

Schwerpunktthema

Praktikable Datenschutzlösungen



Schwerpunktthema

Praktikable Datenschutzlösungen

Ausgabe 1/2020

Impressum:

Die in der ZGP veröffentlichten Beiträge sind nicht unbedingt mit der Auffassung des LIG oder seines Trägers ident.

LIG – Linzer Institut für Gesundheitssystem-Forschung

Obmann: Präs. Dr. Peter Niedermoser

Geschäftsführer: Hon.-Prof. Dr. Felix Wallner

ZGP – Zeitschrift für Gesundheitspolitik

Medieninhaber, Herausgeber und Redaktion: Linzer Institut für Gesundheitssystem-Forschung, Dinghoferstraße 4, 4010 Linz

www.lig-gesundheit.at

Coverfoto: Milles Studio (shutterstock)

Redaktion: Mag. Katharina Wieser, Mag. Sabine Weißengruber-Auer, MBA

Verleger: Verlagshaus der Ärzte GmbH, 1010 Wien

Druck: Ferdinand Berger & Söhne GmbH, 3580 Horn

Liebe Leserin, lieber Leser

die Europäische Datenschutz-Grundverordnung (DSGVO) war sicherlich jene IT-Regulierung mit den stärksten Auswirkungen der letzten Jahre. Aber wie lebt es sich heute, zwei Jahre nach dem Inkrafttreten der DSGVO, mit den umfassenden Vorschriften? Wie wirkt sich die DSGVO auf den Datenverkehr im medizinischen Alltag aus? All diesen Fragestellungen und Aspekten widmet sich die aktuelle Ausgabe der ZGP.

Heute fällt die Bilanz durchwegs positiv aus. Wie immer bei großen Neuerungen gab es zu Beginn viele Unsicherheiten. Doch die meisten Organisationen haben sich mit der Datenschutz-Grundverordnung gut arrangiert. Wie für viele Institutionen ist auch für Ordinationen infolge der DSGVO der administrative Aufwand deutlich mehr geworden – die Bürokratie hat mal wieder zugenommen. Grund genug, sich in dieser Ausgabe praktikablen Datenschutzlösungen für den niedergelassenen Bereich zu widmen sowie konkrete Risikofelder im Ordinationsalltag aufzuzeigen und Tipps zu geben, wie sensible Daten vor unerlaubten Zugriffen geschützt werden können.

Für Ärzte ist der Datenschutz nicht erst seit dem Inkrafttreten der neuen DSGVO ein hochsensibles Thema. Die ärztliche Schweigepflicht begleitet Mediziner seit Beginn ihrer beruflichen Tätigkeit. Kapitel 6 dieser Zeitschrift widmet sich der für Ärzte wichtigen Thematik der ärztlichen Schweigepflicht und gibt Antworten auf die häufigsten Fragen zur Verschwiegenheitspflicht.

Mit der aktuellen Ausgabe der ZGP möchten wir Ihnen einen umfassenden Einblick in alltägliche Datenschutzthemen geben und Ihnen Hilfestellungen bei Fragen in Bezug auf Datenverarbeitung und Datenspeicherung anbieten.

Hon.-Prof. Dr. Felix Wallner
Geschäftsführer LIG

Dr. Peter Niedermoser
Obmann LIG

Inhaltsverzeichnis

Auswirkungen der Datenschutz-Grundverordnung (DSGVO) auf Ärztinnen und Ärzte im niedergelassenen Bereich	9
<i>Mag. Alexander Czadilek, Mag. Ewald Scheucher, Ing. Dr. iur. Christof Tschohl</i>	
Datenschutz in der Arztpraxis	39
<i>Gerhard Stimac</i>	
Datenschutzkonformer Alltag in der Arztpraxis. Wie setzen Ärzte die DSGVO und IT-Sicherheit praktikabel und rechtssicher um?	45
<i>Univ.-Lekt. Nicolas Nagel, CIPP/E, CIPM, CIPT, FIP, CDPO</i>	
Ärztliches Berufsgeheimnis	95
<i>Mag. Kerstin Garbeis, LL.M.</i>	
Die Achtung der ärztlichen Verschwiegenheit in einem Strafverfahren	109
Univ.-Prof. Dr. Alois Birklbauer	
Auf den Standpunkt gebracht	125
<i>Mit Beiträgen von DI Michael Nöhammer und Mag. Markus Dörfler, LL.M.</i>	

Mag. Alexander Czadilek

Rechtsanwaltsanwarter in der Scheucher Rechtsanwalt GmbH

Mag. Ewald Scheucher

*Rechtsanwalt und Geschaftsfuhrer der Scheucher Rechtsanwalt GmbH,
Datenschutzbeauftragter der Arztekammer fur Wien*

Ing. Dr. iur. Christof Tschohl

*Wissenschaftlicher Leiter Research Institute AG & Co KG (Digital Human
Rights Center), Of Counsel der Scheucher Rechtsanwalt GmbH*

Auswirkungen der Datenschutz- Grundverordnung¹ (DSGVO) auf Arztinnen und Arzte im niedergelassenen Bereich

Aus Grunden der besseren Lesbarkeit haben wir entweder die mannliche oder weibliche Form einer Bezeichnung gewahlt. Dies impliziert keinesfalls eine Benachteiligung des jeweils anderen Geschlechts. Frauen und Manner sollen sich vom Inhalt gleichermaen angesprochen fuhlen.

¹ Verordnung (EU) 2016/679 des Europaischen Parlaments und des Rates vom 27. April 2016 zum Schutz naturlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

1. Grundlagen und Begriffe	11
2. Rechtfertigung der Verarbeitung personenbezogener Daten	16
3. Pflichten des Verantwortlichen	28
4. Fazit	36
Literaturverzeichnis	37

Im medizinischen Bereich und insbesondere bei der Verarbeitung von Gesundheitsdaten kommt es zu einem Zusammenwirken der in allen Mitgliedstaaten der EU unmittelbar anzuwendenden EU-Datenschutzgrundverordnung (DSGVO) und verschiedenen nationalen Sonderregelungen. Niedergelassene Ärzte, die in der Regel als datenschutzrechtliche Verantwortliche zu qualifizieren sind, haben eine Vielzahl an datenschutzrechtlichen Bestimmungen zu beachten, deren Verletzung zu hohen Geldstrafen führen kann. Dieser Beitrag soll einen Überblick über die wichtigsten datenschutzrechtlichen Pflichten und Rechtsgrundlagen geben, die niedergelassene Ärzte zu beachten haben. Aufgrund vieler unbestimmter Gesetzesbegriffe in der DSGVO besteht in manchen Bereichen (bis zur Klärung durch die Höchstgerichte) dennoch Rechtsunsicherheit, die der Beitrag transparent macht und damit auf ein überschaubares Maß reduziert.

1. Grundlagen und Begriffe

1.1. Anwendungsbereich der DSGVO

Mit 25. Mai 2018 trat die DSGVO in den Mitgliedstaaten der Europäischen Union in Geltung. Sie soll der Angleichung des Datenschutzrechts in Europa dienen und ist als EU-Verordnung unmittelbar anwendbar. Die DSGVO enthält jedoch auch sogenannte „Öffnungsklauseln“, die es dem nationalen Gesetzgeber ermöglichen, präzisere Regelungen zu treffen bzw. ihn auch verpflichten, nähere Regelungen vorzusehen.

Die DSGVO regelt nur die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten (z.B. elektronische Verwaltung von Patientenakten) Die nicht automatisierte Verarbeitung ist nur erfasst, wenn Daten in einem Dateisystem gespeichert werden. Dateisysteme sind etwa auch (Papier-)Karteien zur Patientenverwaltung, da sie nach bestimmten Kriterien (Name, Aktenzeichen etc.) aufgebaut sind und durchsucht oder ausgewertet werden können. Die Verarbeitung von anonymisierten Daten² fällt hingegen nicht in den Anwendungsbereich der DSGVO.

Gegenstand des Datenschutzrechts ist die Verarbeitung personenbezogener Daten von Betroffenen, also von identifizierten oder identifizierbaren natürlichen Personen (z.B. Patienten), auf welche sich bestimmte Informationen beziehen. Die Verarbeitung erfolgt durch den sogenannten „Verantwortlichen“ (z.B. Ärzte, die eine Ordination betreiben).

Die für datenverarbeitende Stellen wohl weitestreichende Änderung im Vergleich zum bisher bestehenden Datenschutzregime sind die Sanktionsmöglichkeiten der Aufsichtsbehörde (österreichische Datenschutzbehörde, DSB). Verstöße gegen die DSGVO können gemäß Art. 83 DSGVO verwaltungsstrafrechtlich mit Geldbußen von bis zu 20 Millionen Euro oder im Fall eines Unternehmens mit bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nachdem, welcher der Beträge höher ist), geahndet werden.³

2 Daten, die keinen Personenbezug haben – es handelt sich somit um Daten, die niemand auf eine in ihrer Identität bestimmte Person zurückführen kann.

3 Zu den allgemeinen Voraussetzungen für die Verhängung von Geldbußen siehe § 30 DSG.

1.2. Weitere für den niedergelassenen Bereich relevante Rechtsgrundlagen

1.2.1. Ärztegesetz 1998

Für die Übermittlung von Gesundheits- bzw. Patientendaten durch niedergelassene Ärzte an andere Ärzte oder medizinische Einrichtungen sieht die Bestimmung des § 51 Abs. 2 Z 2 ÄrzteG in Österreich eine strengere Regelung als die DSGVO vor. Nach dieser Bestimmung ist eine derartige Übermittlung in Österreich nur mit Einwilligung des Betroffenen zulässig, während die Übermittlung von Patientendaten an andere Ärzte oder medizinische Einrichtungen für die Versorgung oder Behandlung im Gesundheitsbereich nach der DSGVO auch ohne Einwilligung des Betroffenen zulässig wäre.⁴

1.2.2. Gesundheitstelematikgesetz 2012 (GTelG)

Das GTelG regelt die Verarbeitung personenbezogener elektronischer Gesundheitsdaten und genetischer Daten durch Gesundheitsdiensteanbieter und hat im medizinischen Bereich neben den allgemeinen datenschutzrechtlichen Bestimmungen als *lex specialis* besondere Bedeutung. Insbesondere gehen die Bestimmungen des GTelG betreffend die Datensicherheit bei der elektronischen Übermittlung von Gesundheitsdaten und genetischen Daten den allgemeinen Datensicherheitsmaßnahmen gemäß Art. 32 DSGVO vor.⁵

1.3. Begriffsbestimmungen

1.3.1. Personenbezogene Daten

Die DSGVO bezieht sich ausschließlich auf personenbezogene Daten, worunter alle Informationen verstanden werden, die sich auf eine identifizierte oder identifizierbare natürliche Person (= Betroffener) beziehen.⁶ 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 besonderen Merkmalen,

4 Siehe dazu und zur Frage, ob eine derartige Abweichung vom unmittelbaren Unionsrecht zulässig ist, Punkt 2.5.

5 Die Zulässigkeit der im nationalen Recht strenger ausgestalteten Datensicherheitsmaßnahmen lässt sich auf die Öffnungsklausel des Art. 9 Abs. 4 DSGVO stützen.

6 Art. 4 Z 1 DSGVO.

die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.3.2. Verarbeitung personenbezogener Daten

Die DSGVO geht von einem sehr weiten Verarbeitungsbegriff⁷ aus, der jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten umfasst, wie etwa das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Änderung, die Verwendung, die Offenlegung durch Übermittlung, das Löschen oder die Vernichtung. Auf die nicht automatisierte Verarbeitung personenbezogener Daten ist die DSGVO jedoch nur anwendbar, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen⁸, also eine manuell strukturierte Verarbeitung vorliegt. Akten oder Aktsammlungen, die nicht nach bestimmten Kriterien sortiert sind, z.B. in einer rein chronologischen, ansonsten völlig unsortierten Ablage, sind nicht von der DSGVO erfasst.⁹

1.3.3. Gesundheitsdaten

Nach der Definition des Art. 4 Z 15 DSGVO sind Gesundheitsdaten alle personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person – einschließlich der Erbringung von Gesundheitsdienstleistungen – beziehen und aus denen Informationen über den Gesundheitszustand hervorgehen. Ein Gesundheitsdatum liegt immer dann vor, wenn Rückschlüsse auf die Gesundheit einer identifizierbaren Person gezogen werden können.¹⁰

Anknüpfungspunkt ist die Gesundheit einer natürlichen Person, nicht die Krankheit. Daraus ergibt sich, dass nicht nur alle Informationen über den Ablauf und den Inhalt einer medizinischen Behandlung sowie die verschriebenen Medikamente unter den Begriff der Gesundheitsdaten zu subsumieren sind, sondern auch die Feststellung, dass eine Person genesen oder völlig gesund ist.¹¹

Von der weiten Definition des Begriffs „Gesundheitsdaten“ erfasst sind demnach neben den offensichtlichen Fällen, wie Entlassungsbriefe und Labordaten, auch

7 Art. 4 Z 2 DSGVO (nicht abschließende Aufzählung der Verarbeitungsfälle).

8 Art. 1 Abs. 1 DSGVO, sachlicher Anwendungsbereich.

9 Vgl. Erwägungsgrund (ErwGr) 15 DSGVO; siehe auch *Zerdick in Ehmann/Selmayr*, DS-GVO² Art. 2 Rz 3.

10 Siehe dazu auch ErwGr 35 DSGVO.

11 *Lachmayer in Knyrim*, DatKomm Art. 1 DSGVO, Rz 156.

beispielsweise Terminerinnerungen von Ärzten an Patienten und Protokoll Daten, die sowohl den Namen des Patienten als auch den Namen des Arztes enthalten.¹²

1.3.4. Besondere Kategorien personenbezogener Daten („sensible Daten“)

Einer besonderen Schwere unterliegen personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Somit sind alle Gesundheitsdaten „sensible Daten“, für die erschwerte bzw. zusätzliche Voraussetzungen für die Rechtmäßigkeit bzw. Zulässigkeit der Verarbeitung gelten.¹³

1.4. Datenschutzrechtliche Rollenverteilung – Verantwortlicher und Auftragsverarbeiter

Bei der Rechtmäßigkeitsprüfung einer Datenverarbeitung ist zunächst zu beurteilen, welche Rolle die jeweils Beteiligten einnehmen.

Betroffene Person ist diejenige natürliche Person, deren Daten verarbeitet werden.¹⁴ *Verantwortlicher* ist jede (natürliche oder juristische) Person, Organisation oder öffentliche Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung entscheidet.¹⁵ *Auftragsverarbeiter* ist derjenige, der Daten im Auftrag eines Verantwortlichen verarbeitet.

Im niedergelassenen Bereich sind in der Regel der Arzt für Allgemeinmedizin und der Facharzt Verantwortliche im Sinne der DSGVO. Das bedeutet, dass sie hinsichtlich der Datenverarbeitung verschiedene Pflichten treffen, zu denen insbesondere die Dokumentationspflicht, die Informationspflicht gegenüber den Betroffenen, die Rechenschaftspflicht und die Pflicht zur Einhaltung der Datensicherheit zählen. Werden Dienstleister, die z.B. IT-Support und IT-Wartung hinsichtlich der elektronischen Patientenverwaltung zur Verfügung stellen und Zugriff

¹² Pfandlsteiner, Gabauer, Trieb, Rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten, RdM 2019/103, 171.

¹³ Siehe dazu näher Punkt 2.1 und 2.2.

¹⁴ Art. 4 Z 1 DSGVO.

¹⁵ Art. 4 Z 7 DSGVO.

auf Patientendaten haben, hinzugezogen, ist mit diesen Auftragsverarbeitern ein Auftragsverarbeitervertrag gemäß Art. 28 DSGVO abzuschließen.

Nach in Österreich¹⁶ und Deutschland¹⁷ überwiegender Meinung¹⁸ kommt es hinsichtlich eines Laborauftrags und der diesbezüglichen Datenübermittlung zwischen einem behandelnden Arzt und einem Laborarzt nicht zu einem Auftragsverarbeitungsverhältnis. Denn unter den Begriff des Auftragsverarbeiters fallen nicht Akteure, die (i) über eine gewisse Eigenständigkeit bei der Datenverarbeitung sowie besonderes Fachwissen verfügen und (ii) daher dem Verantwortlichen weder unmittelbar unterstellt noch weisungsgebunden sind und (iii) weitgehend autonom über die Mittel und Zwecke der Verarbeitung entscheiden. Keine Auftragsverarbeiter (sondern selbst Verantwortliche) sind neben Steuerberatern, Zivilt Technikern u.a. sohin auch Laborärzte, da sämtliche dieser Eigenschaften auf diese zutreffen.

16 Vgl. etwa *Bergauer*, Die Rollenverteilung nach der DSGVO, jusIT 2018, 60.

17 Vgl. etwa Kurzpapier 13 der Deutschen Datenschutzkonferenz, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

18 Die Entwicklung dieses Meinungsstreites bleibt abzuwarten, insbesondere liegt zu dieser Frage noch keine (höchst)gerichtliche Entscheidung vor.

2. Rechtfertigung der Verarbeitung personenbezogener Daten

2.1. Rechtfertigung gemäß Art. 6 und Art. 9 DSGVO

Art. 6 DSGVO stellt die zentrale Vorschrift der DSGVO zur Zulässigkeit der Verarbeitung personenbezogener Daten dar. Diese Bestimmung steht in engem Zusammenhang mit dem Grundsatz der Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit a DSGVO), da in Art. 6 Abs. 1 DSGVO die Voraussetzungen der Rechtmäßigkeit der Verarbeitung näher normiert werden.¹⁹ Art. 6 DSGVO vermittelt also einen Maßstab für die Rechtmäßigkeit der Verarbeitung, und zwar denjenigen zur Beurteilung der Zulässigkeit als solcher, also das „Ob“ der Datenverarbeitung, nicht das – von den Grundsätzen des Art. 5 DSGVO geprägte – „Wie“.²⁰

Art. 6 Abs. 1 enthält eine abschließende Liste von sechs Fällen (Erlaubnis- bzw. Zulässigkeitstatbestände), in denen die Verarbeitung personenbezogener Daten als rechtmäßig gilt. Neben der Einwilligung (Abs. 1 lit a leg cit) beschreiben die fünf anderen Fälle Szenarien, bei denen eine Verarbeitung in einem besonderen Kontext, wie z.B. der Erfüllung eines Vertrags mit der betroffenen Person, der Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt etc., erforderlich sein kann. Für das Vorliegen einer rechtmäßigen Verarbeitung ist die Erfüllung (mindestens) einer dieser sechs (alternativen) Tatbestände erforderlich, wobei eine „Rangordnung“ untereinander nicht besteht. Diese Regelungstechnik wird auch als „Verbotsprinzip mit Erlaubnisvorbehalt“ bezeichnet.²¹

Art. 9 DSGVO ist eine bereichsspezifische Regelung für die Verarbeitung besonderer Kategorien von Daten („sensible Daten“ – z.B. Gesundheitsdaten, genetische Daten), die – im Vergleich zu Art. 6 DSGVO – zu einem strengeren Rechtsregime führt. In Abs. 1 leg cit wird ein generelles Verbot der Verarbeitung solcher – abschließend aufgezählter – Daten normiert. Art. 2 leg cit statuiert Ausnahmen von diesem Verarbeitungsverbot und schränkt die Verarbeitung auf bestimmte in den lit a bis j angeführte Tatbestände ein, die wesentlich enger als jene für die

19 *Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 6 DSGVO, Rz 1.*

20 *Frenzel in Paal/Pauly, DS-GVO/BDSG2 Art. 6 Rz 7.*

21 *Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 6 DSGVO, Rz 2.*

Verarbeitung „normaler“ oder „nicht sensibler“ Daten sind. Begründet wird dieses strengere Rechtsregime insbesondere mit der besonderen Schutzwürdigkeit dieser Daten²², da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten der Betroffenen auftreten können. Diese Datenarten sind höchstpersönlicher Natur und haben identitätsstiftenden Charakter, weshalb ihr Missbrauch zu gravierenden Konsequenzen für die Grundrechte auf Privatsphäre und der Nichtdiskriminierung der Betroffenen führen kann, die irreversibel sein und langandauernde Folgen haben können.²³

Für die Rechtmäßigkeit der Verarbeitung von Patientendaten im Gesundheitsbereich kommen insbesondere zwei Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO in Betracht:

■ Art. 9 Abs. 2 lit a DSGVO – ausdrückliche Einwilligung der Patienten

und

■ Art. 9 Abs. 2 lit h DSGVO – Erforderlichkeit der Datenverarbeitung für die medizinische Diagnostik oder die Versorgung oder Behandlung im Gesundheitsbereich aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes.

Von Art. 9 Abs. 2 lit h DSGVO sind damit insbesondere alle routinemäßigen Datenverarbeitungsvorgänge in einer Ordination im Zusammenhang mit gesundheitsbezogenen Handlungen der Prävention, Diagnostik, Therapie und Nachversorgung umfasst.

Darunter fallen etwa auch die Übermittlung medizinischer Proben an ein Labor zwecks Diagnostik samt Rückübermittlung der Labordaten oder auch die Übermittlung von Patientendaten an einen Konsiliararzt (zwecks Einholung einer medizinischen Zweitmeinung soweit sie zur erfolgreichen Heilbehandlung erforderlich ist).

Für Zwecke gemäß Art. 9 Abs. 2 lit h DSGVO dürfen personenbezogene Daten jedoch nur durch Fachpersonal, welches einem Berufsgeheimnis oder einer besonderen Verschwiegenheitspflicht unterliegt, verarbeitet werden. In der Regel wird dies auf die mit der Datenverarbeitung in der Ordination betrauten Mitarbeiter zutreffen.

²² Siehe auch ErwGr 51 Satz 1 DSGVO.

²³ Artikel-29-Datenschutzgruppe, Advice paper on special categories of data 4. Vgl. auch *Frenzel in Paal/Pauly, DS-GVO/BDSG* Art. 9 Rz 6.

Art. 9 DSGVO enthält in dessen Abs. 4 eine sogenannte beschränkte Öffnungsklausel. Dies bedeutet, dass Mitgliedstaaten zusätzliche Bedingungen und Beschränkungen einführen oder aufrechterhalten können, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Gemeint sind hiermit Regelungen, die sich nicht lediglich auf die Rechtsgrundlagen der Datenverarbeitung (wie z.B. die Einwilligung) beziehen. Eine Bedingung oder Beschränkung kann sich etwa auf den Umfang der zu verarbeitenden Daten oder innerstaatliche Anforderungen an die Datensicherheit beziehen. Als praxisrelevantes Beispiel für (nicht abdingbare) Datensicherheitsmaßnahmen ist das GesundheitstelematikG 2012 (GTelG 2012) zu nennen. Bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten ist von Gesundheitsdiensteanbietern (z.B. niedergelassenen Ärzte) durch bestimmte Maßnahmen die Gewährleistung der IT-Sicherheit sicherzustellen.²⁴

2.2. Zum Verhältnis von Art. 6 und Art. 9 DSGVO

Das Verhältnis von Art. 6 und Art. 9 DSGVO scheint in der bislang dazu erschienenen Literatur nicht restlos geklärt zu sein, obwohl dies insbesondere für die Frage der Anwendbarkeit von Art. 6 Abs. 4 DSGVO auf die (zweckändernde) Weiterverarbeitung sensibler Daten von Bedeutung ist.²⁵

Manche Autoren meinen, es sei unklar, ob Art. 9 DSGVO eine eigene Rechtsgrundlage für die Zulässigkeit der Verarbeitung darstelle oder ob Art. 9 DSGVO Art. 6 DSGVO nur ergänze und somit immer im Zusammenhang mit dieser Bestimmung zu lesen sei; es spreche aber viel dafür, dass Art. 9 DSGVO eine eigene Rechtsgrundlage darstelle.²⁶ Andere gehen hingegen von einer abschließenden Regelung der Verarbeitung sensibler Daten durch Art. 9 DSGVO aus, wonach die Weiterverarbeitung der Daten für andere Zwecke (allein) auf Grundlage des Art. 6 Abs. 4 DSGVO daher ausgeschlossen sei.²⁷

Nach einer weiteren Meinung enthält Art. 9 Abs. 2 DSGVO keine besonderen Erlaubnistatbestände, sondern lediglich Voraussetzungen für die Ausnahmen vom Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO und sei deshalb nicht anstelle von Art. 6 Abs. 1 DSGVO, sondern zusätzlich – im Sinne einer doppelten bzw. impli-

24 Siehe z.B. § 3 Abs. 4 (Voraussetzungen für die elektronische Übermittlung), § 6 (Vertraulichkeit bei der Übermittlung inkl. Cloud Computing) und § 8 Abs. 1 (IT-Sicherheitskonzept) GTelG 2012.

25 Kastelitz/Hötzendorfer/Tschohl in *Knyrim*, *DatKomm* Art. 9 DSGVO, Rz 5.

26 Korge in *Gierschmann/Schlender/Stentzel/Veil*, *DS-GVO* Art. 9 Rz 3 mwN.

27 Schiff in *Ehmann/Selmayr*, *DS-GVO*² Art. 9 Rz 109.

ziten Prüfung dieser Bestimmungen – zu beachten.²⁸ Demnach müssten für eine zulässige zweckändernde Weiterverarbeitung sensibler Daten ein Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO, ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO und die Voraussetzungen für eine Zweckänderung nach Art. 6 Abs. 4 kumulativ erfüllt sein.²⁹

Die weitere Entwicklung dieses Meinungsstreits und die allfällige (abschließende) Rechtsprechung des EuGH bleibt jedoch abzuwarten. Anzumerken ist, dass die österreichische Datenschutzbehörde in der „Allergie-Tagesklinik“-Entscheidung³⁰ aus dem Jahr 2018 hinsichtlich der Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten in der rechtlichen Begründung des Bescheids festgehalten hat, dass sich die Rechtsgrundlage der Verarbeitung dieser Daten ausschließlich nach Art. 9 Abs. 2 DSGVO richtet.

2.3. Einwilligung in die Datenverarbeitung

Ebenso wie im allgemeinen Erlaubnistatbestand des Art. 6 Abs. 1 lit a DSGVO ist der erste Zulässigkeitstatbestand des Art. 9 Abs. 2 DSGVO die Einwilligung in die Verarbeitung von sensiblen personenbezogenen Daten für einen oder mehrere festgelegte Zwecke. Diese Einwilligung muss im Gegensatz zu Art. 6 Abs. 1 lit a DSGVO ausdrücklich erfolgen, wodurch eine konkludente (schlüssige/stillschweigende) Einwilligung ausgeschlossen ist.³¹

Um die Ausdrücklichkeit der Einwilligung sicherzustellen, empfiehlt sich die Einholung der Einwilligung in Form einer schriftlichen Erklärung, etwa durch Ankreuzen einer Checkbox bei vorformulierten Einwilligungserklärungen. In Frage kommt auch die Einholung einer Unterschrift der betroffenen Person.

Eine Einwilligung ist jede freiwillig für den bestimmten Fall in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung [...], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.³²

28 Petri in *Simitis/Hornung/Spiecker*, Datenschutzrecht Art 9 Rz 3; Bergauer, *jusIT* 2018/83, 232 (233); i.d.S. offenbar auch OGH 24. 7. 2019, 6 Ob 45/19i: „Die Voraussetzungen des Art. 9 Abs. 2 DSGVO sind zusätzlich zu den allgemeinen Verarbeitungsvoraussetzungen des Art. 6 Abs. 1 DSGVO zu beachten.“; Jähnel, *Auswirkungen der DSGVO im medizinischen Bereich*, RdM 2019/123, 251.

29 *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, *DatKomm* Art. 9 DSGVO, Rz 5.

30 DSB-D213.692/0001-DSB/2018 vom 16.11.2018.

31 *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, *DatKomm* Art. 9 DSGVO, Rz 31.

32 Art. 4 Z 11 DSGVO.

In der Regel wird die Verarbeitung personenbezogener Daten im Rahmen der Behandlung durch einen niedergelassenen Arzt durch eine gesetzliche Grundlage legitimiert sein (siehe dazu oben Punkt 2.1. und 2.2.). In bestimmten Fällen kann die Einholung einer Einwilligung aber erforderlich sein, etwa wenn Patientendaten aus Gesundheits-Apps oder (smarte) Hausnotrufs-Armbändern durch den niedergelassenen Arzt verarbeitet werden und die Verarbeitung nicht schon durch den Behandlungsvertrag legitimiert ist.

In einer vielbeachteten Entscheidung³³ aus dem Jahr 2018 betreffend eine Allergie-Tagesklinik hat die österreichische Datenschutzbehörde einige grundlegende Klarstellungen zum Inhalt von Einwilligungen getroffen. Die Datenschutzbehörde hat u.a. ausgesprochen, dass

- Einwilligungen mit der erforderlichen Klarheit zu entnehmen sein muss, für welche Datenverarbeitungen die Einwilligung die Rechtsgrundlage darstellt,
- die Heranziehung von Auftragsverarbeitern einer Einwilligung der betroffenen Person nicht zugänglich ist,
- eine „unwiderrufliche“ Einwilligung Art. 7 Abs. 3 DSGVO widerspricht und nicht vom Betroffenen verlangt werden kann,
- eine Einwilligung in die unverschlüsselte Übermittlung³⁴ von Gesundheitsdaten (Befunden) per E-Mail nicht statthaft ist, da eine Einwilligung dazu dient, eine Rechtsgrundlage für die Datenverarbeitung zu schaffen – nicht aber dazu, um die objektiven Pflichten des Verantwortlichen zur Datensicherheit gemäß Art. 32 DSGVO zum Nachteil des Betroffenen auf diesen abwälzen zu können.

³³ DSB-D213.692/0001-DSB/2018 vom 16.11.2018.

³⁴ Siehe dazu und zur elektronischen Übermittlung von Gesundheitsdaten durch Gesundheitsdiensteanbieter Punkt 2.6.

2.4. Datenvorhaltung für Haftungsfälle (Art. 9 Abs. 2 lit f DSGVO)

Gemäß Art. 9 Abs. 2 lit f DSGVO dürfen Gesundheitsdaten verarbeitet werden, wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist. Diese Bestimmung dient dem Rechtsdurchsetzungsanspruch des Anspruchsinhabers sowie der Funktionsfähigkeit der Justiz. Das strenge Datenschutzregime soll nicht so weit gehen, dass die legitime Durchsetzung von Rechten nicht mehr möglich ist.³⁵

Der Begriff „Rechtsanspruch“ ist weit auszulegen. Ansprüche können sich entweder aufgrund gesetzlicher oder vertraglicher Regelung ergeben; wobei sowohl öffentlich-rechtliche als auch privatrechtliche Rechtspositionen erfasst sind. Gesundheitsdaten dürfen somit vom niedergelassenen Arzt etwa zur (gerichtlichen) Durchsetzung von Honoraransprüchen aufgrund eines Behandlungsverhältnisses gegen Sozialversicherungsträger oder bei Privatleistungen gegen den Patienten bzw. private Krankenversicherungen verwendet werden.

Aber auch die Verteidigung im Fall von Behandlungsfehlervorwürfen in einem allfälligen Strafverfahren oder in einem zivilrechtlichen Schadenersatzverfahren gegen den behandelnden Arzt fällt unter den Tatbestand der „Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“.

Erst bei einer willkürlichen, bewussten Offenlegung von sensiblen Daten (z.B. im Prozessvorbringen), die mit dem Streitgegenstand in keinerlei Verbindung stehen, wird der Rechtfertigungstatbestand des Art. 9 Abs. 2 lit f DSGVO nicht mehr gegeben sein³⁶ – in diesem Fall ist die Verarbeitung rechtswidrig und sanktionsbewährt.

Zu beachten ist auch, dass das Recht auf Löschung der Daten für den Betroffenen gemäß Art. 17 Abs. 3 lit e DSGVO ausgeschlossen ist, wenn die Verarbeitung (darunter fällt auch die Speicherung) der Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

35 Frenzel in Paal/Pauly, DS-GVO/BDSG Art. 9 Rz 37.

36 Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 9 DSGVO, Rz 45.

2.5. Zulässigkeit der Verarbeitung gemäß § 51 Ärztegesetz 1998 (ÄrzteG)

§ 51 ÄrzteG normiert im Wesentlichen in dessen Abs. 1 die ärztliche Dokumentationspflicht, in Abs. 2 die Übermittlung von Patientendaten an Sozialversicherungsträger, Krankenfürsorgeanstalten und andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Patient steht.

Datenschutzrechtlich sind insbesondere die Absätze 2 und 4 leg cit relevant und beachtenswert.

2.5.1. § 51 Abs. 2 Z 2 ÄrzteG

Wie schon oben ausgeführt, richtet sich die Zulässigkeit der Verarbeitung von Patientendaten im Gesundheitsbereich grundsätzlich nach Art. 9 Abs. 2 lit h DSGVO – für den niedergelassenen Arzt ist hier insbesondere der Behandlungsvertrag mit dem Patienten die Rechtfertigungsgrundlage. Begründet wird dieser Ausnahmetatbestand damit, dass im Gesundheitswesen typischerweise höchstpersönliche Daten verarbeitet werden, die auch zwischen verschiedenen Verantwortlichen ausgetauscht werden (müssen). Krankheitsfälle müssen auch in einer bestimmten, sich wiederholenden Routine und mit dem Ziel optimaler Behandlung schnell bearbeitet werden. In solchen Fällen jeweils auf eine Einwilligung des Patienten abzustellen erschwert die Abläufe und tritt in Konkurrenz zu dem für die medizinische Heilbehandlung zentralen Einverständnis in die Behandlung.³⁷

Mit der Bestimmung des § 51 Abs. 2 Z 2 ÄrzteG sieht der österreichische Gesetzgeber aber eine strengere Regelung vor für die Übermittlung von Patientendaten (durch den niedergelassenen Arzt) an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, als die DSGVO – Voraussetzung für die Zulässigkeit der Übermittlung nach Z 2 ist die Einwilligung des Patienten. Es stellen sich zwangsläufig die Fragen, ob eine derartige Abweichung vom unmittelbar anwendbaren Unionsrecht überhaupt zulässig ist und in welcher Form diese Einwilligung erteilt werden kann bzw. muss.

§ 51 Abs. 2 Z 2 ÄrzteG bezieht sich zunächst auf jene personenbezogenen Daten, die im Rahmen der gesetzlich verpflichteten ärztlichen Dokumentation gemäß Abs. 1 leg cit aufgezeichnet werden. Auch die Verarbeitung von Gesundheitsdaten im Rahmen dieser berufsrechtlichen Pflicht zur Führung einer ärztlichen Dokumentation stützt sich auf Art. 9 Abs. 2 lit h DSGVO³⁸. Nach der hier vertretenen

³⁷ Frenzel in Paal/Pauly, DS-GVO/BDSG Art. 9 Rz 41.

³⁸ Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art. 9 DSGVO, Rz 51.

Ansicht³⁹ stellt § 51 Abs. 2 Z 2 ÄrzteG nicht einen eigenen Erlaubnistatbestand zur Datenverarbeitung (hier: Übermittlung), sondern eine Einschränkung der Datenverarbeitung dar. Die Übermittlung von Patientendaten an einen anderen Arzt oder eine medizinische Einrichtung, in deren Behandlung der Patient steht, ist sohin nur unter der Einschränkung der Einwilligung des Patienten zulässig. Die Möglichkeit des nationalen Gesetzgebers, eine solche Einschränkung überhaupt zu normieren, ergibt sich wiederum aus der beschränkten Öffnungsklausel des Art. 9 Abs. 4 DSGVO.

Diese Einwilligung nach § 51 Abs. 2 Z 2 DSGVO ist deshalb auch nicht als ausdrückliche Einwilligung i.S.d. Art. 9 Abs. 2 lit a DSGVO zu verstehen oder mit dieser ident. Aus einer systematischen Interpretation der Bestimmungen des ÄrzteG und der Bestimmungen über die elektronische Gesundheitsakte (ELGA) lässt sich ableiten, dass die Einwilligung nicht nur ausdrücklich, sondern auch konkludent erfolgen kann.

2.5.2. Exkurs: § 51 Abs. 4 – Übermittlung der Patientenakte an einen ärztlichen Nachfolger?^{40,41}

Zum Sachverhalt:

Ein niedergelassener Arzt für Allgemeinmedizin gab seine Ordination aus Altersgründen auf und übergab die elektronischen Patientenakten an eine Kollegin, die ihn längere Zeit vertreten hatte und den Patienten gut bekannt war, da die eigentliche Kassenplanstellennachfolgerin die Patientenakten nicht übernehmen wollte. Durch die Übergabe sollte die reibungslose ärztliche Weiterversorgung der Patienten sichergestellt werden. Die Übernahme der alten Ordinationsräumlichkeiten scheiterte an den zu hohen Mietpreisvorstellungen des Vermieters, weshalb die übernehmende Allgemeinmedizinerin eine Ordination in unmittelbarer Nähe zur alten Ordination eröffnete. Die Patienten wurden von der Übermittlung der Patientenakten durch Anschlag an der Tür der alten Ordination bzw. persönlich durch den übergabenden Arzt informiert. Die übernehmende Ärztin, die auch eine Kassenstelle innehat, holt vor erstmaliger Behandlung eines Patienten des übergabenden Arztes stets die Einwilligung der Patienten zur Verwendung der „alten“ Patientenakte ein.

39 Andere Ansicht *Jahnel*, Auswirkungen der DSGVO im medizinischen Bereich, RdM 2019/123, 252.

40 Siehe dazu näher *Scheucher, Czadilek*, Zur Rechtmäßigkeit der Weitergabe von Patientinnendaten bei Ordinationsaufgabe, RdM 2019/117.

41 Die Scheucher Rechtsanwalt GmbH ist im nachfolgend geschilderten Verfahren als Vertreterin der involvierten Ärzte beteiligt.

Aufgrund eines amtswegig eingeleiteten Verfahrens erachtete die Datenschutzbehörde die elektronische Übermittlung der Patientenakten durch den übergebenden Arzt an die übernehmende Ärztin als rechtswidrig, da nach einer engen Wortinterpretation die übernehmende Ärztin nicht „Ordinationsstättennachfolgerin“ bzw. „Kassenplanstellennachfolgerin“ i.S.d. § 51 Abs. 4 ÄrzteG gewesen sei. Gegen den Bescheid der Datenschutzbehörde erhoben die Ärzte Beschwerde beim Bundesverwaltungsgericht (BVwG), welches den Bescheid der Datenschutzbehörde in seinem Erkenntnis in diesem wesentlichen Punkt bestätigte.

Zentral für die Beurteilung der Rechtmäßigkeit der Datenübermittlung ist die Auslegung des Begriffs des „Ordinationsstättennachfolgers“. Denn nur dieser darf – neben dem Kassenplanstellennachfolger – die ärztliche Dokumentation von seinem ärztlichen Vorgänger übernehmen und mit Einwilligung der Patienten zu Behandlungszwecken verwenden.

Sowohl die Datenschutzbehörde als auch das BVwG gehen vom engsten Wortlaut dieses Begriffes aus, und zwar i.S.d. „ortsidenten Ordinationsstättennachfolgers“. Das BVwG argumentiert, dass die Patienten ausschließlich im Fall der Übergabe der Patientenakten an den ortsidenten Ordinationsstättennachfolger nachvollziehen könnten, wo sich ihre Patientenakte im Falle einer Auflösung einer Ordination befänden. Für eine weite Auslegung des Begriffes, nach der auch andere ärztliche Nachfolger, die im selben Fach tätig sind und im selben Einzugsgebiet ordinieren, vom Begriff des Ordinationsstättennachfolgers umfasst sind, gäbe es deshalb keine Notwendigkeit. Für die Patienten müsse es leicht zu eruieren sein, welcher Arzt ihre Patientenakte bei Auflösung der Altordination übernommen hat – und dies sei nur im Falle einer Übermittlung an den ortsidenten Ordinationsstättennachfolger möglich, denn die Information der betroffenen Patienten erfolge dann durch den ortsidenten Ordinationsstättennachfolger selbst. Im Falle der Übermittlung an den Kassenplanstellennachfolger würde die Information der Patienten durch die zuständige Ärztekammer erfolgen.

Diese Ansicht des BVwG ist jedoch lebensfremd. Bei Kassenplanstellennachfolgern ist die Übergabe der Patientenakten logisch und medizinisch nachvollziehbar, da sie in den allermeisten Fällen im gleichen Fach tätig sein werden und oft im gleichen Einzugsgebiet ordinieren. Bei fachfremden ärztlichen Nachfolgern, die bloß die Ordinationsräumlichkeiten übernehmen, fällt dieses Argument jedoch weg. Ein spezialisierter Radiologe wird kein Interesse daran haben, die Patientenakten von einem Allgemeinmediziner zu übernehmen, umgekehrt werden die Patienten des Altarztes nicht damit rechnen, dass ihre Patientenakten nun beim Radiologen verwahrt werden. Nach der engen Auslegung durch das BVwG wäre aber ausschließlich der spezialisierte Radiologe der Ordinationsstättennachfolger des Allgemeinmediziners und die Patientenakten dürften an keinen anderen ärzt-

lichen Nachfolger (außer an einen Kassenplanstellennachfolger), der aber (im gleichen Fach) die (Weiter)Versorgung der Patienten sicherstellen könnte, übergeben werden.

Auch in all diesen Fällen bliebe den PatientInnen ein Anruf bei der Ärztekammer nicht erspart, um den Altarzt zu eruieren und diesen zu fragen, ob ihre Patientenakten gemäß § 51 Abs. 4 ÄrzteG von ihm selbst verwahrt werden oder ob sie an einen anderen ärztlichen Nachfolger übermittelt wurden.

Legt man den Begriff des Ordinationsstättennachfolgers dahingehend aus, dass auch der „faktische Ordinationsstättennachfolger“ der im gleichen Fach tätig ist, im gleichen Einzugsgebiet ordiniert und das „lebende Unternehmen Arztpraxis“ übernimmt, erfasst ist, ergeben sich für die Patienten keinerlei praktische oder datenschutzrechtliche Nachteile. Denn der ärztliche Nachfolger ist immer über die Ärztekammer respektive den Altarzt eruierbar. Die Verwendung der Patientenakte durch den ärztlichen Nachfolger darf außerdem nur mit Einwilligung des Patienten erfolgen. Zudem spiegelt diese Auslegung auch die geänderten Umstände im österreichischen Gesundheitssystem wider. Anders als noch vor zwanzig Jahren zeigt sich eine steigende Tendenz hin zur Gründung von Gruppenpraxen und Ärztezentren, in denen sich Ärzte zusammenschließen. Statt eine eigene Ordination zu betreiben, ist es – auch im Sinne des Patientenwohls – oft ökonomischer und effizienter, eine Gruppenpraxis oder ein Ärztezentrum zu betreiben. Ein Arzt, der seine Ordination auflöst, dürfte jedoch nach der Rechtsansicht des BVwG seine Patientenakten nicht an einen Kassen- oder Wahlarzt in einer nahegelegenen Gruppenpraxis oder in einem Ärztezentrum übergeben.

Die Problematik der Interpretation des Begriffs „Ordinationsstättennachfolger“ durch das BVwG zeigt sich auch an folgendem Beispiel. Wenn ein Wahlarzt oder ein Kassenarzt, der nicht Kassenplanstellennachfolger ist, die Ordination seines Vorgängers weiterführt, die Ordinationsräumlichkeiten jedoch einen Stock tiefer als die alte Ordination betreibt, weil das Untergeschoß barrierefrei ist und eine nicht barrierefreie Weiterführung der alten Ordination nicht dem Bundes-Behindertengleichstellungsgesetz entspricht, so wäre eine Übergabe der Patientendokumentation nach Ansicht des BVwG datenschutzrechtlich unzulässig.

Im Ergebnis ist – nach Ansicht der Verfasser dieses Beitrages – die gesetzliche Differenzierung zwischen Ordinationsstättennachfolgern, die tatsächlich ihre Ordination in den Räumlichkeiten des Vorgängers etablieren, und (faktischen) Ordinationsstättennachfolgern, die dies nicht tun, sachlich nicht gerechtfertigt und ein Verstoß gegen den Gleichheitsgrundsatz, da Unterschiede im Tatsächlichen nicht auszumachen sind.

Der Begriff „Ordinationsstättennachfolger“ wäre sohin verfassungskonform weit auszulegen, und zwar dahingehend, dass auch andere ärztliche Nachfolger als der ortsidente Ordinationsstättennachfolger unter den Voraussetzungen „gleiches Fach“ und „gleiches Einzugsgebiet“ umfasst sind. Die Übergabe der Patientenakten an diese faktischen Ordinationsstättennachfolger ist dann datenschutzrechtlich zulässig. Diese Auslegung entspricht auch dem obersten Regelungsziel des Gesetzgebers, das Patientenwohl durch die nahtlose ärztliche Weiterversorgung sicherzustellen.

Eine Entscheidung des Verwaltungsgerichtshofes über die Revision gegen das Erkenntnis des Bundesverwaltungsgerichts steht zum Zeitpunkt des Verfassens dieses Beitrages noch aus. Jedenfalls geboten scheint jedoch eine gesetzliche Neuregelung der Übermittlung von Patientenakten im ÄrzteG, welche die Entwicklungen der letzten Jahrzehnte im Gesundheitsbereich und hier vor allem in der lokalen ärztlichen (Weiter)Versorgung berücksichtigt.

2.6. Zulässigkeit der Verarbeitung gemäß Gesundheitstelematikgesetz 2012 (GTelG)

Neben dem Datenschutzrecht haben niedergelassene Ärzte stets auch die Vorgaben des GTelG zu beachten, welches aufgrund der Öffnungsklausel des Art. 9 Abs. 4 DSGVO auch strengere Vorgaben für die Verarbeitung von Gesundheitsdaten vorsieht. Dementsprechend dürfen Gesundheitsdiensteanbieter gemäß § 3 Abs. 4 GTelG Gesundheitsdaten und genetische Daten nur dann übermitteln, wenn

1. die Übermittlung gemäß Art. 9 DSGVO zulässig ist,
2. die Identität (§ 4 GTelG) jener Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, nachgewiesen ist,
3. die Identität (§ 4 GTelG) der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen ist,
4. die Rollen (§ 5 GTelG) der an der Übermittlung beteiligten Gesundheitsdiensteanbieter nachgewiesen sind,
5. die Vertraulichkeit (§ 6 GTelG) der übermittelten Gesundheitsdaten und genetischen Daten gewährleistet ist sowie
6. die Integrität (§ 7 GTelG) der übermittelten Gesundheitsdaten und genetischen Daten gewährleistet ist.

Während sich also die Frage der Rechtfertigung im engeren rechtlichen Sinn nach Art. 9 DSGVO richtet⁴², enthält das GTelG im Verhältnis zu den allgemeinen Anforderungen an die Sicherheit der Verarbeitung (Art. 32 DSGVO) eine Konkretisierung der Sicherheitsvorkehrungen. Das in der Praxis wichtigste Problem ist hierbei die Kommunikation zwischen Ärzten und Patienten sowie der Datenaustausch von Gesundheitsdiensteanbietern untereinander per E-Mail, also durch ungerichtete Kommunikation, insbesondere im Hinblick auf die Übermittlung von medizinischen Befunden.

Der geforderte Nachweis und die Prüfung der eindeutigen Identität von Personen, deren Gesundheitsdaten oder genetische Daten übermittelt werden sollen, kann technisch durch qualifizierte elektronische Signaturen gelöst werden, über die Patienten in der Praxis jedoch selten verfügen. Schon aus diesem Grund ist die ganz normale, unverschlüsselte E-Mail-Kommunikation rechtlich problematisch. Hier sind jedenfalls ergänzende Lösungen notwendig, die in der Regel eine ausschließlich per E-Mail vorgenommene Datenübermittlung ausschließen. Beispielsweise könnte der Arzt einem Patienten eine E-Mail mit Verlinkung auf eine sichere elektronische Ablage⁴³ übermitteln, wenn dem Patienten zuvor die Zugangsdaten persönlich nach Überprüfung seiner Identität übergeben wurden. Auch ein Rückgriff auf den Patientenindex gemäß § 18 GTelG kann zur Überprüfung der eindeutigen Identität auch außerhalb der ELGA herangezogen werden. Strenger sind die Voraussetzungen zur Identitätsprüfung des Gesundheitsdiensteanbieters. Der Nachweis und die Prüfung der eindeutigen Identität (§ 2 Z 2 E-GovG) von Gesundheitsdiensteanbietern haben durch Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen, sowie bereichsspezifische Personenkennzeichen (§ 9 E-GovG) oder durch elektronischen Abgleich mit dem eHealth-Verzeichnisdienst (§ 9 GTelG) oder durch elektronischen Abgleich mit dem Gesundheitsdiensteanbieterindex zu erfolgen. Keine Schwierigkeiten bestehen für niedergelassene Ärzte üblicherweise im Hinblick auf die zu definierende Rolle.

Die Gewährleistung der Vertraulichkeit und der Integrität der Datenübermittlung erfordert praktisch eine verschlüsselte Kommunikation.⁴⁴ Dabei ist schon aus dem Wortlaut des § 3 GTelG eindeutig, dass es keinen Unterschied macht, ob die Kommunikation mit einem anderen Gesundheitsdiensteanbieter oder direkt mit dem Patienten stattfindet. Eine Umgehung dieser Pflichten zur Verschlüsselung, die gleichzeitig auch als Vorgabe des Art. 32 DSGVO zu sehen ist, durch das Einholen

42 Vgl. auch Jahnelt, Auswirkungen der DSGVO im medizinischen Bereich, RdM 2019/123, 252.

43 Zu beachten ist die Sonderregelung für „Cloud Computing“ gemäß § 6 Abs. 3 GTelG 2012, worunter das Anbieten bzw. Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden, zu verstehen ist.

44 Vgl. dazu m.w.N. Pfandlsteiner/Gabauer/Trieb, RdM 2019, 176.

einer Einwilligung in eine unverschlüsselte Kommunikation, ist nach der Rechtsprechung⁴⁵ jedenfalls nicht zulässig. Hier stehen Ärztinnen und Ärzte als Verantwortliche voll in der Haftung, eine Berufung auf anderslautende Vorgaben von Interessenvertretungen ändert an dieser Verantwortung nichts, wie die zitierte Rechtsprechung bereits gezeigt hat.

3. Pflichten des Verantwortlichen

3.1. Führung eines Verarbeitungsverzeichnisses gemäß Art. 30 DSGVO

Als datenschutzrechtliche Verantwortliche haben niedergelassene Ärzte für die Verarbeitung von (Patienten)Daten ein Verzeichnis der Verarbeitungstätigkeiten zu führen⁴⁶, das einen Überblick über alle Verarbeitungstätigkeiten bietet. Da in Ordinationen regelmäßig sensible Daten verarbeitet werden, zu denen Patientendaten im Gesundheitsbereich zählen, sind die Verantwortlichen ausnahmslos zur Führung des Verzeichnisses verpflichtet.⁴⁷ Die Führung des Verzeichnisses ist Ausfluss der Dokumentations- und Rechenschaftspflicht der DSGVO, ermöglicht den Nachweis deren Einhaltung und stellt die Grundlage für die Aufsichtsbehörde dar, die Verarbeitungsvorgänge zu kontrollieren⁴⁸ und insbesondere deren Rechtmäßigkeit zu überprüfen. Es dient auch dem eigenen Datenschutz-Management in der Ordination sowie als Grundlage zur Erfüllung anderer Pflichten (z.B. der Durchführung einer Datenschutz-Folgenabschätzung, der Erfüllung von Betroffenenrechten etc.).

Das schriftlich oder elektronische Verarbeitungsverzeichnis hat sämtliche in Art. 30 Abs. 1 DSGVO angeführten Angaben zu enthalten, z.B. die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen und der Kate-

45 DSB 16. 11. 2018, DSB-D213.692/0001-DSB/2018 Dako 2019/29 (Haidinger) und OGH 23. 10. 2018, 4 Ob 179/18d jusIT 2019/20, 52 (Staudegger) = VbR 2019/8, 25 = ÖBA 2019/2563, 297 = JBl 2019, 378 = RZ 2019/EÜ 108, 172 = Dako 2019/61 (Haidinger/Weiss); Pfandlsteiner/Gabauer/Trieb, RdM 2019, 171.

46 Art. 30 DSGVO.

47 Vgl. Art. 30 Abs. 5 DSGVO.

48 Vgl. ErwGr 82 DSGVO.

gorien personenbezogener Daten, die Kategorien von Empfängern gegenüber denen (Patienten) Daten offengelegt werden und, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung.

Hinweis: Das Verarbeitungsverzeichnis gemäß Art. 30 DSGVO ist nicht ident mit der Dokumentation der Patientendaten gemäß § 51 Abs. 1 DSGVO und unabhängig von dieser Patientenakte zu führen. Entsprechende Muster von Verarbeitungsverzeichnissen, die die üblichen Datenverarbeitungen in Ordinationen abdecken, finden sich kostenlos auf den Webseiten der Landesärztekammern zum Download.

Verstöße gegen die Pflicht zur Führung eines Verarbeitungsverzeichnisses können mit Geldbußen von bis zu zehn Millionen Euro oder zwei Prozent des gesamten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden.⁴⁹

In der Praxis gibt es hierzu verschiedenste Muster und Vorlagen, derer sich Ärzte hier bedienen können. Wichtig ist dabei, sich niemals blind auf die Vollständigkeit solcher Muster zu verlassen, sondern stets sorgfältig an die Realität der jeweiligen Ordination anzupassen, da ansonsten allfällige Mängel auch zu einer Haftung führen können.

3.2. Informationspflicht gemäß Art. 13 und Art. 14 DSGVO

Art. 13 DSGVO normiert bestimmte Informationspflichten für den Verantwortlichen, wenn die Erhebung der personenbezogenen Daten direkt bei der betroffenen Person erfolgt. Hingegen regelt Art. 14 DSGVO die Informationspflichten für den Fall, dass personenbezogene Daten bei Dritten erhoben werden.

Im Gesundheitsbereich wurden durch das 2. Materien-Datenschutz-Anpassungsgesetz⁵⁰ in zahlreichen Gesetzen, wie z.B. dem ÄrzteG⁵¹, Ausnahmebestimmungen von den Informationspflichten beschlossen. Demnach wäre eine Informationserteilung (auch für niedergelassenen Ärzte) gesetzlich nicht zwingend erforderlich, sofern eine Datenverarbeitung nicht über das nach dem jeweiligen Berufsgesetz zulässige Maß hinausgeht. Allerdings ist eine Beschränkung der

49 Art. 83 Abs. 4 DSGVO.

50 BGBl. I 37/2018.

51 § 3b ÄrzteG.

Informationspflichten gemäß Art. 13 und Art. 14 DSGVO durch den nationalen Gesetzgeber nur zulässig, wenn diese notwendig und verhältnismäßig ist. Aus den Gesetzesmaterialien geht nicht hervor, warum der österreichische Gesetzgeber diese pauschale (und nicht auf bestimmte Datenverarbeitungen gerichtete) Beschränkung für notwendig und verhältnismäßig erachtet.

Diese überschießende Ausnahme lässt sohin ernsthafte Zweifel an der Unionsrechtskonformität von § 3b Abs. 2 ÄrzteG 1998 entstehen, da Ausnahmen gemäß Art. 23 Abs. 1 DSGVO den Wesensgehalt der Grundrechte und Grundfreiheiten achten, in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen müssen und nur zu bestimmten Zwecken vorgenommen werden dürfen.⁵² Als einzige der abschließend aufgezählten Ausnahmen für den medizinischen Bereich käme der *„Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“* in Betracht. Inwieweit der Ausschluss der Informationspflichten, der insbesondere zu mehr Transparenz bei der Verarbeitung von Patientendaten beitragen könnte, zum Schutz der öffentlichen Gesundheit beizutragen vermag, ist nicht nachvollziehbar und wohl auch für den Gesetzgeber nicht ersichtlich, da in den Gesetzesmaterialien darauf überhaupt nicht eingegangen wird.

Auch die österreichische Datenschutzbehörde monierte in der „Allergie-Tagesklinik“-Entscheidung⁵³, dass in den auf der Website der Allergie-Tagesklinik abrufbaren Informationen strukturell nicht zwischen Art. 13 und Art. 14 DSGVO unterschieden wurde und daher ein Verstoß gegen die Bestimmungen der DSGVO vorlag. Offensichtlich ließ die Datenschutzbehörde die entsprechende Bestimmung des Krankenanstalten- und Kuranstaltengesetz (KAKuG) über die Ausnahme von den Informationspflichten unangewendet⁵⁴, obwohl die als GmbH geführte Allergie-Tagesklinik in den Anwendungsbereich des KAKuG fällt.

52 Scheucher Rechtsanwalt GmbH/Research Institute AG & Co. KG, Rechtsgutachten zu § 3b ÄrzteG für die Ärztekammer für Wien.

53 DSB-D213.692/0001-DSB/2018 vom 16.11.2018.

54 Allerdings führt die DSB im entsprechenden Bescheid über die allfällige Unionsrechtswidrigkeit der Bestimmung des § 9a KAKuG nicht näher aus.

3.3. Auskunftsrecht

3.3.1. Auskunftsrecht gemäß Art. 15 DSGVO

Betroffene Personen haben gemäß Art. 15 DSGVO das Recht, Auskunft über die sie betreffenden personenbezogenen Daten zu verlangen. Über welche Informationen Auskunft zu erteilen ist, wird in Art. 15 Abs. 1 DSGVO näher geregelt, darunter fallen z.B. die Verarbeitungszwecke, die Kategorien der verarbeiteten personenbezogenen Daten, Empfänger der Daten etc.

Die Betroffenen haben ein Recht, eine kostenlose⁵⁵ Kopie der Daten, die Gegenstand der Verarbeitung sind, zu erhalten.

Die Frist zur Auskunftserteilung beträgt gemäß Art. 12 Abs. 3 DSGVO ein Monat, die bei komplexeren Auskunftsbegehren – unter Anführung der Verzögerungsgründe – um weitere zwei Monate verlängert werden kann. Eine Ausweiskopie oder sonstige zusätzliche Informationen anzufordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, ist zwar häufig zulässig, setzt aber voraus, dass der Verantwortliche begründet, warum er ansonsten Zweifel an der Identität der natürlichen Person hat (Art. 12 Abs. 6 DSGVO).

3.3.2. Auskunftsrecht gemäß § 51 Abs. 1 ÄrzteG

§ 51 Abs. 1 letzter Satz ÄrzteG sieht vor, dass der Arzt verpflichtet ist, dem Patienten Einsicht in die Patientendokumentation zu gewähren oder gegen Kostensatz die Herstellung von Abschriften zu ermöglichen. Da der hier geregelte Kostensatz der unmittelbar anwendbaren DSGVO widerspricht, ist den Patienten, die ihr Recht auf Auskunft gemäß Art. 15 DSGVO geltend machen, unentgeltlich Auskunft über sämtliche sie betreffenden Daten zu erteilen, inklusive der Daten aus der Patientendokumentation gemäß § 51 Abs. 1 ÄrzteG.

3.4. Recht auf Löschung gemäß Art. 17 DSGVO

Das Recht auf Löschung gemäß Art. 17 Abs. 1 DSGVO bzw. die Verpflichtung zur Löschung bei Vorliegen bestimmter Lösungsgründe sind Ausdruck des Grundsatzes auf Datenminimierung⁵⁶. Als Lösungsgründe kommen insbesondere in Betracht:

⁵⁵ Um Missbrauch zu verhindern, kann für jede weitere Kopie ein angemessenes Entgelt verlangt werden.

⁵⁶ Paal in Paal/Pauly, DS-GVO/BDSG Art. 17 Rz 7.

- die betroffene Person widerruft ihre Einwilligung in die Datenverarbeitung,
- die betroffene Person legt Widerspruch gegen die Datenverarbeitung ein,
- die Datenverarbeitung erfolgt unrechtmäßig,
- die Datenverarbeitung ist für die Zwecke, zu denen die Daten erhoben wurden, nicht mehr notwendig.

Besteht ein berechtigter Lösungsgrund, hat der Verantwortliche die Löschung unverzüglich vorzunehmen und den Betroffenen innerhalb einer Frist von einem Monat (verlängerbar auf zwei Monate) von den getroffenen Maßnahmen zu informieren. Bei der Löschung elektronischer Daten kommt es darauf an, dass auf die Daten nicht mehr zugegriffen werden kann.

Kein Recht auf Löschung besteht, wenn einer der Ausnahmetatbestände des Art. 17 Abs. 3 DSGVO vorliegt, z.B. die Löschung der Erfüllung einer rechtlichen Verpflichtung entgegensteht. So sieht etwa § 51 Abs. 3 ÄrzteG vor, dass die Patientendokumentation und die dieser dienlichen Unterlagen für zehn Jahre aufzubewahren sind – einem Antrag auf Löschung ist innerhalb dieser Frist sohin nicht nachzukommen.

3.5. Benennung eines Datenschutzbeauftragten gemäß Art. 37 DSGVO

Der Datenschutzbeauftragte dient insbesondere der internen Kontrolle der Einhaltung der sich aus der DSGVO ergebenden Pflichten. Gemäß Art. 37 Abs. 1 lit c DSGVO müssen Verantwortliche jedenfalls einen Datenschutzbeauftragten benennen, wenn (i) die Kerntätigkeit in der (ii) umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DSGVO (sensible Daten) besteht.

Auch wenn die Kerntätigkeit eines niedergelassenen Arztes in der medizinischen Behandlung der Patienten liegt, kann der Arzt heutzutage seine Heiltätigkeit kaum ohne die Verarbeitung von Gesundheitsdaten erbringen. Aus diesem Grund ist davon auszugehen, dass diese Datenverarbeitung auch eine Kerntätigkeit des Arztes bildet.

Nicht abschließend geklärt ist die Frage, wann eine „umfangreiche“ Verarbeitung von Gesundheitsdaten vorliegt. Von einer umfangreichen Verarbeitung muss wohl

ausgegangen werden, wenn die Datenverarbeitung das übliche Maß bei Weitem übersteigt.⁵⁷

Bei einer üblichen Einzelordination⁵⁸ ist davon auszugehen, dass eine umfangreiche Verarbeitung von Gesundheitsdaten nicht erfolgt und deshalb ein Datenschutzbeauftragter nicht verpflichtend zu benennen ist. Bei Gruppenpraxen ist im konkreten Einzelfall zu prüfen, ob eine Benennung eines (internen oder externen) Datenschutzbeauftragten zwingend erforderlich ist.

3.6. Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO

Bei risikoreichen Datenverarbeitungen verpflichtet Art. 35 DSGVO den Verantwortlichen, vor Aufnahme eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Allerdings ist eine DSFA keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess.⁵⁹ Nach den Leitlinien der Art. 29-Datenschutzgruppe (heute der Europäische Datenschutz-Ausschuss) ist sie ein Verfahren, anhand dessen die Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung mit sich bringt, durch eine Risikoabschätzung und die Ermittlung von Gegenmaßnahmen besser kontrolliert werden sollen.⁶⁰

„Risiko“ wird als ein Szenario mit einem Ereignis und dessen Konsequenzen verstanden, das bezüglich seiner Schwere und seiner Eintrittswahrscheinlichkeit beurteilt wird.⁶¹

Art. 35 Abs. 3 DSGVO regelt ganz allgemein, unter welchen Voraussetzungen eine DSFA verpflichtend durchzuführen ist. Der Mindestinhalt einer DSFA wird in Art. 35 Abs. 7 DSGVO normiert. Insbesondere aus Art. 35 Abs. 3 lit b DSGVO geht hervor, dass in Fällen der umfangreichen Verarbeitung sensibler Daten (z.B. Gesundheitsdaten) die Durchführung einer DSFA erforderlich ist. Allerdings ist der Begriff „umfangreich“ in der DSGVO nicht klar definiert.

57 Paal in Paal/Pauly, DS-GVO/BDSG Art. 37 Rz 9.

58 Vgl. auch ErwGr 91 DSGVO.

59 Trieb in Knyrim, DatKomm Art. 35 DSGVO, Rz 1.

60 Art. 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248, Rev 01.

61 Trieb in Knyrim, DatKomm Art. 35 DSGVO, Rz 1.

Da dem Europäischen Gesetzgeber wohl bewusst war, dass für den Verantwortlichen oft nur schwer erkennbar ist, ob eine DSFA tatsächlich durchzuführen ist, sehen Art. 35 Abs. 4 und 5 DSGVO vor, dass die nationalen Aufsichtsbehörden Listen erstellen, die festhalten, für welche Datenverarbeitungen keine DSFA oder eine DSFA zwingend durchzuführen ist. Die Österreichische Datenschutzbehörde ist dieser Verpflichtung durch Erlassung von zwei Verordnungen, der sogenannten „Whitelist“⁶² und der „Blacklist“⁶³ nachgekommen. Die „Blacklist“ enthält jedoch keine Auflistung von konkreten Datenverarbeitungen, die eine DSFA erfordern, sondern zwei Kriterienkataloge, nach denen der Verantwortliche selbst zu prüfen und zu bewerten hat, ob eine DSFA durchzuführen ist.

Für den niedergelassenen Bereich ist insbesondere die „DSFA-A12: Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdiensteanbieter und Apotheken“ der „Whitelist“ relevant. Für die Datenverarbeitung „Patientenverwaltung und Honorarabrechnung von einzelnen Ärzten und Zahnärzten“ ist somit explizit festgehalten, dass eine DSFA nicht durchzuführen ist. Allerdings bleibt zu beachten, dass in Einzelfällen auch ein einzelner niedergelassener Arzt deutlich mehr personenbezogene Daten verarbeiten kann als z.B. spezialisierte Gruppenpraxen von Ärzten. In solchen Fällen ist aufgrund der umfangreichen Verarbeitung von Gesundheitsdaten auch der einzelne Arzt weiterhin verpflichtet, die Notwendigkeit einer DSFA zu beurteilen. Die Anzahl an Verantwortlichen allein ist sohin kein taugliches Kriterium für die Auslegung des Begriffs „umfangreich“ und die „Whitelist“ vermag die diesbezügliche Rechtsunsicherheit nicht gänzlich zu beseitigen. Zumindest nach der Rechtsprechung der Datenschutzbehörde (Allergie-Tagesklinik-Entscheidung⁶⁴) ist nun klar, dass bei einer Organisation von 17 Ärzten, jedenfalls zu prüfen ist, ob für die einzelnen Datenverarbeitungen eine DSFA durchzuführen ist.

62 DSFA-Ausnahmereverordnung, BGBl. II 108/2018.

63 DSFA-Verordnung, BGBl. II 278/2018.

64 DSB-D213.692/0001-DSB/2018 vom 16.11.2018.

3.7. Meldung von Datenschutzverletzungen gemäß Art. 33 und Benachrichtigung der Betroffenen gemäß Art. 34 DSGVO

Art. 33 DSGVO erlegt dem Verantwortlichen (und in abgeschwächter Form dem Auftragsverarbeiter) im Fall von Datenschutzverletzungen eine Meldepflicht an die Datenschutzbehörde auf, um die aus der Verletzung resultierenden Gefahren für die Rechte und Freiheiten der Betroffenen zu minimieren.⁶⁵ Die Meldung, die innerhalb von 72 Stunden erfolgen muss, setzt die Datenschutzbehörde von der Datenschutzverletzung in Kenntnis und ermöglicht dieser die Inanspruchnahme ihrer Befugnisse gemäß Art. 58 DSGVO.

Unter „Verletzung des Schutzes personenbezogener Daten versteht Art. 4 Z 12 DSGVO eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden“. In Betracht kommen etwa die versehentliche Löschung oder Veränderung von Datensätzen, der irrtümliche Versand von Daten an einen unbefugten Empfänger per E-Mail oder der Verlust eines Datenträgers (z.B. USB-Stick), auf dem (Gesundheits)Daten gespeichert sind.

Eine Ausnahme von der Meldepflicht besteht dann, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führt. Dies ist z.B. dann der Fall, wenn ein falscher E-Mail-Empfänger die übermittelte Nachricht löscht oder wenn die Datensätze auf einem verlorenen USB-Stick ausreichend verschlüsselt sind.

Wenn die Datenschutzverletzung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss gemäß Art. 34 DSGVO auch die Person, deren Daten betroffen sind, von der Verletzung benachrichtigt werden. Eine Benachrichtigung ist nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Maßnahmen getroffen oder sonst sichergestellt hat, dass das hohe Risiko nicht mehr besteht.

Hinweis. Ein Formular für die Meldung einer Datenschutzverletzung gemäß Art. 33 DSGVO stellt die Österreichische Datenschutzbehörde auf ihrer Webseite www.dsb.gv.at zum Download zur Verfügung. Es ist dringend zu empfehlen, die-

⁶⁵ Martini in Paal/Pauly, DS-GVO/BDSG Art. 33 Rz 1.

ses Formular für „Data-Breach“-Meldungen zu nutzen, um alle für die Behörde wesentlichen Informationen zu erfassen.

4. Fazit

Im medizinischen Bereich und insbesondere bei der Verarbeitung von Gesundheitsdaten kommt es zu einem Zusammenwirken der unmittelbar anzuwendenden DSGVO und verschiedenen nationalen Sonderregelungen, die besonders zu beachten sind. Auch Verstöße gegen die nationalen datenschutzrechtlichen Sonderregelungen können zu hohen Geldbußen für Verantwortliche führen.

Hinsichtlich der Erfüllung datenschutzrechtlicher Pflichten besteht teilweise noch immer Rechtsunsicherheit, etwa wann für bestimmte Datenverarbeitungen im medizinischen Bereich eine Datenschutz-Folgenabschätzung durchzuführen ist oder wann verpflichtend ein Datenschutzbeauftragter zu benennen ist. In Österreich wurde bislang jedenfalls versucht, den Bereich der niedergelassenen Ärzte hier durchaus mit Ausnahmeregelungen zu entlasten, wie z.B. mit den Ausnahmeregelungen in der „Whitelist“ zur Datenschutz-Folgenabschätzung.

Allerdings lässt die DSGVO keinen großen Spielraum für Sonderregelungen auf nationaler Ebene zu, mit denen niedergelassene Ärzte im Hinblick auf datenschutzrechtliche Verpflichtungen entlastet würden. Vereinfachungen in der Praxis könnten daher in der Zukunft vor allem durch die Entwicklung von branchenspezifischen Verhaltensregeln, Codes of Conduct im Sinne des Art. 40 DSGVO erfolgen. Dazu bedarf es aber einer Initiative der Branche selbst, die bislang noch nicht sichtbar geworden ist.

Literaturverzeichnis

- Art. 29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt, WP 248, Rev 01, 2017
- Artikel-29-Datenschutzgruppe*, Advice paper on special categories of data, 2011
- Bergauer*, Die Rollenverteilung nach der DSGVO, jusIT 2018, 60
- Bergauer*, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018/83
- Ehmann/Selmayr (Hrsg.)*, DS-GVO², 2018
- Gierschmann/Schlender/Stentzel/Veil (Hrsg.)*, Kommentar DS-GVO, 2020
- Jahnel*, Auswirkungen der DSGVO im medizinischen Bereich, RdM 2019/123
- Knyrim (Hrsg.)*, DatKomm - Praxiskommentar zum Datenschutzrecht, 2019
- Kurzpapier 13 der Deutschen Datenschutzkonferenz, 2013
- Paal/Pauly*, (Hrsg.) Kurzkomentar DS-GVO/BDSG2, 2018
- Pfandlsteiner, Gabauer, Trieb*, Rechtskonforme elektronische Übermittlung von Gesundheitsdaten und genetischen Daten, RdM 2019/103
- Scheucher, Czadilek*, Zur Rechtmäßigkeit der Weitergabe von Patientinnendaten bei Ordinationsaufgabe, RdM 2019/117
- Simitis/Hornung/Spiecker (Hrsg.)*, Datenschutzrecht, 2019

Gerhard Stimac

Geschäftsführer von CGM, INNOMED und HCS

Datenschutz in der Arztpraxis

1. Sicherung der elektronischen Daten	40
2. Datenzugriff verhindern	41
3. Personal und Besucher	42
4. Sicherheitsmaßnahmen im Überblick	43

Personenbezogene Daten unterliegen in Gesundheitseinrichtungen der EU-weiten Datenschutzgrundverordnung und müssen mit allen Mitteln geschützt werden. Mit den passenden Maßnahmen und kompetenten IT-Partnern ist der Datenschutz in Arztpraxen aber keine Wissenschaft. Dieser Beitrag hält einige wertvolle Tipps bereit, die auch aus langjähriger Erfahrung resultieren.

IT-Sicherheitskonzepte unterstützen Ärzte, Apotheker, Labore, Krankenhäuser und jede andere Gesundheitseinrichtung dabei, Daten vor unberechtigter Einsichtnahme von außen zu schützen. Sicherheitslücken gibt es in allen möglichen Bereichen, an die im ersten Moment oft nicht gedacht wird. Die Datenschutzgrundverordnung (DSGVO) stärkt die Rechte von Betroffenen, deren personenbezogenen Daten verarbeitet werden – ein Prozess, der in jeder Arztpraxis tagtäglich erfolgt. Sowohl bei der Verarbeitung dieser Daten als auch bei deren Speicherung, die laut Ärztegesetz für zehn Jahre verpflichtend ist, gilt es, professionelle Maßnahmen zu setzen, um – auch nachträglichen – Missbrauch zu verhindern.

1. Sicherung der elektronischen Daten

Dass die EDV vor unerlaubtem Zugriff gesichert werden muss, liegt auf der Hand. Mit einem Passwort allein ist es aber nicht getan. Für jeden Anwender sollte ein Benutzer angelegt sein. Zudem sollten starke Passwörter vergeben werden, die regelmäßig zu wechseln sind. Beim Verlassen der Praxis sollte sich der Arbeitsplatz automatisch sperren oder der Arbeitsplatz wird manuell gesperrt, wenn er verlassen wird. Tägliche Sicherungen der IT-Daten gehören zum Sicherheitspaket dazu. Wichtig ist dabei allerdings, dass die Sicherungen ebenfalls sicher verstaut werden, am besten in einem brandsicheren Safe. Zusätzlich sollten Sicherungen an anderen Standorten, also nicht an derselben Adresse deponiert werden. Datensicherungen müssen täglich erfolgen, aber mindestens fünf Generationen Ihrer Sicherungen sollten in Form von Tages-, Wochen-, Monats-, Quartals- und Jahressicherung angelegt werden. Festplatten gehören verschlüsselt. Den Server lagert man besten in einem versperrten Fach oder gut belüfteten Kasten. Schließlich gehört eine Alarmanlage für die Ordinationsräumlichkeiten zur modernen Ausstattung.

2. Datenzugriff verhindern

Die einzelnen Arbeitsplatzrechner benötigen zwingend einen Virenschutz. Trotzdem sollten als zusätzliche Schutzmaßnahme keine E-Mails unbekannter Personen geöffnet werden. Eine dubiose Absenderadresse verrät oft bereits den unlauteren Zweck der Mail. Besonders kritisch ist das Öffnen von Anhängen, denn hier versteckt sich mitunter ein Virus, der durch das Öffnen in das EDV-System gelangt. Dass eine telefonische Weitergabe von Passwörtern, PIN-Codes, TAN-Codes und Ähnlichem niemals erfolgen darf, muss selbstverständlich sein.

Ärzte sollten niemals reale Patientendokumente wie Formulare, Rezepte oder Befunde an ihren Arztsoftwarehersteller senden, um zum Beispiel den Arztstempel neu positionieren zu lassen. Derartige Dokumente müssen geschwärzt werden.

Grundsätzlich ist eine „Clean Desk“-Politik ratsam, das bedeutet, dass keine Rezepte, Formulare, Befunde und Ähnliches unbeaufsichtigt auf einem Schreibtisch liegen bleiben. Selbst das gesprochene Wort unterliegt dem Datenschutz, daher sollte in der Anmeldung eine ruhige Atmosphäre herrschen. Details zu Diagnosen, Befunden und Medikamenten sollen grundsätzlich nicht laut im Wartezimmer kommuniziert werden.

3. Personal und Besucher

Mit Dienstleistern, die die Ordinationsräumlichkeiten betreten, sollte der Ordinationsinhaber entsprechende Verträge zur Geheimhaltung und zum Verhalten in diesen Räumlichkeiten abschließen. Sinnvoll sind zudem Besucherlisten, in denen Zutritt und Austritt von Technikern, Pharmareferenten, Lieferanten etc. dokumentiert werden.

Heikel ist auch der Umgang mit Personal, das sich um die EDV kümmert. Fernwartungen dürfen nur von Firmen bzw. Personen durchgeführt werden, mit denen es eine Auftragsverarbeitungsvereinbarung und einen konkreten Auftrag gibt. Bei Fernwartungen sollte immer ein Mitarbeiter der Ordination vor Ort sein und zusehen, was auf dem Rechner passiert. Mit einer unglaublichen Dreistigkeit von Personen, die Daten stehlen möchten, ist zu rechnen. Ausschließlich Fachfirmen dürfen die Hardware entsorgen, denn die Datenträger müssen fachgerecht geschreddert werden.

Die DSGVO erfordert in vielen Bereichen eine besonders durchdachte und verantwortungsvolle Handhabung von Patientendaten. Datenauskunftsbegehren von Patienten sollten immer ernst genommen und innerhalb der vorgesehenen Frist laut DSGVO beantwortet werden. Ärzte sollten immer alle notwendigen Formalitäten hinsichtlich der DSGVO einhalten. Je dezidierter und sichtbarer Datenschutz in der Ordination geschieht, desto vertrauensbildender wirken sich die Maßnahmen im Übrigen auf das Arzt-Patienten-Verhältnis aus.

4. Sicherheitsmaßnahmen im Überblick

- Verträge mit allen Dienstleistern, die die Praxis betreten
- Dokumentation von Zutritt und Austritt von Dienstleistern
- EDV vor unerlaubtem Zugriff sichern: Benutzer pro Anwender, starke Passwörter, Arbeitsplatz sperren
- Sicherungen in brandsicherem Safe und an anderen Standorten
- Tägliche Datensicherung
- Mindestens 5 Generationen von Sicherungen (täglich, wöchentlich, monatlich, quartalsweise, jährlich)
- Virenschutz für jeden Arbeitsplatzrechner
- Keine E-Mails und vor allem keine Anhänge unbekannter Versender öffnen
- Niemals Passwörter, PIN-Codes, TAN-Codes etc. per Telefon weitergeben
- Festplatten verschlüsseln
- Server in einem versperreten Fach/gut belüfteten Kasten lagern
- Alarmanlage für die Ordination
- Fernwartungen nur mit konkretem Auftrag
- Bei Fernwartungen dabeibleiben
- Fachgerechte Entsorgung der Hardware
- Texte schwärzen, die an Dienstleister geschickt werden
- „Clean Desk“-Politik
- Keine Patientendetails laut im Wartezimmer kommunizieren
- Datenauskunftsbegehren von Patienten fristgerecht beantworten
- Notwendige Formalitäten laut DSGVO einhalten

Univ.-Lekt. Nicolas Nagel, CIPP/E, CIPM, CIPT, FIP, CDPO
Global Head of Data Protection CARGO-PARTNER GROUP

Datenschutzkonformer Alltag in der Arztpraxis

Wie setzen Ärzte die DSGVO und IT-Sicherheit praktikabel und rechtssicher um?

Einleitung	47
1. Grundlegendes Verständnis für Datenschutz	49
2. Alltag in der Arztpraxis und Bedrohungsszenarien	58
3. Risikofelder in Ihrer Praxis und Gegenmaßnahmen	63
4. Die wichtigsten Sicherheitsmaßnahmen im Überblick	70
5. Tipps, Tricks und Lösungsvarianten zu alltäglichen Datenschutzthemen	77
6. Betroffenenrechte praktikabel aber gesetzeskonform umsetzen	87
7. Abschließende Anmerkung	94

Einleitung

Etwas mehr als zwei Jahre sind nun seit dem Inkrafttreten der DSGVO ins Land gezogen. Die europäische Datenschutzgrundverordnung gehört dabei zweifelsohne zu der bedeutendsten Gesetzesentwicklung der Europäischen Union in den letzten Jahren. Mit Stichtag 25. Mai 2018 hat sie das österreichische Datenschutzgesetz abgelöst und muss seitdem auch in Österreich unmittelbar angewendet werden. Aber was bedeutet dies für den Gesundheitssektor insbesondere für Ärzte, Krankenanstalten, Labore oder Rehazentren nun konkret?

Wie immer bei gesetzlichen Neuerungen ist anfangs vieles unklar und es gibt viele offene Fragen. Einige davon wurden in den letzten zwei Jahren beantwortet, manche sind jedoch noch immer ein Graubereich und bieten Raum für Spekulation.

Oftmals ist Fachliteratur so allgemein gehalten, dass man sich als Anwender fragt: „Und was bedeutet dies nun für meine Branche? Was muss ich konkret tun? Was darf ich nicht mehr und was schon?“

Diese grundlegenden Fragen werden hier beantwortet. Natürlich kann ein Fachartikel nicht eine umfassende und vor allem abschließende Handlungsanweisung darstellen, dennoch bietet er zumindest das Drehbuch für die Umsetzung in der Praxis und versucht alltägliche Dinge mit den rechtlichen Anforderungen zu verknüpfen und schlussendlich zu lösen.

Gerade der Gesundheitsbereich gehört aufgrund der Art der Informationen, die über Patienten tagtäglich anfallen und verarbeitet werden, zu einem der gefährdetsten und heikelsten Bereiche im Datenschutz. Man findet sich daher schnell in der Riege der heiklen Branchen, wie Finanzdienstleister, Versicherungen oder Werbetreibenden, wieder.

Daher ist es unabdingbar, die sensiblen Informationen von Patienten, aber auch von Mitarbeitern ausreichend zu schützen und die gesetzlichen Vorgaben einzuhalten.

Abschließend sei angemerkt, dass es sich bei den folgenden Kapiteln stets um Empfehlungen und eine persönliche Sichtweise, aber um keine abschließenden Anweisungen handelt. Dieser Artikel soll ein praktisches Hilfsmittel sein, damit die gesetzlichen Vorgaben unkompliziert angewendet werden können.

Da der Bereich Datenschutz & Datensicherheit ein schnelllebiger und sich rasch verändernder Bereich ist und der stetigen Weiterentwicklung unterliegt, ist es zudem ratsam, sich weiterhin kontinuierlich mit dem Thema und etwaigen Spezialanforderungen im Gesundheitsbereich zu beschäftigen und – wo notwendig – professionelle Unterstützung zu Rate zu ziehen.

1. Grundlegendes Verständnis für Datenschutz

1.1. „Datenschutz“, „Datensicherheit“, „Compliance“, „IT-Sicherheit“ – Was verbirgt sich dahinter?

All diese Begriffe werden im Alltag in unterschiedlichster Art und Weise verwendet, oftmals jedoch schnell verwechselt und unter Umständen sogar vermischt. Nachfolgend sollen in kurzer und prägnanter Form die Unterschiede erklärt werden, um den Grundstein für die nachstehenden Kapitel zu schaffen.

1.1.1. Datenschutz

Datenschutz schützt nicht per se Daten, sondern als Grundrecht eben den Menschen und Informationen über diesen.

Dies ist sichergestellt durch eine Reihe von Gesetzen. Darunter die DSGVO, das „neue“ österreichische Datenschutzgesetz, das Telekommunikationsgesetz, die Europäische Menschenrechtskonvention, die Grundrechtecharta der EU und viele weitere nationale Sondergesetze, die sich oftmals an bestimmten Branchen orientieren, wie etwa das Gesundheitstelematikgesetz.

Wenn daher von Datenschutz gesprochen wird, meint man entweder das uns allen zustehende Grundrecht oder aber die rechtlichen Normen, auf denen dieses Grundrecht basiert. Datenschutz ist aber keinesfalls mit Datensicherheit gleichzusetzen.

1.1.2. Datensicherheit/IT-Sicherheit

Die Datensicherheit (auch oftmals als IT-Sicherheit bezeichnet) ist ein Teilaspekt des Datenschutzes. Teilaspekt deswegen, da in bestimmten Teilen der DSGVO (z.B. Datenschutzgrundsätze) ganz allgemein auf eine ausreichende Datensicherheit als Grundvoraussetzung für einen angemessenen Datenschutz abgestellt wird.

Aufgabe der IT-Sicherheit ist die systematische Absicherung eines informationsverarbeitenden IT-Verbundes. Gefahren für die Informationssicherheit oder Bedrohungen des Datenschutzes eines Unternehmens oder einer Organisation sollen dabei verhindert oder abgewehrt werden.

Die Auswahl und Umsetzung von IT-Sicherheitsstandards zählt zu den Aufgaben des jeweiligen IT-Sicherheitsmanagements und erstreckt sich etwa auf Bereiche wie die physische Sicherheit, Schutz vor unbefugten Fremdzugriffen, Datensicherung, Verschlüsselung und das Ausrollen relevanter Updates und Patches.

Die IT-Sicherheit ist auch ein Teilaspekt der Informationssicherheit. Wenn man mit einem Informationssicherheitsexperten spricht, erachtet dieser wiederum den Datenschutz und die IT-Sicherheit als Teilaspekt der Informationssicherheit und ordnet dieser alles unter. Man merkt, die gesamte Abgrenzung ist durchaus komplex und selbst unter Experten nicht eindeutig lösbar.

1.1.3. Informationssicherheit

Kompliziert ausgedrückt bezeichnet man als „Informationssicherheit“ Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Einfacher erklärt schützt die Informationssicherheit schlicht Informationen jedweder Art. Egal, ob es sich dabei um ein Papierdokument handelt, um ein Smartphone oder den Unternehmensserver. Dabei wird auch nicht unterschieden, ob es sich um personenbezogene Daten handelt oder um ausschließliche Betriebs- und Geschäftsgeheimnisse oder Daten von juristischen Personen.

Informationssicherheit dient daher ganz allgemein dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken. In der Praxis orientiert sich die Informationssicherheit unter anderem an der internationalen ISO/IEC 27000-Normenreihe und im deutschsprachigen Raum am BSI IT-Grundschutz.

1.1.4. Compliance

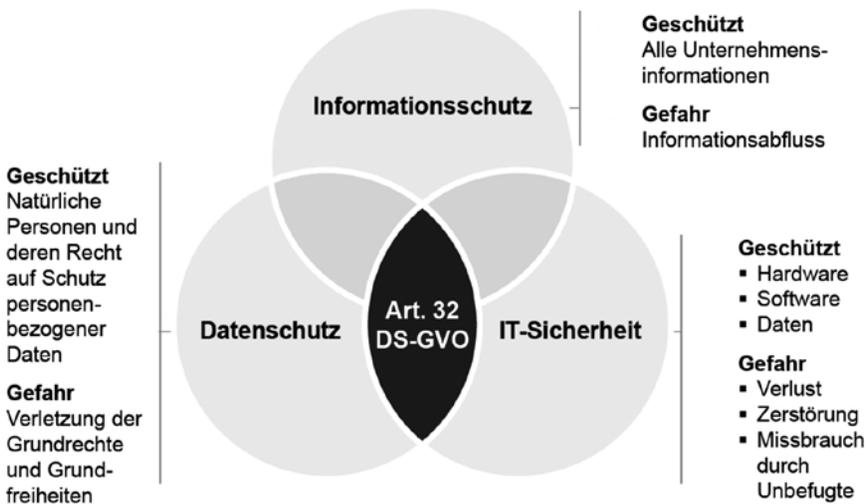
Compliance ist die betriebswirtschaftliche und rechtswissenschaftliche Umschreibung für die Regeltreue (auch Regelkonformität) von Unternehmen, also die Einhaltung von Gesetzen, Richtlinien und freiwilligen Kodizes.

Die Gesamtheit der Grundsätze und Maßnahmen eines Unternehmens zur Einhaltung bestimmter Regeln und damit zur Vermeidung von Regelverstößen wird als „Compliance-Management-System“ bezeichnet. Die Verantwortung zur Einhal-

tung der „Compliance“ liegt bei der jeweiligen Unternehmensführung. Natürlich muss sich auch jeder Mitarbeiter an aufgestellte oder gesetzliche Regelungen halten. Dass die Mitarbeiter auch wissen, was einzuhalten ist, ist Aufgabe des Betriebsinhabers.

1.1.5. Überblick

Die nachstehende Grafik soll die drei wichtigsten Themenbereiche und deren Anwendungsbereich besser veranschaulichen. Man erkennt, dass Informationen/Daten nur dann ausreichend geschützt werden (dargestellt durch den ominösen Artikel 32 der DSGVO, der für „geeignete technische und organisatorische Maßnahmen“ steht), wenn stets alle drei Themenbereiche beachtet, umgesetzt und eingehalten werden.



1.2. Deshalb sollten sich Ärzte mit Datenschutz und IT-Sicherheit beschäftigen

Die IT und somit auch die IT-Sicherheit sind in den vergangenen Jahrzehnten für die Gesundheitsbranche immer wichtiger geworden. Insbesondere das (Breitband-)Internet, Entwicklungen wie ELGA und immer mehr vernetzte Medizingeräte tragen dazu erheblich bei.

Dies bietet der Medizin viele Vorteile. Neben diesen Vorteilen bergen die „neuen Technologien“ aber auch Gefahren und Risiken. Durch die Vernetzung, leichtere Vervielfältigungsmöglichkeiten, schnelle Datenweitergabe und Sicherheitslücken ergeben sich unterschiedliche IT- und Datenschutzrisiken, die man als Arzt auf keinen Fall vernachlässigen sollte. Daher ist ein Grundwissen über Datenschutz und IT-Sicherheit für alle im Gesundheitswesen Tätige genauso wichtig, wie über betriebswirtschaftliche Themen Bescheid zu wissen.

Im Zusammenspiel zwischen Medizin, Datenschutz und IT-Sicherheit müssen neben den datenschutzspezifischen Vorgaben der DSGVO und des österreichischen Datenschutzgesetzes noch die ärztliche Verschwiegenheit, resultierend aus dem Ärztegesetz, aber auch aus dem Arztgelöbnis eingehalten werden.

Für Ärzte gelten im Sinne der Vertraulichkeit von Informationen die höchsten anwendbaren Verschwiegenheitspflichten. Diese drei- oder vierfache Absicherung seitens des Gesetzgebers resultiert wiederum aus den im Alltag genutzten hochsensiblen Daten ihrer Patienten und dem Bedarf an größtmöglicher Sorgfalt beim Umgang mit diesen Daten.

Im Alltag ist die datenschutz- und IT-sicherheitspezifische Beurteilung eines Sachverhalts insbesondere relevant in folgenden Fällen:

- bei der Neuanschaffung von Computer Hardware oder Software,
- bei der Übernahme einer bestehenden Praxis,
- bei einem Neubau einer Praxis,
- bei der Anschaffung von Medizingeräten,
- beim Zusammenschluss von Praxen,
- bei der Beauftragung von neuen Dienstleistern,
- bei der Einstellung neuer Mitarbeiter,
- beim Abschluss von Verträgen,
- beim typischen Alltagsablauf einer Praxis.

Ähnlich einer Diagnose samt Behandlungsplan sollte auch in diesen Fällen eine Analyse erfolgen, mit einer damit einhergehenden Maßnahmenplanung. Wie auch in der medizinischen Diagnostik ist dabei „Dr. Google“ nur selten ein kompetenter Ansprechpartner in Sachen Datenschutz und IT-Sicherheit und birgt zumeist mehr Gefahren, Halbwahrheiten und teils falsche „Lösungen“ als dass er weiterhilft.

Für komplexe Themenbereiche bietet es sich an, einen Berater seines Vertrauens zu wählen. Wobei Berater oder selbsternannte Experten, die stets „alles“ anbieten, oftmals mit Vorsicht zu genießen sind.

1.3. Warum Datenschutz und IT-Sicherheit Chefsache ist

Wie zuvor erläutert, sind Ordinationsinhaber als „datenschutzrechtliche Verantwortliche“ dafür verantwortlich, dass alle Datenschutz- und IT-Sicherheitsvorgaben eingehalten werden. Sollte etwa aus Unachtsamkeit, Fahrlässigkeit, Versehen, warum auch immer etwas passieren, so trifft dies den Ordinationsinhaber auch persönlich. Er sollte daher die Absicherung seiner Praxis nachvollziehen und verstehen können. Gerne als Ergänzung oder Vier-Augen-Prinzip gemeinsam mit einem geschickten Mitarbeiter.

Die Erfahrung zeigt auch, dass man, sobald man auch nur eine Grundahnung oder gewisse Fachausdrücke im entsprechen Themengebiet kennt, auch entsprechend ernst genommen wird. Weiters laufen informierte Ordinationsinhaber auch nicht Gefahr, jede (zum Teil unnötige) Dienstleistung oder jedes Produkt angeboten oder aufgeschwatzt zu bekommen.

1.4. Datenverarbeitung im Jahr 2020 – was ist heutzutage möglich?

Daten, sprich Informationen über Menschen oder Organisationen sind das neue Äquivalent zu Gold oder Öl. Führt man sich ein paar Statistiken näher vor Augen, so erkennt man schnell warum dies so ist:

- Der weltweite Datenbestand verdoppelt sich alle zwei Jahre!
- Alle jemals in der Menschheitsgeschichte gesammelten Daten vom Jahre 0 bis 2016 entsprechen jener Datenmenge der Jahre 2016 bis 2018.
- 50 Milliarden Geräte waren 2019 mit dem Internet verbunden.

- Eine durchschnittliche Person interagiert heutzutage ca. 5000-mal pro Tag mit dem Internet.
- Pro Internetminute werden 42 Mio. Nachrichten und 188 Mio. E-Mails verschickt, 400.000 Apps downgeloadet oder 4 Mio. Google-Suchen durchgeführt.

Dies führt im Speziellen zu Ausformungen wie detaillierten Profilen die über einzelne Personen erstellt werden (Grafik auf der nächsten Seite).

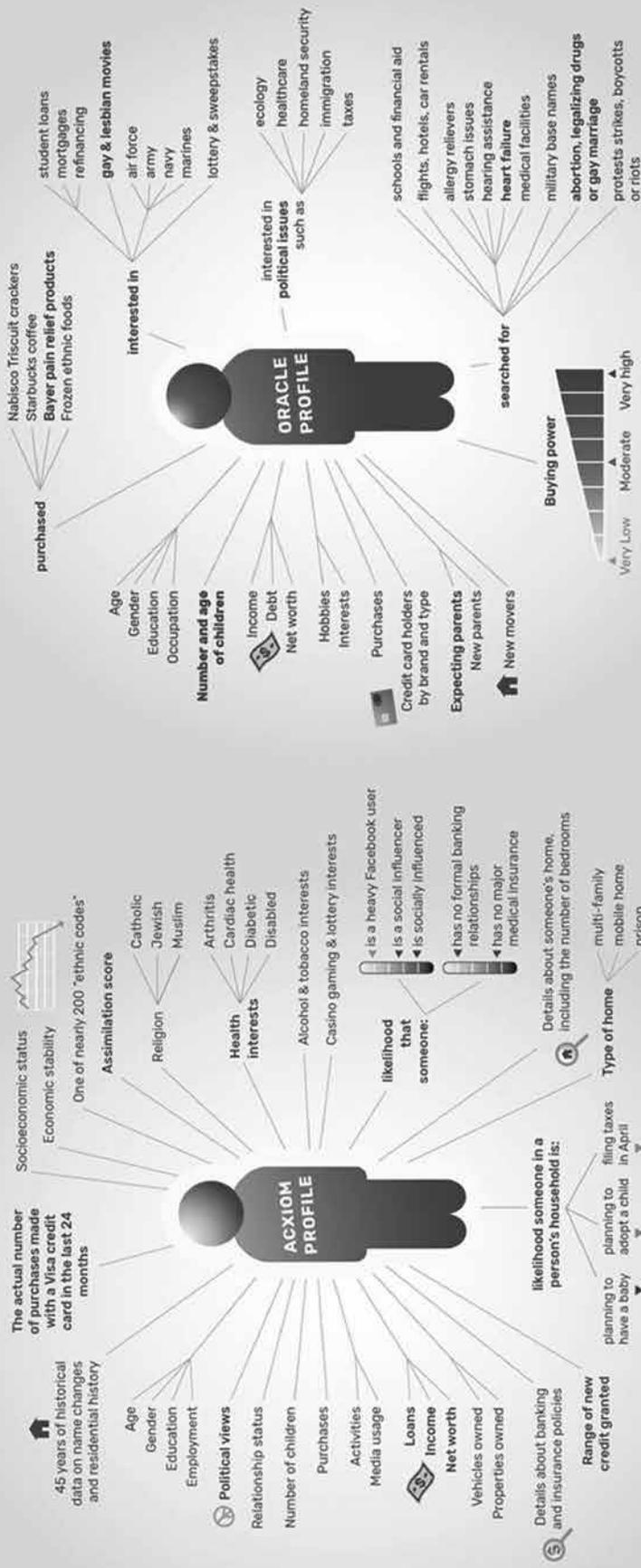
Diese Profile beinhalten Informationen wie etwa zum Finanzstatus, zu gesundheitlichen Problemen, politischen Überzeugungen oder zu Fällen wie den „Cambridge-Analytica-Fall“.

Worum ging es dabei? Cambridge Analytica ist ein Unternehmen, das sich auf Datenanalysen und Micro-Targeting oder anders ausgedrückt individuelle Einflussnahme auf einzelne Personen oder kleine Gruppen spezialisiert hat. Dieses Unternehmen rühmte sich unter anderem mit der „Beeinflussung der Wähler“ der US-Präsidentenwahl rund um Donald Trump als auch der BREXIT-Abstimmung. So konnten „Wähler auf der falschen Seite“ etwa beeinflusst werden, zuhause zu bleiben, „richtige Wähler“ dazu motiviert werden, wählen zu gehen, und „unentschlossene Wähler“ auf die „richtige Seite“ zu ziehen. Zusätzlich können die einzelnen Wähler bzw. Gruppen über Fake-Profile, Social Bots und Dark Posts mit vorausgewählten Informationen beliefert werden.

Aber womit schaffte dies Cambridge Analytica? Mit Daten. Im konkreten Fall mit den Daten von Facebook-Profilen. Der hauseigene Algorithmus versuchte einzelne Personen entsprechend zu „analysieren“. Und dies mit Erfolg. Denn mit nur 68 „Likes““, die User üblicherweise leicht bei Facebook verteilen, lässt sich bestimmen, welche Hautfarbe, sexuelle Orientierung der User hat oder wie es um dessen Gesundheit steht oder wie sein finanzieller Status aussieht.

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle



Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.

Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles

Hier eine Grafik, die verdeutlicht, wie gut ein Algorithmus einen User kennt:



Und wenn man nicht auf Facebook ist, kann man über den Zugang zu anderen Daten ebenfalls Profile erstellen, wie etwa über

- WhatsApp-Nachrichten,
- Bestellungen auf Amazon und anderen Online-Shops,
- Suchanfragen bei Google,
- SMS-Nachrichten,
- E-Mails,
- Daten aus Smartphone-Apps,
- Fotos,
- GPS-Daten,
- Daten privater Clouds,
- Daten aus diversen Online-Accounts
- etc. ...

1.5. Datenschutz – etwas gänzlich Neues seit 2018?

Bei der auftauchenden Frage, ob „Datenschutz“ etwas völlig Neues sei, muss man dies doch deutlich verneinen. In Österreich gab es bereits seit dem Jahr 1978 ein Datenschutzgesetz, welches den Schutz personenbezogener Daten zum Ziel hatte. Nach der „EU-Richtlinie 1995 zum Datenschutz“ kam es dann zu einer Modernisierung des Datenschutzes und im Jahr 2000 trat das „Datenschutzgesetz 2000“ in Kraft. Dieses galt in Österreich 18 Jahre und wurde zum 25. Mai 2018 sodann von der DSGVO entsprechend abgelöst.

Auch das österreichische Ärztegesetz gibt es bereits seit dem Jahr 1949 mit Aktualisierungen 1984 und 1998, die allesamt entsprechend strenge Verschwiegenheitsverpflichtungen beinhalten.

Der hippokratische Eid, seit 1948 vielmehr das Ärztegelöbnis, welches in Genf vom Weltärzteverband beschlossen und seither mehrmals überarbeitet wurde (Deklaration von Genf), hat zudem noch viel länger Bedeutung für Ärzte weltweit.

Datenschutzgesetze und gesundheitspezifische Normen stellen somit keine Neuerungen in der österreichischen Rechtsordnung dar, sondern sind bereits seit jeher fester Bestandteil selbiger.

2. Alltag in der Arztpraxis und Bedrohungsszenarien

2.1. Problematischer Alltag

Aufgrund von Stress im Alltag gehen Theorie und Praxis manchmal getrennte Wege. Viele Termine, ungeduldige Patienten, Notfälle oder Zeitverzögerungen können dazu führen, dass der Vorsatz, auf die strikte Einhaltung von organisatorischen Abläufen und Vorgaben zu achten, „vergessen“ wird oder er faktisch schwer befolgt werden kann.

Im schlimmsten Fall hat man dadurch bereits eine Datenschutzverletzung versehentlich oder wissentlich begangenen oder unter Umständen einen IT-Sicherheitsvorfall zu verantworten. Die Palette der Folgen reicht dabei von kleineren Auswirkungen, wie Unannehmlichkeiten für Patienten, über womöglich unwiderruflich verschlüsselte Computer in der Praxis bis hin zu gehackten Patientendatenbanken, den Stillstand der Ordination oder Verwaltungsstrafverfahren und Schadenersatzklagen.

Nicht selten sieht der Alltag in einer Praxis so aus: Es ist frühmorgens und die ersten Patienten warten bereits. Am Empfang wird der erste Patient über sein Wehklagen befragt, oft in Hörweite der anderen Patienten. Parallel ruft eine Dame an, deren Testergebnisse und Befunde im Lärmpegel der Praxis lautstark besprochen werden. Für die Patienten im Wartebereich ist hörbar, dass Frau Müller wieder Probleme mit ihren Werten hat. Gerade in ländlichen Gegenden ist der Arztbesuch ja für manche quasi der analoge Kaffeehausbesuch.

Die Ordinationsmitarbeiterin bewegt sich vom Empfang weg, dadurch bleiben einsehbare Bildschirme oder Dokumente auch mal unbeaufsichtigt. Was soll auch schon groß passieren?

Inzwischen hat ein Herr Steiner angerufen – zumindest behauptet er das –, um sich über seinen Befund zu erkundigen. Freundlich wird ihm Auskunft erteilt und der Befund an die von ihm mitgeteilte E-Mail-Adresse übermittelt.

Im Behandlungsraum hingegen lässt sich im Trubel leicht ein Blick auf die Unterlagen anderer Patienten erhaschen.

Im Wartezimmer hat sich ein technikinteressierter Jugendlicher ins Praxis-WLAN eingeloggt. Die neuen WLAN-Router sind gut platziert, das heißt möglichst zentral in der Praxis, und decken diese komplett ab.

Die Google-Cloud ist zudem wirklich günstig für Kleinunternehmen. Daher sind Sie als Arzt letztes Jahr auch dorthin gewechselt und speichern Ihre Daten dort ab. Für wichtige Daten betreiben Sie aber weiterhin auch ein Backup-Prozedere, auf einer NAS (=Network Attached Storage), die sich „gut gesichert“ im Abstellkammerl befindet. Ihr Neffe hat Ihnen diese netterweise sogar eingerichtet, wodurch Sie auch keinen teuren IT-Dienstleister mehr benötigen.

Die Schilderung dieses fiktiven und überspitzt formulierten „Tagesablaufs“ beinhaltet jede Menge potenzieller Datenschutz- und Datensicherheitsverletzungen. Er soll aber aufzeigen, dass im Alltag eine Menge Stolperfallen lauern, die man leicht vermeiden kann.

2.2. Bedrohungen für die Gesundheitsbranche und den Arzt

Anzumerken sei hier, dass grundlegend zu unterscheiden ist zwischen

- einem Dritten, der konkret oder abstrakt etwas Böses zu tun beabsichtigt, und
- dem Arzt und seinen Mitarbeitern, die aus Unachtsamkeit oder Fahrlässigkeit Datenschutz- oder Datensicherheitsverletzungen verursachen.

Beide Varianten stellen valide Bedrohungsfelder dar.

Die letzten Jahre zeigen, dass die Gesundheitsbranche häufig Opfer von Cyberangriffen war. Anfang 2016 waren etwa dutzende Krankenhäuser in den USA und Deutschland Opfer von Cyber-Attacken, in deren Folge die IT-Infrastruktur ganz oder teilweise abgeschaltet werden musste und der Krankenhausbetrieb tagelang extrem eingeschränkt war.

Im Frühjahr 2017 waren wiederum 81 Krankenhäuser oder Gesundheitsanbieter des britischen Gesundheitswesens von dem Ransomware-Angriff „WannaCry4“ betroffen. Von den 81 Institutionen waren 37 Krankenhäuser, darunter 27 Akutkrankenhäuser, direkt infiziert. 44 Krankenhäuser waren indirekt betroffen, da diese als Vorsichtsmaßnahme einige ihrer IT-Systeme hinunterfahren mussten. Auch in Österreich und Deutschland waren Praxen betroffen.

Einige weitere Beispiele zur Verwundbarkeit von Medizingeräten aus einer IT-Sicherheitsstudie:

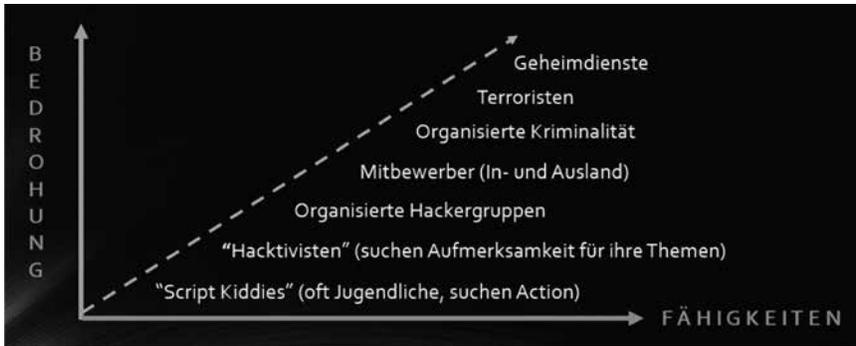
- Infusionspumpen für Medikamente zur Abgabe von Morphiumtropfen, Chemotherapeutika und Antibiotika, die aus der Ferne manipuliert werden können, um die Dosierung für die Patienten zu ändern.
- Bluetoothfähige Defibrillatoren, die so manipuliert werden können, dass zufällige Schocks auf das Herz eines Patienten übertragen werden oder dass ein medizinisch notwendiger Schock verhindert wird.
- Speicherung von Röntgenbildern, auf die Außenstehende im Netzwerk eines Krankenhauses zugreifen können.
- Temperatureinstellungen an Kühlschränken, die Blut und Medikamente enthalten, die zurückgesetzt werden konnten, wodurch Qualität und Haltbarkeit beeinflusst werden können.
- Digitale Krankenakten, die so verändert werden können, dass Ärzte Fehldiagnosen treffen, falsche Medikamente verschreiben oder ungerechtfertigte Behandlungen durchführen.
- Viele unterschiedliche Geräte hatten dieselben Sicherheitslücken: fehlende Authentifizierung, sodass auf das Gerät zugegriffen werden kann, um es zu manipulieren; schwache Passwörter oder voreingestellte Herstellerpasswörter wie „Admin“, „0000“ oder „1234“; eingebettete Webserver und Verwaltungsschnittstellen, mit denen Geräte einfach identifiziert und bearbeitet werden können

Diese intramuralen Beispiele zeigen, wie weit Cyberangriffe reichen. Vieles davon wäre aber sehr einfach zu verhindern.

Auch niedergelassene Ärzte können leicht Opfer für Angreifer werden. Wobei, wer sind eigentlich „Angreifer“? Angreifer reichen von sogenannten „Script Kiddies“, also zumeist Jugendliche, die ihre erlernten Fähigkeiten (z.B. via Tutorials in YouTube) einfach ausprobieren wollen, bis hin zu organisierten Hackergruppen, die damit Geld verdienen wollen.

Ordinationen gelten in Hackerkreisen als sogenannte „low hanging fruits“, begehrtere Opfer, die zur gutverdienenden Gesellschaftsschicht gehören. Gleichzeitig rechnet diese Gruppe nicht damit, Opfer von Cyberattacken zu werden, und ist oftmals nicht gut abgesichert. Die Einfallstore sind also breit. Einerseits kann klassisches „Hacking“ zur Anwendung kommen, aber auch simples „Überlisten“ des Ordinationsinhabers bzw. seines Personals. Dies nennt sich „Social Engineering“ (= soziale Manipulation) und bedeutet „zwischenmenschliche Be-

einflussung mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen“, sie zum Beispiel zur Preisgabe von vertraulichen Informationen oder zum Anklicken eines Links zu bewegen.



Wir alle kennen typische „Phishing“-E-Mails unserer vermeintlichen Bank. In der Regel erkennen wir dies und löschen die E-Mail. Derartige „Attacken“ sind jedoch nicht immer so trivial gestaltet und in perfekter Variante oftmals nicht zu unterscheiden oder nur schwierig als „Social Engineering“ wahrzunehmen.

Beim sogenannten „Spear-Phishing“ wird gezielt nach bestimmten Personen „gefischt“ und eine Nachricht entsprechend vertrauenswürdig ausgestaltet. Dies könnte dann ein befreundeter Kollege sein, der Ihnen eine E-Mail schreibt. Der Absender ist exakt die E-Mail-Adresse, die Sie kennen. Seine Ansprache und sein Schreibstil ist exakt jener, den Sie von ihm gewohnt sind. In seiner E-Mail nimmt er Bezug zu einem Thema, über das Sie sich schon öfters unterhalten haben. Er schickt Ihnen den Link/ein PDF zu einer interessanten Studie. Der Link (oder das PDF) sieht seriös aus.

Klicken Sie nun auf diesen Link/dieses PDF? Ehrlich gesagt ... Warum nicht?

Leider verbarg sich nun dahinter

- ein Verschlüsselungstrojaner, der Ihre Festplatte schrottet oder
- eine Spionagesoftware, die sich soeben heimlich installiert hat
- oder ...

Technisch wäre dies sicherlich verhinderbar gewesen – z.B. mittels elektronischer Signatur Ihres Kollegen, die Sie bei einem Fehlen stutzig hätte werden lassen. Solche Signaturen sind aber noch nicht weit verbreitet und privat nutzt kaum jemand so etwas.

Man erkennt also, dass immer etwas passieren kann. Im Fall der Fälle ein entsprechendes Backup zu haben und womöglich gute Antivirensoftware installiert zu haben, sollte daher in keinem Betrieb fehlen!

Wichtigste Regel: Das Erkennen von Schwächen und Stärken einer Ordination (IT-Systeme, Infrastruktur und Räumlichkeiten).

Offensichtliche Schwachstellen müssen sofort behoben werden. Dies sind zum Beispiel ein Laptop oder PC ohne Virenschutz oder ein nicht aktualisiertes System oder aktive Netzwerkkomponenten mit Standardpasswörtern (z.B. 1234).

3. Risikofelder in einer Praxis und Gegenmaßnahmen

3.1. Räumlichkeiten

Die im vorherigen Kapitel beschriebene Schwachstellenanalyse kann auf die unterschiedlichsten Bereiche einer Praxis ausdehnt werden. Wir beginnen mit den Räumlichkeiten:

3.1.1- Empfang

Der Empfang bietet faktisch betrachtet viel Raum für Gefahrenpotenzial, wenn grundlegende Datenschutzregeln unberücksichtigt bleiben.

Konkrete Sicherheitsmaßnahmen wären hier:

- Bildschirmarbeitsplätze so zu platzieren, dass Eingänge im Blickfeld der Mitarbeiter sind.
- Sichtschutzfolien sollten dort verwendet werden, wo ein Blick auf Monitore potenziell möglich ist.
- Setzen von Bildschirmschonern bzw. Bildschirmsperren bei fehlender Aktivität am Rechner inkl. Passwortschutz.
- Keine Dienste für Patienten anbieten, wie das Ausdrucken von Dokumenten, wenn dazu ein fremdes USB-Gerät (z.B. USB-Stick) angeschlossen werden muss.
- Klare Trennung des Personalbereichs und des Patientenbereichs.
- Keine Gespräche über Patienteninformationen in Hörreichweite von anderen Personen.
- Direkte Einsichtnahme in Unterlagen und Dokumente verhindern.

3.1.2. Wartebereich

Der Wartebereich birgt einige Gefahren:

- Klare Trennung von Wartebereich und Empfang.
- Keine schnelle Besprechung mit Patienten im Wartebereich, wo andere Personen mithören können.

- Keine zugänglichen Netzwerkdosen oder sonstigen IT-Geräte.
- Getrenntes WLAN für „Gäste“ verwenden.

3.1.3. Behandlungsraum

Der Behandlungsraum bedarf besonderen Schutzes und der Aufmerksamkeit:

- Keine Patientendaten (z.B. Akten, Befunde etc.) offen liegen lassen.
- Nicht einsehbarer Bildschirm für Patienten (es sei denn, dies ist notwendig im Zuge der Behandlung).
- Bildschirmsperre bei Verlassen des Raumes inkl. Passwortschutz.
- Kein gleichzeitiges Hereinholen anderer Patienten, wenn noch Punkte zu besprechen sind.

3.1.4. IT-Räume

In jenen Teilen der Ordination, in denen sich die IT-Infrastruktur befindet, gilt es, besondere Sorgfalt walten zu lassen:

- Umfassende physische Absicherung etablieren (z.B. versperrte Tür, Fenster-sicherung).
- Klimatisierter Raum im Idealfall, um Überhitzung von Hardware zu vermeiden.
- Idealerweise Notstromversorgung, Brandmelder und/oder Löschanlage.
- Alarmanlage.
- Restriktion, wer Zugang erhält, und Protokollierung des Zugangs.

3.1.5. Lager-/Archivräume

Lagerräume und Archive führen oftmals ein Schattendasein, bergen aber zumindest ähnliche Risiken wie die operativen Systeme und Räume.

- Vertrauliche Daten gesperrt verwahren bzw. archivieren.
- Fachgerechte Entsorgung von „Altpapier“ (z.B. Shreddern).
- Alte Datenträger (z.B. Festplatten, USB-Sticks, CDs, DVDs) verschlüsselt lagern und ebenso fachgerecht vernichten.
- Absicherung gegen Brand, Wasserschäden, Frost, Diebstahl, ...

3.2. IT-Geräte

IT-Geräte bergen resultierend aus ihrer Natur und Anfälligkeit diverse Risiken im Alltag. Diesen adäquat zu begegnen, hat besondere Bedeutung.

3.2.1. PC/Laptop

Der klassische PC oder der Laptop sind typische Einfallstore für Angreifer. Diese Geräte sind üblicherweise mit dem Internet und Intranet verbunden, haben Netzwerkzugriff und werden intensiv genutzt. Eine umfassende Absicherung ist eine entscheidende Barriere zwischen Angreifer und den Ordinationsdaten. Im Idealfall werden sensible Daten, etwa jene von Patienten, nur verschlüsselt auf dem PC/Laptop gespeichert. Wird beispielsweise Windows 10 von Microsoft als Betriebssystem verwendet, so kostet das Aktivieren der Verschlüsselung keinen einzigen Euro.

Zusätzlich sollte(n)

- ein guter Virenschutz auf allen PCs installiert sein,
- immer die Sicherheitsupdates des Herstellers installiert sein,
- eine Firewall genutzt und
- eine Zugriffssicherung (= Nutzernamen + sicheres Passwort) verwendet werden.

Eine Gefahr sind auch die zahlreichen Schnittstellen, die ein handelsüblicher PC/Laptop heutzutage mit sich bringt: WLAN, Bluetooth, LAN, USB-Ports, SD-Kartenslots, NFC uvm. Hier gilt: Alles was Sie nicht benötigen, deaktivieren Sie bitte! „Bluetooth Hacks“ sind etwa mit einer kleinen YouTube Anleitung schnell vollbracht und können auch nur schlecht verhindert werden.

3.2.2. Smartphone/Tablet

Smartphones und Tablets sind aus unserem Alltag nicht mehr wegzudenken. Diese mobilen Endgeräte sind jedoch wie ein PC/Laptop zu behandeln und bieten zudem noch weitere Gefahrenquellen. „Spionage-Apps“ könnten zum Beispiel alle Daten auf dem jeweiligen Gerät auslesen. Ein Smartphone kann zudem äußerst leicht als Wanze oder Videoüberwachung missbraucht werden. Sowohl das eingebaute Mikrofon als auch die eingebaute Kamera bieten beste Voraussetzungen für Angreifer. Im Internet können auf bestimmten Webseiten Millionen von Webcams direkt angesteuert und eingeschaltet werden – ohne dass es der Nutzer selbst mitbekommt.

Schutzmaßnahmen für PC/Laptops gelten analog auch für Smartphones/Tablets: Virenschutz, Updates installieren, keine veralteten Geräte nutzen, Zugriffssicherung (Pin, Fingerabdruck etc.) nutzen, keine unseriösen Apps installieren, wenn möglich privates und dienstliches Telefon strikt trennen, nur notwendige Schnittstellen anschalten, dafür aber den gesunden Menschenverstand stets einschalten.

Aber auch die physischen/manuellen Gefahren sind nicht zu unterschätzen. So können sensible Daten abfotografiert werden (z.B. Patientenakt) und unbefugten Personen zugänglich gemacht werden.

Ein Fall aus der jüngsten Vergangenheit: Eine medizinische Fachangestellte arbeitete in einer großen radiologischen Praxis. Eine Patientin vereinbarte einen Untersuchungstermin. Die Mitarbeiterin rief das elektronische Terminblatt (Name und Geburtsdatum der Patientin, zu untersuchender Körperbereich) der Patientin auf. Anschließend fotografierte die Mitarbeiterin das Terminblatt mit ihrem Smartphone und leitete es per WhatsApp an ihre Tochter weiter, mit dem Kommentar: „Mal sehen, was unsere Nachbarin schon wieder hat.“ Ein klarer Fall einer Datenschutzverletzung und der Verletzung der ärztlichen Schweigepflicht. Der Mitarbeiterin wurde gekündigt.

3.2.3. USB-Geräte

Unterschiedliche USB-Geräte bergen teilweise immense Gefahrenquellen im Alltag. Zumeist unterschätzt man diese, da wir selbst nicht auf die Idee kämen, einen „USB-Stick“ als Angriffswaffe zu nutzen.

Dabei kann das „Angriffsszenario“ sehr unterschiedlich ausfallen.

- **„Fremde USB-Sticks“:** Ein Patient bittet darum, ihm ein Dokument oder Ähnliches auszudrucken. Der Stick enthält aber (ohne Wissen des Inhabers) nicht nur die auszudruckende Datei, sondern auch noch eine Malware – von der Sie höchstwahrscheinlich nicht einmal etwas mitbekommen.
- **„Fundobjekt“:** Ein „zufällig“ in der Arztpraxis gefundener Stick wird am Empfang abgegeben. Steckt nun ein Mitarbeiter diesen Stick in den PC, hat der Hacker (und damit die Schadsoftware) ein leichtes Spiel.
- **„Verführer USB-Stick“:** Ein Stick wird folgendermaßen beschriftet: Mitarbeiterlöhne 2020. Eine Masche, die gefühlt in 99 % aller Unternehmen funktioniert. Mit hoher Wahrscheinlichkeit wird der Finder des USB-Sticks ihn in einen PC oder Laptop einstecken – und schlussendlich so unter Umständen das Ordinationsnetzwerk infizieren.

Das USB-Gerät beinhaltet meistens eine eigene Treiber-Software, die sich automatisch installiert, sobald es an den PC angeschlossen wird. Das automatische Installieren bedeutet für den Benutzer eine Bequemlichkeit im Umgang mit dem USB-Gerät. Die Gefahr ist groß, dass sich so die Malware auf dem PC mitinstalliert.

Wie kann man sich nun wehren? Nun, das ist in diesem Fall gar nicht so einfach. Die drei wichtigsten Dinge in diesem Zusammenhang sind sicherlich:

Awareness – Awareness – Awareness!

Man sollte klare Regeln für die Ordination aufstellen und alle Mitarbeiter hinsichtlich dieser Gefahren sensibilisieren. Awareness ist hier nur der „moderne Begriff“ für Bewusstseinsbildung oder Sensibilisierung – gesunde Skepsis hilft hier ergänzend.

Anbei noch eine Liste von Hacker-Werkzeugen, die man sich im Internet für wenige Euros (9–129 €) besorgen kann:

- **USB-Killer:** Ein USB-Killer sieht wie ein ganz normaler USB-Stick aus. Steckt man ihn allerdings in einen USB-Port, lädt er sich elektrisch auf und stößt nach kurzer Zeit 220 Volt aus. Dies führt meistens zur unmittelbaren Zerstörung des Rechners, ohne dass es dafür sichtbare Spuren gibt. Eine Absicherung vor so hohen Spannungen für die USB-Schnittstelle ist nicht vorgesehen. Ziel eines solchen USB-Killers ist schlicht die Beschädigung oder Zerstörung von Geräten mit USB-Anschlüssen.
- **Tastatur-Logger:** Ein Tastatur-Logger (USB-Keylogger) ist ein kleines Gerät, das einfach zwischen Tastatur und Rechner gesteckt wird. Es zeichnet nun sämtliche Tastatureingaben auf, wie etwa medizinische Berichte, Benutzeridentifikation und Passwörter. Der Logger kann so konfiguriert werden, dass er periodisch und völlig automatisch seinen Inhalt versendet.
- **„USB-Stick als Tastatur“:** Ein präparierter USB-Stick kann auch so konfiguriert werden, dass er sich als USB-Tastatur anmeldet und dann automatisch Befehle ausführt. Dies kann dem Stehlen von Passwörtern dienen oder dem Herunterladen von Malware aus dem Internet. In der Folge dieses Angriffs richtet der Angreifer meistens eine sogenannte „Hintertür“ (Backdoor) zum Netzwerk ein und kann dann jederzeit aus der Ferne auf ein System zugreifen.
- **USB-Netzwerkkarte:** Eine als USB-Stick getarnte Netzwerkkarte, eine sogenannte USB-Netzwerkkarte, kann die Kontrolle über den gesamten Netzwerkverkehr eines Rechners übernehmen. Dabei baut das Gerät einen sogenann-

ten „Tunnel“ auf und stellt eine ausgehende Verbindung zu einem System im Internet her. Der Hacker verbindet sich ebenfalls mit diesem System und kann darüber anschließend auf das Tool vom Internet her zugreifen. Hier wird deutlich, dass ausgehende Verbindungen auch überwacht werden sollten. Zu oft wird die Firewall nur dazu verwendet, Angriffe von außen abzublocken.

3.3. IT-Zugänge

Eine Ordination verfügt über unterschiedliche Zugänge zu verschiedensten IT-Systemen.

3.3.1. Kabelgebundene Zugänge

Obwohl die Technik immer mehr in Richtung drahtlose Übertragung voranschreitet, gibt es noch zahlreiche kabelgebundene Zugänge und Anschlüsse in einer Praxis. Dazu gehören etwa LAN, Modem, Telefon, Fax, Voice over IP, Stromanschlüsse usw.

All diese Zugänge bedürfen einer entsprechenden Absicherung – physisch wie digital. Dabei sind es Dinge, an die man zumeist nicht gleich denkt, die zu Problemen führen können. Eine Netzwerkdose im Wartebereich etwa. Diese hat dort schlicht nichts zu suchen oder soll zumindest physisch unbrauchbar gemacht werden. Die eigene Infrastruktur sollte immer bestmöglich geschützt sein. Ordinationsinhabern ist anzuraten, sich ihre Ordination einmal aus „Angreifersicht“ anzusehen.

3.3.2. Drahtlose Zugänge

Ein möglicher Angreifer muss sich nicht innerhalb der Praxisräume befinden, um darauf zugreifen zu können. Deshalb sollte bei der physischen Ausrichtung des WLAN-Routers immer darauf geachtet werden (sofern möglich), dass er eher in der Mitte des Gebäudes platziert ist und nach innen und nicht nach außen strahlt. Übersicht der drahtlosen Zugänge: WLAN, GSM, GPRS; LTE, UMTS, 5G, Bluetooth, Hotspots, Funk etc.

Ältere Wireless-Hardware, wie ein Baby-Phone, alte Bluetooth-Geräte, eine Wireless-Tastatur mit USB-Dongle oder ein 2,4 GHz-Schnurlostelefon können sowohl die Ursache für Interferenzen sein als auch Einfallstore für Hacker darstellen, da sie fast immer nicht behobene Schwachstellen aufweisen.

3.4. Medizingeräte

Medizingeräte als auch die Software von Medizingeräten sind grundsätzlich sehr anfällig gegen Cyberangriffe. Die Gründe sind vielfältig: nicht gepatchte Software, veraltete Betriebssysteme, Geräte, die aus Zeiten stammen, als IT-Sicherheit (noch) keine Anforderung war, oder aber auch schlichte Sicherheitslücken, die noch nicht entdeckt wurden.

Als Einfallstore kommen meistens E-Mail-Anhänge und offene Netzwerke, aber auch Malware, Ransomware, Viren und Würmer in Frage. Fernwartungszugänge und Remote-Zugriffe sind ebenso beliebte Einfallstore.

Wie kann man hier proaktiv tätig werden?

- Bei der Ausschreibung Firmen favorisieren, die IT-Sicherheit in ihren Produkten anbieten und sie priorisieren.
- Von Herstellern, die das Produkt auch in die USA liefern, die dort geforderte „Herstellereklärung zur Sicherheit von Medizinprodukten (MDS2)“ erbeten.
- Das Gespräch mit den Herstellern suchen und deren Weisungen in Bezug auf Anti-Viren-Software, Härtung des Systems, Firewalls etc. befolgen
- Bei Vertragsabschluss sollte die Installierung von regelmäßigen Software-Updates verlangt werden.
- Von den Geräteherstellern verlangen, dass die IT-basierten Produkte wichtige Sachverhalte auch protokollieren.
- Ein Zonenkonzept mit einer oder mehreren Firewalls zwischen den Zonen etablieren und damit das Netzwerk segmentieren.
- Verschiedene Benutzer und Benutzergruppen mit unterschiedlichen Zugriffsrechten (Leserecht, Lese- und Schreibrecht) ausstatten. Jeder Mitarbeiter arbeitet möglichst mit seiner eigenen Kennung (Audit-Logs).
- Mitarbeiter sollten regelmäßig in die Themen „Datenschutz“ und „Datensicherheit“ eingewiesen werden und ein Auge für merkwürdige Sachverhalte oder Ereignisse entwickeln.

4. Die wichtigsten Sicherheitsmaßnahmen im Überblick

IT-Sicherheit ist nicht immer hochtechnisch, komplex und unverständlich. Natürlich wird man für einige Themen einen IT-Ansprechpartner benötigen – keine Frage – bei vielen Dingen hilft aber Folgendes:

1. gesunder Menschenverstand,
2. grundlegendste Sicherheitsmaßnahmen befolgen.

Die meines Erachtens elf wichtigsten Sicherheitsmaßnahmen für eine Praxis wären wie folgt:

4.1. Sichere Passwörter nutzen

Über sichere und ebenso unsichere Passwörter könnte man wohl ein eigenes Buch verfassen. Das Thema „Passwörter“ ist für mich in den Top 3 der wichtigsten Sicherheitsmaßnahmen.

Ich kenne den Alltag in zahlreichen Unternehmen, und das Ergebnis meiner eigenen, kleinen Studien deckt sich mit jenen in globalen Studien der IT-Sicherheitsbranche: Passwörter sind aus Unwissenheit, Faulheit oder purer Absicht zumeist schlicht unsicher gewählt!

Das große Problem daran ist, dass man heutzutage Passwörter sehr einfach „knacken“ kann. Dazu benötigt man ein fünfminütiges YouTube-Video, eine freie kostenlose Software und ab geht's ans „hacken“. Als langjähriger Datenschützer habe ich das Ganze auch selbst getestet – uns es funktioniert tatsächlich sehr einfach.

Wenn wir einen Blick auf die „weltweit meistgewählten Passwörter 2019“ werfen, finden sich darunter Passwörter wie „123456“, „qwertz“, „password“ oder „12345678“. „iloveyou“ bringt es immerhin auf Platz 8 des Rankings.

Viele Nutzer nutzen im Alltag nicht minder schwache Passwörter wie den Namen der Kinder oder des Hundes, usw. Im besten Fall werden diese dann noch mit einer Zahl (meistens „1“ oder „0“) und einem Sonderzeichen (meistens „!“ oder „?“) versehen – oder das Ganze wird sogar kombiniert. Und dies auch nur, weil die meisten Passwortvorgaben dies so verlangen.

Im meinem Fall hätten wir dann das sensationell starke Passwort „Jonas18!“. Seltsamerweise erfüllt dies die klassischen Mindestanforderungen wie Groß- und Kleinbuchstaben, Sonderzeichen, Zahlen und acht Zeichen.

Wie lange dauert es, ein solches Passwort mit einem üblichen Laptop oder PC zuhause zu knacken? Im besten Fall mehrere Minuten; im schlimmsten Fall ein paar Millisekunden.

Dazu wird auch keine besonderes „Hackerwissen“ genutzt, sondern das oben beschriebene Gratis-Tool. Dieses macht nichts anderes als Kombinationen auszuprobieren. Das Ganze nennt man dann etwas hipper „Brute Force Attacke“. Bei einer Bankomatkarte würde man quasi, ohne drohender Kartensperre nach drei Fehlversuchen, sich von „0000“ bis „9999“ durcharbeiten. Irgendwann wird man schon den richtigen Pin erwischen. Genau dieses Prinzip wird hier angewandt. Warum die „Fehlversuchssperre“, die es ja auch für Accounts gibt, nicht greift, hat mit „Hashwerten“ zu tun, die an dieser Stelle aber nicht weiter ausgeführt sein sollen.

Sichere Passwörter zu wählen, ist daher wahrlich einer der entscheidendsten Faktoren für die IT-Sicherheit. Für eine Praxis wie auch privat. Gefährlich ist es im Übrigen auch, wenn man überall das gleiche Passwort verwendet. Dies erleichtert das „Hacken“ ungemein. Ein Angreifer muss nur mehr die 3000 wichtigsten Websites wie Amazon, Gmail, Zalando & Co. durchprobieren und hat auf allen Accounts dann Zugriff. Im Idealfall auch auf E-Mails und so kann er durch einen Passwortreset („Passwort-vergessen“-Option) einen Nutzer aus den eigenen Accounts aussperren.

Die wichtigsten Faktoren für ein sicheres Passwort:

- komplex (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen),
- keine ganzen Wörter verwenden (Namen, Orte etc.),
- möglichst lange (14 Zeichen aufwärts dauern dann derzeit schon Milliarden Jahre zu knacken),
- keine Notizen verwenden (der Notizzettel am Monitor ist ein No-Go),
- für jedes Log-In ein anderes Passwort.

Beim letzten Punkt werden einige nun denken: „Wie soll ich mir das nur merken bei all den Log-Ins beruflich und privat?“

Dazu gibt es eine einfache Lösung: Dies ist ein „Passwort-Safe“. Diesbezüglich gibt es viele freie und kostenlose Anbieter (z.B. „KeePass“ oder „PasswordSafe“). Im Prinzip ist es ein mit einem Master-Passwort versehener digitaler Safe

(wie ein Notizheft), in den alle Passwörter geschützt (verschlüsselt) eingepflegt werden. Dieses Masterpasswort sollte natürlich erst recht den obigen Kriterien entsprechen, nirgendwo anders genutzt und sicher gewählt werden. Einige dieser Safes pflegen die Passwörter dann sogar direkt auf der jeweiligen Website ein und nehmen Nutzern so Arbeit ab.

Fazit: „PRAXISNAME-POSTLEITZAHL“-Passwörter sollten schon lange der Vergangenheit angehören!

4.2. Physische Absicherung der Praxis

Nicht nur die digitale Absicherung einer Praxis ist wichtig, auch die physischen Zugänge zum und im Gebäude sollten abgesichert werden. Dazu zählen die Türen zur Praxis, aber auch die Serverräume, Fenster, Archivräume, verschließbare Kästen, Balkone, Luftschächte und vieles mehr. Die Maßnahmen können dabei von einer Alarmanlage, Sicherheitsschlössern über eine Videoüberwachung außerhalb der Öffnungszeiten bis hin zu Zutrittsregelungen zu einzelnen Bereichen reichen.

4.3. Datensicherungen (Backups) erstellen

Vielleicht kennen Sie das T-Shirt eines IT-Fachmanns mit dem Schriftzug „No Backup – No Mercy“. Dieser beliebte Spruch rührt daher, dass Backups (Datensicherungen) oftmals wenig Beachtung geschenkt wird. „Unvorhersehbare“ Ereignisse können vielfältiger Natur sein: ein Brand, ein Hochwasser, defekte Hardware (eine Festplatte hält nicht ewig), ein Virus, ein Verschlüsselungstrojaner, unbeabsichtigtes Löschen, Stromausfälle, Softwarefehler und so weiter ...

Wie oft ein Backup erstellt wird, hängt vor allem vom eigenen Arbeitsvolumen ab. Wenn man weniger kritische Daten erstellt und man diese jederzeit wieder eingeben kann, dann genügt wohl ein tägliches Backup. Bei einem Backup wird oft folgendes Prinzip angewandt: Man erstellt ein komplettes Backup etwa am Wochenende, danach erfolgt täglich nur ein sogenanntes inkrementelles Backup, das heißt, nur die geänderten Dateien werden gespeichert.

Bei der Speicherung von Patientendaten, und somit auch beim Backup, empfiehlt es sich, die Daten verschlüsselt zu speichern. Falls das Backup abhandenkommt, sind die Patientendaten im verschlüsselten Backup sicher vor unberechtigten Einblicken und einer böswilligen Verwertung. Das sichere Passwort der Verschlüsselung ist separat zu speichern (z.B. Zettel, USB-Stick, CD, ...) bzw. sicher aufzubewahren.

Ganz wichtig ist: Man sollte regelmäßig testen, ob ein Wiederherstellen der Dateien oder Systeme auch wirklich funktioniert! Ein Backup kann auch nicht funktionieren oder das Speichermedium defekt sein (z.B. Magnetbänder oder Festplatte).

Man sollte zudem sicherstellen, dass genügend freier Speicherplatz auf dem Speichermedium für ein Backup vorhanden ist und dass allfällige Alarmierungsmeldungen, wie SMS oder E-Mail, bei der zuständigen Person ankommen.

4.4. Updates/Patches installieren

Sicherheitsupdates der Hersteller sollen regelmäßig, unter Umständen automatisch installiert werden! Egal, ob es sich um die Patientenverwaltungssoftware handelt oder um das Virenschutzprogramm, Webbrowser, E-Mail-Programm, Medizingeräte oder Betriebssystem – nicht upgedatete (= gepatchte) Systeme bergen unnötigerweise Sicherheitsrisiken.

Das Einspielen von Updates erfordert Aufmerksamkeit und Konsequenz. Das typische „Wegklicken“ einer Nachricht wie „Update jetzt installieren“ sollte tunlichst vermieden werden. Dazu sollte mit allen Mitarbeitern eine Routine erarbeitet werden.

4.5. Klare Richtlinien aufstellen

Es macht Sinn, dass klare Regeln und Richtlinien aufgestellt werden. Klare Regeln sind ebenso klar zu befolgen. Schwammige Vorgaben wie „Bitte passt auf!“ helfen im Prinzip weder dem Ordinationsinhaber noch seinen Mitarbeitern.

Dieses Regelwerk muss keinesfalls 50 Seiten umfassen. Wichtig ist, dass die grundlegende „Message“ überkommt und auch seitens der Mitarbeiter verstanden wird.

4.6. Verantwortlichkeiten definieren

Auch in kleinen Ordinationen sollte klar definiert sein, wer was machen darf/soll/muss. Konkret mit Bezug darauf, wer welche Informationen einsehen darf oder wer wo Zugriff bekommt (Software, Räumlichkeiten, Backups etc.). Auch dies kann womöglich auf einer einzigen A4-Seite dargestellt werden. Ordinationsinhaber

ber sollten mit ihren Mitarbeitern darüber diskutieren, wo sich Risiken ergeben und wie diese ganz konkret abgemildert oder ausgeschlossen werden können.

4.7. Need-to-know-Prinzip leben

Datenzugriffs- als auch Datenerhebungsmöglichkeiten sollten immer auf das erforderliche Mindestmaß beschränkt werden. Eine der goldenen Regeln der Informationssicherheit ist das „Need-to-know-Prinzip“: Jeder Nutzer (und auch jeder Admin) sollte nur auf jene Datenbestände zugreifen und die Programme ausführen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt.

Denn es gilt: Solange ein Nutzer zum Beispiel auf vertrauliche Daten gar nicht zugreifen kann, kann auch ein möglicher Angreifer mit dem gekaperten Benutzerkonto auf eben diese Daten nicht zugreifen. Das Gleiche gilt für die Datenerhebung. Was nicht unnötigerweise erhoben oder gespeichert wird, kann erst gar nicht abhandenkommen.

Im Übrigen verlangt die DSGVO mit dem Prinzip der Datensparsamkeit, Privacy by Design & Default als auch Vertraulichkeit, dass personenbezogene Informationen nur jenen zugänglich gemacht werden dürfen, die diese auch tatsächlich benötigen. Gerade im Alltag ist man aber leicht versucht, dies, aus welchen Gründen auch immer, zu umgehen.

4.8. Schulungen und Bewusstseinsbildung durchführen

Regelmäßige Schulungen und Bewusstseinsbildung (Awareness) sind wichtige Erfolgsfaktoren bei der IT-Sicherheit. Wie in früheren Kapiteln beschrieben, gibt es keine 100 %ige Sicherheit und der Faktor Mensch kann nie ganz ausgeschlossen werden (Stichwort „Phishing“). Schulungen oder Trainings sind daher besonders wichtig. Allerdings neigt man dazu, Gehörtes auch wieder allzu rasch zu vergessen. Die Regelmäßigkeit ist daher entscheidend. Solche Schulungen müssen auch nicht tage- oder stundenlang sein. Dies wäre vom Lerneffekt sogar eher kontraproduktiv. Ein bis zwei Stunden reichen völlig aus, sofern sie gut strukturiert und interessant gestaltet sind.

Sollten Mitarbeiter noch völlig unbedarft in den Themen „Datenschutz“ und „Datensicherheit“ sein, empfiehlt es sich, der Thematik eine eigene Schulung zu widmen. Dabei ist die Regelmäßigkeit ein entscheidender Punkt.

4.9. Netzwerksegmentierung

Ebenso nicht vernachlässigen sollte man eine Netzwerksegmentierung bzw. ein vernünftiges Zonenkonzept. Dies gilt auch für kleinere Ordinationen und kann viele potenzielle Risiken schon vorab umschiffen. Jedenfalls getrennt sein müssen das „Gäste-WLAN“ und das „Praxis-WLAN“. Dies gilt analog für etwaige kabelgebundene Netzwerke.

Auch Medizingeräte sollten zumindest in eine eigene Zone des Ordinationsnetzwerks verfrachtet werden. Selbiges gilt für Datensicherungen, sofern diese nicht ohnehin „offline“ erfolgen. Zwischen diesen Zonen bestehen dann separate Firewalls, die nur den erlaubten Ports und IP-Adressen den Datenaustausch ermöglichen.

4.10. Experten Schwachstellen prüfen lassen

Es empfiehlt sich, Schwachstellen von Zeit zu Zeit professionell prüfen zu lassen. Diese Schwachstellenprüfungen der IT-Systeme bzw. der datenschutzspezifischen Umsetzungen sollte von Profis durchgeführt werden.

Wenn Ordinationsinhaber einen Bericht mit den schwerwiegenden und kritischen Schwachstellen erhalten haben, sollten sie aktiv werden. Die Schwachstellen sollten behoben werden oder es ist, wenn dies nicht möglich sein sollte, der Zugang zu den betroffenen PCs, Servern oder Programmen zu limitieren.

Ein Tipp am Rande: Man sollte sich immer genau ansehen, welchen „Experten“ man beauftragt. Welche Erfahrung hat er? Welche Referenzen? Was macht er alles konkret? Wie lange macht er das wirklich schon? Vor zehn Jahren waren Datenschützer eine seltene Riege – heutzutage schimpft sich plötzlich fast jeder „Experte“. Hier ist durchaus eine gesunde Vorsicht geboten.

4.11. IT-Sicherheitswerkzeuge nutzen

Moderne Betriebssysteme verfügen schon in ihrer Grundausstattung über einige gute Eigenschaften. Oft sind die Tools jedoch suboptimal eingestellt. Um Systeme sicher zu machen, sollten möglichst alle Einfallspforten blockiert werden.

Wenn man zum Beispiel ein neues IT-Tool gekauft hat, sollte man sich nicht in (falscher) Sicherheit wiegen. Es könnte sein, dass das Sicherheitstool nicht richtig

konfiguriert wurde oder dass es jedes Mal bei einer Änderung des Netzwerkes auch einer Konfigurationsänderung bedarf, bevor der Schutz effektiv und vollständig wirksam wird.

Häufig wird bei den Einstellungen der Anti-Viren-Software vergessen, dass man neu an den PC angeschlossene USB-Geräte ebenfalls nach Viren durchsuchen sollte – mit unter Umständen gravierenden Folgen. Der Benutzer ändert dann unüberlegt die Einstellungen, weil er nicht immer warten möchte, bis der Stick verwendet werden kann.

Zu den wichtigsten Einstellungen und Möglichkeiten gehören:

- Verschlüsselungsmöglichkeiten (z.B. Bitlocker bei Windows 10 von Microsoft).
- Einspielen von automatischen Updates (Betriebssystem, Software, ...).
- Auswertung von Log-Dateien des Systems, der Applikationen und der Sicherheitsfunktionen.
- Whitelisting: Nur bekannte Software kann gestartet werden.
- Blacklisting: Bestimmte Programme werden als böse angesehen, der Start/die Installation wird verhindert.

Die Netzwerkzugangskontrolle ist ebenfalls entscheidend. Hier werden nur Geräte zugelassen, bei denen die Hardware-Adresse (= die sogenannte MAC-Adresse) bekannt ist. Schließt nun ein Angreifer einen Laptop an das Netzwerk, so protokolliert und alarmiert die Software den Administrator über diesen potenziellen Angriff.

Je mehr Sicherheitsmaßnahmen ergriffen werden, desto schwieriger macht man es Angreifern!

5. Tipps, Tricks und Lösungsvarianten zu alltäglichen Datenschutzthemen

Die Theorie der DSGVO zu kennen ist das Eine – die reale Umsetzung im Praxisalltag das Andere.

5.1. Datenübermittlung an Patienten und andere Gesundheitsdiensteanbieter

5.1.1. Grundproblematik

Warum die Datenübermittlung an Patienten und andere Gesundheitsdiensteanbieter derart viel Zündstoff birgt, ergibt sich aus der ärztlichen Verschwiegenheit, dem Datengeheimnis der DSGVO und des DSG, dem Gesundheitstelematikgesetz und den technischen Mängeln mancher Übertragungsarten.

Viele davon sind nämlich nicht so sicher, wie wir dies auf Anhieb einschätzen würden. Ein gutes Beispiel dafür ist die klassische E-Mail. Sicher sind E-Mails nur in ganz bestimmten Fällen, nämlich nur dann, wenn eine Verschlüsselung zwischen Sender und Empfänger besteht. Eine E-Mail ohne Verschlüsselung muss man sich, analog zum Briefverkehr, als Postkarte vorstellen, die für jedermann leicht lesbar und abfangbar ist.

Dem verschlossenen Brief würde analog die verschlüsselte E-Mail gegenüberstehen. Mit dem Unterschied, dass diese nicht unberechtigt geöffnet werden kann, wie dies beim physischen Brief der Fall wäre.

5.1.2. E-Mail

Wie erwähnt, sollten aufgrund der technischen Problematik über E-Mail nie unverschlüsselt sensible Informationen und Daten ausgetauscht werden, auch nicht mit Patienten. Die Grundlagen der Verschlüsselung an dieser Stelle zu erläutern würde den Rahmen dieses Artikels sprengen.

Meines Erachtens müssen bei Versand sensibler und/oder gesundheitspezifischer Informationen eine Transportverschlüsselung (zB TLS) und auch eine Inhaltsverschlüsselung (zB OpenPGP, S/MIME) implementiert sein. Dies müssen jedoch beide Kommunikationspartner entsprechend implementieren, was mich zur Praktikabilität im Alltag bringt.

Viele Patienten wissen nicht, was eine E-Mail-Verschlüsselung ist, bzw. wie man diese einrichtet. Im Ergebnis wird man daher folgendes Szenario anwenden müssen:

- Mit dem E-Mail-Provider ist abzuklären, ob eine Transportverschlüsselung (z.B. TLS) besteht.
- Wenn nicht, sollte diese aktiviert werden.
- Sensible Informationen per ZIP/RAR-Datei packen und mit einem Passwort versehen (Achtung Kriterien wie zuvor beschrieben beachten) – dabei „AES 256“ als Verschlüsselungsstandard auswählen.
- Patienten vor Ort das Passwort mitteilen damit diese die Datei öffnen können.
- Im E-Mail-Text oder Betreff keine Hinweise auf sensible Informationen liefern (z.B. „Anbei wie besprochen Ihr Befund bezüglich Krebsabstrich.“).

Wenn dies zu kompliziert ist, muss man auf eine lokale Abholung oder den Briefversand umsteigen.

Achtung! Der Arzt kann rechtlich den Patienten nicht einwilligen lassen, dass dieser mit einer unverschlüsselten Übermittlung einverstanden ist. Dies wäre unrechtmäßig.

5.1.3. Instant-Messenger-Apps

Für Instant-Messenger-Apps wie „WhatsApp“ gilt im Grunde dasselbe wie für E-Mails. Mit einer besonderen Problematik als Ergänzung: Der App-Anbieter kann im schlimmsten Fall den Inhalt mitlesen.

Hier sind daher insbesondere alle Messenger zu meiden, die nicht „Open-Source“ sind. Dies bedeutet, wo der Quellcode der App frei einsehbar und vor allem überprüfbar ist. So können etwaige Hintertüren ausgeschlossen werden. Ist die App nicht Open-Source, kann dies daher nicht ausgeschlossen werden.

Meine Empfehlung hinsichtlich sicherer Messenger-Apps wäre hier „Signal“, da

- Open-Source,
- Ende zu Ende als auch transportverschlüsselt,

- Kostenlos,
- für alle gängigen Betriebssysteme verfügbar,
- mehrfach sicherheitsüberprüft.

„WhatsApp“ fällt, wie viele andere Messenger, leider in die Kategorie „Nicht Open-Source“. Wenn es auch derzeit weit verbreitet und beliebt ist, sollte man für sensible Daten besser sichere Messenger-Apps nutzen.

5.1.4. Fax

Auch ein Fax stellt eine unverschlüsselte Datenübertragung dar.

Aufgrund gesetzlicher Regelung gibt es eine (für mich systematisch nicht verständliche) Ausnahme, wann man ein Fax trotzdem verwenden darf, nämlich dann, wenn

- die Faxanschlüsse (einschließlich Ausdruckmöglichkeiten zu Faxanschlüssen, die in EDV-Anlagen installiert sind) vor unbefugtem Zugang und Gebrauch geschützt sind,
- die Rufnummern, insbesondere die verspeicherten Rufnummern, regelmäßig, insbesondere nach Veränderungen der technischen Einrichtung sowie nach der Neuinstallation von Faxgeräten nachweislich auf ihre Aktualität geprüft werden,
- automatische Weiterleitungen, außer an die jeweiligen Gesundheitsdiensteanbieter selbst, deaktiviert sind,
- die vom Gerät unterstützten Sicherheitsmechanismen genützt werden und
- allenfalls verfügbare Fernwartungsfunktionen nur für die vereinbarte Dauer der Fernwartung aktiviert sind.

5.1.5. Telefon

Ein Telefon birgt zwar grundsätzlich auch die Gefahr des „Abhörens“, dies ist aber nur in sehr aufwendigen Fällen möglich. Die größere Problematik ist hier, dass schlicht nicht jene Person am Telefon ist, die sie zu sein vorgibt. Nur weil sich jemand als „Herr Müller“ ausgibt, bedeutet dies nicht, dass es auch Herr Müller ist.

Daher: Sofern man Personen am Telefon nicht zu 100 % zuordnen kann (etwa, weil man diese persönlich gut kennt), sollten ohne vereinbartes Lösungswort keine Auskünfte erteilt werden!

Das System des Lösungsworts ist nicht kompliziert, man kennt es vom Handyanbieter oder diversen anderen Dienstleistern und ist zudem praktikabel und empfehlenswert.

5.2. Lieferanten/Dienstleister beauftragen

Bei Lieferanten bzw. Dienstleistern muss zunächst aus Datenschutzsicht geklärt sein, ob es sich um einen schlichten Dienstleister (z.B. Putzfrau, Installateur etc.) handelt oder um einen Auftragsverarbeiter im Sinne der DSGVO, der personenbezogene Daten im Auftrag des Ordinationsinhabers verarbeitet. In diesem Fall muss dieser zumindest

- einen Auftragsverarbeitervertrag mit dem Dienstleister abschließen und sicher aufbewahren (bitte nicht unüberlegt etwas aus dem Internet „kopieren“),
- keinen falschen „Experten“ beschäftigen, der noch nie etwas von Datenschutz oder Datensicherheit gehört hat und
- darauf achten, wo die Daten schlussendlich gespeichert/verarbeitet werden (z.B. Drittstaaten wie USA, Indien & Co.).

Typische Auftragsverarbeiter sind etwa

- die Inanspruchnahme von Webhostern,
- die Inanspruchnahme einer Cloud-Lösung oder eines Zahlungs-Hubs,
- die Inanspruchnahme eines IT-Dienstleisters zur Wartung oder Fernwartung,
- die Beauftragung von Newsletter-Versanddienstleistern,
- Datenträgerentsorgung durch Dienstleister,
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten,
- Werbeadressenverarbeitung in einem Lettershop,
- der Einsatz von Google Analytics,
- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung,
- Rechenzentren & Cloud-Anbieter,
- Auslagerung der Backup-Sicherheitspeicherung und anderer Archivierungen.

Im ersten Fall (schlichter Dienstleister) würde ich dennoch die Unterzeichnung einer Verschwiegenheitsvereinbarung einfordern.

5.3. Datenschutzverletzungen & Datensicherheitsvorfälle

Niemand ist davor gefeit, dass nicht doch einmal etwas passiert. Und unter Umständen kann man persönlich gar nichts dafür (z.B. Hackerangriff). Dennoch gilt es, die Regeln für sogenannte Datenschutzverletzungen, insbesondere die Melde- und Informationspflichten, strikt einzuhalten.

Die DSGVO sieht diesbezüglich vor:

- Jede Datenschutzverletzung muss immer mit den Fakten hinsichtlich der Datenschutzverletzung, ihren Auswirkungen und den getroffenen Abhilfemaßnahmen dokumentiert werden.
- Bei einem Risiko für den Betroffenen muss dies der Datenschutzbehörde gemeldet werden.
- Bei einem hohen Risiko für den Betroffenen müssen Ärzte zudem die betroffenen Personen informieren.

Kurzum zu den beiden letzten Punkten: Da Ärzte meist gesundheitspezifische Informationen von Betroffenen verarbeiten und diese im Fall einer Datenschutzverletzung betroffen sind, ist zumeist von einem hohen Risiko für die betroffenen Personen auszugehen.

In diesen Fällen müssen Ärzte eine Meldung an die Datenschutzbehörde durchführen und die betroffenen Personen darüber informieren. Meldeformulare gibt es z.B. auf der Webseite der österreichischen Datenschutzbehörde. Nur in Fällen, in denen man davon ausgehen kann, dass kein Risiko für die Betroffenen besteht, kann eine solche Meldung unterbleiben. Ärzte sollten daher immer die möglichen Konsequenzen für die Betroffenen als auch das Schadenspotenzial und die Eintrittswahrscheinlichkeit bedenken.

5.4. Cloud oder eigener Server? Vergleich der Vor- und Nachteile beider Varianten

Ob man für die Ordination einen eigenen Serverraum einrichtet, Backups erstellt und man sich selbst (oder über Dienstleister) um die ausreichende Wartung kümmert oder aber in die Cloud wechselt, bleibt den Ordinationsinhabern überlassen.

Aus rechtlicher Sicht ist Folgendes zu beachten:

Die Speicherung von Gesundheitsdaten in Datenspeichern, die einem Verantwortlichen (dem Ordinationsinhaber) bedarfsorientiert von einem Auftragsverarbeiter

bereitgestellt werden (z.B. „Cloud Computing“), darf nur dann erfolgen, wenn die Daten mit einem dem aktuellen Stand der Technik entsprechenden Verfahren verschlüsselt worden sind.

Aus diesem Grund dürfen Ordinationsinhaber nur einen Cloudanbieter wählen, der auch eine Verschlüsselung der Daten anbietet.

Es gibt aber auch noch andere Vor- und jeweils Nachteile bei der Nutzung der einen oder anderen Variante.

Interner stationärer Server

Vorteile	Nachteile
<ul style="list-style-type: none"> • Daten verlassen nicht die Organisation. • Der Ordinationsinhaber behält die Zugriffskontrolle. • Funktioniert auch während eines Internet-(Zugriffs)-Ausfalls. • Spezielle dongle-geschützte Schutzmaßnahmen funktionieren. 	<ul style="list-style-type: none"> • Server-Wartung wird durch externe Mitarbeiter geleistet. • Server-Raum kostet Miete und ist evtl. nicht optimal eingerichtet. • Updates muss man selber installieren (lassen). • Kein ortsunabhängiges Back-up vorhanden. • Kosten: Vor-Ort-Service für Arbeiten am Server kosten mehr.

Externer Cloud-Server

Vorteile	Nachteile
<ul style="list-style-type: none"> • Provider kümmert sich um alles (Hardware- und Software-Updates, Back-up etc.). • Professioneller Umgang mit der Informationssicherheit kann erwartet werden. • Skalierbarer Speicher. • Back-ups der Daten auf mehrere Standorte verteilt. • Man zahlt nur, was man braucht. • Oftmals ISO-27001-Zertifikat vorhanden. 	<ul style="list-style-type: none"> • Patientendaten sind außerhalb der Praxis gespeichert. • Man gibt die Kontrolle darüber ab. • Zum Teil ungewiss, in welchem Land die Daten gespeichert werden, bzw. entsprechende Vertragsklausel notwendig. • Ohne Internetzugriff kann man (oftmals) nicht arbeiten. • Verträge über Auftragsverarbeitung müssen abgeschlossen werden. • Redundanter Internetanschluss wird empfohlen.

5.5. Wird ein Datenschutzbeauftragter benötigt?

Ein klares „Ja“! Zumindest wird man das wohl von einem unseriösen Berater zu hören bekommen, der dieses Service gegen Entgelt gerne anbieten wird. Unter Umständen hat er damit aber womöglich sogar Recht.

Die Beantwortung dieser Frage hängt primär damit zusammen, ob man eine „umfangreiche Verarbeitung von Patienten-/Gesundheitsdaten“ betreibt.

Was ist „umfangreich“? Nun, dies wird durch die DSGVO selbst nicht definiert. Es gibt aber einige andere Quellen, die man für eine Auslegung heranziehen sollte. Im Ergebnis lässt sich Folgendes sagen:

- Ein einzelner (ja, ein „EINZELNER“) Arzt benötigt keinen Datenschutzbeauftragten.
- Zwei bis neun Ärzte (bzw. medizinische Angestellte) bewegen sich in einem Graubereich: Hier kommt es darauf an, ob sie
 - nur regional, österreichweit oder womöglich über Grenzen hinweg tätig sind,
 - wenige oder viele Patienten betreuen und
 - wenige oder viele Informationen zu einem einzelnen Patienten verarbeiten.(Je mehr hier für ein üppiges Tätigkeitsfeld spricht, umso mehr spricht auch für einen Datenschutzbeauftragten.)
- Ab zehn angestellten Ärzten (bzw. medizinische Angestellte) würde ich meinen: JA (hier gibt es schon Entscheidungen der Datenschutzbehörde und Empfehlungen branchenspezifischer Stellen, die dies aktuell zumindest stützen).

5.6. Aufbewahrungsfristen und die sichere Datenlöschung/Datenvernichtung

5.6.1. Speicherdauer von personenbezogenen Daten

Einer der wichtigsten Grundsätze des Datenschutzrechts lautet: Daten dürfen personenbezogen nur so lange gespeichert werden, als diese für die Zweckerreichung notwendig sind. Danach sind diese sicher zu löschen oder zu anonymisieren.

Dieser sehr simpel anmutende und logisch erscheinende Gedanke ist in der Realität aber oftmals der am schwierigsten zu erfüllende. Sei es aufgrund der Komplexität, technischer Implikationen oder aber aufgrund des Aufwands der rechtmäßigen Umsetzung.

Vor allem ist auf den jeweiligen Verarbeitungszweck abzustellen, es sind gesetzliche Aufbewahrungsfristen zu beachten und zu guter Letzt auch Aufbewahrungswünsche (z.B. zur Beweissicherung) zu berücksichtigen.

Hierbei sei auch gleich erwähnt, dass ein erheblicher Unterschied besteht, ob ein Gesetz die Aufbewahrung verpflichtend vorschreibt (wie z.B. für steuerrelevante Unterlagen oder für medizinische Daten) oder ob man Unterlagen aufgrund seines eigenen Interesses aufheben möchte. Letzteres ist nur dann möglich, wenn eine Interessensabwägung zu eigenen Gunsten ausfällt.

5.6.2. Aufbewahrungsfristen im Gesundheitssektor

Im Gesundheitsbereich gibt es eine Vielzahl von Vorschriften, welche die Archivierung von relevanten Unterlagen betreffen. Die nachstehende Liste ist daher nicht als zwingend abschließend zu betrachten.

Thema	Dauer
Aufbewahrungspflichten nach der Allgemeinen Strahlenschutzverordnung (AllgStrSchV) (u.a. §§ 16, 19, 31)	7 Jahre
Aufbewahrungspflicht nach § 43 Abs. 1 Chemikaliengesetz (ChemG)	7 Jahre
Aufbewahrungspflicht nach § 7 Giftverordnung	7 Jahre
Aufzeichnungen der Erzeuger und Arzneimittelgroßhändler über psychotrope Stoffe nach § 8 Psychotropenverordnung	3 Jahre
Vormerkungen von Erzeugern und Arzneimittelgroßhändler nach § 8 Suchtgiftverordnung	3 Jahre
Aufbewahrung der Unterlagen nach Art. 3 und 4 der EU-Verordnung 111/2005 für die Überwachung des Handels mit Drogenausgangsstoffen	3 Jahre
Aufbewahrungspflicht nach § 46 Arzneimittelgesetz (AMG)	15 Jahre
Aufbewahrungspflicht nach § 15 Abs. 1 Arzneimittelbetriebsordnung (AMBO)	5 Jahre

Thema	Dauer
Aufbewahrungspflicht chargenbezogener Unterlagen nach § 15 Abs. 9 Arzneimittelbetriebsordnung (AMBO)	15 Jahre
Aufbewahrung ärztlicher Aufzeichnungen und Dokumentationen gem. § 51 Abs. 3 ÄrzteG	10 Jahre
Aufbewahrung von Krankengeschichten in Krankenanstalten gem. § 10 Abs. 1 Z 3 KaKuG	30 Jahre*
Röntgenbilder, Videoaufnahmen und andere Bestandteile von Krankengeschichten, deren Beweiskraft nicht 30 Jahre hindurch gegeben ist, sowie bei ambulanten Behandlungen 10 Jahre	
Aufbewahrung von Dokumentationen und Zustimmungserklärungen im Zusammenhang mit medizinisch unterstützter Fortpflanzung gem. § 18 Fortpflanzungsmedizingesetz (FMedG)	30 Jahre
Dokumentationen im Zusammenhang mit Gewebeentnahmen gem. §§ 5, 16 Gewebesicherheitsgesetz (GSG)	mind. 10 Jahre; bzgl. Teile, die für eine lückenlose Rückverfolgbarkeit unerlässlich sind 30 Jahre
Dokumentation bei Organentnahmen und -transplantationen gem. §§ 3e, 3f KaKuG	30 Jahre
Dokumentation von Eingängen, Abgängen und Anwendungen von Blut oder Blutbeständen im Rahmen des Blutdepots gem. § 8f KaKuG	30 Jahre
Behandlungsdokumentation von medizinischen Masseuren und Heilmasseuren nach § 3 MMHmG	10 Jahre
Dokumentationspflichten nach der Verordnung über die Konformitätsbewertung von Medizinprodukten	5 bzw. 15 Jahre
Implantatregister von Medizinproduktebetreibern nach § 10 Medizinproduktebetreiberverordnung	30 Jahre
Aufbewahrung des Haushaltsbuches sowie der Belege für Personenbetreuer nach § 160 GewO	2 Jahre

5.6.3. Sichere Datenlöschung und Datenvernichtung

In diesem Abschnitt geht es um die sichere Löschung bzw. Vernichtung von Daten. Doch wie weiß man, was als „sicher“ gilt?

Hier gibt es wiederum einige Standards und Normen wie die DIN 66399 oder die ISO 21964-1, die beträchtlich weiterhelfen. Anbei die wichtigsten Datenträger und deren verlangte Vernichtungsmethode für sensible Informationen:

Datenträger	Vernichtungsmethode
Papierdokumente	Klassifikation P4 (oder höher) Partikelgröße max. 160 mm ²
CDs, DVDs etc.	Klassifikation O4 (oder höher) Partikelgröße max. 30 mm ²
elektronische Datenträger	Klassifikation E4 (oder höher) Partikelgröße max. 30 mm ²
Festplatten mit magnetischem Datenträger	Klassifikation H4 (oder höher) Partikelgröße max. 2000 mm ² Mehrfach zerteilt und verformt

Im Zweifel erkundigt man sich bei seinem „Aktenvernichter-Lieferanten“ nach den Klassifizierungen.

Schützenswerte digitale Daten sollten stets mit sicheren Löschmodulen gelöscht werden. Dazu gibt es einige Tools, die kostenlos sind und sichere Methoden (Mehrfachüberschreibung von Daten) der Löschung diesbezüglich anbieten. Solche Methoden sind etwa:

- 5220.22-M-Standard des US-Verteidigungsministeriums,
- VSITR-Standard des Bundesamts für Sicherheit/Informationstechnik (BSI),
- Bruce-Schneier-Algorithmus,
- Peter-Gutmann-Algorithmus.

Vielen Nutzern ist nicht bewusst, dass ein einfaches Löschen („Delete“-Befehl, Verschieben in den Papierkorb, „Quick-Format“) der Daten in keinem Fall ausreichend ist. Zwar wissen die meisten Nutzer, dass ein Wiederherstellen eines Dokuments aus dem Papierkorb problemlos möglich ist. Den meisten ist aber nicht bewusst, dass auch nach Löschen des Papierkorbs und sogar nach Formatieren der Festplatte die Daten problemlos mit einer herkömmlichen Datenrettungs-Software wiederhergestellt werden können.

Anonymisieren ist einer Löschung übrigens gleichzusetzen. Achtung! Anonyme Daten sind durch niemanden mehr auf eine individuelle Person zurückzuführen (faktische Unmöglichkeit).

6. Betroffenenrechte praktikabel aber gesetzeskonform umsetzen

Ein ebenso spannender Themenbereich der DSGVO ist die Umsetzung bzw. Erfüllung der Rechte von natürlichen Personen. Diese sind nicht zur Gänze neu, aber durch die DSGVO sicherlich gestärkt worden. Vor allem kann ein Zuwiderhandeln oder gar Ignorieren empfindlich teuer werden.

6.1. Identitätsfeststellung – aber wie?

Grundlegend ist wiederum, dass man sich vor der weiteren Behandlung einer Anfrage zunächst von der Identität der Person überzeugen sollte bzw. keine Zweifel an dieser haben darf. Erkennt man eine Person bei einem Telefonat bereits an der Stimme, wird dies keine allzu großen Probleme verursachen. Anders sieht dies aber aus, wenn beispielsweise eine E-Mail des Absenders „michael.mueller@gmail.com“ im Eingang des E-Mail-Programms auftaucht. Man hat keine Garantie, dass diese E-Mail tatsächlich von einem Michael Müller stammt. Auch eine bekannte Telefonnummer ist keine Garantie. Mit Tools um wenige Euros können Betrüger jede x-beliebige Telefonnummer als auch E-Mail-Adresse imitieren.

Gibt der Ordinationsinhaber eine Auskunft an eine Person, die gar nicht die betroffene Person ist, hätte er eine schwerwiegende Verletzung des Datengeheimnisses zu verantworten.

Aber welche sicheren Methoden gibt es und welche sind davon praktikabel?

- Persönliche Vorsprache in der Praxis mit amtlichem Lichtbildausweis
Sofern eine Person physisch in die Ordination kommt und sich ausweisen kann oder sie dort bekannt ist, gibt es keine Zweifel an der Identität dieser Person und somit keinen Bedarf an weiteren Überprüfungen.

- **Qualifizierte elektronische Signatur i.S.d. §4 Abs. 1 Signatur- und Vertrauensdienstegesetz bei E-Mails**

Diese Möglichkeit gibt es prinzipiell, jedoch werden nur sehr wenige Personen so eine Signatur nutzen. Grundsätzlich kann man diese bedenkenlos akzeptieren.
- **Identitätsfeststellung per Video-Telefonie**

Video-Telefonie ist für viele schnell und zumeist kostenlos verfügbar. Im Grunde gelten hier dieselben Regeln wie bei der physischen Anwesenheit.
- **Post-Ident-Verfahren, bei dem der Empfänger durch einen Postdienstleister zweifelsfrei identifiziert wird**

Dieses im Finanzsektor (z.B. Bankkontoeröffnung) etablierte Verfahren ist ebenso als sicher einzustufen, jedoch zeitlich betrachtet langsam und nicht unaufwendig.
- **Video-Ident-Verfahren (z.B. „MyIdentityCheck“ der österreichischen Staatsdruckerei)**

Ein ebenso etabliertes Verfahren, welches jedoch mit Kosten verbunden ist. Zeitlich nehmen diese Checks für die jeweiligen Personen nur wenige Minuten in Anspruch.
- **Abfrage und Abgleich diverser personenbezogener Infos mit bereits gespeicherten Daten**

Eine derzeit akzeptierte Methode ist es, die verschiedensten persönlichen Informationen, die nur die betroffene Person kennen sollte, bei dieser abzufragen. Diese Methode kann zwar bei sehr spezifischen und persönlichen Informationen treffsicher sein bzw. ist sie mit hoher Wahrscheinlichkeit geeignet, die Person identifizieren, 100 % sicher ist dies jedoch nicht, wenn man die Person als „Angreifer“ gut genug kennt.
- **Eigenhändig unterschriebenes Begehren mit angeschlossenen Vergleichsmuster der Unterschrift (z.B. Reisepass)**

Diese Methode wird derzeit akzeptiert, da die Kombination aus Ausweiskopie und unterschriebenem Formular für die Korrektheit der Identität spricht. Restlos bin ich davon jedoch nicht überzeugt, da man zu einer solchen Ausweiskopie unter Umständen schnell gelangen kann und eine Unterschrift zu fälschen auch nicht allzu aufwendig erscheint.

Mein Rat daher: Man sollte in solchen Fällen zumindest per eingeschriebenem Brief oder persönlich an die vermeintlich betroffene Person beauskunften. Dies kann man bei elektronischen Anfragen z.B. auch mittels USB-Stick mit

den darauf gespeicherten und verschlüsselten Daten(!) erfüllen. Das Passwort für die verschlüsselten Daten übermittelt man (wie von Kreditkarten bekannt) mittels separatem Brief. Mit Einverständnis der Person kann man die Informationen auch mündlich oder physisch auf Papier übergeben.

Wie kann man der Person nun sicher die verlangten Informationen zukommen lassen?

Hier gelten ganz allgemein jene Regeln, die in den vorherigen Kapiteln aufgezeigt wurden. Je nach technischem Verständnis der jeweiligen Person kann dies von persönlicher Übergabe, verschlüsseltem E-Mail-Verkehr aber auch Downloadbereitstellung über eine sichere Plattform (z.B. IPraxiswebsite mit geschütztem Login) erfolgen.

6.2. Recht auf Auskunft

Das Recht auf Auskunft ermöglicht es einer Person, eine Information (= Auskunft) darüber zu erhalten, ob ihre Daten etwa von einem Arzt verarbeitet werden, sie bekommt dann Auskunft über den konkreten Inhalt und hat das Recht, eine Kopie von der Verarbeitung zu verlangen.

Der Inhalt ist durch die DSGVO klar vorgegeben. Auch die zeitliche Frist dafür: 1 Monat. In Ausnahmefällen und triftigen Gründen kann diese um 2 Monate verlängert werden, worüber der Betroffenen aber zu informieren ist. Eine Auskunft muss auch dann erteilt werden, auch wenn keine Daten von der Person verarbeitet wurden (sogenannte „Negativauskunft“). Alle Betroffenenrechte sind laut DSGVO kostenlos zu erfüllen. Nur in exzessiven Fällen (z.B. wöchentliches Auskunftsbegehren der gleichen Person) kann dafür ein angemessenes Entgelt verlangt werden.

Die Daten sind dabei so bereitzustellen, wie sie konkret vorliegen. Ein Arzt darf die Daten nicht durch eine Aufbereitung abändern, da er hierdurch den Informationsgehalt der Daten verändern könnte. Eine ergänzende Erläuterung ist hingegen zulässig und kann dazu dienen, den Auskunftsanspruch zu erfüllen, etwa die Erklärung von Abkürzungen, Fachbegriffen und Symbolen.

Die Auskunft ist in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.

Eine wichtige Ausnahme der Auskunftspflicht: Sie darf nicht die Rechte und Freiheiten anderer Personen beeinträchtigen. Dies etwa, weil ein Arzt dabei seine

ärztliche Verschwiegenheit verletzen müsste. In solch einem Fall ist diese „schädigende“ Information herauszufiltern, zu schwärzen oder dergleichen.

6.3. Recht auf Berichtigung

Ein eher banal wirkendes Recht ist das von betroffenen Personen, unverzüglich die Berichtigung sie betreffender unrichtiger oder die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Im Alltag geschieht es aber durchaus des Öfteren, dass Daten, aus welchen Gründen auch immer, unrichtig oder nicht vollständig sind. Sofern der Betroffene Recht hat, muss der Arzt die betreffenden Daten korrigieren bzw. ergänzen.

6.4. Recht auf Widerspruch

Das Recht auf Widerspruch kommt in der Praxis vor allem bei zwei Konstellationen zur Anwendung. Einerseits beim Direktmarketing, was bei Ärzten standesrechtlich nicht erlaubt ist. Andererseits kommt das Widerspruchsrecht bei Datenverarbeitungen zum Tragen, wo es sich auf das „berechtigte Interesse“ des Arztes als Rechtsgrundlage stützt.

In diesen Fällen gilt es, das Interesse der Person an der Einstellung der Datenverarbeitung und die Interessen des Arztes an der weiteren Verarbeitung abzuwägen. Wer entscheidet nun, wessen Interessen überwiegen? Letzten Endes die Datenschutzbehörde oder die Bundesverwaltungsgerichte im Fall einer Beschwerde der Person. Dies kann man sich wie eine Waagschale vorstellen: Dessen Interessen überwiegen, der „gewinnt“.

Beispiel: Ein Arzt betreibt eine Videoüberwachung seiner Praxis (innen/außen) außerhalb der Öffnungszeiten. Seine Rechtsgrundlage gemäß DSGVO ist in der Regel das „berechtigte Interesse“. So weit, so gut. Nun beschwert sich ein Patient bei ihm, da er der Meinung ist, die Videoüberwachung sei unzulässig. Unter Berücksichtigung aller Interessen wird das Interesse am Schutz der Praxis, der Gerätschaften, der Patientendaten, des Eigentum etc. schwerer wiegen als das Interesse eines Patienten, der außerhalb der Öffnungszeiten erfasst wird. Zudem speichert der Arzt die Daten ja nicht länger als ein bis zwei Wochen, und Zugriff auf das Videomaterial hat im Fall eines Einbruchs oder Verdacht des Diebstahls und dergleichen nur ein Mitarbeiter oder der Arzt selbst. Die Waagschale neigt sich auf die Seite des Arztes und der Widerspruch der betroffenen Person ist unberechtigt.

Hinsichtlich der Patientendaten in ELGA besteht ein generelles und ein abgestuftes Opt-Out-Recht für Patienten. Dieses ist jedoch entweder direkt im ELGA-Portal oder aber über die ELGA-Widerspruchsstelle durch den Patienten wahrzunehmen.

6.5. Recht auf Löschung

Das Recht auf Löschung wurde unter dem medienwirksamen Schlagwort „Recht auf Vergessenwerden“ bekannt. Ein Arzt ist demnach dazu verpflichtet, personenbezogene Daten dann zu löschen oder zu anonymisieren, sobald diese nicht mehr benötigt werden.

Das Recht auf Löschung gilt jedoch nicht absolut und grenzenlos. Gewisse Daten dürfen gar nicht gelöscht (ärztliche Aufbewahrungspflichten, Abrechnungsdaten, Geltendmachung von Rechtsansprüchen, etc.) oder müssen berechtigt (und zeitlich begrenzt) aufbewahrt werden.

Werden personenbezogene Daten unrechtmäßig verarbeitet, sind diese längst zu löschen oder ist ein Widerspruch berechtigt, dann sind Ärzte angehalten, diese auch wirklich zu löschen. Das „sichere“ Löschen wurde im Kapitel zuvor behandelt.

6.6. Recht auf Einschränkung

Das Recht auf Einschränkung betitle ich gerne als Ergänzungsrecht zum Recht auf Löschung. Was bedeutet „einschränken“ konkret?

Wie bei der Löschung bereits erörtert, ist das Merkmal des Löschens, dass personenbezogene Daten und Informationen nicht mehr abrufbar sind – für niemanden.

Beim Einschränken von Daten werden hingegen die Daten nicht gelöscht, allerdings derart „eingeschränkt“, besser gesagt „gesperrt“, dass diese nicht mehr verarbeitet werden können. Um diese konkrete Zweckbegrenzung zu erreichen, sind die betroffenen personenbezogenen Daten entsprechend zu markieren. Allgemeiner Zweck dieses Rechts ist die Beweissicherung und um verfrühtes Löschen von Datenbeständen in unklaren Rechtssituationen zu vermeiden, etwa wenn der Betroffene, wie zuvor beschrieben, eine Berichtigung verlangt.

6.7. Recht auf Datenübertragbarkeit

Bei diesem bereits sperrig lautenden Recht hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Arzt bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat zudem das Recht, diese Daten einem anderen Verantwortlichen (z.B. anderer Arzt), dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

Aufgrund des üblichen Datenaustausches im Gesundheitssektor bereitet dieses Recht in der Regel keine größeren Probleme.

6.8. Recht auf Information (oder besser: Informationspflicht)

Das Recht auf Information ist unter all den Betroffenenrechten das einzige, welches Ärzte proaktiv erfüllen müssen. Alle anderen Rechte sind grundsätzlich reaktiv handzuhaben, das heißt, wenn die betroffene Person dieses Recht gegenüber dem Arzt wahrnimmt.

Für Ärzte wird es hier aber etwas kompliziert. Im Grunde aber auch wiederum nicht.

Das Ärztegesetz regelt grundsätzlich, dass das Recht auf Information (streng genommen neben dem Recht auf Einschränkung und Widerspruch) gemäß der DSGVO hinsichtlich jener Verarbeitungstätigkeiten, die im Ärztegesetz angeführt sind, ausgeschlossen ist. Diese Regelung gilt derzeit als umstritten und führt zu einer Rechtsunsicherheit im Alltag.

Mein Tipp daher: Die Informationspflichten sollten auch derzeit, unabhängig von rechtlichen Plänkeleien, erfüllt werden. Gerade das Recht auf Information möchte die Transparenz gegenüber betroffenen Personen von Datenverarbeitungen wahren. Zudem ist die Umsetzung für Ordinationen auch kein unverhältnismäßiger Aufwand. Ja, es ist ein Einmalaufwand und ab und zu muss ein Zettel umgeschrieben werden. Das war es aber dann zumeist auch schon.

Was steht nun hinter diesem Recht auf Information, besser: Informationspflicht?

In Bezug auf die Informationspflichten muss die betroffene Person jederzeit klar und eindeutig erkennen können, welche ihrer personenbezogenen Daten von wem für welche Zwecke verarbeitet werden. Insbesondere (beabsichtigt sowie

unbeabsichtigt) „geheime“ Verarbeitungen stehen im Fokus und sollen nun der Vergangenheit angehören.

Wie löst man das in der Praxis am besten?

Zumal empfiehlt es sich, die Information nicht mündlich zu geben. Ärzte sollten daher eine A4-Seite (wenn nötig zwei) mit dem durch die DSGVO vorgegebenen Informationsinhalt verfassen. Dies wären:

- Identität des Verantwortlichen (d.h. Unternehmensdaten und Kontaktdaten der Ordination),
- Kontaktdaten des Datenschutzbeauftragten,
- Verarbeitungszweck(e) und Rechtsgrundlage(n) gemäß DSGVO,
- die konkreten berechtigten Interessen, sofern der Arzt welche als Rechtsgrundlage heranzieht,
- Empfänger der personenbezogenen Daten,
- Drittstaaten, in die unter Umständen Daten transferiert werden,
- Speicherdauer,
- Aufklärung über Betroffenenrechte,
- Aufklärung über Widerrufsrecht,
- Aufklärung über Beschwerderecht,
- Aufklärung über Bereitstellung der Daten,
- Bestehen einer automatisierten Einzelentscheidung oder Profiling.

Real betrachtet ist die Hälfte der zu gebenden Information ein Standardtext. Die andere Hälfte muss auf die Ordinationstätigkeiten abgestimmt werden. Das Erstellen sollte hier durchaus ein Experte übernehmen.

Im Endeffekt erhält ein Arzt dann 1 bis 2 A4-Seiten, die er in seiner Praxis, im Idealfall beim Empfang, aushängen kann.

Ebenso muss er einen derartigen Informationshinweis

- bei etwaigen Bewerbungsverfahren gegenüber Bewerbern geben,
- auf der Website anbringen bzgl. der Websitedatenverarbeitungen und
- aushängen, wenn er eine Videoüberwachung installiert hat.

Zusammenfassend kann man sagen, dass ein Arzt keine Verarbeitung von Daten durchführen darf/soll, wenn die betroffene Person nicht darüber Bescheid weiß. Eine Ausnahme gibt es aber dennoch: Das Berufsgeheimnis darf nicht verletzt werden.

Beispiel: Dies wäre etwa der Fall, wenn ein Arzt im Zuge der Abfrage von Gesundheitsdaten eines Patienten von diesem erfährt, dass sein Bruder Karl und Onkel Manfred auch schon dieses oder jenes Leiden hatten. In diesem Fall müssten gemäß der DSGVO grundsätzlich Karl und Manfred von der Verarbeitung ihrer Daten informiert werden (sofern deren Kontaktdaten oder Adressdaten bekannt sind). Da das Berufsgeheimnis jedoch beachtet werden muss, kann eine solche Information unterbleiben.

7. Abschließende Anmerkung

Dieser Artikel soll Ärzten im realen Praxisalltag weiterhelfen und wird die eine oder andere Frage sicher beantworten können. Er ist jedoch bitte nicht als allumfassende Handlungshilfe zu verstehen, die bei penibler Einhaltung ein zu 100 % datenschutz- oder datensicherheitskonformes Agieren ermöglicht, bei dem sonst nichts mehr beachtet werden muss. Dafür reicht die vorgegebene Artikellänge (die ich zugegebenermaßen bei weitem gesprengt habe) leider nicht aus.

Sofern ein Arzt nun aber versucht, weite Teile dieses Artikels für seine Praxis zu nutzen oder dies sogar schon umgesetzt hat, so hat er schon einen großen Schritt in Richtung Datenschutz- und Datensicherheitskonformität gemacht.

Zum Schluss darf ich allen Leserinnen und Lesern noch Alles Gute mit dem Datenschutz, der Datensicherheit und auch für Ihre Ordination im Allgemeinen wünschen!

Mag. Kerstin Garbeis, LL.M.

*Juristin und Gruppenleiterin Projekte & Kommunikation,
Ärztchammer für Oberösterreich*

Ärztliches Berufsgeheimnis

1. Gesetzliche Absicherung der ärztlichen Verschwiegenheitspflicht	96
2. Ärztliches Berufsgeheimnis nach § 54 Abs 1 ÄrzteG	97
3. Ausnahmen vom ärztlichen Berufsgeheimnis	99
4. Sanktionen bei Verletzung des Berufsgeheimnis	106
5. FAQs zur ärztlichen Verschwiegenheitspflicht	107

Die ärztliche Schweigepflicht hat im österreichischen Gesundheitswesen einen hohen Stellenwert. Der vorliegende Beitrag erläutert, wie diese im Gesetz abgesichert ist, was es dabei in der Praxis zu beachten gilt, welche Ausnahmen von der Schweigepflicht bestehen und wann der Arzt sogar Auskunftspflicht hat. Außerdem schildert er, welche strafrechtlichen Maßnahmen die Verletzung der ärztlichen Schweigepflicht zur Folge haben kann. Zum Abschluss werden die wichtigsten Fragen zur Verschwiegenheitspflicht zusammengefasst dargestellt und beantwortet.

1. Gesetzliche Absicherung der ärztlichen Verschwiegenheitspflicht

Die Schweigepflicht, die gerade im Gesundheitsbereich ein besonders sensibles Gut darstellt, ist in der österreichischen Rechtsordnung mehrfach, auch strafrechtlich, abgesichert.

- Nach § 121 StGB machen sich Personen, die ein Geheimnis offenbaren oder verwerten, das den Gesundheitszustand einer Person betrifft und das ihnen bei berufsmäßiger Ausübung eines gesetzlich geregelten Gesundheitsberufes (zum Beispiel Ärztinnen und Ärzte) anvertraut wurde und damit ein berechtigtes Interesse der geschützten Person verletzt wird, strafbar.¹
- Darüber hinaus sind die Bestimmungen des § 9 KAKuG und die entsprechenden landesgesetzlichen Ausführungsbestimmungen zu beachten. Nach § 9 Absatz 1 besteht eine Verschwiegenheitspflicht für alle bei den Trägern von Krankenanstalten und in den Krankenanstalten beschäftigten Personen sowie für weitere Personen² bezüglich des Gesundheitszustands, aber auch aller anderen persönlichen, wirtschaftlichen und sonstigen Verhältnisse des Patienten, die in Ausübung des Berufs bekannt geworden sind. Bei Organtransplantationen auch hinsichtlich der Person des Spenders und des Empfängers. Anzumerken ist, dass § 9 KAKuG nur subsidiäre Anwendung findet, soweit nicht bereits aufgrund anderer gesetzlicher oder dienstrechtlicher Vorschriften eine Verpflichtung zur Verschwiegenheit besteht.³
- Zivilrechtliche Absicherung der Schweigepflicht durch § 1328a ABGB in Form eines Schadenersatzanspruches gegen jene Personen die rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreifen oder Umstände aus der Privatsphäre eines Menschen offenbaren bzw. verwerten.

1 Bei § 121 StGB handelt es sich um ein Privatanklagedelikt, wobei die Begehung mit einer Freiheitsstrafe von bis zu sechs Monaten oder mit einer Geldstrafe von bis zu 360 Tagessätzen bedroht ist.

2 Mitglieder von Ausbildungskommissionen und die Mitglieder von Kommissionen zur Beurteilung klinischer Prüfungen

3 *Stöger* in GmundKomm § 9 KaKuG Rz 1: Von Lit und Rechtspraxis wird § 9 KAKuG so ausgelegt, dass dieser alle Berufsgruppen, die aufgrund anderer gesetzlicher Grundlagen zur Verschwiegenheit verpflichtet sind, vom Anwendungsbereich des § 9 KAKuG nicht umfasst sind.

- Für Ärzte besteht ein berufsrechtlicher Schutz des ärztlichen Berufsgeheimnisses nach § 54 ÄrzteG.

Dieser Beitrag wird in der Folge die Pflichten zur ärztlichen Verschwiegenheit, die gesetzlich normierten Ausnahmen, sowie Melde- und Anzeigepflichten, darstellen.

2. Ärztliches Berufsgeheimnis nach § 54 Abs. 1 ÄrzteG

2.1. Inhalt und Grundlagen

Das ärztliche Berufsgeheimnis bildet eine wesentliche Säule der ärztlichen Berufspflichten: Nach Abs. 1 sind der Arzt und seine Hilfspersonen zur Verschwiegenheit über alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse verpflichtet. Anders als bei § 121 StGB sind vom Berufsgeheimnis alle persönlichen, gesellschaftlichen und psychosozialen Umstände des Patienten geschützt. Der Geheimnisbegriff umfasst dabei sowohl eine objektive als auch eine subjektive Komponente. Bei der **objektiven Komponente** geht es darum, dass es sich bei einem Geheimnis um Tatsachen handeln muss, die nur dem Geheimnisträger selbst oder einem beschränkten Personenkreis bekannt sind. Geschützt ist ein Geheimnis aber nur dann, wenn es sich bei den Tatsachen, die nur einem beschränkten Personenkreis bekannt sind, um solche handelt, bezüglich derer ein **subjektives** Interesse des Geheimnisträgers besteht, sie Außenstehenden nicht bekannt zu machen. Neben diesen beiden Komponenten wird von Hon.-Prof. Dr. Felix Wallner einem weiteren dritten Tatbestandsmerkmal eigenständige Bedeutung beigemessen: Laut Wallner⁴ handelt es sich erst dann um ein Geheimnis, wenn eine **Schutzwürdigkeit des Geheimhaltungsinteresses**

4 Wallner, Grenzen der Verschwiegenheitspflicht der Gesundheitsberufe, RdM 2013/106.

ses besteht. Nur jene Informationen, an denen ein berechtigtes Interesse zur Geheimhaltung besteht, sind von der Verschwiegenheitspflicht umfasst.⁵

Die Pflicht zur Wahrung des Berufsgeheimnisses i.S.d. § 54 Abs. 1 ÄrzteG gilt in gleichem Maß für angestellte, niedergelassene und Wohnsitzärzte⁶, grundsätzlich auch gegenüber anderen Ärzten und endet nicht mit der Beendigung der ärztlichen Tätigkeit oder dem Tod des Arztes.⁷

2.2. Zweck

Als eines der Hauptargumente für die Verschwiegenheitspflicht des Arztes werden von Literatur und Judikatur⁸ immer wieder die Gewährleistung eines vertrauensvollen Verhältnisses zwischen Arzt und Patient genannt: Auf der einen Seite soll sich der Patient dem Arzt umfassend anvertrauen können, ohne befürchten zu müssen, dass Dritte von diesen vertrauensvollen, sensiblen Gesprächen und somit etwas über den Gesundheitszustand des Patienten erfahren. Auf der anderen Seite benötigt der Arzt aber einen möglichst umfassenden Informationsstatus des Patienten, um diesen erfolgreich (heil)behandeln zu können.

5 Schutzwürdigkeit des Geheimhaltungsinteresses liegt beispielsweise dann nicht vor, wenn Patienten in, von ihnen angestregten Schadenersatzverfahren, die Sachverhaltsermittlung durch Berufung auf das ärztliche Berufsgeheimnis verhindern.

6 *Schneider*, Ärztliche Ordinationen und selbständige Ambulatorien, 327.

7 *Wallner*, Ärztliches Berufsrecht² (2018), 173.

8 VwGH 16.9.1986, 85/14/007 sowie unter anderem *Stolzlechner*, Überlegungen zur ärztlichen Verschwiegenheits-Anzeige- und Meldepflicht, RdM 2000, 67.

3. Ausnahmen vom ärztlichen Berufsgeheimnis

Vom Grundsatz der Verschwiegenheit sieht der Gesetzgeber in den §§ 54 Abs. 2 ff. ÄrzteG mehrere Ausnahmen vor.

3.1. Meldepflichten des Arztes (Abs. 2 Z 1)

Die Verschwiegenheitspflicht besteht dann nicht, wenn „nach gesetzlichen Vorschriften eine Meldung der Ärztin/des Arztes über den Gesundheitszustand bestimmter Personen vorgeschrieben ist.“ Die Anzeigepflichten nach Abs. 4 des § 54 ÄrzteG⁹ stellen eine solche Meldepflicht dar. Weitere gesetzliche Meldepflichten finden sich unter anderem im Epidemiegesetz, Geschlechtskrankheitengesetz, AIDS-Gesetz und Tuberkulosegesetz. Daneben sind nach § 57 AMG Arzneimittelnebenwirkungen zu melden sowie beispielsweise auch Zwischenfälle i.Z.m. der Verarbeitung, Lagerung und Verteilung von Bluttransfusionen oder Transfusionen von Blutbestandteilen.

3.2. Mitteilungen oder Befunde an Kostenträger (Abs. 2 Z 1 sowie Abs. 3)

Keine Verschwiegenheitspflicht besteht bei der Übermittlung von Mitteilungen oder Befunden des Arztes an die Sozialversicherungsträger und Krankenfürsorgeanstalten oder sonstigen Kostenträger in dem Umfang, als es für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet und erforderlich ist. Seit der Ärztegesetz-Novelle 1998 wurde die Ausnahmeregelung der Sozialversicherungsträger, um Krankenfürsorgeanstalten und sonstige Kostenträger erweitert. Laut Gesetzesmaterialien¹⁰ zur ÄrzteG-Novelle soll damit auf Konstellationen Bedacht genommen werden, in welchen die Kosten

9 Siehe Seite 6, „Anzeigepflicht bei gerichtlich strafbaren Handlungen“.

10 ErläutRV 1386 20. GP, Seite 96.

für die krankheitsvorbeugenden ärztlichen Maßnahmen von Gebietskörperschaften übernommen werden.¹¹

Der Umfang der Übermittlungspflicht hängt vom jeweiligen Honorierungssystem ab.¹² Bei reinen Pauschalhonorierungssystemen, die keine Rücksicht auf die jeweiligen Einzelleistungen nehmen, wird die Pflicht zur Verschwiegenheit viel enger auszulegen sein als bei Honorarsystemen, die bei der Abrechnung auf Einzelleistungen abstellen.¹³ Im Zusammenhang mit der Abrechnung von Einzelleistungen darf unter anderem auf das „Ökonomiegebot“ des § 133 Abs. 2 S 1 ASVG¹⁴ verwiesen werden. Die Einhaltung des Ökonomiegebots kann nur so weit überprüft werden, als dem Sozialversicherungsträger umfangreichere Daten, als bei der Pauschalabrechnung zur Verfügung gestellt werden müssen. Allerdings ist auch hier nur die Übermittlung jener Daten notwendig, die zur Überprüfung der verrechneten Leistungen unbedingt erforderlich sind.¹⁵

Die Ausnahmebestimmung des Abs. 2 Z 1 ist nicht auf private Krankenversicherungsunternehmen anwendbar, greift doch in derartigen Konstellationen die ausdrückliche gesetzliche Bestimmung nach § 11b VersVG. Danach dürfen Gesundheitsdaten an private Unternehmen dann übermittelt werden, wenn diese für die Beurteilung der Deckungszusage notwendig sind und der Versicherte bzw. Patient dem Leistungserbringer (z.B. Krankenhaus) einen Auftrag zur Direktverrechnung mit der Versicherung erteilt hat. Eine darüber hinausgehende Datenweitergabe ist nach § 11a VersVG nur mit vorheriger schriftlicher Genehmigung des Versicherungsnehmers zulässig.

Nach § 54 Abs. 3 ÄrzteG besteht eine Verschwiegenheitspflicht des Arztes auch insoweit gegenüber den Krankenversicherungsträgern, Krankenanstalten, sonstigen Kostenträgern nicht, als diese Unterlagen für die Honorar- oder Medikamentenabrechnung automationsunterstützt übermittelt werden.

11 Z.B. Impfungen an Jugendlichen oder MuKiPa-Impfungen laut Impfpass sowie Länder als Sozialhilfeträger, wenn diese für die Abdeckung der Krankenbehandlung herangezogen werden, vgl. VwGH 16.6.2009, 2008/10/0007. Insgesamt sind aber unter den Begriff der „sonstige Kostenträger“ nur solche Stellen zu subsumieren, welche auch tatsächlich die Kosten der ärztlichen Behandlung tragen.

12 *Stolzlechner*, Überlegungen zur ärztlichen Verschwiegenheits- Anzeigepflicht, RdM 2000, 69.

13 Z.B. Fallpauschalen, die sich nach dem Alter des Patienten richten: Übermittlung lediglich des Namens und Alters des Patienten zulässig.

14 § 133 Abs. 2 S1 ASVG lautet: Die Krankenbehandlung muss ausreichend und zweckmäßig sein. Sie darf jedoch das Maß des Notwendigen nicht überschreiten.

15 So auch BVwG (BVwG W178 2111326-1) bezüglich einer Bestimmung des Wiener Ärzte-Gesamtvertrages, wonach diese keinen Selbstzweck verfolgen, sondern es immer darum ginge dem Krankenversicherungsträger die Beurteilung zu erleichtern, ob bei der Krankenbehandlung das Maß des Notwendigen überschritten worden bzw. eine Leistung tatsächlich erbracht worden sei.

3.3. Entbindung durch den Patienten (Abs. 2 Z 3)

Eine Entbindung von der Verschwiegenheitspflicht ist jederzeit durch die von der Offenbarung des Geheimnisses bedrohte Person – in den meisten Fällen der Patient – möglich. Im Hinblick darauf, dass es sich bei der Möglichkeit zur Entbindung um ein höchstpersönliches Recht¹⁶ handelt, entscheidet über den Umfang der Entbindung immer die betroffene Person selbst – auch bei minderjährigen Personen.¹⁷ Die Entbindung an sich muss nicht schriftlich erfolgen. Bei mündlicher Entbindung ist ein entsprechender Vermerk in der Patientendokumentation zu empfehlen, da die ärztliche Dokumentation Beweiskraft besitzt. Fälle, in denen der Patient nicht in der Lage ist, zu entbinden (z.B. Bewusstlosigkeit) und somit eine Information über den Gesundheitszustand des Patienten an die Angehörigen nicht möglich wäre, lassen sich in der Praxis durch das Rechtsinstrument der „mutmaßlichen Einwilligung“¹⁸ lösen: Der Patient würde einer Weitergabe der Informationen mit hoher Wahrscheinlichkeit zustimmen, wäre er dazu imstande. Die österreichische Literatur¹⁹ sieht in der mutmaßlichen Einwilligung einen eigenständigen Rechtfertigungsgrund zur Durchbrechung der ärztlichen Schweigepflicht. Folgt man hier der Argumentation von Wallner, dass es in solchen Fällen am Tatbestandserfordernis des „Geheimhaltungsinteresses“ des Patienten fehle, liegt überhaupt kein Geheimnis vor und die Regeln über die Ärztliche Verschwiegenheitspflicht kommen nicht zur Anwendung.²⁰

3.4. Durchbrechung zum Schutz höherwertiger Interessen (Abs. 2 Z4)

Zum Schutz höherwertiger Interessen im Sinne der öffentlichen Gesundheitspflege und der Rechtspflege ist ebenfalls eine Durchbrechung der ärztlichen Verschwiegenheitspflicht möglich. Neben diesen beiden explizit genannten Fällen ist eine Durchbrechung nach der Rechtsprechung des OGH bei Vorliegen eines höherwertigen Interesses im Allgemeinen möglich.²¹ Um die Besonderheit der ärztlichen Verschwiegenheitspflicht nicht auszuhöhlen, ist eine Durchbrechung allerdings nicht zum Schutz von materiellen Gütern, sondern immer nur bei Gefährdung von Leib und Leben zulässig. Die Interessenabwägung hat dabei immer

16 Das Recht ist nicht an eine andere Person übertragbar.

17 § 173 ABGB: Zweifelsregel für Einwilligung in medizinische Behandlungen an Minderjährigen.

18 OGH 23.5.1984, 1 Ob 550/84 sowie OGH 27.7.2017, 2 Ob 162/16m.

19 Riesz, Ärztliche Verschwiegenheitspflicht, 83.

20 Wallner, Grenzen der Verschwiegenheitspflicht der Gesundheitsberufe, RdM 2013/106.

21 OGH 12.12.2002, 6 Ob 267/02m.

der betroffene Arzt an sich durchzuführen, wobei das Interesse an Geheimhaltung umso höher zu bewerten ist, je schwerwiegender die Konsequenzen der Durchbrechung für die betroffene Person sind.²² In behördlichen Verfahren ist zu unterscheiden, ob es sich um ein zivilgerichtliches Verfahren, Verwaltungsverfahren oder Strafverfahren handelt. In zivilgerichtlichen Verfahren, aber auch in Verwaltungsverfahren beziehungsweise Verwaltungsstrafverfahren kommt dem Arzt als Zeugen grundsätzlich ein Entschlagungsrecht zu, wenn er „eine ihm obliegende, staatlich anerkannte Pflicht zur Verschwiegenheit“ verletzt wurde, soweit keine Entbindung vorliegt.²³ Der Arzt hat in diesen Verfahren daher eine Interessenabwägung zwischen den Interessen der von der Offenbarung des Geheimnisses bedrohten Person und den Interessen der Rechtspflege wahrzunehmen und dann auszusagen, wenn diese Interessenabwägung zugunsten der Rechtspflege ausgeht. Da im gerichtlichen Strafverfahren kein Entschlagungsrecht für Ärzte, mit Ausnahme der Fachärzte für Psychiatrie und psychotherapeutische Medizin enthalten ist, haben diese im Strafverfahren grundsätzlich auszusagen und sind auch verpflichtet, ihre ärztliche Dokumentation herauszugeben.

Die Offenbarung des Geheimnisses ist auch bei einwilligungsunfähigen Patientinnen und Patienten zulässig, als es im Zusammenhang mit der Bereitstellung der für die Behandlungskontinuität unerlässlichen Eckdaten gegenüber den mit der Pflege betrauten Personen erforderlich ist.

3.5. Durchbrechung gegenüber anderen Ärzten zur Aufklärung einer gerichtlich strafbaren Handlung gegenüber Kindern und Jugendlichen (Abs. 2 Z5)

Diese Ausnahme, die im Rahmen der Gewaltschutzgesetznovelle 2019 in das Ärztegesetz aufgenommen wurde, soll zur leichteren Verifizierung bzw. Falsifizierung von Misshandlungs- oder Missbrauchsverdachtsfällen²⁴ beitragen und soll einen ärztlichen Beitrag leisten, um Kindesmisshandlungen oder Kindesmissbrauch entgegenzuwirken.

22 Wallner, *Ärztliches Berufsrecht* 2 (2018), 180f.

23 § 321 Abs. 1 Z 3 ZPO, § 49 Abs. 1 Z 2 AVG sowie § 24 VStG.

24 Misshandeln, quälen, vernachlässigen oder sexuell missbrauchen.

3.6. Anzeigepflicht bei gerichtlich strafbaren Handlungen (Abs. 4)

Im Rahmen des neuen Gewaltschutzgesetzes 2019 wurden neben umfangreichen Änderungen im Strafgesetzbuch auch Änderungen bei der Anzeige- und Meldepflicht in den Berufsgesetzen der Gesundheitsberufe vorgenommen. So kommt es auch zu Änderungen bei § 54 ÄrzteG. Das Ziel der Gesetzesreform war es, klare, einheitliche und effektive Regelungen der Anzeigepflicht der betroffenen Berufsgruppen in den einzelnen Berufsgesetzen zu schaffen.²⁵

Nach § 54 Abs. 4 ÄrzteG ist ein Arzt zur Anzeige an die Kriminalpolizei (= „normale“ Polizeidienststelle) oder die Staatsanwaltschaft verpflichtet, wenn sich bei der Ausübung der beruflichen Tätigkeit der begründete Verdacht ergibt, dass durch eine gerichtlich strafbare Handlung

a. der Tod, eine schwere Körperverletzung²⁶ oder eine Vergewaltigung herbeigeführt wurde (Abs. 4 Z 1)

Ziffer 1 wurde zugunsten der Zielrichtung des Schutzes insbesondere von Frauen und Kindern um den Straftatbestand der Vergewaltigung erweitert. Diese Erweiterung ist in der Praxis zu begrüßen, können doch damit bisher schwierige Grenzfälle einer Vergewaltigung, die selbst noch keine schwere Verletzung zur Folge hatten, für den behandelnden Arzt zukünftig besser eingeordnet werden.

b. Kinder oder Jugendliche misshandelt, gequält, vernachlässigt oder sexuell missbraucht werden oder worden sind (Abs. 4 Z 2)

Ziffer 2 entspricht dem bisherigen Abs. 5 und kann bei mutmaßlichen minderjährigen Opfern nach Abs. 6 weiterhin eine Anzeige unterbleiben, wenn sich der Verdacht gegen einen Angehörigen im Sinne des § 72 StGB²⁷ richtet,

²⁵ 157/ME 26. GP 1.

²⁶ Der Begriff der schweren Körperverletzung ist nach § 84 StGB zu beurteilen. Demnach handelt es sich dann um eine schwere Körperverletzung, wenn diese oder die Gesundheitsschädigung länger als 24 Tage dauert oder die Körperverletzung an sich schwer ist. An sich schwere Körperverletzung: Wichtige Organe oder Körperteile sind in einer Weise beeinträchtigt, dass damit wesentliche Funktionseinbußen oder erhebliche Veränderungen des äußeren Erscheinungsbildes verbunden sind.

²⁷ Verwandte und Verschwägte in gerader Linie, Ehegatte oder eingetragener Partner und die Geschwister des Ehegatten oder eingetragenen Partners, Geschwister und deren Ehegatten oder eingetragene Partner, Kinder und Enkel, die Geschwister der Eltern und Großeltern, Vettern und Basen, der Vater oder die Mutter ihres Kindes, Wahl- und Pflegeeltern, Wahl- und Pflegekinder, sowie Personen, über die die Obsorge zusteht oder unter deren Obsorge diese stehen, zu verstehen. Ebenfalls wie Angehörige werden Personen behandelt, die miteinander in Lebensgemeinschaft leben sowie Kinder und Enkel von diesen.

dies das Wohl des Kindes oder Jugendlichen erfordert und eine Mitteilung an die Kinder- und Jugendhilfeträger bzw. eine Einbeziehung der einer Kinderschutzeinrichtung an einer Krankenanstalt erfolgt. Hier wurde der Kreis der Angehörigen erweitert – bestand doch bisher nur bei nahen Angehörigen eine Ausnahme.

- c. Nicht handlungs- oder entscheidungsfähige oder wegen Gebrechlichkeit, Krankheit oder einer geistigen Behinderung wehrlose Volljährige misshandelt, gequält, vernachlässigt oder sexuell missbraucht werden oder worden ist.**

3.7. Ausnahmen von der Anzeigepflicht

Durch das Gewaltschutzgesetz 2019 wurden Ausnahmen von der ärztlichen Anzeigepflicht in das ÄrzteG aufgenommen. Nach § 54 Abs. 5 ÄrzteG besteht keine Pflicht zur Anzeige, wenn

- 1. Die Anzeige dem ausdrücklichen Willen des volljährigen handlungs- oder entscheidungsfähigen Patienten widersprechen würde, sofern keine unmittelbare Gefahr für diesen oder eine andere Person besteht und die klinisch-forensischen Spuren ärztlich gesichert sind**

Diese Änderung, die erst im Zuge eines Abänderungsantrages während der Sitzung des Nationalrates, in der über das Gewaltschutzgesetz abgestimmt wurde, aufgenommen wurde, soll der Stärkung des Opferschutzes²⁸ dienen. Für behandelnde Ärzte eröffnet sich damit eine schwer zu lösende Konfliktsituation, in der sie das Für und Wider einer Anzeige abwägen müssen: Zum einen sollen Opfer einer gerichtlichen Straftat selbst entscheiden können, wie sie mit Verletzungen, die durch eine solche Handlung herbeigeführt wurden, umgehen wollen, zum anderen muss aber der Arzt beurteilen und entscheiden, ob tatsächlich keine unmittelbare Gefahr für die verletzte oder andere Personen besteht. Gerade in Fällen von häuslicher Gewalt, bei welchen z.B. der Ehemann schwört, dass er seine Ehefrau nie wieder schlagen wird, stehen die Opfer oftmals unter starkem psychischem Druck und sprechen sich eher gegen eine Anzeige aus. Für den behandelnden Arzt wird es trotz neuer Rechtslage ratsam sein, derartige Verletzungen weiterhin anzuzeigen, muss doch dieser die schwierige Entscheidung treffen, ob weiterhin eine unmittelbare Gefahr für das Opfer oder eine dritte Person besteht. Bei einer Verletzung, die als schwer einzustufen ist, wird wohl in den meisten Fällen eher von einer weiterhin bestehenden unmittelbaren Gefahr auszugehen

28 AA-150 26. GP14.

sein. Eine Anzeige kann aber allenfalls dann unterbleiben, wenn der Behandler die Nichtanzeige gut begründen kann und diese Gründe auch in der Dokumentation festgehalten werden.

2. Die Anzeige im konkreten Fall die berufliche Tätigkeit beeinträchtigen würde, deren Wirksamkeit eines persönlichen Vertrauensverhältnisses bedarf, sofern nicht eine unmittelbare Gefahr für diese oder eine andere Person besteht.

Im Detail geht es bei diesem Ausnahmetatbestand um Fälle, bei denen ein Absehen von der Anzeigepflicht zur Wahrung eines Vertrauensverhältnisses, das zur weiteren Behandlung unerlässlich ist, notwendig ist. Diese Ausnahme, die auf Drängen der Berufsgruppe der Psychotherapeuten mittels Initiativantrags in das Gesetz aufgenommen wurde, gilt nicht nur für diese Berufsgruppe, sondern selbstverständlich auch für alle Ärzte. Beruht doch gerade das Arzt-Patienten-Verhältnis auf einem besonderen Vertrauensverhältnis, welches die Basis jeder ärztlichen Behandlung darstellt. Die Erforderlichkeit einer Anzeige wird im Einzelfall im Zuge einer berufsspezifischen Interessenabwägung in erster Linie anhand fachlicher Kriterien zu beurteilen sein.²⁹

3. Der Arzt, der seine berufliche Tätigkeit im Dienstverhältnis ausübt, eine entsprechende Meldung an den Dienstgeber erstattet hat und durch diesen eine Anzeige an die Kriminalpolizei oder Staatsanwaltschaft erfolgt ist.

Da es für die Strafverfolgung eher hinderlich wäre, wenn mehrfach Anzeigen zur selben Straftat bei der Sicherheitsbehörde eingehen, kann für Verdachtsfälle eine Anzeige durch den behandelnden Arzt dann unterbleiben, wenn derartige Fälle im Dienstweg gemeldet werden und die Anzeige durch den Dienstgeber erfolgt. Eine direkte Meldung ohne Einhaltung des Dienstwegs ist bei Gefahr im Verzug oder bei „*fehlender Bereitschaft des Dienstgebers zur Anzeige*“ möglich bzw. geboten.³⁰

29 970/A 26. GP 48.
30 970/A 26. GP 48.

4. Sanktionen bei Verletzung des Berufsgeheimnis

Ein Verstoß gegen die ärztliche Verschwiegenheitspflicht kann auf mehrere Arten geahndet werden. Zum einen droht eine strafrechtliche Verurteilung nach § 121 StGB, wenn diejenige Person, die vom Verstoß betroffen ist, einen entsprechenden Antrag stellt. Alternativ besteht die Möglichkeit einer verwaltungsstrafrechtlichen Verurteilung nach § 199 Abs. 3 ÄrzteG durch die zuständige Bezirksverwaltungsbehörde mit einer Geldstrafe von bis zu € 2.180. Schlussendlich begeht der Arzt durch die Verletzung des Berufsgeheimnisses ein Disziplinarvergehen nach § 136 Abs. 1 Z2 ÄrzteG. Zuletzt hat hier der VfGH entschieden, dass eine disziplinare Verurteilung nur dann möglich ist, wenn derselbe Arzt wegen derselben Tat nicht bereits anderweitig bestraft wurde.³¹ Unter Umständen wird der Arzt auch schadenersatzpflichtig, wenn die betroffene Person einen Schaden erleidet.

31 VfGH 17.12.2009, B 446/09.

5. FAQs zur ärztlichen Verschwiegenheitspflicht

Welche Informationen unterliegen dem ärztlichen Berufsgeheimnis?

Geschützt sind alle Tatsachen und Informationen, die nicht allgemein zugänglich sind und bei denen ein Interesse des Betroffenen besteht, diese geheim zu halten. Unter den Geheimnisbegriff fallen nicht nur Informationen über den betroffenen Patienten selbst, sondern auch Informationen über Dritte, die dem Arzt im Zuge der Berufsausübung bekannt werden.

Gilt die ärztliche Verschwiegenheitspflicht auch gegenüber Berufskollegen?

Die ärztliche Verschwiegenheitspflicht gilt grundsätzlich gegenüber jedermann, d.h. auch gegenüber Berufskollegen. Sind in einen ärztlichen Behandlungsprozess mehrere Ärzte eingebunden (z.B. Zuweisung an einen Facharzt oder Übermittlung einer Blutprobe an einen Facharzt für medizinisch-chemische Labordiagnostik), kann von einer konkludenten Zustimmung des Patienten ausgegangen werden.

Wer kann den Arzt von der ärztlichen Schweigepflicht entbinden?

Da es sich bei der ärztlichen Verschwiegenheitspflicht um ein höchstpersönliches Recht des Betroffenen handelt, kann auch nur dieser selbst den Arzt von dieser Pflicht entbinden. Dieser Grundsatz gilt auch bei Minderjährigen – soweit diese über die nötige Entscheidungsfähigkeit verfügen, können nur sie selbst entbinden.

Muss eine Entbindung von der ärztlichen Verschwiegenheitspflicht schriftlich erfolgen?

Nein, grundsätzlich sind an die Entbindung keine Formerfordernisse geknüpft. Für Ärzte ist es allerdings ratsam, eine mündliche Entbindungserklärung in die ärztliche Dokumentation aufzunehmen, da diese Beweiskraft besitzt. Entbindungserklärungen gegenüber privaten Versicherern müssen allerdings schriftlich erfolgen.

Hat der Arzt als Zeuge in behördlichen Verfahren auszusagen?

In einem gerichtlichen Zivilverfahren, in Verwaltungsverfahren und auch in Verwaltungsstrafverfahren ist der Arzt an die ärztliche Verschwiegenheitspflicht gebunden und muss die Aussage verweigern, außer er wurde zuvor vom Patienten entbunden. Daneben ist eine Aussage dann zulässig, wenn eine Interessenabwä-

gung zwischen den Interessen des Betroffenen und der Rechtspflege ergibt, dass die Interessen der Rechtspflege als höherwertig einzuschätzen sind.

Gilt die ärztliche Schweigepflicht im Verfahren über Obsorgeangelegenheiten?

Steht das Wohl von minderjährigen Kindern während ihrer Entwicklungsphase auf dem Spiel, besteht nach Auffassung des OGH keine berufliche Verschwiegenheitspflicht des Arztes und er hat in einem solchen Verfahren auszusagen.

Darf ein Arzt im Strafverfahren aussagen?

Er darf nicht nur, er muss sogar aussagen. Die Möglichkeit zur Entschlagung bzw. Aussageverweigerung besteht lediglich für Fachärzte für Psychiatrie und psychotherapeutische Medizin.

Ist der Arzt an das Berufsgeheimnis bei eigenen Angelegenheiten gebunden?

Wenn ein Arzt selbst einen Patienten verklagt (z.B. nicht bezahltes Honorar) oder von einem Patienten verklagt wird (z.B. Klage auf Schadenersatz), ist der Arzt nicht an die ärztliche Schweigepflicht gebunden.

Gibt es eine Anzeigepflicht bei Hundebissen?

Nicht jeder Hundebiss ist meldepflichtig. Eine gesetzliche Meldepflicht besteht nach § 1 Abs. 1 Z 1 Epidemiegesetz lediglich bei Bissverletzungen durch wutkranke- oder verdächtige Tiere. Eine derartige Anzeige hat binnen 24 Stunden an die Bezirksverwaltungsbehörde, in deren Gebiet sich der Kranke oder Krankheitsverdächtige aufhält oder der Tod eingetreten ist, zu erfolgen.

Konsequenzen bei Verletzung des Berufsgeheimnisses für den Arzt?

Auf Antrag des vom Berufsgeheimnis Geschützten kann der Arzt strafrechtlich verurteilt werden. Außerdem drohen eine Strafe durch die Bezirksverwaltungsbehörde sowie ein Disziplinarverfahren. Erleidet der Patient einen Schaden, kann der Arzt auch zu Schadenersatzzahlungen verurteilt werden.

Univ.-Prof. Dr. Alois Birklbauer

**Abteilung für Praxis der Strafrechtswissenschaften und Medizinstrafrecht
der Universität Linz**

Die Achtung der ärztlichen Verschwiegenheit in einem Strafverfahren

1. Grundlagen der ärztlichen Verschwiegenheitspflicht	110
2. Die Aussagepflicht von Ärztinnen und Ärzten in einem allfälligen Strafverfahren	113
3. Die Sicherstellung von Patientenunterlagen trotz ärztlicher Verschwiegenheitspflicht	118
4. Zusammenfassende Schlussfolgerungen	121

Die ärztliche Verschwiegenheit ist ein hohes Gut. Sie bildet jene Vertrauensbasis für Patientinnen und Patienten, derer es bedarf, damit sie den Ärztinnen und Ärzten die entsprechenden Informationen für Diagnose und Behandlung geben. Das Ausmaß des Vertrauens ist entscheidend davon geprägt, ob bzw. inwieweit die behandelnden Ärztinnen und Ärzte diese Verschwiegenheit auch gegenüber staatlichen Behörden zu wahren haben. Die folgenden Überlegungen zeigen Defizite bei den gesetzlichen Vorschriften über die ärztliche Verschwiegenheitspflicht im Zusammenhang mit einem allfällig geführten Strafverfahren auf. Dabei soll zunächst die Verankerung der Verschwiegenheitspflicht in den entsprechenden materiell-rechtlichen Bestimmungen aufgezeigt werden, mit der der Gesetzgeber deren Wichtigkeit zu unterstreichen versucht. Daran anschließend soll auf ausgewählte strafprozessuale Vorschriften eingegangen werden, die zum einen die für Ärztinnen und Ärzte bestehende Möglichkeit, ihre Aussage zu verweigern, regeln, zum anderen den Ermittlungsbehörden Möglichkeiten einräumen, Behandlungsunterlagen sicherzustellen und die daraus gewonnenen Ergebnisse in einem Strafverfahren zu verwerten. Zusammenfassende Schlussfolgerungen bilden das Ende des Beitrags.

1. Grundlagen der ärztlichen Verschwiegenheitspflicht

1.1. Berufsrechtliche Regelung

Berufsrechtlich ist die ärztliche Verschwiegenheitspflicht gemeinsam mit der Anzeige- und Meldepflicht in § 54 Ärztegesetz (ÄrzteG) geregelt. Sie betrifft nach dessen Abs. 1 Ärztinnen und Ärzte sowie ihre Hilfspersonen gleichermaßen und umfasst alle ihnen in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse. Abs. 2 durchbricht die Verschwiegenheitspflicht für verschiedene Konstellationen, unter anderem für den Fall, dass nach gesetzlichen Vorschriften eine Meldepflicht über den Gesundheitszustand bestimmter Personen besteht (Z 1), die durch die Offenbarung des Geheimnisses bedrohte Person die Ärztin bzw. den Arzt von der Geheimhaltung entbunden hat (Z 3) oder die Offenbarung des Geheimnisses zum Schutz höherwertiger Interessen unbedingt erforderlich ist (Z 4), wobei unter dieser Ziffer die Rechtspflege explizit genannt ist (lit. b).

Die Verletzung der ärztlichen Verschwiegenheitspflicht bildet eine Verwaltungsübertretung, die mit Geldstrafe bis zu 2.180 Euro bedroht ist (§ 199 Abs. 3 ÄrzteG). Dabei normiert diese Strafbestimmung eine ausdrückliche Subsidiarität gegenüber einer in die Zuständigkeit der Strafgerichte fallenden Strafnorm.

1.2. Strafrechtliche Regelung

Eine solche gerichtliche Strafnorm bildet der mit „Verletzung von Berufsgeheimnissen“ betitelte § 121 Strafgesetzbuch (StGB). Den Tatbestand verwirklicht nach Abs. 1 unter anderem, wer ein Geheimnis offenbart oder verwertet, das den Gesundheitszustand einer Person betrifft und das ihm bei berufsmäßiger Ausübung eines gesetzlich geregelten Gesundheitsberufes ausschließlich kraft seines Berufes anvertraut worden oder zugänglich geworden ist. Abs. 4 normiert Gleiches für Hilfskräfte.

Da in § 121 StGB auf einen „gesetzlich geregelten Gesundheitsberuf“ abgestellt wird, ist der Anwendungsbereich der genannten Norm insofern weiter als jener des § 54 ÄrzteG, als z.B. auch Physiotherapeuten, Masseur oder Apotheker als

Tatsubjekte in Betracht kommen. Dagegen ist er enger hinsichtlich des Geheimnisschutzes. Werden von § 54 ÄrzteG alle den Ärztinnen und Ärzten „in Ausübung ihres Berufes anvertrauten oder bekannt gewordenen Geheimnisse“ erfasst, zu den z.B. auch solche über Vermögensverhältnisse, ethisch-religiöse Einstellungen oder Liebschaften zählen, so erfasst § 121 StGB nur Geheimnisse, die „den Gesundheitszustand einer Person“ betreffen. Freilich wird auch dieser Bereich durchaus weit verstanden. Es werden nicht nur jene Umstände unter den Schutzbereich der Norm subsumiert, die den physischen, sondern auch solche, die den psychischen Zustand einer Person betreffen.¹ Beispiele dafür sind Schwangerschaften, Fehl- und Totgeburten, Suizidversuche, Umstände aus dem sexuellen Intimbereich, Alkoholabhängigkeit usw.²

Was unter einem „**Geheimnis**“ zu verstehen ist, definieren weder das ÄrzteG noch das StGB näher. Unter allgemeinen Gesichtspunkten können nur Tatsachen davon erfasst sein, die entweder einer Person oder einem sehr **begrenzten Personenkreis bekannt** und anderen Personen nicht oder nur schwer zugänglich sind. Darüber hinaus muss der Betroffene ein **berechtigtes Geheimhaltungsinteresse** haben³, wie etwa an ehelichen, beruflichen oder anderen persönlichen Schwierigkeiten.⁴ Was ohnehin „die Spatzen von den Dächern pfeifen“, ist mangels Kenntnis für einen begrenzten Personenkreis ebenso kein Geheimnis wie Tatsachen, die sich frei im Internet oder sozialen Netzwerken recherchieren lassen, selbst, wenn ein Geheimhaltungsinteresse des Betroffenen bestehen mag.

Als zusätzliches Erfordernis gegenüber § 54 Abs. 1 ÄrzteG verlangt § 121 StGB, dass die Offenbarung oder Verwertung des Geheimnisses geeignet ist, ein berechtigtes Interesse der Person zu verletzen, welche die Tätigkeit der den Gesundheitsberuf ausübenden Person in Anspruch genommen hat. Dabei ist unter „Offenbarung“ jede Mitteilung des Geheimnisses an einen Dritten zu verstehen, dem dieses zumindest noch nicht sicher bekannt war.⁵ Durch das Erfordernis der Eignung, ein **berechtigtes Interesse zu verletzen**, handelt es sich bei § 121 um ein **abstraktes Gefährdungsdelikt**.⁶ Damit kommt es nicht darauf an, dass tatsächlich ein konkret schutzwürdiges Interesse des Betroffenen verletzt wurde, sondern die Möglichkeit der Verletzung reicht bereits aus. Als Beispiel für diese Eignung wird etwa der Gesundheitszustand von Sportlern oder Politikern ge-

1 Leukauf/Steininger/Tipold StGB⁴ § 121 Rz 14; Lewisch in *Wiener Kommentar* (WK)² StGB § 121 Rz 6.

2 Dazu Thiele in *Salzburger Kommentar zum StGB* (SbgK) § 121 Rz 49 f.

3 Lewisch in WK2 StGB § 121 Rz 6; s. auch Erläuternde Bemerkungen zur Regierungsvorlage (EBRV) 1971, 260.

4 OGH P 111/74 = RS010575.

5 Lewisch in WK2 § 121 Rz 7; Thiele in SbgK § 121 Rz 59 f; Fabrizy StGB¹³ § 121 Rz 1; Leukauf/Steininger/Tipold StGB⁴ § 121 Rz 24.

6 Thiele in SbgK § 121 Rz 17.

nannt, soweit er mit deren Tätigkeit in Zusammenhang steht.⁷ Dass die betroffene Person zur geoffenbarten Tatsache öffentlich steht und sie als richtig einräumt, ändert nichts an der Tatbestandserfüllung.

1.3. Rechtfertigung der Verletzung der Verschwiegenheitspflicht

Nach § 121 Abs. 5 StGB ist der Täter nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist. Damit schafft die Norm eine ähnlich gerechtfertigte Durchbrechung der ärztlichen Verschwiegenheitspflicht wie § 54 Abs. 2 ÄrzteG.

Im Gesundheitsbereich lassen sich gegenüber Behörden oder Dritten kaum Gründe für diesen besonderen Rechtfertigungsgrund finden. Denkbar wäre allenfalls die Mitteilung des Gesundheitszustands, der eine Verkehrsuntauglichkeit zur Folge hat, an die Führerscheibehörde, um einen Führerscheinentzug zu bewirken und dadurch riskante Autofahrten des Kranken zu unterbinden.

Eine Rechtfertigung bildet es mit Blick auf die Rechtspflege, was § 54 Abs. 2 Z 4 lit. b ÄrzteG ausdrücklich hervorhebt, wenn Ärztinnen und Ärzte in einem Strafverfahren als Zeuginnen oder Zeugen aussagen müssen und eine Verletzung dieser Aussagepflicht Sanktionen für sie nach sich ziehen würde. Dabei bildet die drohende Sanktionierung zum einen ein „berechtigtes privates Interesse“, das eine Verletzung der Verschwiegenheitspflicht verständlich macht. Zum andern besteht in solchen Fällen auch ein „berechtigtes öffentliches Interesse“ an einer Offenbarung des Gesundheitsgeheimnisses, weil der Gesetzgeber durch die Möglichkeit von Aussageverweigerungs- bzw. Aussagebefreiungsrechten von Zeugen in den jeweiligen Verfahrensvorschriften eine Entscheidung getroffen hat, welche Konstellationen von Interessenskonflikten er bei Zeuginnen und Zeugen anerkennen wollte. Kann ein Zeuge oder eine Zeugin ein solches Recht für sich in Anspruch nehmen, hat das Interesse der Rechtspflege auch an der Aufklärung eines strafrechtlichen Tatbestands zugunsten der schützenswerten Sphäre des Zeugen oder der Zeugin zurückzutreten und sein bzw. ihr individuelles Recht auf Aussageverweigerung Vorrang (zu den Aussageverweigerungs- und Aussagebefreiungsrechten siehe 2.2).

⁷ Lewisch in WK2 StGB § 121 Rz 8.

1.4. Fazit

Zusammenfassend lässt sich zu den vorhandenen strafrechtlichen Normen, welche die ärztliche Verschwiegenheitspflicht betreffen, festhalten, dass jegliche Offenbarung von Geheimnissen, die den Gesundheitsbereich einer Person betreffen – seien diese Teil der Diagnose oder einer Behandlung – tatbestandsmäßig im Sinne von § 121 Abs 1 StGB (und wohl auch § 54 Abs. 1 ÄrzteG) sind, wenn sie durch Ärztinnen oder Ärzte erfolgt. Geschieht dies im Rahmen von gerichtlichen Verfahren, entfällt jedenfalls dann das strafrechtliche Unrecht, wenn der Angehörige des Gesundheitsberufs als Zeuge oder Zeugin vernommen wird und eine unrichtige oder unvollständige Aussage strafrechtliche Sanktionen (falsche Beweisaussage nach § 288 StGB) nach sich ziehen würde. Dies folgt letztlich aus § 121 Abs. 5 StGB (und mittelbar auch aus § 54 Abs. 2 Z 4 lit. b ÄrzteG), der eine Strafbarkeit ausschließt, wenn die Offenbarung durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

2. Die Aussagepflicht von Ärztinnen und Ärzten in einem allfälligen Strafverfahren

In einem Strafverfahren können Personen als Beschuldigte oder Zeugen vernommen werden. Während Beschuldigte aus verfassungsrechtlichen Gründen keine Pflicht zur (wahrheitsgemäßen) Aussage trifft (so genannter Nemo-tenetur-Grundsatz, wonach niemand verpflichtet ist, sich selbst zu belasten; siehe etwa § 7 Abs. 2 Strafprozessordnung [StPO] bzw. Art. 6 der Europäischen Menschenrechtskonvention [EMRK] und Art. 90 Abs. 2 Bundes-Verfassungsgesetz [B-VG]), müssen Zeuginnen und Zeugen richtig und vollständig aussagen (vgl. § 154 Abs. 2 StPO). Infolge der unterschiedlichen Verpflichtungen zur Aussage ist die Einstufung als Beschuldigter oder Zeuge vor Beginn einer Vernehmung durch eine entsprechende Rechtsbelehrung essentiell. Wird diese unterlassen, steht die solcherart als „Erkundigung“ erfolgte Einvernahme unter Nichtigkeitssanktion, weil dadurch die Bestimmungen über die Vernehmung von Beschuldigten und Zeugen in absolut unsachlicher Weise umgangen werden (vgl. § 152 Abs. 1 StPO).

2.1. Vernehmung als Beschuldigter

„Beschuldigter“ ist nach § 48 Abs. 1 Z. 2 StPO jeder Verdächtige, sobald er auf Grund bestimmter Tatsachen konkret verdächtig ist, eine strafbare Handlung begangen zu haben und zur Aufklärung dieses konkreten Verdachts Beweise aufgenommen oder Ermittlungsmaßnahmen angeordnet bzw. durchgeführt werden⁸. Durch das konkrete Verdachtserfordernis grenzt sich der Beschuldigtenbegriff von jenem des „Verdächtigen“ ab. Dazu zählt nach § 48 Abs. 1 Z 1 StPO jede Person, gegen die auf Grund eines Anfangsverdachts (§ 1 Abs. 3 StPO) ermittelt wird. Durch diese erst im Jahre 2014 eingeführte Differenzierung zwischen „Verdächtigen“ und „Beschuldigten“, die sich am Ausmaß des vorhandenen Verdachts orientiert, soll eine geringere Stigmatisierung am Beginn des Strafverfahrens bewirkt werden. Mit Blick auf die Rechte von Beschuldigten und Verdächtigen ist jedoch keine Änderung der bis dahin geltenden Rechtslage eingetreten⁹. § 48 Abs. 2 StPO normiert nämlich, dass – soweit die Bestimmungen der StPO auf den Beschuldigten verweisen und im Einzelnen nichts anderes bestimmt wird – diese Normen auch auf Verdächtige anzuwenden sind. Damit liegt der StPO weiterhin ein so genannter „materieller Beschuldigtenbegriff“ zu Grunde, für den nicht erst ein bestimmtes Verdachtsausmaß Voraussetzung für die Gewährung von Beschuldigtenrechten ist, sondern bereits der geringste Verdacht einer allfälligen Strafbarkeit das Recht einräumt, sich zu verteidigen, wodurch jedenfalls die Pflicht zur wahrheitsgemäßen Aussage oder zur sonstigen Kooperation entfällt und der oben skizzierte Nemo-tenetur-Grundsatz uneingeschränkt gilt¹⁰.

Steht beispielsweise ein Arzt oder eine Ärztin im Verdacht, einen „Kunstfehler“ begangen zu haben, der eine Gesundheitsschädigung beim Patienten oder der Patientin hervorgerufen hat (im Regelfall Verdacht einer fahrlässigen Körperverletzung nach § 88 StGB), besteht keine Pflicht, sich bei der Einvernahme wahrheitsgemäß zu verantworten oder überhaupt mit den Strafverfolgungsbehörden zu kooperieren. Im Gegenteil ist es ratsam, sich zunächst gar nicht zu äußern, sondern Kontakt mit einem Rechtsbeistand aufzunehmen, um das weitere Vorgehen zu besprechen, zumal seitens des Gerichts Erstaussagen häufig zentrale Bedeutung bei der Beweiswürdigung eingeräumt wird (insbesondere, wenn der Vernommene noch nicht anwaltlich beraten war).

8 Grundlegend zum Verdachtserfordernis: Oberlauer, *Der Verdacht. Zum Begriff und Spektrum eines Rechtsbegriffs*, ÖJZ 2018, 62.

9 siehe dazu etwa Swiderski, *Vorüberlegungen zur geplanten Neuregelung des Beschuldigtenbegriffs*, ÖJZ 2014, 402; Soyler/Stuefer in *WK-StPO § 48 Rz 5 f.*

10 Grundlegend zum Nemo-tenetur-Grundsatz Birkbauer, *Die DNA-Analyse im Dienste des Strafverfahrens*, JBl 2003, 337.

Der erwähnte Nemo-tenetur-Grundsatz entbindet nur von der Pflicht, sich durch aktives Verhalten zu belasten, etwa, indem irgendwelche Behandlungsunterlagen oder sonstige Beweismittel den Strafverfolgungsbehörden nicht übergeben werden müssen. Freilich dürfen Beweise, die unabhängig vom Willen des Betroffenen existieren, sichergestellt werden¹¹. Der genannte Grundsatz schützt damit keineswegs vor der Verwendung vorhandener Beweismittel. Insofern kann es ein Beschuldigter auch nicht verhindern, dass eine Durchsuchung seiner Wohnung oder seiner Berufsräumlichkeiten erfolgt, mit dem Ziel, dort verfahrensrelevante Beweismittel zu finden. Solche Beweismittel dürfen sichergestellt und regelmäßig auch verwertet werden, worauf unter Punkt 3 mit Blick auf die ärztliche Verschwiegenheitspflicht noch näher eingegangen wird.

2.2. Vernehmung als Zeugin und Zeuge

Zeuge ist nach § 154 Abs. 1 StPO eine vom Beschuldigten verschiedene physische Person, die zur Aufklärung der Straftat wesentliche oder sonst den Gegenstand des Verfahrens betreffende Tatsachen mittelbar oder unmittelbar wahrgenommen haben könnte und darüber im Verfahren aussagen soll. Durch die Abgrenzung vom Beschuldigtenbegriff („eine vom Beschuldigten verschiedene Person“) kommen als Zeuginnen oder Zeugen nur Personen in Betracht, die sich durch ihre Aussage nicht selbst belasten können. Selbst wenn die Abgrenzung der Rollen „Beschuldigter“ oder „Zeuge“ formeller Natur ist, gibt es in der StPO letztlich eine materielle (inhaltliche) Rollenzuschreibung, zumal jeder Zeuge bei seiner Vernehmung das Recht hat, die Aussage zu verweigern, wenn seine Aussage die Gefahr einer strafgerichtlichen Verfolgung nach sich ziehen würde (§ 157 Abs. 1 Z 1 StPO). Auf diese Aussageverweigerungsmöglichkeit ist ein Zeuge vor Beginn seiner Vernehmung bzw. spätestens dann, wenn während der Vernehmung Anhaltspunkte für eine solche Belastungsmöglichkeit hervorkommen, hinzuweisen (vgl. § 159 Abs. 1 StPO).

Von der bereits erwähnten in § 154 Abs. 2 StPO normierten Pflicht zur vollständigen Aussage bestehen insofern Ausnahmen, als zusätzlich zur Möglichkeit der Aussageverweigerung bei Gefahr einer Selbstbelastung in den §§ 155–158 StPO verschiedene weitere Vernehmungsverbote bzw. Aussagebefreiungs- und Aussageverweigerungsrechte vorgesehen sind. Bei den in § 157 StPO normierten Aussageverweigerungsrechten sind auch solche enthalten, die anerkannte gesetzlich geregelte Verschwiegenheitspflichten betreffen. Sie alle beziehen sich nur auf die Verpflichtung zur Aussage, nicht jedoch auf deren Inhalt. Insofern besteht durch

¹¹ vgl. *Birklbauer in WK-StPO Vor §§ 118, 123 und 124 Rz 8 ff.*

die genannten Verbote bzw. Rechte keine Einschränkung von der Pflicht für Zeuginnen und Zeugen, im Falle einer Aussage sich wahrheitsgemäß zu verantworten.

Die in § 157 Abs. 1 Z 2 bis 4 StPO normierten Aussageverweigerungsrechte betreffen juristisch-wirtschaftliche Berufe (z.B. Rechtsanwälte, Notare oder Wirtschaftstreuhänder; Z 2), Medienleute (z.B. Medieninhaber oder Medienmitarbeiter; Z 4) sowie unter Z 3 verschiedene medizinisch-psychosoziale Berufe wie Psychotherapeuten, Psychologen oder generell Mitarbeiterinnen und Mitarbeiter anerkannter Einrichtungen zur psychosozialen Beratung und Betreuung. Aus dem klassischen medizinischen Bereich fallen nur Fachärztinnen und Fachärzte für Psychiatrie unter diese Bestimmung und keineswegs Ärztinnen und Ärzte generell über das, was ihnen in dieser Eigenschaft bekannt geworden ist. Damit sind diese, soweit sie nicht zugleich beispielsweise auch als Psychotherapeuten tätig sind, trotz gesetzlich normierter Verschwiegenheitsverpflichtung zur Aussage als Zeugin oder Zeuge in einem Strafverfahren verpflichtet, was jedenfalls unbefriedigend ist und sich auch in Forderungen äußert, dies zu reformieren¹².

Es soll nicht unerwähnt bleiben, dass für manche Tatsachen das (bedingte) Aussageverweigerungsrecht nach § 158 StPO eine Lösung bieten kann. Nach Abs. 1 Z 3 der genannten Bestimmung kann der Zeuge die Beantwortung einzelner Fragen verweigern, soweit sie Umstände aus dem höchstpersönlichen Lebensbereich des Zeugen oder einer anderen Person betreffen. Zum höchstpersönlichen Lebensbereich gehören weitgehend auch Tatsachen aus dem Gesundheitsbereich sowie sonstige Umstände, von denen Ärztinnen und Ärzte Kenntnis haben, weil sie ihnen von ihren Patientinnen und Patienten anvertraut wurden. Für die in § 158 StPO normierten Aussageverweigerungsrechte ist aber essentiell, dass ein Zeuge zur Beantwortung solcher Fragen verpflichtet werden kann, „wenn dies wegen der Bedeutung ihrer Aussage für den Gegenstand des Verfahrens unerlässlich ist“ (§ 158 Abs. 2 StPO). Diese Verpflichtung zur Beantwortung kann dann auch durch Beugemittel (Geldstrafe bis zu 10.000 Euro und in wichtigen Fällen Freiheitsstrafe bis zu sechs Wochen; vgl. § 93 Abs. 4 StPO) erzwungen werden, weshalb im Zusammenhang mit § 158 StPO auch von „bedingten Aussageverweigerungsrechten“ gesprochen wird¹³.

Mit Blick auf die Praxis ist noch hervorzuheben, dass ein Zeuge nur verpflichtet ist, über „Tatsachen“ auszusagen. Werturteile, subjektive Einschätzungen oder Vermutungen gehören nicht dazu.¹⁴ Die Frage, wie ein Arzt etwa den Gesund-

12 siehe etwa Schmoller, *Zur Reichweite der Verschwiegenheitspflicht von Ärzten, Psychologen und Psychotherapeuten*, RdM 1996, 131.

13 so etwa Kirchbacher in *WK-StPO* § 158 Rz 2.

14 vgl. Kirchbacher in *WK-StPO* § 154 Rz 8.

heitszustand im Nachhinein einschätzen würde, ist keine Frage nach Tatsachen (aus der Vergangenheit), die den Gegenstand der Vernehmung bilden (dürfen). Insofern empfiehlt es sich für Ärztinnen und Ärzte vor einer Vernehmung als Zeugin oder Zeuge, sich zu vergegenwärtigen, welche Tatsachen ihnen erinnerlich sind, um sich nicht zu allgemeinen Vermutungen hinreißen zu lassen. Eine richtige Aussage kann es vor diesem Hintergrund mitunter sein, sich nicht mehr erinnern zu können, anstatt zu mutmaßen, wie es gewesen sein könnte. Vorhandene Dokumentationen sollten zur besseren Erinnerung freilich herangezogen werden, zumal sie im Rahmen eines Strafverfahrens auch sichergestellt werden könnten und damit dem Gericht zur Verfügung stehen, wodurch eine Abweichung der Zeugenaussage von diesen Unterlagen im Verfahren zu unangenehmen Konfrontationen führen kann.

2.3. Fazit

Bereits als Verdächtige eines Strafverfahrens dürfen Ärztinnen und Ärzte jegliche Kooperation und damit jegliche Aussage verweigern. Vom Grundrecht auf Verteidigung ist es auch erfasst, als Verdächtiger oder Beschuldigter unwahre Angaben zu machen. Dagegen sind Zeuginnen und Zeugen verpflichtet, richtig und vollständig auszusagen. Ein Verstoß gegen diese Pflicht ist als falsche Beweisaussage gerichtlich sanktioniert (§ 288 StGB).

Um bestimmte Interessenkonflikte und Verschwiegenheitsverpflichtungen zu respektieren, befreit das Gesetz verschiedene Personen von ihrer Pflicht, als Zeugen oder Zeuginnen aussagen zu müssen. Neben der Gefahr der Selbstbelastung, die für alle Zeuginnen und Zeugen gilt, ist im medizinischen Bereich nur für Fachärztinnen und Fachärzte der Psychiatrie eine Möglichkeit zur Aussageverweigerung vorgesehen (§ 157 Abs. 1 Z 3 StPO), um ihre gesetzlich anerkannte Verschwiegenheitspflicht zu schützen. Andere Ärztinnen und Ärzte haben nur die Möglichkeit, Fragen über Tatsachen aus dem Gesundheitsbereich ihrer Patientinnen und Patienten als solche des „höchstpersönlichen Lebensbereichs“ unbeantwortet zu lassen (vgl. § 158 Abs. 1 Z 3 StPO), wobei sie allerdings vom Gericht zur Beantwortung dieser Fragen gezwungen werden können, wenn dies wegen der besonderen Bedeutung der Aussage für den Verfahrensgegenstand unerlässlich ist (§ 158 Abs. 2 StPO). Eine Verpflichtung zur Beantwortung von Fragen besteht jedoch immer nur, sofern diese „Tatsachen“ betreffen. Werturteile oder subjektive Einschätzungen fallen nicht darunter.

3. Die Sicherstellung von Patientenunterlagen trotz ärztlicher Verschwiegenheitspflicht

Im Rahmen eines Strafverfahrens können Gegenstände sichergestellt werden (§ 109 Z 1 lit. a StPO). Grundvoraussetzung nach § 110 Abs. 1 Z 1 StPO ist, dass die Sicherstellung aus Beweisgründen für das Strafverfahren erforderlich ist. Formell ist sie von der Staatsanwaltschaft anzuordnen und der Kriminalpolizei durchzuführen (§ 110 Abs. 2 StPO). Durch die Beschränkung der Sicherstellung auf „Gegenstände“ und der fehlenden expliziten Regelung für die Sicherstellung von „Daten“ erfolgt eine solche, wenn sie z.B. in einer (digitalen) Patientendokumentation festgehalten werden, durch Sicherstellung des Datenträgers, allenfalls des Computers, wenn sie direkt auf diesem gespeichert sind.

3.1. Sicherstellung als Grundrechtseingriff im Ermittlungsverfahren

Um die Sicherstellung von Gegenständen, die unter anderem in das Grundrecht auf Eigentum eingreift, möglichst schonend durchführen zu können, ist nach § 111 Abs. 1 StPO jede Person, die sicherzustellende Gegenstände in ihrer Verfügungsmacht hat, verpflichtet, diese auf Verlangen herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Hausdurchsuchung effektiert werden. Durch den Verweis auf § 93 Abs. 2 StPO ist überdies klargestellt, dass die Verpflichtung durch Beugemittel (Geldstrafe bis zu 10.000 Euro oder sogar Haft bis zu sechs Wochen; vgl. § 93 Abs. 4 StPO) erzwungen werden kann, freilich infolge des bereits erwähnten Nemo-tenetur-Grundsatzes nur dann, wenn die von der Sicherstellung betroffene Person nicht selbst tatverdächtig ist. Als solche trifft sie keine Pflicht zur Kooperation.

Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so versucht § 111 Abs. 2 StPO den Grundrechtseingriff insofern maßvoll zu gestalten, als nach dieser Bestimmung jeder, der nicht selbst tatverdächtig ist, Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder

herstellen zu lassen hat. Damit soll es der Betroffene letztlich in der Hand haben, die Sicherstellung seines Computers, die seine Arbeitsfähigkeit beeinträchtigen bzw. die Verfügbarkeit seiner Daten beschränken könnte, durch ein gelinderes Mittel abzuwenden.

3.2. Gerichtliche Kontrolle vor Sichtung der Daten

Die Sicherstellung durch die Kriminalpolizei ist vorläufig. Die Beschlagnahme durch das Gericht (§ 115 StPO) bildet das Anschlussstück und setzt die Erforderlichkeit des Beweismittels (im Original) für das weitere Verfahren voraus. Um über eine Beschlagnahme entscheiden zu können, ist zu prüfen, ob eine weitere Relevanz des sichergestellten Gegenstands für das Strafverfahren besteht.

Gerade mit Blick auf gesetzlich anerkannte Verschwiegenheitspflichten sieht die StPO eine gleichsam „Vorschaltung des Gerichts“ vor, welches darüber zu entscheiden hat, welche Datensätze von einer Sichtung durch Kriminalpolizei oder Staatsanwaltschaft unmittelbar nach der Sicherstellung auszunehmen sind. Widerspricht die von der Sicherstellung betroffene Person, auch wenn sie selbst der Tat beschuldigt ist, der Sicherstellung von schriftlichen Aufzeichnungen oder Datenträgern, so sind nach § 112 Abs. 1 StPO diese Unterlagen auf geeignete Art und Weise gegen unbefugte Einsichtnahme zu sichern und bei Gericht zu hinterlegen. Der Betroffene muss dann nach § 112 Abs. 2 StPO binnen einer angemessenen, 14 Tage nicht unterschreitenden Frist jene Teile der Aufzeichnungen oder Datenträger konkret bezeichnen, deren Offenlegung eine Umgehung seiner Verschwiegenheit bedeuten würde. Das Gericht hat dann zu entscheiden, welche Aktenteile zum Akt genommen werden dürfen. Jene Unterlagen, die nicht zum Akt genommen werden dürfen, sind dem Betroffenen auszufolgen. Aus deren Sichtung gewonnene Erkenntnisse dürfen bei sonstiger Nichtigkeit nicht für weitere Ermittlungen oder als Beweis verwendet werden, damit die gesetzlich anerkannte Verschwiegenheitspflicht auch effektiv geschützt werden kann.

Auf den ersten Blick scheint durch diese Möglichkeit ein ausreichender Schutz für Daten, die einer gesetzlich geregelten Verschwiegenheitspflicht unterliegen, vor unbefugter Einsichtnahme zu bestehen, indem ein unabhängiger Richter gleichsam vor zu großer Neugier der Ermittlungsbehörden schützt. Bei näherer Betrachtung ergibt sich hinsichtlich der ärztlichen Verschwiegenheitspflicht jedoch ein völlig anderes Bild. § 112 StPO erfasst nämlich nach seinem klaren Wortlaut nur Daten und Unterlagen eines „gesetzlich anerkannten Rechts auf Verschwiegenheit, das bei sonstiger Nichtigkeit nicht durch Sicherstellung umgangen werden darf“. Berufsgeheimnisse, die vor einer Umgehung durch Sicherstellung ge-

schützt sind, nennt § 144 Abs. 2 StPO abschließend, indem dort auf § 157 Abs. 1 Z 2 bis 4 StPO verwiesen wird. Damit reicht die Widerspruchsmöglichkeit nur soweit wie der Schutz jener Berufsgruppen mit Verschwiegenheitspflichten, denen ein ausdrückliches Recht auf Verweigerung der Zeugenaussage zusteht. Für den medizinischen Bereich betrifft dies, wie bereits unter Punkt 2.2 dargestellt, nur Fachärztinnen und Fachärzte für Psychiatrie. Damit haben andere Ärztinnen und Ärzte nicht nur kein Recht, ihre Aussage als Zeuginnen und Zeugen in einem allfälligen Strafverfahren zu verweigern, sondern auch keine Möglichkeit, die Notwendigkeit der Sichtung von Daten und Unterlagen, die aus ihrem Bereich sichergestellt wurden, einer Vorab-Kontrolle durch das Gericht im Rahmen von § 112 StPO unterziehen zu lassen¹⁵. Dadurch wird die für den Gesundheitsbereich essentielle und gesetzlich geregelte Verschwiegenheitspflicht wesentlich entwertet. Pointiert ausgedrückt müssten Ärztinnen und Ärzte ihre Patientinnen und Patienten darüber informieren, dass sie zwar zur Verschwiegenheit gegenüber Dritten verpflichtet sind, aber keine Möglichkeit haben, in einem allfälligen Strafverfahren die von Patientinnen und Patienten geoffenbarten Tatsachen vor einer gerichtlichen Verwertung zu schützen.

Mit Blick auf die Praxis sei vor diesem Hintergrund hervorgehoben, dass der Umfang der Dokumentation in Patientenakten sich auf jene unbedingt notwendigen Tatsachen beschränken sollte, die für die medizinische Behandlung und Diagnose unbedingt notwendig sind. Wenn Patientinnen und Patienten Umstände aus ihrem Privatleben schildern, um Belastungen und Stress zu beschreiben, mag dies für eine Diagnose und Behandlung zwar bedeutsam sein. Mit Blick auf den Umstand, dass im Falle eines Gerichtsverfahrens solche in Patientendokumentationen beschriebene Umstände nicht aus dem Verfahren ausgeklammert werden können, sollte aber vorab bei der Eintragung von höchstpersönlichen und/oder privaten Umständen in die Patientendokumentation Zurückhaltung geübt werden. Dies nicht zuletzt deswegen, weil Patientinnen und Patienten ein zum Teil völlig überzogenes Verständnis von der ärztlichen Verschwiegenheitspflicht haben, welches sich weder in den strafprozessualen Rechtsvorschriften noch in der täglichen juristischen Praxis widerspiegelt.

¹⁵ vgl. *Tipold/Zerbes in WK-StPO § 112 Rz 10*.

3.3. Fazit

Verfahrensrelevante Informationen aus Patientendokumentationen können im Rahmen eines Strafverfahrens sichergestellt und in weiterer Folge verwendet werden (vgl. §§ 109 ff StPO). Ärztinnen und Ärzte können, sofern sie nicht selbst verdächtig sind, zur Herausgabe solcher Daten mittels Beugemittel verpflichtet werden (§ 111 iVm § 93 StPO). Infolge ausdrücklicher gesetzlicher Regelung (vgl. § 112 StPO) besteht für die betroffenen Ärztinnen und Ärzte keine Möglichkeit, bei sichergestellten Datensätzen vor deren Sichtung eine Kontrolle des Gerichts hinsichtlich der Verfahrensrelevanz der sichergestellten Daten zu erwirken. Dadurch besteht im Rahmen eines Strafverfahrens nur ein geringer Schutz vor unberechtigten Eingriffen in von Patientinnen und Patienten mit Blick auf die ärztliche Verschwiegenheitspflicht bekannt gegebenen Daten.

4. Zusammenfassende Schlussfolgerungen

Die ärztliche Verschwiegenheitspflicht wird als so bedeutsam angesehen, dass sie durch Strafnormen (§ 121 StGB) ebenso geschützt ist wie durch berufsrechtliche Vorschriften (§ 54 iVm § 199 Abs. 3 ÄrzteG). Um Gerichtsverfahren effizient führen zu können, entfällt jedoch das strafrechtliche Unrecht einer Verletzung der Verschwiegenheitspflicht, wenn der Angehörige des Gesundheitsberufs als Zeuge vernommen wird und eine unrichtige oder unvollständige Aussage strafrechtliche Sanktionen (falsche Beweisaussage nach § 288 StGB) nach sich ziehen würde. Dies folgt letztlich aus § 121 Abs. 5 StGB und mittelbar auch aus § 54 Abs. 2 Z 4 lit. b ÄrzteG, die eine Strafbarkeit für solche Fälle ausschließen.

Eine Strafbefreiung setzt freilich voraus, dass Ärztinnen und Ärzte als Zeuginnen und Zeugen zur Aussage in einem Strafverfahren verpflichtet sind. Um gesetzlich anerkannte Verschwiegenheitsverpflichtungen zu respektieren, befreit das Gesetz bestimmte Personen von ihrer Pflicht, als Zeuge oder Zeugin auszusagen zu müssen. Neben der Gefahr der Selbstbelastung, die für alle Zeuginnen und Zeugen gelten, ist im medizinischen Bereich nur für Fachärztinnen und Fachärzte der Psychiatrie eine Möglichkeit zur Aussageverweigerung vorgesehen (§ 157 Abs. 1 Z 3 StPO). Andere Ärztinnen und Ärzte haben nur die Möglichkeit, Fragen

über Tatsachen aus dem Gesundheitsbereich ihrer Patientinnen und Patienten als solche des „höchstpersönlichen Lebensbereichs“ unbeantwortet zu lassen (vgl. § 158 Abs. 1 Z 3 StPO), wobei sie allerdings vom Gericht zur Beantwortung solcher Fragen gezwungen werden können, wenn dies wegen der besonderen Bedeutung der Aussage für den Verfahrensgegenstand unerlässlich ist (§ 158 Abs. 2 StPO). Werden sie zur Aussage verpflichtet, kann die dadurch erfolgte Offenbarung von Gesundheitsgeheimnissen keine Strafbarkeit nach § 121 StGB bzw. § 54 iVm § 199 Abs. 3 ÄrzteG nach sich ziehen.

Unabhängig von der Verpflichtung zur Aussage von Ärztinnen und Ärzten können verfahrensrelevante Informationen aus Patientendokumentationen im Rahmen eines Strafverfahrens sichergestellt und in weiterer Folge verwendet werden (§§ 109 ff StPO). Ärztinnen und Ärzte können, sofern sie nicht selbst verdächtig sind, zur Herausgabe solcher Daten mittels Beugemittel verpflichtet werden (§ 111 iVm § 93 StPO). Infolge ausdrücklicher gesetzlicher Regelung (vgl. § 112 StPO) besteht für die betroffenen Ärztinnen und Ärzte keine Möglichkeit, bei sichergestellten Datensätzen vor deren Sichtung eine Kontrolle des Gerichts hinsichtlich der Verfahrensrelevanz der sichergestellten Daten zu erwirken. Dadurch besteht im Rahmen eines Strafverfahrens nur ein geringer Schutz vor unberechtigten Eingriffen in von Patientinnen und Patienten mit Blick auf die ärztliche Verschwiegenheitspflicht bekannt gegebene Daten. Ein diesbezüglicher Reformbedarf ist hier evident und sollte in Diskussionsprozessen forciert werden.

Friedrich Oelenhainz, Detail aus «Porträt des späteren Fürsten Johann I. von Liechtenstein», 1776.
© LIECHTENSTEIN. The Princely Collections, Vaduz–Vienna



VALUES WORTH SHARING

«Meine Bank legt Wert auf Werte.»

Peter Bollmann, LGT Kunde seit 2009



Private
Banking

lgt.at/values

Auf den StandPunkt gebracht

Die Rubrik „Auf den StandPunkt gebracht“ beinhaltet Positionen und ExpertInnenwissen aus der Standesvertretung der Ärzte und Ärztinnen in Österreich und aus weiteren Interessensgruppen zum Schwerpunktthema „Homogene Finanzierung von Spitalsambulanzen und Kassenärzten“.

Dieses Mal mit Beiträgen von

DI Michael Nöhammer, Leiter der Abteilung IT, Statistik, Projektmanagement und Grundlagenarbeit, Österreichische Ärztekammer

Mag. Markus Dörfler, LL.M., Partner bei Höhne, In der Maur & Partner Rechtsanwälte GmbH & Co KG

Dr Michael Nöhhammer

Leiter der Abteilung IT, Statistik, Projektmanagement und Grundlagenarbeit, Österreichische Ärztekammer

Sichere elektronische Kommunikation zwischen Arzt und Patient

Durch die verstärkte Nachfrage von Patienten nach elektronischer Übertragung der sie betreffenden Befunde und dem zunehmenden Einsatz telemedizinischer Maßnahmen entstehen Fragestellungen, die ich nachfolgend beleuchten möchte.

Bei der elektronischen Übertragung von Gesundheitsdaten bzw. Patientendaten sind insbesondere die Vorgaben des Gesundheitstelematikgesetzes wie auch jene der DSGVO zu beachten, wonach

- die Übermittlung gemäß Art. 9 DSGVO zulässig ist und
- durch effektive und dem Stand der Technik entsprechende Datensicherheits- und Kontrollmaßnahmen unbefugte Dritte vom Zugriff auf Gesundheitsdaten und genetische Daten und somit deren Kenntnisnahme ausgeschlossen werden können.

Der „Ausschluss unbefugter Dritter“ macht ein weites Feld der IT-Sicherheit und des Datenschutzes auf, das ich hier nicht weiter betrachten werde. Als Schlagworte seien hier die Themenfelder IT-Sicherheitskonzept, Benutzerrechte und physische Sicherheit genannt.

Was verstehe ich unter „sicherer Kommunikation“?

Für mich sollten zwei Punkte jedenfalls beachtet werden:

- Die Kommunikation darf für unbefugte Dritte nicht einsehbar sein.
- Der Anbieter muss vertrauenswürdig sein.

Nicht einsehbare Kommunikation

Als selbstverständliche Maßnahme muss die „Transportverschlüsselung“ gelten, d.h. die Absicherung des Kommunikationskanals, um hier einen sicheren Datentransport zu gewährleisten. Die dafür erforderlichen Protokolle heißen u.a. „TLS“, „Perfect Forward Secrecy“. Als jederzeit aktualisierte Informationsquelle kann https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/TLS-Protokoll/TLS-Protokoll_node.html dienen.

Neben der Transportverschlüsselung sollte jedenfalls eine „Inhaltsverschlüsselung“ stattfinden. Dabei wird vor dem Versand der Inhalt verschlüsselt, nach der Übertragung kann der Inhalt entschlüsselt und auf Integrität geprüft werden.

Die Umsetzung dieser Maßnahme erfordert den Einsatz elektronischer Zertifikate, das sichere Verarbeiten und Aufbewahren dieser Zertifikate ist nicht trivial. Die saubere technische Umsetzung dieser Aufgaben garantiert (oder auch nicht) die korrekte Verschlüsselung der Inhalte.

Jedenfalls muss bei korrekter Umsetzung eine – auch vom Anbieter nicht einsehbare – „Ende-zu-Ende-Verschlüsselung“ stattfinden. Dadurch ist gesichert, dass auch beim Zusammenbruch der Transportverschlüsselung der Inhalt nicht eingesehen oder unbemerkt verändert werden kann.

Vertrauenswürdiger Anbieter

Eine Organisation muss sicherstellen, dass die Kommunikationslösung von einem vertrauenswürdigen Anbieter, dem sog. „Auftragsverarbeiter“ gemäß Art. 28 DSGVO stammt. Mit diesem ist auch ein entsprechender Vertrag abzuschließen (Auftragsverarbeitervereinbarung). In dieser Vereinbarung sind u.a. die Durchführung der Aufgaben sowie der Zweck der vorgesehenen Verarbeitung festzuhalten.

Die Beurteilung der Vertrauenswürdigkeit obliegt der Organisation, welche die Datenverarbeitung durch den Auftragsverarbeiter durchführen lassen möchte (in der DSGVO „Verantwortlicher“ genannt), hilfreich können jedenfalls u.a. die Fragen sein:

- Bietet die Lösung eine „Ende-zu-Ende-Verschlüsselung“ an?
- Ist sichergestellt, dass der Anbieter den Inhalt der Kommunikation nicht einsehen kann?
- Ist der Quelltext der Lösung frei verfügbar und kann dieser daher von einem Experten geprüft werden?
- Wie wird die Identität der Teilnehmer geprüft (z.B. Handysignatur, e-ID)?
- Werden elektronische Zertifikate von anerkannten Zertifizierungsstellen verwendet?
- Was passiert mit den Daten nach der Übertragung?
- Sichert der Anbieter eine DSGVO-konforme Arbeit zu?

- Werden Sub-Auftragsverarbeiter beschäftigt?

Mögliche Lösungen

Ich möchte einige Produktkategorien/technische Lösungen anführen, die bei der Bewältigung der Aufgaben unterstützen.

- Videotelefonie
Es sind viele Produkte am Markt verfügbar. Die Kernfrage ist die nach dem vertrauenswürdigen Anbieter.
- Nachrichten/Chat
Auch hier gibt es sehr viele Produkte, vor allem von weltweit agierenden Anbietern.
- E-Mail
Mit den Technologien S/MIME oder PGP sind verschlüsselte E-Mails möglich. Der Umgang mit den notwendigen Zertifikaten ist sehr mühsam, daher haben sich diese Technologien nicht flächeneckend durchgesetzt.
- Plattformen zum Dokumentenaustausch
Am Markt sind viele Lösungen verfügbar, auf DSGVO-Konformität ist auch hier zu achten.

Fazit

Die Auswahl eines vertrauenswürdigen Anbieters ist die wichtigste Aufgabe bei der Festlegung der elektronischen Kommunikationsmöglichkeiten. Weltweit agierende Anbieter werden wohl kaum zur Unterfertigung einer DSGVO-Konformitätserklärung bereit sein. Speicherorte außerhalb Österreichs (bzw. der EU oder des EWR) sind jedenfalls tabu.

Es gibt in Österreich ansässige Anbieter von Kommunikationslösungen, diese wenden sich an österreichische Ordinationen bzw. Organisationen. Ich empfehle, sich von diesen Anbietern eine Lösung zeigen und anbieten zu lassen.

Mag. Markus Dörfler, LL.M.

Partner, Höhne, In der Maur & Partner Rechtsanwälte GmbH & Co. KG

Datenschutz in Zeiten der Quarantäne

Für die aktuelle Ausgabe war geplant, datenschutzrechtliche Tipps zu präsentieren. Der Corona-Virus hat nicht nur den Abgabetermin des Autors durcheinandergewirbelt, es treten nun auch datenschutzrechtliche Probleme auf, die vor wenigen Monaten noch undenkbar gewesen wären. Dabei könnte man im ersten Moment meinen, dass die Corona-Krise keine unmittelbaren Auswirkungen auf das datenschutzrechtliche Verhalten der Ärzte hat. Dies ist jedoch unrichtig. Um den geneigten Leser nicht zu langweilen, werden drei akute Themen im Folgenden besprochen:

1. Was muss ich beim Homeworking meiner Mitarbeiter beachten?

Ärzte, die mehrere Mitarbeiter beschäftigen, lassen diese – sofern möglich – Arbeiten im Homeoffice erledigen (etwa Terminvereinbarungen oder Durchführen von administrativen Arbeiten). Was ist hier datenschutzrechtlich zu beachten?

In diesem Fall muss der Arzt als Dienstgeber sicherstellen, dass geeignete technische und organisatorische Maßnahmen ergriffen werden, um den Schutz der Patientendaten zu gewährleisten, wenn die Daten im Rahmen des Homeoffice von Mitarbeitern verarbeitet werden. Achtung: Der Arzt muss auch für Datenlecks eintreten, wenn diese an einem zuhause eingerichteten Arbeitsplatz auftreten. Wichtig ist, die Mitarbeiter auf die Einhaltung des sogenannten „Datengeheimnisses“ gem. § 6 österreichisches Datenschutzgesetz nochmals hinzuweisen und entsprechend zu schulen. Hierfür empfehlen sich geeignete Leitfäden für den Umgang mit Tele-Arbeit sowie eine entsprechende schriftliche Weisung, aus der etwa hervorgeht, dass nur bereitgestellte Hardware (Laptop und Handy) verwendet werden darf, die Geräte nicht an öffentlichen Orten verwendet werden dürfen, mit welchen technischen Sicherheitsmaßnahmen der Zugriff auf die Ordinationsdaten erfolgt und wie die bereitgestellte Hardware vor unberechtigtem Zugriff (Stichwort: Bildschirmsperre) geschützt wird. Sollte der Mitarbeiter seine privaten Endgeräte nutzen dürfen, muss der Arzt Regeln zur klaren Trennung von Ordinations- und Privat-

daten aufstellen. Leider müssen solche Weisungen an die jeweilige Struktur und Arbeitsabläufe angepasst werden, sodass es keine Muster gibt.

2. Ist Tele-Medizin datenschutzrechtlich zulässig?

Unter dem Begriff Tele-Medizin versteht man die Erbringung medizinischer Leistungen Mithilfe von Informations- und Kommunikationstechnologien, wobei die Patientin bzw. der Patient und Gesundheitsdiensteanbieter (etwa: der Arzt) nicht am selben Ort anwesend sind. Datenschutzrechtlich ist die Frage, ob Tele-Medizin zulässig ist oder nicht, leicht zu beantworten: Sofern geeignete technische und organisatorische Maßnahmen zur technischen Sicherheit, zur Integrität der Daten sowie zur Authentizität der Daten vorliegen, ist Tele-Medizin zulässig. Das bedeutet, dass der jeweilige Arzt dafür sorgen muss, dass die Kommunikation mit dem Patienten mit einem nach dem Stand der Technik entsprechenden Verschlüsselungsverfahren verschlüsselt und sichergestellt ist, dass der Kommunikationspartner tatsächlich der Patient ist und die Kommunikation vor Manipulation geschützt ist.

Welches konkrete System telemedizinisch zulässig ist oder nicht, hängt vom Einzelfall ab. Selbst Software, die man aus dem Privatbereich kennt (etwa Messenger-Apps) können genutzt werden, wenn die oben genannten Kriterien erfüllt sind. Achtung: Insbesondere bei kostenloser Software muss der Arzt darauf achten, nicht mit den Daten der Patienten zu bezahlen (dies ist jedoch leider bei dem am meisten verbreiteten Messenger-System der Fall).

Neben der datenschutzrechtlichen Komponente gibt es noch eine standesrechtliche Komponente. Standesrechtlich ist Tele-Medizin nicht verboten. Es liegt jedoch ausschließlich in der ärztlichen Verantwortung des behandelnden Arztes zu entscheiden, wann auf den physischen Kontakt zwischen Arzt und Patient im Einzelfall verzichtet werden kann. Der jeweilige behandelnde Arzt muss bei der Frage, ob auf den persönlichen Kontakt verzichtet werden kann, auch die technische Barriere berücksichtigen. So wird ein Dermatologe bei einem schlecht aufgelösten Foto einer Hautveränderung wohl nicht auf den physischen Kontakt verzichten können.

Wichtig: Allein aus der Tatsache, dass die Sozialversicherung Abrechnungsmodalitäten für telemedizinische Behandlungen geschaffen hat, lässt sich noch nicht ableiten, dass jede telemedizinische Behandlung per se zulässig ist. Zu beachten ist auch, dass die jeweiligen kassenrechtlichen Vorgaben erfüllt sind.

3. Darf auf einer Krankenstandsbestätigung die Diagnose „Covid-19“ angeführt werden?

Nein. Gem. Art 54 Ärztegesetz besteht die ärztliche Verschwiegenheitspflicht nicht, wenn nach gesetzlichen Vorschriften eine Meldung vorgeschrieben ist. Da es sich bei dem „neuen Corona-Virus“ um eine anzeigepflichtige Krankheit im Sinne des Epidemiegesetzes handelt, sind die jeweiligen Bezirksverwaltungsbehörden über diesen Krankheitsfall zu informieren, nicht jedoch der Dienstgeber.

Ob der Dienstnehmer verpflichtet ist, den Dienstgeber über die Krankheit aufzuklären, ist derzeit noch offen – die Aufgabe des Arztes, den Dienstgeber des Patienten aufzuklären, besteht jedenfalls nicht.“

Friedrich Oelenhainz, Detail aus «Porträt des späteren Fürsten Johann I. von Liechtenstein», 1776.
© LIECHTENSTEIN. The Princely Collections, Vaduz–Vienna



VALUES WORTH SHARING

«Meine Bank legt Wert auf Werte.»

Peter Bollmann, LGT Kunde seit 2009



Private
Banking

lgt.at/values

Die Zeitschrift für Gesundheitspolitik (ZGP) des Linzer Instituts für Gesundheitssystem-Forschung (LIG) versteht sich als Medium zur Veröffentlichung neuer Denkanstöße und Perspektiven zu aktuellen Problemen des österreichischen Gesundheitssystems. Sie will damit einen Beitrag zur innovativen Weiterentwicklung des österreichischen Gesundheitssystems leisten. Themenbereiche sind etwa intra- und extramurale Versorgung, Nahtstellenmanagement, Finanzierung, Organisation und Akteure des Gesundheitssystems. Die ZGP richtet sich an Personen aus Politik, Sozialversicherung, Kammern, Wissenschaft und an alle, die am Gesundheitssystem interessiert sind.

Erscheinungsweise: vierteljährlich

Gerne lassen wir Ihnen unverbindlich und kostenlos ein Exemplar zukommen.

Bestelladresse:

Linzer Institut für Gesundheitssystem-Forschung (LIG)
Dinghoferstraße 4, 4010 Linz
Tel.: ++43/732/77 83 71-320
Fax: ++43/732/78 36 60-320
E-mail: lig@aekoee.at

Bestellformular: <http://www.lig-gesundheit.at/abonnieren>

LIG
GESUNDHEITSSYSTEM-FORSCHUNG

LINZER
INSTITUT
FÜR

aekoee Ärztekammer
für Oberösterreich