur Regierungsvorlage 108 BlgNr XXVI. GP
- Erläuterungen zur Regierungsvorlage 1936 BlgNr XXIV. GP
- Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl 210/1958 idF BGBl III 139/2018

- Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste (Rahmenrichtline), ABl L 108/33
- Richtlinie 2018/1972/EU des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), ABl L 321/36
- Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl I 165/1999 idF BGBl I 120/2017
- VO (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), ABl L 2016/119

Ehrenwörtliche Erklärung

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen inländischen oder ausländischen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

Mag. iur. Lea Strasser

Wien, Jänner 2020 Mag. iur. Lea Strasser

Zusammenfassung

Das Ziel dieser Masterarbeit war es die Grundlagen der rechts- bzw datenschutzkonformen sowie technisch sicheren Datenverarbeitung in einer Arztpraxis herauszuarbeiten sowie die damit verbundene Patientenkommunikation unter dem Aspekt des Datenschutzes und der Datensicherheit zu beleuchten. In einem ersten Schritt erfolgt die Betrachtung der allgemeinen Zulässigkeit einer lokalen Datenverarbeitung der Patientendaten in einer Ordination anhand einer vollständigen Datenschutzprüfung. Ergänzend wird in einem zweiten Schritt die Datenverarbeitung mittels einer Cloud-Computing Lösung einer datenschutz- bzw datensicherheitsrechtlichen Prüfung unterzogen. Als Erkenntnis wird festgestellt, dass die allgemeine Zulässigkeit zu bejahen ist. Abschließend geht diese Arbeit in ihrem letzten Teil auf die Kommunikationsmittel und –Arten im Detail ein, die zu ärztlichen Kommunikationszwecken aus datensicherheitsrechtlicher Sicht eingesetzt werden können. Diese Arbeit, insbesondere deren letzter Teil, eignet sich auch als Anleitung für Ärzte im Umgang mit der Patientenkommunikation.