Arztterminvermittlung über Doctolib

Datenschutz-Anspruch und Wirklichkeit

Stand: 08.06.2021

Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

1 Was ist Doctolib? 4
1.1 Französisches Startup 4
1.2 Das Angebot 5
1.3 Der Markt 6
1.4 Erkenntnisse 7
2 Anforderungen an ärztliche Apps 9
3 Das Regelwerk und die Internet-Präsenz von Doctolib 10
3.1 Grundinformationen zum Unternehmen 10
3.2 Überblick über die Dokumente 11
3.3 Doctolibs Datenschutzbekenntnis 12
4 Datenschutzrechtliche Verantwortlichkeiten 13
4.1 Verantwortlichkeit und Auftragsdatenverarbeitung 14
4.2 Die Rolle der Patientinnen und Patienten 15
4.3 Die Rolle der Gesundheitsfachkraft 15
4.4 Verantwortlichkeit der Doctolib GmbH 16
4.5 Auftragsverarbeitung durch Doctolib 17
4.6 Gemeinsame Verantwortlichkeit 18
5 Medizinrechtliche Verantwortlichkeit 18
6 Gesundheitsdaten als besondere Kategorie 19
7 Import des Patientendatenstamms 20
7.1 Darstellung durch Doctolib 20
7.2 Auftragsdatenverarbeitung 21
7.3 Mitwirkung bei einem Berufsgeheimnisträger 21
8 Technisch-organisatorische Maßnahmen 24
9 Werbung – freiwillige Meinungsumfragen 25
10 Umsetzung der Betroffenenrechte 26
10.1 Informationspflichten generell 26
10.2 Informationspflichten speziell 26
11 Löschung 27
11.1 Darstellung durch Doctolib 27
11.2 Bewertung 28
12 Einbindung sozialer Netzwerke 29
13 Cookies 30

13.1 Einwilligungserteilung in nicht nötige Cookies 31
13.2 Speicherdauer und Auslandsübermittlung 31
14 Auslandsdatentransfer 31
14.1 Hosting bei AWS 31
14.2 Datenverarbeitung in den USA 33
15 Zertifizierung 34
16 Ergebnisse 35
17 Abschlussbemerkungen 36
Ausgewählte Literatur 37
Abkürzungen 38

Apps im Gesundheitsbereich werden für immer mehr Menschen zum alltäglichen Hilfsmittel bei deren Umgang mit ihrem körperlichen und seelischen Wohl sowie in der Kommunikation mit medizinischen Leistungserbringern. Die Beachtung des Datenschutzes ist von zentraler Bedeutung dafür, dass das Vertrauensverhältnis zu den medizinischen Leistungserbringern gewahrt bleibt. Dies gilt nicht nur für Diagnose und Behandlung, sondern schon für die Rahmenbedingungen der Leistungserbringung, etwa für die ärztliche Terminvermittlung. Das Unternehmen Doctolib spielt bei der Terminvermittlung auf dem deutschen und französischen Gesundheitsmarkt eine dominante Rolle. Es bekennt sich zum Datenschutz, doch ist es fraglich, ob dieses Bekenntnis mit der Realität in Einklang steht. Das Unternehmen ist ein Beispiel dafür, dass Transparenz und praktizierter Datenschutz bei Marktteilnehmern entwickelungsfähig sind.

1 Was ist Doctolib?

1.1 Französisches Startup

Doctolib ist ein **ursprünglich französisches Unternehmen**, das eine Onlinebuchungsplattform zur Verfügung stellt, über die Patientinnen und Patienten ihre Arzttermine einfach online und in Echtzeit rund um die Uhr vereinbaren können. Es wurde Ende 2013 von Stanislas Niox-Chateau[1], Jessy Bernal und Ivan Schneider in Frankreich gegründet. Doctolib bot von Anfang an – anders als Konkurrenten in Frankreich – nicht nur Reservierungen, sondern verbindliche Terminbuchungen an. 2016 hatte das Unternehmen in Frankreich schon ca. 230 Beschäftigte an 30 Standorten.

2016 wurde eine **Tochter in Deutschland** gegründet. Geschäftsführer der in Berlin ansässigen Firma, die mit 5 Mitarbeitern begann, war zunächst Simon Krüger. Berlin ist inzwischen neben Paris der zweite Stammsitz des Gesamtunternehmens. Krüger wurde im März 2019 als Deutschlandchef abgelöst durch Ilias Tsimpoulis, der das Unternehmen bis heute als „Managing Director Deutschland" leitet.

Beim Start in Deutschland wurde das Unternehmen u.a. mit rund 23 (andere Angaben 26) Mio. € von Accel Partners und bekannten Business Angels aus Frankreich, beispielsweise BlaBlaCar-Gründer Nicolas Brusson, mit **Wagniskapital** unterstützt. Ende 2017 schloss es eine weitere Finanzierungsrunde mit 35 Mio. € ab. Dabei beteiligte sich erneut die französische Investmentbank Bpifrance; neu eingestiegen ist das Pariser Beteiligungsunternehmen Eurazeao.[2] Im März 2019 sammelte der Doctolib-Konzern weitere 150 Mio. € frisches Kapital ein, woraus sich eine Unternehmensbewertung von mehr als einer Milliarde Euro ergab. Doctolib gilt seitdem als „Unicorn".[3] Die Finanzierungsrunde erfolgte unter Führung des amerikanischen Finanzinvestors General Atlantic, der hierzulande unter anderem an dem aufstrebenden Mobilitätsdienstleister Flixbus beteiligt ist. In der Runde waren unter anderem wieder die US-Fondsgesellschaft Accel, die auch Aktionär von Spotify oder Dropbox ist,

[1] Scherkamp, Ein Franzose möchte deutsche Termin-Startups plattmachen, 13.06.2016, https://www.businessinsider.de/gruenderszene/allgemein/doctolib-start-deutschland/.
[2] Schnor, 35 Millionen Euro für Arzttermin-Plattform Doctolib, 28.11.2017, https://www.businessinsider.de/gruenderszene/allgemein/doctolib-arzttermin-startup-35-millionen-euro/.
[3] Haak, Doctolib wird zum Einhorn, 20.03.2019, https://www.businessinsider.de/gruenderszene/health/doctolib-einhorn/.

beteiligt sowie der Einzelinvestor Ludwig Klitzsch, Chef und Inhaber der Gesundheitsgruppe Ideamed aus dem bayerischen Bad Wiessee.

1.2 Das Angebot

Doctolib soll mit seiner **Online-Termin-Buchungsplattform** den Alltag für medizinische Leistungserbringer, insbesondere für Arztpraxen, sowie für Patienten erleichtern. Für die Arztpraxen gibt es ein übersichtliches und individuell anpassbares Kalender-Tool, für Patienten eine Online-Buchungsplattform, auf der sie Arzttermine buchen können. Beide Tools sind miteinander verbunden. Die Buchungen können rund um die Uhr in Echtzeit vorgenommen werden. Gemäß Eigenangaben des Unternehmens erfolgen 50 % der Terminbuchungen über Doctolib außerhalb der regulären Praxis-Öffnungszeiten.[4] Rückbestätigungen entfallen und Doppelbuchungen werden verhindert. Automatische Erinnerungen per SMS oder E-Mail sollen dafür sorgen, dass der Arztbesuch von den Patienten nicht vergessen wird. Solche Erinnerungen erfolgten auch bei Patienten, die telefonisch mit der Praxis direkt einen Termin verabredeten, ohne sich vorher bei Doctolib angemeldet zu haben.[5] Darüber sowie über die Möglichkeit der Online-Stornierung soll das Risiko von Terminausfällen reduziert werden.

Doctolib bietet **zudem** ein Onlineverzeichnis, über das die eingebundenen sowie sonstige Ärzte einfach gefunden werden können. Die Ärzte zahlen für die Inanspruchnahme des Dienstes ein Monats-Abo, das verschiedene Service-Angebote (z.B. Erinnerungsservice, Umsatzrechner) einschließt. Über die Funktion „Digitale Warteliste" werden Patienten über freigewordene Terminzeiten informiert und können diese direkt für sich buchen. Am Tagesende kann der Arzt Statistiken und Auswertungen z.B. zur Auslastung der Praxis, die häufigsten Termingründe und Ähnliches ansehen. Auf den digitalen Kalender kann er über das Internet Zugriff nehmen, mit Hilfe einer App auch vom Smartphone aus. Eine weitere Funktion zur Patientenbindung ist die Möglichkeit, Feedbackbögen nach erfolgter Untersuchung zu versenden.

Am 06.04.2020 erweiterte Doctolib sein Angebot um **Tele-Konsultationen** über das Internet. In einem sog. „digitalen Wartezimmer" können Vorbefunde oder Bilddateien vorab mit dem Arzt geteilt werden. Aufgrund der Zertifizierung durch die Kassenärztliche Bundesvereinigung (KBV, s.u. 15) werden die Kosten für die per Videosprechstunde vorgenommenen Untersuchungen von den gesetzlichen Krankenkassen erstattet.[6] Langfristiges Ziel des Unternehmens ist es, sich als Medizinplattform zu etablieren. Nach eigenen Angaben hat Doctolib derzeit in Deutschland jeden Monat mehr als vier Millionen Nutzer. Doctolib will den Rückenwind der Pandemie für weiteres Wachstum nutzen.[7]

Docotlib adressiert **alle medizinischen Fachrichtungen**: Zahnmedizin, Allgemeinmedizin (Hausarzt), Kinder- und Jugendmedizin, Augenheilkunde/Ophthalmologie, Hals-Nasen-Ohrenheilkunde (HNO),

[4] In Kooperation mit Ilias Tsimpoulis, 18.08.2020, Umsatzrechner für die Arztpraxis – objektiv, transparent und individuell, https://www.arzt-wirtschaft.de/online-terminbuchung-videosprechstunde/umsatzrechner-fuer-die-arztpraxis-objektiv-transparent-und-individuell/.
[5] Jules, 27.10.2019, https://forum.kuketz-blog.de/viewtopic.php?t=4910.
[6] Doctolib bietet ab sofort kostenlose Videosprechstunde an, 06.04.2020, https://www.presseportal.de/pm/139561/4564986.
[7] Nützel, Videosprechstunde beim Arzt: Nachfrage und Kritik nehmen zu, www.heise.de 08.04.2021, https://heise.de/-6008098.

Haut- und Geschlechtskrankheiten / Dermatologie, Orthopädie und Unfallchirurgie, Psychiatrie und Psychotherapie, Innere Medizin und Kardiologie, Allergologie, Neurologie, Innere Medizin und Rheumatologie, Frauenheilkunde und Geburtshilfe, zahnmedizinische Prophylaxe, Urologie, Innere Medizin, plastische, rekonstruktive und ästhetische Chirurgie, Kieferorthopädie.[8]

Im Rahmen der aktuellen **Corona-Pandemie** bietet sich Doctolib als Terminvermittler an und wurde zum preisgünstigen Technologiepartner des Landes Berlin bei den Corona-Impfungen, worüber das Unternehmen zugleich seinen Dienst populär machen kann.[9] Eine solche Partnerschaft besteht in Frankreich auch zwischen Doctolib und dem nationalen Gesundheitsministerium. Ein einstweiliges Anordnungsverfahren hiergegen von Medizinerverbänden und Gewerkschaften wegen der Einbindung von Amazon Webservices (AWS) vor dem Obersten Gericht Frankreichs, dem Conseil d´Etat, wurde mit Beschluss vom 12.03.2021 zurückgewiesen (s.u. 14.1).[10] Nach dem Start der dezentralen Impfversorgung gegen Covid 19 wirbt Doctolib bei Haus- und Allgemeinärzt:innen mit einem 50%-Rabatt auf den „Online-Kalender inkl. Impfmanagement für die ersten drei Monate!“.

Doctolib versteht sich als „**klassisches Fach- und Verbrauchermedium**“, das auch auf Twitter, Facebook und weiteren sog. sozialen Medien aktiv ist. Die Arztpraxen, die Kunden von Doctolib sind, werden *automatisch bei Google in der Ergebnisliste angezeigt. Für Ihre Präsenz auf Google Maps erstellt das Team von Doctolib einen professionellen ´Google My Business`-Eintrag. Und auf Ihrer bestehenden Webseite wird der Button für die Online-Buchung prominent integriert*.[11]

1.3 Der Markt

Doctolib ist nicht nur erfolgreich im Einsammeln von Wagniskapitel; damit korrespondiert dessen Expansion auf dem **Software-Markt im Medizinbereich**. Innerhalb des ersten Jahres schaffte es das Unternehmen in Deutschland 1.000 Ärzte aus fünf Großstädten (Berlin, München, Köln, Düsseldorf, Hamburg) auf seiner Plattform zusammenzubringen und 1,5 Mio. Arzttermine zu vereinbaren. Es hatte 50 Beschäftigte. Die monatliche Gebühr für die Nutzung des Portals lag und liegt weiterhin bei 129 €. Insgesamt nutzten bis dahin nach eigenen Angaben insbesondere in Frankreich schon 30.000 Ärzte sowie 800 Gesundheitseinrichtungen das Portal.[12]

[8] https://www.doctolib.de/.
[9] Hoffmann, Berlins offizieller Impftermin-Dienstleister Warum stellt die Firma Doctolib dem Senat nur ein paar Tausend Euro in Rechnung, 28.12.2020, https://www.tagesspiegel.de/berlin/berlins-offizieller-impftermin-dienstleister-warum-stellt-die-firma-doctolib-dem-senat-nur-ein-paar-tausend-euro-in-rechnung/26754188.html; Die mühsame Buchung von Impfterminen in Berlin, 07.05.2021, https://www.tagesspiegel.de/berlin/fehlermeldungen-bei-doctolib-die-muehsame-buchung-von-impfterminen-in-berlin/27169982.html.
[10] The urgent applications judge does not suspend the partnership between the Ministry of Health and Doctolib for the management of COVID-19 vaccination appointments, 12.03.2021, https://www.conseil-etat.fr/en/news/the-urgent-applications-judge-does-not-suspend-the-partnership-between-the-ministry-of-health-and-doctolib-for-the-management-of-covid-19-vaccinati, s.u. Kap. 14.1.
[11] Umsatzrechner für die Arztpraxis, www.arzt-wirtschaft.de 18.08.2020 (Fn. 4).
[12] Maas/Heckel/Ermisch/Binner, Doctolib: Kräftige Finanzspritze für den Arzttermin-Service, 28.11.2017, https://gruender.wiwo.de/doctolib-kraeftige-finanzspritze-fuer-den-arzttermin-service/; Schubert, Kampf um die Arzttermine im Internet, 27.11.2017, https://zeitung.faz.net/faz/unternehmen/2017-11-28/3230cbdc9f0eecedbfb2ead587466e4a/.

Inzwischen hat Doctolib sein Angebot auf den italienischen Markt ausgeweitet.[13] Europaweit gilt Doctolib als größtes Terminbuchungsportal. Es war im Jahr 2019 mit rund 80.000 Ärzten und 35 Millionen Webseiten-Besucherinnen und -Besuchern **Marktführer**. In Deutschland nutzten 2019 ca. 4.000 Ärzte und 56 Gesundheitseinrichtungen wie Krankenhäuser oder Versorgungszentren den Dienst.[14] Doctolib arbeitete Mitte 2020 dann schon mit etwa 125.000 Ärzten sowie 2.300 Gesundheitseinrichtungen in Europa insgesamt. Die Online Plattform verzeichnete ca. 50 Millionen Besuche monatlich, davon mehr als 3 Millionen in Deutschland. Europaweit waren 1.400 Mitarbeiter bei Doctolib in 40 Städten beschäftigt. In Deutschland waren mehr als 300 Mitarbeiter an zehn Standorten beschäftigt, die etwa 10.000 Ärzte betreuten.[15] Zum Stichtag 01.02.2021 gibt Doctolib auf seiner Webseite an, dass in Frankreich und Deutschland 50 Mio. Patienten sowie 150.000 Ärzte sowie sonstige Gesundheitsfachkräfte den Dienst nutzen.[16]

Ein **Konkurrent auf dem deutschen Markt** ist Jameda, das zum Burda-Konzern gehört. Jameda führt ein Verzeichnis von allen 275.000 niedergelassenen Ärzten in Deutschland und führt Bewertungen durch. Bei Doctolib erfolgen keine Bewertungen der vermittelten Leistungserbringer. Mit sechs Millionen Patientenbesuchen im Monat war Jameda 2019 in diesem Bereich noch deutlich größer als der deutsch-französische Konkurrent. Als weitere Konkurrenten werden genannt: Betty24[17], Arzttermine24[18], Arztbuchen24[19] und Doctena[20].

1.4 Erkenntnisse

In ihrem Jahresbericht 2019 beschreibt die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), dass Patientinnen und Patienten über ärztliche Terminerinnerungen von Doctolib überrascht wurden, ohne zuvor mit dem Unternehmen zu tun gehabt zu haben und ohne hierzu eine Einwilligung erteilt zu haben. Die BlnBDI forderte, dass die Inanspruchnahme eines Dienstleisters bei der Terminverwaltung gegenüber den Patientinnen und Patienten transparent gemacht werden müsse. Die Wahrnehmung der Aufgabe von **Terminerinnerungen** bedürfe einer ausdrücklichen Einwilligung, da solche Erinnerungen nicht mehr zur Behandlung zu zählen seien. Von den Dienstleistern wie Doctolib erwartet sie, dass sie ihre Kunden – die Ärztinnen und Ärzte – auf diese Pflichten hinweisen.[21]

Martin Tschirsich vom Chaos Computer Club und Christoph Saatjohann von der Fachhochschule Münster stellten auf dem Chaos Computer Congress Ende Dezember 2020 **Mängel** bei der Verarbeitung von Gesundheitsdaten vor. Sie gaben an, dass ihnen ein Datensatz von Doctolib zugespielt worden sei. Die anonymen Absender hatten erklärt, sie hätten Ende 2019 nach Erstellen

[13] https://info.doctolib.it/.
[14] Otto, Gründer der Woche: Doctolib – Arzttermine ganz einfach online buchen, Woche 24/16, https://www.starting-up.de/news/gruender-der-woche/doctolib.html; Kroker, Doctolib füllt eine Lücke für Patienten und Praxen, 22.06.2019, https://www.wiwo.de/technologie/digitale-welt/online-terminvergabe-doctolib-fuellt-eine-luecke-fuer-patienten-und-praxen/24479464.html.
[15] Videosprechstunde, Presseportal 06.04.2020 (Fn. 6).
[16] https://www.doctolib.de.
[17] https://www.betty24.de/aboutbetty24.aspx.
[18] Nicht mehr vertreten, vgl. https://www.founderio.com/de/startup/95025.
[19] https://www.facebook.com/Arztbuchen24-210997902243762/.
[20] https://de.doctena.de/.
[21] BlnBDI, Jahresbericht 2019, Kap. 6.3 (S. 103 ff.).

eines Gratis-Benutzeraccounts auf der Homepage des Portals über ein relativ einfaches Verfahren Zugriff auf die Daten nehmen können. Darin hätten sich praxisübergreifend unter anderem Telefonnummern und E-Mail-Adressen sowie die Terminkalender der Praxen, etwa von Psychotherapeuten befunden. Erschließbar seien auf diese Weise 150 Mio. Terminvereinbarungen gewesen, die auf eine Synchronisierung mit den Terminkalendern der Arztpraxen zurückzuführen sein dürften. Die Daten reichten den Angaben zufolge bis ins Jahr 1990 zurück.[22]

Im Netz findet sich eine nicht datierte von Stanislas Niox-Chateau (CEO & Mitbegründer Doctolib) gezeichnete **Stellungnahme**, die wohl Doctolib zugeordnet werden kann, „um klar zu stellen, was am 21. Juli 2020 passiert ist und wie wir die Gesundheitsdaten unserer Nutzer schützen". Dabei wird auf den Vortrag des Chaos Computer Clubs (CCC) auf dem im Dezember 2020 durchgeführten Kongress „Remote Chaos Experience" Bezug genommen und bestätigt, dass am 21.07.2020 über eine technische Schwachstelle 6.128 Termine (darunter 45 Termine in Deutschland) erfasst worden seien. Doctolib habe den Angriff innerhalb weniger Stunden gestoppt und die Sicherheitslücke behoben. Die Behauptung über ein Leck von 1 Mio. oder150 Mio. Terminen sei falsch. Der „illegale Angriff" habe keine Termine betroffen, die direkt über Doctolib gebucht wurden, sondern „über eine mit Doctolib verbundene Softwarelösung eines Drittanbieters".[23]

Die vorliegende Untersuchung startete mit einer Datenschutzanfrage des Gutachtenautors per Mail vom 23.03.2021 an die Datenschutzbeauftragte von Doctolib. Dieser wurde ein vierseitiger Katalog zugesendet mit **Fragen zum Datenschutz**, die sich aus der Webseitenpräsentation, aus journalistischen Quellen und einigen weiteren Vertragsunterlagen von Doctolib ergaben. Am letzten Tag der gesetzten Antwortfrist von 2 Wochen, also am 08.04.2021, ging von Doctolib folgende Antwort ein: *Den angehängten Fragebogen werden wir gerne vollumfänglich beantworten, bitten jedoch noch um etwas Geduld Ihrerseits, sodass wir in angemessenem Umfang auf Ihre Fragen eingehen können.* Mit Mail vom 09.04.2021 wurde daraufhin von mir eine weitere Antwortfrist von einer Woche eingeräumt, worauf folgende Antwort von Doctolib einging: *Sie können in spätestens einer Woche mit einer Antwort unsererseits rechnen. Haben Sie vielen Dank für die Geduld.* Am 15.04.2021 erhielt ich eine Mail von der Leiterin der Rechtsabteilung von Doctolib, Grit Karg, mit folgendem Text: *Ich leite die Rechtsabteilung von Doctolib in Deutschland und würde mich freuen, wenn wir zunächst miteinander sprechen könnten. Ich würde gerne verstehen, was der genaue Hintergrund Ihrer Fragen ist und wofür die Antworten verwendet werden sollen.*

In einem **Telefonat mit der Leiterin der Rechtsabteilung** an 16.04.2021 teilte ich dieser mit, dass die Fragen des Netzwerks Datenschutzexpertise dazu dienten, das Angebot von Doctolib, das aus Datenschutzsicht interessant sei, zu verstehen und offene Aspekte zu klären. Der faktische Hintergrund

[22] Datenlecks in deutschen Arztpraxen Massenhaft sensible Patientendaten waren für Unbefugte zugänglich, 30.12.2020, https://www.spiegel.de/netzwelt/web/arztpraxen-sensible-patientendaten-waren-fuer-unbefugte-zugaenglich-a-b786d37c-8dc5-4e03-b20d-a51bb9751264; https://media.ccc.de/v/rc3-11342-tut_mal_kurz_weh_neues_aus_der_gesundheits-it; Wasner, Datenpanne bei Online-Terminbuchungsportal, 19./25.01.2021, https://www.medical-tribune.de/praxis-und-wirtschaft/praxismanagement/artikel/datenpanne-bei-online-terminbuchungsportal/.

[23] https://f.hubspotusercontent30.net/hubfs/5479688/B2B%20-%20Press/Meine%20Stellungnahme-%20um%20klar%20zu%20stellen-%20was%20am%2021.%20Juli%202020%20passiert%20ist%20und%20wie%20wir%20die%20Gesundheitsdaten%20unserer%20Nutzer%20schu%CC%88tzen..pdf.

der juristischen Fragen wurde von mir ausführlich erläutert. Es wurde darauf hingewiesen, dass das geplante Gutachten aus eigenem Antrieb einer Nicht-Regierungsorganisation erstellt wird und keine Fremdfinanzierung erfolgt. Die Leiterin der Rechtsabteilung erklärte, Docotlib habe nichts zu verbergen; die umfangreichen Fragen würden aber einen hohen Aufwand auslösen. Vertragsdokumente von 2019, auf die ich bei meinen Fragen Bezug genommen habe, seien inzwischen aktualisiert worden. Die Struktur der Datenverarbeitung sei jedoch nicht geändert worden. Ich bot – zur Vermeidung von zu viel Aufwand – an, statt der Beantwortung der Fragen einige erbetene Dokumente zuzusenden, u.a. einen aktuellen Vertrag zur Auftragsverarbeitung. Eine erbetene Zusage, vor einer Veröffentlichung des Gutachtens des Netzwerks Datenschutzexpertise dieses Doctolib zur Prüfung zur Verfügung zu stellen, wurde von mir abgelehnt mit dem Hinweis, dass damit für das Netzwerk Datenschutzexpertise das Risiko entstehen könne, gerichtlich von einer Veröffentlichung abgehalten zu werden. Ein Gutachten werde nach besten Wissen und Gewissen erstellt und bedürfe für eine Veröffentlichung nicht einer Freigabe durch Doctolib. Als späteste Rückmeldefrist wurde der 30.04.2021 angegeben. Mit Mail vom 15.05.2021 kündigte die Justiziarin des Unternehmens an, sich mit Antworten in der darauf folgenden Woche zu melden, was jedoch nicht geschah.

2 Anforderungen an ärztliche Apps

Auf dem deutschsprachigen Markt gibt es mehr als 100.000 **Gesundheits-Apps** – von Fitness- und Entspannungsprogrammen hin bis zu Diagnose-Apps, Symptom-Checkern und Medikationsmanagern sowie medizinischen Vermittlungsdiensten. Die Bereitschaft der Bevölkerung, sich auf digitale Lösungen im Gesundheitswesen einzulassen, hat stark zugenommen und ist inzwischen groß. Einheitliche verbindliche Datenschutzvorgaben für derartige Apps existieren bisher nicht. Entsprechende Pläne, wie sie 2016 vom damaligen Bundesgesundheitsminister Hermann Gröhe angekündigt wurden[24], sind nicht umgesetzt worden.

Anzuwenden sind die allgemeinen Regelungen **des Medizinrechts und des Datenschutzrechts**. Medizinrechtlich ist der Schutz des Patientengeheimnisses (berufliche Schweigepflicht, § 9 MBÖÄ, § 203 Abs. 1 Nr. 1 StGB) von zentraler Relevanz. Datenschutzrechtlich steht die Anwendung der europäischen Datenschutz-Grundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) sowie des Telemedienrechts (u.a. Telemediengesetz – TMG) im Vordergrund.

Das Aktionsbündnis Patientensicherheit e.V. hat 2019 eine „**Checkliste** für die Nutzung von Gesundheits-Apps“ veröffentlicht, die Nutzenden Anhaltspunkte für die App-Auswahl geben.[25] Bewertungsaspekte sind demnach vertrauenswürdige Zertifizierungen, gut auffindbare, verständliche und informative Datenschutzerklärungen, ein erkennbares vertrauenswürdiges Geschäftsmodell, Neutralität und das Fehlen kommerzieller Interessen.

Ende 2019 wurde das Sozialgesetzbuch (SGB) V mit dem Digitale-Versorgung-Gesetz[26] um einen § 33a erweitert, der „**Digitale Gesundheitsanwendungen**“ regelt. Diese kurz „DiGA“ bezeichneten Anwendungen sind digitale, vom Arzt verschriebene Medizinprodukte, die vom Bundesinstitut für

[24] Schmergal, In der App-Falle, Der Spiegel 17/2016, 41.
[25] https://www.aps-ev.de/app-checkliste/.
[26] G. v. 09.12.2019, BGBl. I S. 2562.

Arzneimittel und Medizinprodukte in ein Verzeichnis nach § 139e SGB V aufgenommen werden. Hierfür ist es nötig, dass in Bezug auf das Produkt u.a. nachgewiesen wird, dass es „den Anforderungen an den Datenschutz entspricht und die Datensicherheit nach dem Stand der Technik gewährleistet". Die konkreten Anforderungen durch Datenschutz und Datensicherheit sind in § 4 Digitale Gesundheitsanwendungen-Verordnung (DiGAV)[27] geregelt. Darin ist u.a. vorgesehen, dass für den Einsatz der Anwendung eine separate Einwilligung einzuholen ist, die Verarbeitung in einem Staat mit angemessenem Datenschutzniveau erfolgen muss, andere Zwecke als die Gesundheitsanwendung, insbesondere Werbezwecke ausgeschlossen sein müssen, und die Betreibermitarbeiter zur Verschwiegenheit zu verpflichten sind. In einer Anlage 1 zur DiGAV präzisiert ein „Fragebogen gemäß § 4 Absatz 6" die datenschutzrechtlichen Anforderungen.[28]

Bei der Anwendung von Doctolib handelt es sich nicht um eine DiGA i.S.d. Gesetzes. Wegen ihrer Nähe zur medizinischen Behandlung sind aber entsprechende **hohe Anforderungen** zu stellen.

In Art. 42 DSGVO ist die **datenschutzrechtliche Zertifizierung** von Verarbeitungsprozessen vorgesehen. Die hierfür notwendigen Prozesse, die u.a. die Etablierung von Zertifizierungsstellen voraussetzen (Art. 43 DSGVO), waren im Juni 2021 noch nicht etabliert, so dass bisher auch noch keine Gesundheitsanwendungen gemäß der DSGVO zertifiziert werden konnten.

3 Das Regelwerk und die Internet-Präsenz von Doctolib

Selbst für erfahrene Verbraucher- und Datenschützer oder Medizinrechtler ist es nicht einfach, das **unübersichtliche (vertragliche) Regelwerk** von Doctolib, das weitgehend im Internet verfügbar ist, zu durchdringen und für eine einheitliche Interpretation zusammenzuführen, auf deren Grundlage dann eine rechtliche Bewertung durchgeführt werden kann. Ein Grund hierfür ist, dass Doctolib davon ausgeht, in unterschiedlichen rechtlichen Funktionen tätig zu sein – im Verhältnis zu Patienten, zu medizinischen Leistungserbringern sowie zu anderen Unternehmen – und sich teilweise als Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO und teilweise als Auftragsverarbeiter einstuft (s.u- 4.4, 4.5). Die Texte richten sich an unterschiedliche Adressaten – insbesondere an die Patientinnen und Patienten sowie an die medizinischen Leistungserbringer, die von vom Unternehmen „Gesundheitsfachkräfte" genannt werden – mit teilweise unterschiedlichen Aussagen. Die aus Datenschutzsicht relevanten Informationen sind auf unterschiedliche Dokumente, die teilweise aufeinander verweisen, verteilt.

3.1 Grundinformationen zum Unternehmen

Folgende Angaben zum Unternehmen sind allgemein verfügbar[29]:

Doctolib GmbH, Mehringdamm 51, 10961 Berlin. Telefon: +49 (0)89 20702884. E-Mail: kontakt@doctolib.de. Geschäftsführer: Stanislas Niox-Château, Dr. Ilias Tsimpoulis, Handelsregister: Amtsgericht Charlottenburg (Berlin), HRB 175963 B, Umsatzsteuer-Identifikationsnummer: DE306923884, Datenschutzbeauftragte: Frau Justine Bourdeu (Email: datenschutz@doctolib.de), Zuständige Datenschutzbehörde für die Doctolib GmbH ist die Berliner Beauftragte für Datenschutz

[27] DiGAV v. 08.04.2020, BGBl. I S. 768.
[28] BGBl. I 2020, 779-792.
[29] https://www.doctolib.de/terms/legal-notice.

und Informationsfreiheit, Friedrichstr. 219, 10969 Berlin. Eine frühere Adresse des Unternehmens (Wilhelmstrasse 118, Aufgang C, 10963 Berlin) ist nicht mehr gültig.

Die Doctolib GmbH ist ein Tochterunternehmen der **Doctolib SAS**, 54 Quai Charles Pasqua, 92300 Levallois-Perret, Frankreich Telefon: +33 (0)1 83 355 358, E-Mail: support@doctolib.fr, Geschäftsführer: Stanislas Niox-Château, Handelsregister (Frankreich): RCS Nanterre 794 598 813, SIRET: 79459881300036, Umsatzsteuer-Identifikationsnummer: FR1479459881, Federführende Aufsichtsbehörde für die Unternehmensgruppe ist die nationale französische Datenschutzaufsichtsbehörde, die Commission Nationale de l'Informatique et des Libertés (CNIL).

Doctolib nimmt an keinen formellen **Streitbeilegungsverfahren** teil, auch nicht an der von der Europäischen Kommission bereitgestellten Plattform für außergerichtliche Online-Streitigkeiten in Verbraucherangelegenheiten (https://ec.europa.eu/consumers/odr).

Doctolibs **Webseite verlinkt** auf Facebook, Instagram, Twitter, Medium, LinkedIn und YouTube.

Doctolib wirbt mit folgenden **Zertifikaten bzw. Gütesiegeln**: „Zertifiziertes Hosting" (der Begriff bezieht sich offenbar auf die unter 14.1. dargestellte HDS-Zertifizierung), TÜV Saarland – geprüfter Datenschutz[30], IPS – datenschutz-cert – Gütesiegel[31] (s.u. 15). Außerdem wirbt Doctolib für sich damit, am 17.11.2020 den „German Medical Award 2020" verliehen bekommen zu haben, womit in Zusammenarbeit mit der Landeshauptstadt Düsseldorf und unter der Schirmherrschaft von Karl-Josef Laumann, Minister für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, ein Preis verliehen wurde für „besonderes Engagement und fortschrittliche Patientenversorgung".[32]

Doctolib wirbt zudem für sich damit, dass es bei „Cyrating", das jeden Monat die **Cybersicherheit** und DSGVO-Konformität bewerte, mit einem Cybersicherheits-Score von 83/100 bewertet würde und damit von 109 bewerteten Gesundheitsunternehmen zu den Top 3 Unternehmen mit einem Score von über 80 zähle und immer wieder den ersten Platz erziele. Docotlib sei „in puncto Cybersicherheit die #1".[33]

3.2 Überblick über die Dokumente

Folgende Internet-Dokumente enthalten Aussagen zum Datenschutz bei Docotlib:

1- Allgemeine Nutzungsbedingungen für Patienten (ANB),[34]
2- Begriffsbestimmungen (BB),[35]
3- Datenschutzhinweise für Patienten (DHPat),[36]
4- Grundsätze zum Schutz von Gesundheitsdaten für Ärzte und Behandler und Gesundheitseinrichtungen, (Datenschutzcharta, DChartaG),[37]

[30] https://www.tuev-saar.de/zertifikat/tk44448/.
[31] https://ips.datenschutz-cert.de/doctolib.
[32] https://info.doctolib.de/blog/doctolib-erhaelt-german-medical-award-2020/.
[33] https://info.doctolib.de/datenschutz/.
[34] https://www.doctolib.de/terms.
[35] https://res.cloudinary.com/doctolib/image/upload/v1601026133/legal/DE_Def_Patient.pdf.
[36] https://www.doctolib.de/terms/agreement.
[37] https://cdn2.hubspot.net/hubfs/5479688/B2B%20-%20Data%20security/Datenschutzgrundsa%CC%88tze%20fu%CC%88r%20A%CC%88rzte.pdf.

5- Grundsätze zum Schutz von Gesundheitsdaten für Patienten (DChartaP),[38]
6- Datenschutzhinweise für personenbezogene Daten – Gesundheitsfachkräfte (DHGes),[39]
7- Liste der Verarbeitungen für die Doctolib in seiner Eigenschaft als verantwortliche Stelle/ Auftragsverarbeiter handelt (Liste).[40]
8- Cookie-Richtlinie (Informationen über Cookies, CookieRL),[41]

Herangezogen werden bei der rechtlichen Bewertung von Doctolib folgende weiteren Dokumente, die nicht im Internet gefunden werden konnten:

9- AGB Nutzer (AGBN),[42]
10- Ab dem 25. Mai 2018 geltende Datenschutzbestimmungen DOCTOLIB (DSBest),
11- Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO (DAV).

Nicht als Vertragsbedingung formuliert, aber als Nutzerinformation zum Datenschutz bestimmt sind zwei weitere im Internet verfügbare Dokumente:

12- Datenschutz und Sicherheit (DuS),[43]
13- Sie haben die Kontrolle über Ihre Gesundheitsdaten (Regeln und FAQ, FAQ)[44].

Eine Hierarchie unter den in Bezug genommenen Regeln ist nicht festzustellen. Sie werden daher in der folgenden Darstellung gleichrangig behandelt. Im Gutachten *kursiv* gesetzte Texte sind Originalzitate von Doctolib. Zwecks Zuordnung der einzelnen Zitate werden die oben dargestellten Dokumente mit eckigen Klammer (z.B. [1]) gekennzeichnet.

3.3 Doctolibs Datenschutzbekenntnis

Wer die Unterlagen von Doctolib als unbefangener Leser zur Kenntnis nimmt, kann vom Datenschutzengagement begeistert sein. Das Unternehmen bekennt sich zur **Beachtung des Datenschutzrechtes und zur ärztlichen Vertraulichkeit** (Patientengeheimnis). Beispiel dafür ist die Einleitung zu den „Datenschutzbestimmungen DOCTOLIB“ (DHPat [3]):

Für DOCTOLIB hat die Sicherheit und die Geheimhaltung personenbezogener Daten seiner Nutzer oberste Priorität. Daher verpflichtet sich DOCTOLIB, alle deutschen und europäischen Vorschriften zum Schutz personenbezogener Daten einzuhalten.
DOCTOLIB hält sich an die von den jeweiligen Kammern und Verbänden erlassenen Standesregeln für Ärzte und Heilberufler.
DOCTOLIB wendet, wie folgt aufgeführt, eine äußerst strenge Datenschutzpolitik an, um die Sicherheit der persönlichen Gesundheitsdaten seiner Nutzer zu gewährleisten:
Jeder Nutzer verfügt alleinig über seine Daten. DOCTOLIB kann diese Daten nur zu den im Folgenden aufgeführten Zwecken verarbeiten.
Die Verarbeitung der Daten erfolgt nachvollziehbar, vertraulich und nach hohen Sicherheitsstandards.

[38] https://cdn2.hubspot.net/hubfs/5479688/B2B%20-%20Data%20security/Charter%20-%20%20Datenschutzgrundsa%CC%88tze%20fu%CC%88r%20Patienten.pdf.
[39] https://info.doctolib.de/datenschutzerklaerung/.
[40] https://res.cloudinary.com/doctolib/image/upload/v1603208641/legal/Liste_traitements-DE-Octobre_2020.pdf.
[41] https://www.doctolib.de/cookies.
[42] Stand 12.08.2019.
[43] https://info.doctolib.de/datenschutz/.
[44] https://about.doctolib.de/datenschutz.html.

DOCTOLIB verpflichtet sich, in Übereinstimmung mit dem am 30. Juni 2017 geänderten Bundesdatenschutzgesetz (im Weiteren "BDSG") und mit der Datenschutz-Grundverordnung vom 27. April 2016 (im Weiteren „DSGVO"), zu einer kontinuierlichen Kontrolle und Verbesserung der bestehenden Datenschutz-Maßnahmen.
DOCTOLIB verfügt über ein eigenes Datenschutz-Team, das darauf spezialisiert ist, das bestehende bereits sehr hohe Sicherheitsniveau nicht nur zu halten, sondern stetig weiter zu verbessern. Zu diesem Team gehören neben Juristen auch ein Datenschutzbeauftragter, ein Chief Security Officer sowie ein speziell im Datenschutz und in Datensicherheit ausgebildetes Team an Entwicklern.
Personenbezogene Gesundheitsdaten der Nutzer werden in zwei gesondert zertifizierten Rechenzentren mit physischem Wachschutz gehostet.

Dotolib bekennt sich nicht nur zum rechtlich geforderten Datenschutz, sondern behauptet, **mehr als rechtlich gefordert** beim Schutz der Gesundheitsdaten zu tun: *Unser Engagement geht über unsere rechtlichen Verpflichtungen hinaus* (FAQ [13]). Worin genau der Datenschutzmehrwert des Angebots liegt, wird nicht erläutert.

Weiterhin wird erklärt:

Wir arbeiten mit den Behörden, die für den Schutz von personenbezogenen Daten zuständig sind, zusammen. Auch stehen wir im stetigen Austausch mit den öffentlichen Akteuren des Gesundheitswesens sowie den Vertretern der Patienten, Ärzte, Behandlern und der Gesundheitseinrichtungen. So stellen wir sicher, dass wir unseren Verpflichtungen zum Schutz der personenbezogenen Gesundheitsdaten in vollem Umfang nachkommen (FAQ [13]).

Eine Nachfrage beim für die Doctolib GmbH **zuständigen Datenschutzbehörde**, der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI), ergab, dass es nicht zutrifft, dass eine Zusammenarbeit erfolgt. Wohl aber gäbe es einen Austausch mit Doctolib im Rahmen von datenschutzrechtlichen Kontrollen.

In den folgenden Kapiteln soll überprüft werden, ob die vollmundigen Datenschutzbekenntnisse aus rechtlicher und aus tatsächlicher Sicht begründet sind.

4 Datenschutzrechtliche Verantwortlichkeiten

Beteiligte im Doctolib-Verfahren sind neben der Doctolib GmbH die Patientinnen und Patienten als Benutzer, die medizinischen Leistungserbringer, deren Termin verwaltet werden, eingebundene soziale Netzwerke sowie weitere Stellen, insbesondere informationstechnische Dienstleister für Doctolib, Datenquellen, die von Doctolib verwendet werden, sowie Dritte, für die z.B. Meinungsumfragen oder Werbemaßnahmen durchgeführt werden.

Die medizinischen Leistungserbringer, für die Doctolib Termine vergibt und denen weitere Services angeboten werden, sind niedergelassene Ärzte sowie Zahnärzte, Heilpraktiker, Therapeuten und seit der Corona-Pandemie auch Impfeinrichtungen. Doctolib verwendet für diese den übergeordneten Begriff der „**Gesundheitsfachkraft**", wobei nicht zwischen der natürlichen handelnden Person (so [2]) und einer im Gesundheitsbereich tätigen juristischen Person unterschieden wird (§ 2 Abs. 2 AGBN – [9]). Dies ist aus rechtlicher Sicht angreifbar, da insofern unterschiedliche Regelungen gelten: Während das Medizinrecht die Person des Berufsgeheimnisträgers, also vorrangig die leitende Ärztin oder den Arzt adressiert, wenden sich die Regelungen des Datenschutzrechtes an die verantwortliche Stelle.

Dabei handelt es sich oft um eine juristische Person, z.B. Krankenhäuser, deren Leitung nicht bei ärztlichem Personal liegen muss.

4.1 Verantwortlichkeit und Auftragsdatenverarbeitung

„**Verantwortlicher**“ i.S.v. Art. 4 Nr. 1 DSGVO ist diejenige Stelle oder Person, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Rechtliche Folge der datenschutzrechtlichen Verantwortlichkeit ist, dass folgende Einstandspflichten bestehen: Rechtmäßigkeit der Verarbeitung (u.a. Art. 6ff. DSGVO), Dokumentations- und Protokollpflichten (Art. 5 Abs. 2, 30, 35 DSGVO), Umsetzung der Betroffenenrechte (Art. 12 ff., 34 DSGVO), Umsetzung der gebotenen technisch-organisatorischen Maßnahmen (Art. 24, 25, 32 DSGVO).

„**Auftragsverarbeiter**“ ist nach Art. 4 Nr. 8 DSGVO die Stelle, „die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Voraussetzung für eine rechtlich wirksame Auftragsverarbeitung ist gemäß Art. 28 DSGVO, dass diese auf Grundlage eines Vertrages erfolgt, der die vollständige Weisungsabhängigkeit vom Verantwortlichen gewährleistet. Den Einsatz der Mittel und insbesondere der „geeigneten technischen und organisatorischen Maßnahmen“ kann dem Auftragsverarbeiter vom Verantwortlichen überlassen werden. Die Verarbeitung muss sich aber auf Hilfstätigkeiten beschränken. Das Nutzen der Daten für eigene Zwecke ist ausgeschlossen. Bestimmt ein Auftragsverarbeiter die Zwecke der Datenverarbeitung unter Verstoß gegen die DSGVO selbst, so gilt er gemäß Art. 28 Abs. 10 DSGVO „in Bezug auf diese Verarbeitung als Verantwortlicher“.

Es gibt weiterhin die rechtliche Konstruktion der **gemeinsamen Verantwortlichkeit**, die in Art. 26 DSGVO geregelt ist. Der EU-Gesetzgeber wollte mit der seit 2018 geltenden Regelung angesichts der komplexen Realität von verschachtelten informationstechnischen Vorgängen eine klare Zuordnung der Verantwortungsbereiche schaffen. Die Verantwortlichen sollen ihre DSGVO-Pflichten in einer Vereinbarung gemäß Art. 26 DSGVO klar und transparent verteilen.[45] Gemeinsame Verantwortlichkeit ist gegeben, wenn eine Verarbeitung selbständige Entscheidungen verschiedener Stellen voraussetzen, d.h. wenn eine Verarbeitung ohne die aktive Beteiligung jeder der Stellen nicht denkbar ist, also ein kumulatives Zusammenwirken erfolgt.[46] Eine zeitgleiche und gemeinsam abgestimmte Entscheidung über Zwecke und Mittel ist nicht nötig.[47] So kann die gemeinsame Verantwortung dadurch entstehen, dass im Voraus von einem Anbieter festlegte Zwecke und Mittel von einem Nutzer akzeptiert werden, indem er diese für sich in Anspruch nimmt.[48] Beteiligt sein können zwei, aber auch viele Stellen. Für die Feststellung der gemeinsamen Verantwortlichkeit kommt es auf die objektiven tatsächlichen Umstände an, ein schriftlicher Vertrag ist nicht begriffsnotwendig.[49]

[45] Specht-Riemenschneider/Schneider MMR 2019, 504; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, S. 61.
[46] Weichert DANA 2019, 5.
[47] So aber Kremer CR 2019, 227; Bertermann in Ehmann/Selmayr, Art. 26 Rn. 10.
[48] DSK, Kurzpapier Nr. 16, Stand 19.03.2018, S. 3.
[49] EuGH 10.7.2018 – C-25/17 (Zeugen Jehovas), Rn. 67, NJW 2019, 285 = NZA 2018, 991 = NVwZ 2018, 1787 = EuZW 2018, 897; vgl. EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = NZA 2018, 919 = ZD 2018, 357 = NVwZ 2018, 1386 = EuZW 2018, 534 = MMR 2018, 591 = BB 2018, 1480 = DuD 2018, 518; EuGH 29.07.2019 – C-40/17 (Fashion ID), NJW 2019, 2755‘; NVwZ 2019, 1749; NZA 2019, 1125; MMR 2019, 579.

4.2 Die Rolle der Patientinnen und Patienten

Für die Nutzung des Ärzteverzeichnisses von Doctolib ist kein personalisiertes Konto nötig. Entsprechendes gilt für die Doctolib-Präsenz in Social Communities, soweit von diesen nicht die Einrichtung eines Kontos gefordert wird. Um die Online-Terminvereinbarung, die Telekonsultation und die Dokumentenverwaltung zu nutzen, bedarf es dagegen für die Patientinnen und Patienten eines **nutzerspezifischen Internet-Accounts.** Es besteht Klarnamenpflicht; Pseudonyme sind nicht zugelassen (Nr. 3.1, 4.1, 8 ii ANB [1]). Bei der Registrierung erhält der Nutzer eine SMS an eine von ihm angegebene Mobilfunknummer oder eine Mailnachricht mit einem Prüfcode, der zur Freischaltung des Nutzeraccounts eingegeben werden muss. Mit der Freischaltung kommt eine Nutzungsvereinbarung zustande, mit der die AGB einbezogen werden (§ 3 Abs. 2 AGBN [9]). Eine finanzielle Gegenleistung hierfür erbringt der Nutzer nicht (Nr. 1 ANB [1]).

In den Grundsätzen zum Schutz der Gesundheitsdaten für Patienten (GChartaP [5])wird diesen zugesagt: *2. Sie haben die Kontrolle über Ihre persönlichen Gesundheitsdaten. Wir können nicht frei über diese verfügen. 4. Sie können jederzeit auf Ihre persönlichen Gesundheitsdaten zugreifen oder Ihren Account löschen.*

Der Nutzer ist für die von ihm im Account z.B. zwecks einer Terminvereinbarung eingegebenen Daten verantwortlich, auch soweit sie dritte Personen, z.B. aus seinem Haushalt oder seiner Familie, betreffen. Eine darüber hinausgehende Verantwortlichkeit besteht nicht. D.h. i.d.R. handelt es sich bei den Nutzenden um „betroffene Personen“ (**Betroffene**) i.S.v. Art. 4 Nr. 1 DSGVO.

In Bezug auf den **Dokumentenverwaltungsservice** wird der Patient bzw. Nutzer für allein verantwortlich erklärt: *Der Nutzer bleibt der alleinige Eigentümer der Dokumente, die er dem Dokumentenverwaltungsservice hinzufügt, sowie der Dokumente, die von den Gesundheitsfachkräften mit ihm geteilt werden* (Nr. 12.2 S. 1, 12.12.3-12.5 ANB [1]). In seinen „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4]) heißt es unter 2. adressiert an die Gesundheitsfachkräfte: *Ihre Patienten haben die Kontrolle über ihre Gesundheitsdaten. Weder Sie noch wir können frei über diese Daten verfügen.*

Soweit in den **Dokumenten** Daten Dritter aufgeführt sind, versteht sich Doctolib insofern offenbar als im unjuristischen Sinn als Auftragsverarbeiter des Nutzers; als Betroffene werden diese rechtlich nicht als „Verantwortliche“ eingestuft. In Bezug auf Drittdaten ist eine gemeinsame Verantwortlichkeit von Nutzers und Doctolib gegeben, da nicht nur der Nutzer, sondern auch Doctolib über die Zwecke der Verarbeitung bestimmt (vgl. 4.1, 4.6).

Die Aussage Doctolibs über die ausschließliche Verfügungsmacht des Nutzers ist nicht ganz zutreffend. In der Liste der Verarbeitungen (Liste [7]) nimmt Doctolib für sich in Anspruch aufgrund eines „**berechtigten Interesses**“ die Stamm- und Metadaten bei der Plattformverarbeitung nutzen zu dürfen.

4.3 Die Rolle der Gesundheitsfachkraft

Die Gesundheitsfachkraft schließt mit Doctolib einen Nutzungsvertrag auf Abonnement-Basis ab. Gegenstand sind in erster Linie das Vereinbaren von Terminen und die Durchführung von Videosprechstunden (Telekonsultation). Insofern versteht sich Doctolib als *technischer Vermittler zwischen Nutzer und Gesundheitsfachkraft*; alleiniger Verantwortlicher sei die Gesundheitsfachkraft (Nr. 10, 11.3 ANB [1]).

In § 8 Abs. 1 S. 1 des Auftragsverarbeitungsvertrags (DAV 11) heißt es: *Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.* Diese Aussage ist juristisch in Bezug auf Datensätze unzutreffend: Der sachenrechtliche **Eigentumsbegriff** kann sich nicht auf Datensätze beziehen. Insofern bestehen Nutzungs- und Bestimmungsrechte, die u.a. durch das Datenschutzrecht vorgegeben werden.

Tatsächlich ist die Gesundheitsfachkraft in Bezug auf alle Datenverarbeitungsprozesse bei der Terminvermittlung und der Telekonsultation **Verantwortliche** i.S.v. Art. 4 Nr. 1 DSGVO. Die Verantwortlichkeit besteht sowohl für die Verarbeitung im Arztinformationssystem wie auch für sämtliche Nutzungsdaten über den Doctolib-Account, sobald und soweit sich der Nutzer für eine Terminvereinbarung oder eine Videosprechstunde bei der Gesundheitsfachkraft einwählt. Davor besteht keine Verantwortlichkeit.

4.4 Verantwortlichkeit der Doctolib GmbH

Die Doctolib GmbH gehört zur Doctolib-Gruppe, deren **Zentrale in Paris** liegt; sie ist eine Tochter des Pariser Unternehmens. Aus datenschutzrechtlicher Sicht liegt in Frankreich keine Verantwortlichkeit, auch soweit die ursprünglich dort entwickelte Software vom der Doctolib GmbH eingesetzt wird.

Die Doctolib GmbH ist für den **Betrieb der Webseite** www.doctolib.de verantwortlich. Dies gilt für sämtliche auf der Webseite dargestellten Inhalte, auch wenn diese von Drittanbietern übernommen worden sind.

Eine Verantwortlichkeit Doctolibs besteht auch für seine **Seiten in Social Communities**.

Doctolib beschreibt seine Verantwortlichkeit in DHPat [3] im Abschnitt 4 (Verantwortlicher) wie folgt: *Doctolib handelt in seiner Eigenschaft als Verantwortlicher für die Datenverarbeitung insbesondere bei Verarbeitungen bezüglich des Anlegens und der Verwaltung der Nutzerkonten, der Navigation der* Nutzer *auf der Webseite sowie der Nutzung der Doctolib-Plattform. Die Gesundheitsfachkräfte, also die Abonnenten der Services, handeln in ihrer Eigenschaft als Verantwortliche für die Verarbeitung personenbezogener Daten im Rahmen jeder Behandlung oder Nachsorge der Patienten. Doctolib handelt dann als Auftragsverarbeiter.*

In den FAQ [13] macht Docotlib darüber hinausgehend folgende Aussage: *Nur Patienten und ihre Ärzte haben die Rechte an den personenbezogenen Gesundheitsdaten, Doctolib verarbeitet diese nur im Auftrag der jeweiligen Gesundheitsfachkräfte. Doctolib ist nicht der Eigentümer der* personenbezogenen *Gesundheitsdaten der Patienten und kann nicht frei über diese verfügen.* Der Begriff eines **Dateneigentümers** existiert im Datenschutzrecht nicht und wird hier falsch verwendet. Er suggeriert, dass das Unternehmen keine eigenen Interessen mit den Daten verfolgt.

Die Verantwortlichkeit einer Stelle hängt von der Festlegung der verfolgten Zwecken ab (s.o. 4.1). Doctolib ist insofern in DHPat ([3], Abschnitt 5) unter der Überschrift *Zwecke der Datenerhebung* wenig präzise: *Bei der Benutzung der Doctolib-Plattform teilt der Nutzer bestimmte persönliche Daten mit, die Doctolib benötigt, um den angeforderten Service bereitzustellen.*

Präzisiert werden die **Zwecke** in einer *Liste der Verarbeitungen für die Doctolib in seiner Eigenschaft als verantwortliche Stelle handelt* (Liste [7] 3.1).[50] Darin werden folgende Zwecke aufgeführt:

Verwaltung der Doctolib-Nutzerkonten, Verwalten und Teilen von Dokumenten der Nutzer und deren Angehöriger, Bereitstellung von gesundheitsbezogenen Informationen zu den Services, Durchführung von fakultativen Umfragen, Bereitstellung von Informationen für Nutzer in Bezug auf die Verwaltung ihres Nutzerkontos, Betrieb der Videosprechstunde, Prävention und Bekämpfung von Computerkriminalität, Bereitstellung eines Supports für die Nutzer, Beschwerden und Wahrnehmung von Rechten.

4.5 Auftragsverarbeitung durch Doctolib

Doctolib gibt an, als Auftragsverarbeiter **für die Gesundheitsfachkraft** tätig zu sein. Dies gilt für die Terminabsprachen und die Versendung von SMS oder E-Mails zur Bestätigung von Terminen (Nr. 6.1, 6.2 ANB [1]): *Die Rolle von Doctolib ist auf die eines einfachen Vermittlers und technischen Dienstleisters beschränkt* (Nr. 7.1 S. 1 ANB [1]; ebenso DSBest [10]).

Präzisiert werden die **Zwecke** in der *Liste der Verarbeitungen, für die Doctolib in seiner Eigenschaft als Auftragsverarbeiter handelt* (Liste [7] 3.2; ebenso DSBest [10]).[51] Darin werden folgende Zwecke aufgeführt:

Bereitstellung eines Online-Kalenderservices und Online-Services für die Terminvereinbarung, Bereitstellung eines Telekonsultationsservices, Verwaltung der Betreuung des Patienten, Teilen von Dokumenten durch die Gesundheitsfachkraft, Beschwerden und Wahrnehmung der Rechte von Patienten, Fakultative Durchführung von Umfragen im Auftrag des für die Verarbeitung Verantwortlichen, Zusenden von Informationen und Empfehlungen an Patienten, Bearbeitung von Streitfällen, Verwaltung des Terminkalenders und der Versorgung des Patienten bei Epidemien.

Eine Auftragsverarbeitung kann nur angenommen werden, wenn zwischen dieser und der verantwortlichen Datenverarbeitung eine klare **technische (faktische) Trennung** vorgenommen wird. Werden im Auftrag verarbeitete Daten für eigene Zweck genutzt, dann ist die Stelle auch insofern als Verantwortlicher zu behandeln (Art. 28 Abs. 10 DSGVO). Unzulässig ist schon die Verknüpfung von für verschiedene Verantwortliche im Auftrag verarbeiteten Daten (Mandantentrennung). [52]

Eine solche **Mandantentrennung** scheint bei Doctolib nicht gewährleistet zu sein. Wie aus dem insofern unwidersprochenen Vortrag von Tschirsich/Saatjohann (s.o. 1.3 am Ende) entnommen werden kann, waren Daten von unterschiedlichen Auftraggebern technisch einfach zusammenführbar. Dadurch wird gegen die Vorgaben des Art. 28 DSGVO verstoßen. Dies hat zur Folge, dass Doctolib eine eigenständige Verantwortlichkeit zukommt.

[50] https://res.cloudinary.com/doctolib/image/upload/v1603208641/legal/Liste_traitements-DE-Octobre_2020.pdf.
[51] https://res.cloudinary.com/doctolib/image/upload/v1603208641/legal/Liste_traitements-DE-Octobre_2020.pdf.
[52] Datenschutzkonferenz (DSK), Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur - Orientierungshilfe Mandantenfähigkeit, Version 1.0 v. 11.10.2012, https://www.lda.bayern.de/media/oh_mandantenfaehigkeit.pdf.

4.6 Gemeinsame Verantwortlichkeit

Docotlib macht keinerlei Ausführungen zur gemeinsamen Verantwortlichkeit mit anderen Stellen. Dies scheint rechtlich wenig problematisch, soweit diese gemeinsame **Verantwortlichkeit mit dem Nutzenden** geteilt wird, etwa bei der Verarbeitung von Drittdaten. Durch die Nutzungsregelungen auf der Webseite werden die Verantwortlichkeiten gemäß Art. 26 DSGVO zwar verwirrend dargestellt aber insofern relativ klar festgelegt.

Hinsichtlich der **Plattform-Nutzungsdaten** besteht eine gemeinsame Verantwortlichkeit von Doctolib und den jeweiligen Gesundheitsfachkräften. Die Zwecke der Datenverarbeitung werden nicht nur vom Plattformbetreiber festgelegt, sondern auch von der Gesundheitsfachkraft, da diese Daten zur Organisation der Terminabwicklung oder zur Durchführung der Telekonsultationen unabdingbar sind. Eine Verarbeitung kann nicht zugleich als Auftragsverarbeitung und eigenverantwortliche Verarbeitung eingestuft werden.

Soweit Docotlib **Social Media** einbindet (s.u. 12) oder **Werbecookies** verwendet, besteht eine gemeinsame Verantwortlichkeit mit den Betreibern, bei der Einbindung von Ads z.B. mit Google. Es ist nicht ersichtlich, dass insofern Vereinbarungen vorliegen, die den Anforderungen des Art. 26 DSGVO genügen.

5 Medizinrechtliche Verantwortlichkeit

In seinen „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4]) heißt es unter 3.: *Die persönlichen Gesundheitsdaten Ihrer Patienten sind vertraulich: Sie sind nur für Sie und Ihre Patienten bestimmt*. In den Begriffsbestimmungen verwendet Doctolib den Begriff „vertrauliche Informationen“ für die Daten, die im Sinne des § 203 StGB unter die berufliche Schweigepflicht (Patientengeheimnis) fallen (BB [3]).

Unter § 7 AGBN-S. 2, 3 [9] heißt es unter der Überschrift „Datenschutz“: *DOCTOLIB gilt als Subunternehmer und Gehilfe der Gesundheitsfachkräfte, der die Bearbeitung der personenbezogenen Daten im Sinne einer Autragsdatenverarbeitung und in einer Gehilfenstellung durchführt. In diesem Rahmen entbindet der Nutzer den Gesundheitsfachkräften von der gesetzlichen Schweigepflicht.*

Medizinrechtlich verantwortlich für die Behandlung von Patienten ist personell vorrangig die Leitung bei einer „Gesundheitsfachkraft“, soweit es sich dabei um eine Stelle handelt, die als juristische Person die Gesundheitleistung erbringt. Handelt es sich bei der Gesundheitsfachkraft um einen Arzt, so sind die Berufsordnungen der Landesärztekammern anwendbar, die sich weitgehend an der Musterberufsordnung der Ärztekammern (MBOÄ) orientieren. Gemäß § 9 MBOÄ gilt für die Ärzte eine berufliche Schweigepflicht. Für andere verkammerte Heilberufe (z.B. Zahnärzte, Psychologen) gelten entsprechende Geheimhaltungspflichten. Ein Verstoß gegen diese Pflichten ist nach § 203 Abs. 1 Nr. 1 StGB strafbar. Von dieser Regelung betroffen sind Ärzte, Zahnärzte, Apotheker oder Angehörige eines anderen Heilberufs mit staatlich geregelter Ausbildung. Dies hat zur Folge, dass weitgehend alle Kunden von Doctolib, die dort **Gesundheitsfachkräfte** genannt werden, einer beruflichen Schweigepflicht unterliegen.

Strafbar ist die **unbefugte Offenbarung eines fremden Geheimnisses**, namentlich eines zum persönlichen Lebensbereich gehörenden Geheimnisses. Voraussetzung hierfür ist, dass der

Geheimnisträger oder der Betroffene ein sachlich begründetes Geheimhaltungsinteresse hat. Darunter fallen im medizinischen Bereich Angaben zur Krankheit (Art, Verlauf, Anamnese, Diagnose, Therapie, Prognose), festgestellte Auffälligkeiten und Mängel, Patienten betreffende Dokumente, Akten und Daten, Untersuchungsmaterial und Untersuchungsergebnisse, Angaben über persönliche, familiäre, berufliche, wirtschaftliche oder finanzielle Umstände. Erfasst wird schon der Umstand einer medizinischen Behandlung oder, dass eine Kranken-, Unfall- oder Lebensversicherung abgeschlossen wurde.[53] Wegen des grundrechtlichen Bezugs des Patientengeheimnisses ist der Begriff weit auszulegen. Darunter fällt schon die Identität eines konkreten Patienten, die Tatsache der Behandlung, die Terminfestlegung hierfür oder das Aufsuchen der schweigepflichtigen Gesundheitsfachkraft.[54] Terminvereinbarungen und die Wahrnehmung von Untersuchungs- und Behandlungsterminen unterliegen also der beruflichen Schweigepflicht.

Es ist unklar, inwieweit Mitarbeiter von Doctolib Kenntnis von Berufsgeheimnisse der Gesundheitsfachkräfte nehmen können. Im Anhang 1 zum Auftragsvertrag (DAV [11]) heißt es: *End-to-End-Verschlüsselung: Verschlüsselung vertraulicher Arzt-/Patientendaten, so dass kein Doctolib-Mitarbeiter oder eine andere Person diese Daten lesen, ändern oder abrufen kann.* Diese Aussage kann nicht zutreffen, da bei der Terminverwaltung, also der Terminanfrage eines Patienten über die Plattform und der Terminbestätigung, die vom Berufsgeheimnis erfasst wird, eine entschlüsselte Verarbeitung im Klartext erfolgen muss, die zur einer **Kenntnisnahme** durch Doctolib führt. Es ist unklar, worauf sich die Aussage von Doctolib zur Kenntnisnahme bezieht. Auch der Import der Stammdaten, bei denen es sich um „vertrauliche Arzt-/Patientendaten" handelt, erfolgt unverschlüsselt.

Die Gesundheitsfachkraft ist verantwortlich, dass sämtliche Personen, die als Mitwirkende, also hier als Mitarbeiter von Doctolib, in die Behandlung und Beratung einbezogen werden, zur Wahrung des **Patientengeheimnisses verpflichtet** werden (§ 203 Abs. 4 S. 2 Nr. 1 StGB). Unter § 5 Abs. 2 des Auftragsvertrags (DAV [11]) verpflichtet sich Doctolib, *dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter die Vertraulichkeit der Daten gemäß Art 28 Abs. 3, 29, 32 DSGVO wahren und diese entsprechend auf das Datengeheimnis verpflichtet und in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen worden sind.* Dieser Passus genügt nicht den Anforderungen des § 203 StGB, da keine ausdrückliche Bezugnahme auf diese Regelung erfolgt.

6 Gesundheitsdaten als besondere Kategorie

Doctolib definiert in seinen **Begriffsbestimmungen** Gesundheitsdaten wie folgt (BB [3]):
"Personenbezogene Gesundheitsdaten" bezeichnet alle personenbezogenen Daten, die von einer Gesundheitsfachkraft bei Tätigkeiten zur Prävention, Diagnose, Behandlung oder psychologischen und medizinisch-psychologischen Behandlung, insbesondere im Rahmen der Nutzung der Services, erhoben werden.

Damit definiert das Unternehmen diese Datenkategorie **enger als Art. 4 Nr. 15 DSGVO**: Danach sind „Gesundheitsdaten" *personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit*

[53] BGH 10.02.2010 – VIII ZR 53/09, NJW 2010, 2511; Eisele in Schönke/Schröder, § 203 Rn. 5; Pohle/Ghaffari CR 2017, 490; Dochow, S. 817 ff.
[54] Dochow, S. 819 f. m.w.N.

einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Es kommt also nicht darauf an, dass die Daten von einer Gesundheitsfachkraft erhoben werden; auch ein Behandlungszusammenhang wird vom Gesetz nicht gefordert. ErwGr 35 S. 2 DSGVO stellt klar, dass dazu auch „Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsleistungen“ erhoben werden. **Terminverwaltungsdaten** einer Gesundheitsfachkraft sind also Gesundheitsdaten i.S.d. DSGVO, auch schon bevor sie von einer Fachkraft verarbeitet werden.

Noch nicht als Gesundheitsdaten zu kennzeichnen sind die Daten, die ein Internet-Nutzer bei der Einrichtung eines Kontos bei Doctolib eingibt. Aus diesen Daten werden Gesundheitsdaten, wenn sie im Rahmen einer **Kommunikation mit der Gesundheitsfachkraft**, etwa einer Terminvereinbarung oder einer Videosprechstunde, verwendet werden.

Die **Verarbeitung von Gesundheitsdaten** ist gemäß Art. 9 Abs. 1, 2 DSGVO nur unter engen Voraussetzungen zulässig. Im Hinblick auf Doctolib kommt es darauf an, dass für den konkreten Zweck in die Verarbeitung „ausdrücklich eingewilligt“ (Art 9 Abs. 2 lit. a DSGVO) wurde und/oder diese für „die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich“ erforderlich ist (Art. 9 Abs. 2 lit. h DSGVO).

Hat ein Nutzer ein Konto bei Doctolib eingerichtet und verabredet er über dieses Konto bei einer Gesundheitsfachkraft einen Termin, so liegt hierin eine **ausdrückliche Einwilligung** i.S.v. Art. 9 Abs. 2 lit. a DSGVO zur Verarbeitung dieser Daten im Rahmen der Erforderlichkeit. Die Datenverarbeitung durch Doctolib ist dann im Rahmen der Zweckfestlegung zulässig.

7 Import des Patientendatenstamms

Nimmt eine Gesundheitsfachkraft, etwa einer Arztpraxis, die Dienste von Doctolib in Anspruch, so bedarf es hierfür zunächst der Einrichtung einer Schnittstelle zwischen dem Arztinformationssystem (AIS) und Doctolib (Anhang 1 zu DAV [11]).[55] Über eine Kombinationssuche mit dem Namen stammdat. werden alle Patientenstammdaten herausgesucht und als *.csv-Datei von Doctolib als Excel-Datei importiert. Dabei war es zumindest in der Vergangenheit technisch nicht ausgeschlossen, dass auch Diagnosen, die z.B. in Freifeldern eingetragen sind, vom AIS exportiert wurden. Die Daten werden in eine Terminverwaltungslösung von Doctolib integriert, worüber die Ärzte dann ihre Termine verwalten können. Werden Termine ohne Einbindung von Doctolib mit einer Gesundheitsfachkraft vereinbart, so werden diese in die bestehenden Datenbestände eingepflegt.

7.1 Darstellung durch Doctolib

In den „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4], ähnlich DChartaP [5], DuS [12]) heißt es unter 9.: *Nur Sie und Ihre Patienten haben Zugriff auf die personenbezogenen Gesundheitsdaten. Kein Mitarbeiter bei Doctolib kann auf diese Daten zugreifen, es sei denn, Sie selbst stellen über Ihre Doctolib-Software eine entsprechende Anfrage für den Import von Daten aus Ihrer*

[55] Im DAV-Formular wird unterschieden zwischen 1. *Schnittstelle zwischen dem Doctolib Kalender und dem Kalender des Informationssystems,* 2. *lokale Schnittstelle, die es dem Doctolib Kalender ermöglicht, die Patientendaten aus dem Informationssystems zu synchronisieren, 3. VPN IP Sec zwischen dem Server und Doctolib (zur Bestätigung der Verfügbarkeit).*

alten Software oder eine Wartungs- oder Supportanfrage. In einem solchen Fall handeln wir stets unter Ihrer Aufsicht.

Es bleibt bei dieser Formulierung unklar, was mit dieser Passage bezweckt wird. Nicht nur der Zweck der importierten Daten bleibt im Unklaren, sondern auch, wie oft ein solcher Datenimport erfolgt und welche Daten er umfasst. Der Umfang der Daten ist aber vom Zweck abhängig und muss auf die Erforderlichkeit hierfür beschränkt bleiben.

In § 2 Abs. 2 S. 2 des Vertrags zur Auftragsverarbeitung (DAV [11]) heißt es: *Auf ausdrücklichen Wunsch des* Auftraggebers *und unter seiner Kontrolle und Verantwortung kann der Auftragnehmer ihn zusätzlich dabei unterstützen, die personenbezogenen Daten seiner Patienten in die Anwendung zu importieren.*

7.2 Auftragsdatenverarbeitung

Der Import des gesamten Patientenstammdatensatzes kann nicht über eine ausdrückliche **Einwilligung** der Betroffenen legitimiert werden, da diese von der Existenz des Doctolib-Angebots möglicherweise keine Kenntnis haben und hierzu keine Erklärung abgegeben haben. Deshalb nimmt Doctolib für sich in Anspruch, als Auftragsverarbeiter i.S.v. Art. 28 DSGVO für die Gesundheitsfachkraft tätig zu sein.

Bei Beachtung der Anforderungen des Art. 28 DSGVO ist eine **Verarbeitung von Gesundheitsdaten** legitimiert, ohne dass eine Einwilligung erforderlich ist. Bei Daten, die zugleich unter das Patientengeheimnis fallen, sind aber zusätzlich die Regelungen des § 203 StGB zu beachten.[56] Die Konferenz der deutschen Datenschutzaufsichtsbehörden erklärte zwar, dass regelmäßig keine Auftragsverarbeitung gegeben ist, wenn Berufsgeheimnisträger fremde Fachleistungen in Anspruch nehmen.[57] Etwas anderes muss aber wohl gelten, wenn solche Fachleistungen ausschließlich nach Weisung erfolgen. Dies kann bei einem Service zur verbindlichen Terminvereinbarung der Fall sein, auch wenn dem Auftragsverarbeiter hierbei ein gewisser Spielraum bei der Entscheidung über die Umsetzung des Auftrags verbleibt.[58]

Die Auftragsverarbeitung beschränkt sich aber nicht nur auf den Vorgang des Datenimports, sondern muss sich auf die gesamte weitere **Verarbeitungskette** erstrecken. Dies gilt für die Speicherung der Daten, den Abgleich im Fall einer Terminvereinbarung sowie die Löschung – unabhängig davon, ob die Daten verwendet worden sind oder nicht. Dies ist der Formulierung in § 2 Abs. 2 DAV [11] nicht zu entnehmen, weshalb der Auftragstext insofern fehlerhaft ist.

7.3 Mitwirkung bei einem Berufsgeheimnisträger

Gemäß § 203 Abs. 3 S. 1 StGB liegt kein Offenbaren im Sine der Vorschrift vor, wenn die Gesundheitsfachkraft einen bei ihr **berufsmäßig tätigen Gehilfen** zugänglich macht. Hierauf nimmt offenbar Doctolib unter § 7 AGBN-S. 2 [9] Bezug. Solche Gehilfen sind Personen, die in einem Beschäftigungsverhältnis mit der schweigepflichtigen Person stehen. Zwischen Schweigepflichtigem und Gehilfen muss ein innerer (i.d.R. arbeitsrechtlicher) Zusammenhang bestehen.[59] Diese

[56] Datenschutzkonferenz Kurzpapier Nr. 13 v. 17.12.2018, S. 2.
[57] Datenschutzkonferenz Kurzpapier Nr. 13 v. 17.12.2018, S. 4.
[58] Hartung in Kühling/Buchner, Art. 28 Rn. 30.
[59] Eisele in Schönke/Schröder, § 203 Rn. 25.

Voraussetzungen sind bei einem externen informationstechnisch ausgerichteten Dienstleister nicht gegeben.

Gemäß § 203 Abs. 3 S. 2 StGB ist eine Offenbarung auch an sonstige Personen zulässig, die an der „beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen **mitwirkenden Personen** erforderlich ist".

In der Gesetzesbegründung zu § 203 Abs. 3, 4 StGB werden **Beispiele für „mitwirkende Tätigkeiten"** gegeben. Darunter fallen „Schreibarbeiten, Rechnungswesen, Annahme von Telefonanrufen, Aktenarchivierung und -vernichtung, Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten sowie Mitwirkung an der Erfüllung von Buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers".[60] Der Katalog in der Gesetzesbegründung ist nicht abschließend. Das neue Gesetz will „keinen möglichen Rechtsgrund, auf dem eine sonstige Mitwirkung beruhen kann, ausschließen".[61] Typischerweise besteht ein Vertragsverhältnis. Notwendig ist die **Einbindung in die berufliche Tätigkeit** und das Einvernehmen hierüber mit dem Berufsgeheimnisträger. Die Einbindung soll sich nicht auf informationstechnische Aktivitäten beschränken, sondern kann umfassend Unterstützungsleistungen einbeziehen.[62]

Die Erforderlichkeit ist hier also grds. weit auszulegen. Sie umfasst in jedem Fall informationstechnische Dienstleitungen für Gesundheitskräfte. Nicht nur der Betrieb einer Arztsoftware, sondern auch die informationstechnische Abwicklung der Terminvereinbarung kann als erforderlich für Behandlung und Beratung angesehen werden.[63] Nimmt daher Doctolib in § 7 AGBN-S. 2, 3 [9] als „Subunternehmen" und „Auftragsverarbeiter" eine Aufgabe einer Gesundheitsfachkraft wahr, so ist insofern eine Offenbarung zulässig. Rechtsfolge einer gesetzlich erlaubten Mitwirkung i.S.v. § 203 Abs. 3 S. 2 StGB ist, dass die mitwirkende Person ebenso wie der Geheimnisträger selbst gemäß § 53a StPO zeugnisverweigerungsberechtigt ist. Zugleich ist sie aber auch im gleichen Umfang geheimhaltungspflichtig (§ 203 Abs. 4 StGB).

Sowohl bei der der Auftragsverarbeitung wie auch der Mitwirkung muss für die Betroffenen die **Gesundheitsfachkraft als Verantwortliche erkennbar** sein.

In den „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4]) heißt unter 9. S. 3, 4 unter Bezugnahme auf den Datenimport aus der Arztsoftware: *In einem solchen Fall handeln wir stets unter Ihrer Aufsicht. Zudem verpflichtet jeder Arzt und Behandler Doctolib vertraglich zur Einhaltung einer umfassenden Schweigepflicht.*

Gesetzlich wird gefordert, dass die Tätigkeit, bei der ein Geheimnis zur Kenntnis genommen wird oder werden kann, erforderlich ist. Die **Erforderlichkeit der Dienstleistung** setzt voraus, dass diese nicht ohne Kenntnis des fremden Geheimnisses durchgeführt werden kann. Bei der Feststellung der Erforderlichkeit muss zwar eine Prüfung des konkreten Einzelfalls erfolgen, doch kann kein strenger

[60] BT-Drs. 18/11936, 22; Härting MDR 2018, 2.
[61] BT-Drs. 18/11936, 22 f.; Eisele JR 2018, 83.
[62] Grosskopf/Momsen CCZ 2018, 99.
[63] BT-Drs. 18/11936, 22; Härting MDR 2018, 2; Ruppert K&R 2017, 612, 613; Eisele JR 2018, 84.

Maßstab angelegt werden (s.o.).[64] Es liegt in der Freiheit des Berufsgeheimnisträgers, seine Arbeitsweise selbst festzulegen. Hierzu gehört auch die Einbindung externer Unterstützung. Insofern genügt eine gesteigerte „Dienlichkeit".[65]

Nicht mehr erforderlich sind untergeordnete Dienstleistungen, bei denen in großem Umfang Patientengeheimnisse offenbart werden müssen. Es ist zu unterscheiden zwischen der Erforderlichkeit der Dienstleistung und der Erforderlichkeit der Offenbarung. Die Dienstleistung ist erforderlich, wenn sie vom Berufsgeheimnisträger und seinem Team nicht erbracht werden kann und **keine zumutbare Alternative** besteht. Gründe dafür, dass die Leistung nicht erbracht werden kann, können in fehlenden materiellen oder kognitiven Ressourcen liegen. Der Geheimnisträger hat einen weitgehenden Ermessensspielraum.[66] Auch das Ziel der Kostenersparnis sowie Qualitäts- und Verfügbarkeitsgründe können eine Erforderlichkeit begründen, wenn diese Gründe erheblich sind.[67]

Hinsichtlich der **Erforderlichkeit der konkreten Offenbarungen** muss dagegen ein strenger Maßstab angelegt werden. Die Grundsätze der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sind anwendbar, wobei wegen der Sensitivität der Daten besonders hohe Anforderungen zu stellen sind.[68] Verfügbare technische Mittel der Datenminimierung sind einzusetzen.[69] Bei der Verarbeitung von Berufsgeheimnissen kommt als Anforderung hinzu, dass möglichst wenige Personen bei einem externen Dienstleister eingebunden werden.

Diesen Anforderungen genügt Doctolib nicht, wenn es zwecks Terminvereinbarung einen **Stammdaten-Import** in Bezug auf sämtliche Patientinnen und Patienten vornimmt: Für die Feststellung der freien Termine in einer Arztpraxis bedarf es keiner namentlichen Zuordnung. Patienten, die kein Konto bei Doctolib haben, können auch keine Termine vereinbaren und sind hierfür nicht nötig. Die BlnBDI hat korrekt dargestellt, dass es für Terminerinnerungen durch Doctolib im Auftrag der Gesundheitsfachkraft einer Einwilligung der Betroffenen bedarf.[70] Terminerinnerungen sind für die Erbringung der ärztlichen Leistungen nicht erforderlich. Die Erforderlichkeit einer Auslagerung dieser Funktion auf einen Dienstleister ist nicht ersichtlich. Und selbst wenn man der Ansicht wäre, dass die Mitwirkungsbefugnis nach § 203 StGB sich auch auf Terminerinnerungen erstrecken würde, wäre es möglich und nötig, hierfür die Einwilligung bei den tatsächlich terminierten Patienten in die Datenübermittlung an Doctolib einzuholen.

Unzulässig ist auch, wenn der Subunternehmer und Auftragsverarbeiter die erlangten **Daten für eigene Zwecke** weiterverwendet. Die Offenbarungsbefugnis des § 203 Abs. 3 S. 2 StGB beschränkt sich auf das Erforderliche hinsichtlich der Unterstützung des berechtigten Berufsgeheimnisträgers. Ein eigenes geschäftliches Ziel darf der Mitwirkende mit den ihm offenbarten Daten nicht verfolgen. Die Mitwirkung muss gemäß der Weisung des primär zur Geheimhaltung Verpflichteten erfolgen. Dem

[64] Ruppert K&R 2017, 612, 613.
[65] Strenger Grosskopf/Momsen CCZ 2018, 102.
[66] Eisele JR 2018, 84.
[67] Momsen/Savić, KriPoZ 2017, 301; weitergehend Pohle/Ghaffari CR 2017, 493, die die wirtschaftliche Beurteilung vollständig dem Berufsgeheimnisträger überlassen; ähnlich die Gesetzesbegründung BT-Drs. 18/11936, 17 f.
[68] Dochow, S. 1355 ff. m.w.N.
[69] Eisele JR 2018, 84 f.; Weichert in DWWS, Art. 5 Rn. 48.
[70] BlnBDI, Jahresbericht 2019, Kap. 6.3 (S. 104).

Berufsgeheimnisschutz liegt eine eigene Zweckkomponente inne. Diese liegt in der Wahrung der Vertraulichkeit im Rahmen des Behandlungs- oder Beratungsverhältnisses. Es ist nicht erkennbar, wofür Doctolib den Gesamtpatientenstamm der einbezogenen Gesundheitskräfte nutzt.

Doctolib kann sich für die Verarbeitung und Nutzung der Daten aus dem Stammdatensatz und den Terminvereinbarungen für eigene Zwecke auch nicht auf die in § 7 AGBN-S. 3 [9] enthaltene **Schweigepflichtentbindung** berufen. Voraussetzung für eine solche Entbindung ist, dass diese informiert erfolgt (sog. informed consent). Informiert werden muss über Zweck, Verantwortliche, verwendete Daten und deren Verwendung. Aus medizinischer Sicht ist zusätzlich über Risiken und mögliche Schäden zu informieren.

Es ist das erklärte Ziel von Doctolib, eine umfassende **Kundendatenbank** aufzubauen und zu betreiben. In DHGes [6] wird als Verarbeitungszweck angegeben „*Pflege einer Kundendatenbank*“, in der Name, Vorname, Telefonnummer, E-Mail-Adresse und in Bezug auf Gesundheitskräfte *Spezialisierung, LANR-Nummer, Anschrift* zu speichern sind. Als Legitimation wird nicht das Vertragsverhältnis zwischen Doctolib und den Gesundheitskräften bzw. den Patienten genannt, sondern ein „berechtigtes Interesse“. Ein Rückgriff auf ein solches berechtigtes Interesse ist nur nötig, wenn keine vertragliche Rechtfertigung für eine Speicherung besteht, also z.B. Patienten erfasst werden, auch wenn diese keinen Account bei Doctolib zwecks Inanspruchnahme von Online-Leistungen eingerichtet haben.

8 Technisch-organisatorische Maßnahmen

Im Anhang 1 des Auftragsvertrags werden detailliert technisch-organisatorische Sicherungsmaßnahmen dargestellt (DAV [11]). Wie die technische Umsetzung des Terminbuchungsservices genau erfolgt und welche Funktion der Import der Patientenstammdaten dabei hat, geht aus den vorliegenden Unterlagen nicht hervor. Es kann abgeleitet werden, dass sämtliche personenbezogenen Prozesse zunächst auf **Rechnern von Doctolib sowie von Auftragsverarbeitern** des Unternehmens verarbeitet werden und die Ergebnisse über eine Schnittstelle in das Informationssystem der Gesundheitsfachkraft überspielt werden.

In den „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4] u. DChartaP [5]) heißt es unter 10: *Wir ergreifen zahlreiche mögliche Maßnahmen, um die Sicherheit der persönlichen Gesundheitsdaten Ihrer Patienten zu gewährleisten. Wir verschlüsseln diese Daten systematisch und auf mehreren Ebenen: Die Kommunikation mit unseren Servern wird verschlüsselt, die Daten werden vor ihrer Speicherung verschlüsselt, und die Speichermedien, auf denen diese verschlüsselten Daten abgespeichert sind, werden selbst verschlüsselt. Unser Sicherheitsteam arbeitet täglich daran, die Sicherheit dieser Daten zu gewährleisten und zu erhöhen.*

Weitergehende Zusagen werden in den FAQ [13]gemacht: *Die personenbezogenen Gesundheitsdaten von Patienten werden in Deutschland und Frankreich auf Servern gespeichert, die speziell für Gesundheitsdatenhosting zertifiziert (HDS) und mit den höchsten Sicherheitsstandards verschlüsselt sind. Nur Patienten sowie ihre Ärzte und Behandler können auf die Daten zugreifen.*

In *den* FAQ [13] macht Doctolib weitere Angaben zu den eingesetzten Sicherungsmaßnahmen (ebenso DuS [12]): *Doctolib ergreift zahlreiche Maßnahmen, um die Sicherheit der personenbezogenen Gesundheitsdaten der Patienten zu gewährleisten. Wir verschlüsseln diese Daten systematisch und auf mehreren Ebenen:*

- *Die Kommunikation mit unseren Servern wird verschlüsselt*
- *Die Daten werden vor ihrer Speicherung verschlüsselt*
- *Die Speichermedien, auf denen diese verschlüsselten Daten abgespeichert sind, werden selbst verschlüsselt.*

Alle *Dokumente, die Sie teilen, werden mittels einer Ende-zu-Ende-Verschlüsselung verschlüsselt, damit stellen wir sicher, dass nur Sie und Ihr Arzt auf diese Dokumente zugreifen können. Unser Sicherheitsteam arbeitet täglich daran, die Sicherheit dieser Daten zu gewährleisten und weiter zu erhöhen.*

Die Art der Verschlüsselung wird nicht dargestellt. Es ist davon auszugehen, dass der Abgleich der Terminkalender mit den Abfragen sowie sonstige **Auswertungsprozesse unverschlüsselt** erfolgen. Genaueres hierüber ist den Unterlagen nicht zu entnehmen.

Bei den Serviceleistungen von Doctolib handelt es sich um eine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1“ (s.o. 6). Daher muss gemäß Art. 35 Abs. 3 lit. b DSGVO eine **Datenschutz-Folgenabschätzung** durchgeführt werden, in der eine systematische Beschreibung der Verarbeitungsvorgänge, eine Bewertung der Risiken für die Betroffenen und eine Beschreibung, wie diese Risiken bewältigt werden sollen, enthalten sein muss (Art. 35 Abs. 7 DSGVO). Den vorliegenden Unterlagen ist nicht zu entnehmen, dass eine solche Folgenabschätzung durchgeführt worden ist, und wenn ja, welche Risiken mit welchen Maßnahmen bewältigt werden sollen.

9 Werbung – freiwillige Meinungsumfragen

In den „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4] und DChartaP [5]) heißt es: *6. Wir verwenden die personenbezogenen Gesundheitsdaten Ihrer Patienten nicht zu Werbezwecken oder zum Verkauf von Dienstleistungen. Dies entspricht nicht dem Geschäftsmodell von Doctolib. 7. Wir verkaufen die persönlichen Gesundheitsdaten nicht an Dritte.*

Dieses Bekenntnis wird in den FAQ bekräftigt [13]: *Doctolib verwendet diese Daten nicht anderweitig, verkauft diese nicht und gibt sie unter keinen Umständen an kommerzielle Anbieter weiter* (ebenso DSBest [10]).

Die Aussagen stehen im **Widerspruch** zu weiteren Aussagen: Unter *Zweck der Verarbeitung* führt Doctolib in DSBest [10]eine Verarbeitung *in Bezug auf Werbung und Cookies* auf, wofür die Einwilligung eingeholt werde.

Unter der Überschrift „*COOKIES" UND TAGS IM INTERNET“* wird die geplante **Werbenutzung** detaillierter beschrieben: *DOCTOLIB kann gelegentlich Internet-Tags (auch “Aktionstags” genannt; Single-Pixel-GIFs, ClearGIFs, unsichtbareGIFs und 1x1-GIFs) verwenden und sie über eine Partnerwerbung oder einen Spezialpartner für Webanalysen verwenden, der sich eventuell im Ausland befinden kann (und daher die entsprechenden Informationen einschließlich der IP-Adresse des Nutzers speichern kann). Diese Tags werden sowohl in den Online-Werbungen untergebracht, damit die Surfer Zugang zur Webseite haben, als auch auf ihren verschiedenen Seiten. Diese Technologie erlaubt DOCTOLIB, die Antworten der Besucher auf der Webseite und die Effizienz ihrer Aktionen zu bewerten (z.B. Anzahl der Zugriffe einer Seite und der gesuchten Informationen) sowie die Nutzung dieser*

Webseite durch den Nutzer. Der externe Dienstleister (Werbepartner oder Web-Analyst) kann gegebenenfalls mit diesen Tags Informationen über die Besucher der Webseite und anderer Internet-Webseiten sammeln, Berichte über die Tätigkeit der Webseite für DOCTOLIB erstellen und andere Services zu ihrer Nutzung und zum Internet liefern.

Als *„Nebenzweck"* benennt das Unternehmen zudem unter *Zweck der Verarbeitung* in den DSBest [10]: *„um freiwillige Meinungsumfragen über die Services von Doctolib anonym oder kurzfristig anonym durchzuführen".* Freiwillige **Meinungsumfragen** können nicht (kurzfristig) anonym, sondern müssen zumindest in der Erhebungsphase personenbezogen durchgeführt werden. Was mit der entsprechenden Formulierung gemeint bzw. beschrieben wird, ist unklar.

Eine Werbenutzung ist mit medizinischen Anwendungen **nicht verträglich**. Dies gilt nicht nur für Digitale Anwendungen gemäß dem SGB V, sondern auch für sonstige ärztlich genutzte informationstechnische Dienstleistungen.[71]

10 Umsetzung der Betroffenenrechte

Gemäß den Art. 12 ff. DSGVO haben Betroffene umfangreiche Betroffenenrechte. Dazu gehören ohne Betroffeneninitiative zu erfüllende Informationspflichten gegenüber den Betroffenen sowie Ansprüche auf Auskunft, Berichtigung, Löschung (dazu s.u. 11), Verarbeitungseinschränkung und Widerspruch.

10.1 Informationspflichten generell

Gemäß Art. 12 Abs. 1 DSGVO müssen „alle Informationen … und alle Mitteilungen …, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" vermittelt werden. Diesen Anforderungen wird Doctolib in vieler Hinsicht nicht gerecht:

Es werden unübliche, vom Gesetz abweichende und **unpräzise Begriffe** verwendet (z.B. „Gehilfe", „Gesundheitsfachkraft", „Gesundheitsdaten", „vertrauliche Informationen").

Die **Vielzahl der verwendeten Dokumente** und deren Gestaltung macht es für Betroffene und Anwendende unklar, welche Aussage mit welchem Inhalt gelten soll.

Widersprüchliche Formulierungen in den verschiedenen Dokumenten bzw. solche, die widersprüchlich erscheinen, verwirren bei der Lektüre zusätzlich.

10.2 Informationspflichten speziell

Gemäß Art. 14 Abs. 1 lit. c DSGVO muss ein Verantwortlicher Betroffene über Datentransfers an Empfänger oder zumindest über „Kategorien von Empfängern" informieren. Empfänger sind gemäß Art. 4 Nr. 9 DSGVO Stellen, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich dabei um Dritte oder um Auftragsverarbeiter handelt.[72] Im Fall einer Nutzung von Dienstleistern durch Gesundheitsfachkräfte und eines damit verbundenen Datentransfers an den Dienstleister, so wie dies beim Terminerinnerungsservice von Doctolib der Fall ist, müssen die Betroffenen hierüber informiert werden. Diese Pflicht obliegt in erster Linie den

[71] DSK v. 07.11.2019, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, Kap. II.3 (S. 5 f.).
[72] Weichert in DWWS, Art. 4 Rn. 99.

Gesundheitsfachkräften als Verantwortliche. Professionelle Dienstleister haben ihre in Datenschutzfragen weniger erfahrene Kunden, um die es sich regelmäßig bei Arztpraxen und sonstigen Gesundheitsfachkräften handelt, **auf ihre datenschutzrechtlichen Pflichten**, etwa bei der Sicherstellung der Betroffenenrechte, **hinzuweisen** (Art. 28 Abs. 3 lit. e DSGVO, vgl. § 7 DAV [11]).[73] Dies wurde in der Vergangenheit von Doctolib teilweise unterlassen, was die BlnBDI dies in ihrem Jahresbericht 2019 kritisierte.[74]

Diese Informationspflicht besteht auch in Bezug auf Patienten, deren **Daten per Import** von Doctolib nach dem Vertragsabschluss mit der Gesundheitsfachkraft übernommen werden und die zumeist auch nicht über ein Konto bei Doctolib verfügen (Bestandspatienten). Art. 13 Abs. 1 lit. e DSGVO besagt, dass „gegebenenfalls die Empfänger oder Kategorien von Empfängern" benannt werden müssen. Damit verpflichtet diese Regelung nicht nur zum Zeitpunkt der Erhebung. Vielmehr verpflichtet die Regelung auch nachträglich zur Information, wenn eine Auftragsverarbeitung oder Datenübermittlung gegeben ist.[75] Anderenfalls könnte sich ein Verantwortlicher immer dadurch einer Information über den Empfänger entziehen, dass er darlegt, die Datenweitergabe zum Erhebungszeitpunkt noch nicht abgesehen zu haben. Es kann auch nicht zutreffen, dass keine Informationspflicht bei Altdaten besteht, wohl aber bei neu erhobenen Daten, da sich insofern die Risiken für die Betroffenen nicht unterscheiden. Der Begriff „gegebenenfalls" bezieht sich darauf, dass auf die Information zu verzichten ist, wenn keine Datenweitergabe „gegeben" ist.

11 Löschung

Gemäß Art. 5 Abs. 1 lit. c und lit. e DSGVO dürfen Daten nur solange gespeichert werden, wie diese erforderlich sind. Gemäß Art. 17 Abs. 1 lit. a DSGVO hat der Betroffene nach **Wegfall der Erforderlichkeit** einen Löschanspruch. Die Aufbewahrungsfrist von Daten im Rahmen der ärztlichen Dokumentation beträgt grds. 10 Jahre (§ 630f Abs. 3 BGB, vgl. § 10 Abs. 3 MBOÄ).

11.1 Darstellung durch Doctolib

In DHPat ([3], Abschnitt 5 2.) macht Doctolib Aussagen zur **Aufbewahrungsdauer**:

Alle gesammelten personenbezogenen Daten werden in Abhängigkeit von dem Zweck der Verarbeitung und der für die Services geltenden rechtlichen Aufbewahrungsfristen für einen begrenzten Zeitraum verarbeitet und aufbewahrt.

Doctolib *legt die Aufbewahrungsfristen für personenbezogene Daten nur in seiner Eigenschaft als für die Datenverarbeitung Verantwortlicher fest. Im Rahmen der Verarbeitung in seiner Eigenschaft als Auftragsverarbeiter handelt Doctolib nur auf Weisung des für die Datenverarbeitung Verantwortlichen und bestimmt nicht selbst die Aufbewahrungsdauer der personenbezogenen Daten.*

[73] Petri in SHS, art. 28 Rn. 70.
[74] BlnBDI, Jahresbericht 2019, Kap. 6.3 (S. 105).
[75] Dix in SHS, Art. 13 Rn. 7; Schwartmann/Schneider in Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2018, Art. 13 Rn. 41; a.A.wohl Bäcker in Kühling/Buchner, Art. 13 Rn. 29.

Für jede Frage oder Klärung bezüglich der Aufbewahrungsdauer von personenbezogenen Daten, für die Doctolib nur ein Auftragsverarbeiter ist, empfehlen wir, dass Sie sich direkt an Ihre Gesundheitsfachkraft*, die für die Datenverarbeitung verantwortlich ist, wenden.*

Nach *Ablauf der Aufbewahrungsfristen werden die personenbezogenen Daten der Nutzer dauerhaft gelöscht oder anonymisiert.*

In jedem Fall werden gesetzliche Aufbewahrungspflichten, insbesondere im Zusammenhang mit medizinischen Daten eingehalten.

In den FAQ [13] macht Doctolib allgemeine Angaben zur Aufbewahrungsdauer der Daten: *Die personenbezogenen Gesundheitsdaten werden 10 Jahre aufbewahrt. Diese Aufbewahrungsfrist ist für ärztliche Aufzeichnungen gesetzlich vorgeschrieben. Ärzte können Doctolib jederzeit auch zu einer kürzeren oder längeren Aufbewahrungsfrist anweisen. Nach Beendigung des Vertrages mit einem Arzt oder Behandler werden die Daten innerhalb von 3 Monaten gelöscht. Die Daten, die bei der Anlegung eines Nutzerkontos angelegt werden, gelten: Sie können diese jederzeit in Ihrem Konto löschen.*

Im Anhang des Auftragsvertrags (DAV [11]) heißt es zur Speicherdauer: *Löschfrist … Innerhalb des Arztkontos: … 20 Jahre für Gesundheitseinrichtungen*.

In den Datenschutzhinweisen für die Gesundheitskräfte werden präzise Festlegungen für die Speicherfristen vorgenommen (DHGes 3. [6]). Danach werden **Verbindungs- und Nutzungsdaten** der Webseiten oder der Doctolib-Plattform (Datum und Uhrzeit des Webseitenbesuches oder Nutzung der Services, Sitzungs-ID) 6 Monate und die für die Navigation verwendete IP-Adresse 1 Jahr gespeichert. Als Zweck wird die Nutzungsanalyse der Anwendungen und der Geräte (Navigation auf der Webseite und Nutzung der Doctolib-Plattform) sowie die Vorbeugung und Bekämpfung der Computerkriminalität (Spamming, Hacking, DDos-Angriffe usw.) genannt, wofür Doctolib ein „berechtigtes Interesse“ habe.

E-Mail- und SMS-Adresse sowie Navigationsdaten werden danach unbefristet gespeichert, solange die Betroffenen keinen Widerspruch einlegen. Zweck der Daten sind Marketingmaßnahmen, auch über soziale Netzwerke. Gerechtfertigt wird auch diese Datenspeicherung mit dem „berechtigten Interesse“ von Doctolib. An einer anderen Stelle wird für die Speicherung von Navigationsdaten eine Dauer von 13 Monaten angegeben, wobei als Rechtsgrundlage die Einwilligung der Betroffenen angegeben wird.

11.2 Bewertung

Für die für „Gesundheitseinrichtungen“ vorgesehene **Aufbewahrungsdauer von 20 Jahren** gibt es keine rechtliche Grundlage. Der Verweis auf die Verantwortlichkeit der Gesundheitskräfte und deren Weisungen ist wenig hilfreich, da diese mangels Überblick über die verschiedenen Daten, deren Zwecke und der damit verbundenen Speicherdauer regelmäßig die Vorgaben von Doctolib ohne spezifische Weisungen übernehmen.

Soweit Daten einer ärztlichen Dokumentationspflicht unterliegen, sind diese nach 10 Jahren zu löschen. **Terminverwaltungsdaten** sind aber keine Behandlungsdaten, die in die Patientenakte zu übernehmen sind und unterliegen nicht der ärztlichen Dokumentationspflicht. Diese erfasst nur „die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen“ (§ 10 Abs. 1 MBOÄ,

vgl. § 630f Abs. 2 BGB). Terminverwaltungsdaten können und müssen grds. zeitnah nach Terminablauf gelöscht werden. Die Erforderlichkeit dieser Daten ist spätestens 3 Monate nach Terminablauf nicht mehr gegeben, so dass dann auch eine Löschpflicht besteht. Eine längere Aufbewahrung ist unzulässig.

Die Speicherdauer auch der weiteren Daten, etwa der **Metadaten der Plattformbenutzung**, sind mit 6 Monaten bzw. 1 Jahr länger als erforderlich.

12 Einbindung sozialer Netzwerke

Unter DHPat (Abschnitt 9 Abs. 1, [3], ähnlich DHGes [6]) heißt es: *Jeder Nutzer hat die Möglichkeit, auf die Symbole für die sozialen Netzwerke von Twitter, Facebook, LinkedIn und Google Plus zu klicken, die sich auf der Doctolib-Webseite oder -Plattform befinden. … Wenn der Nutzer auf diese Schaltflächen klickt, hat Doctolib möglicherweise Zugang zu persönlichen Informationen, die der Nutzer als öffentlich und über seine Twitter-, Facebook-, LinkedIn- und Google-plus-Profile zugänglich gemacht hat. Doctolib erstellt oder verwendet jedoch keine unabhängige Datenbank über Twitter, Facebook, LinkedIn und Google Plus, die von persönlichen Daten ausgeht, die der Nutzer dort veröffentlichen kann, und Doctolib wird keine für den Datenschutz relevanten personenbezogenen Daten, die auf diese Weise erhoben wurden, verarbeiten.*

Entsprechendes führt Doctolib in seinen ab 25. Mai 2018 geltenden Datenschutzbestimmungen aus (DSBest [10]): *Wenn Sie auf die Symbole für soziale Netzwerke Twitter, Facebook, Linkedin und Google Plus auf unserer Website oder in unserer mobilen Anwendung klicken und wenn Sie die Hinterlegung von Cookies akzeptiert haben, indem Sie Ihre Navigation auf unserer Website oder unserer mobilen Anwendung fortsetzen, können schließlich auch Twitter, Facebook, Linkedin und Google Plus Cookies auf Ihren Geräten (Computer, Tablet, Mobiltelefon) ablegen. Diese Arten von Cookies werden nur mit Ihrer Zustimmung auf Ihren Geräten platziert, indem Sie unsere Website oder mobile Anwendung weiter durchsuchen. Sie können jedoch jederzeit Ihre Einwilligung zur Speicherung dieser Art von Cookies über unsere Cookie-Verwaltungsrichtlinie widerrufen.*

Doctolib betreibt bei den aufgeführten Social-Media-Betreibern eigene Seiten. Werden diese von Nutzern aufgerufen, so besteht – anders als dies die Ausführungen von Doctolib suggerieren – eine **gemeinsame Verantwortlichkeit** des Social-Media-Betreibers und Doctolibs (s.o. 4.1. u. 4.6). Soweit dies ersichtlich ist, bietet keiner der von Doctolib genutzten Social-Media-Betreibern Vereinbarungen an, die den Anforderungen des Art. 26 DSGVO genügen.[76] Sämtliche Vorgaben dieser Social-Media-Betreiber verweigern Mitverantwortlichen Informationen, die für die Wahrnehmung der Mitverantwortlichkeit der Seitenbetreiber erforderlich sind. Dies führt dazu, dass Doctolib tatsächlich seine datenschutzrechtliche Verantwortlichkeit nicht wahrnehmen kann. Um sich rechtmäßig zu verhalten, muss Doctolib auf die Nutzung der und Verlinkung zu den aufgeführten Social Media verzichten.

Dies gilt insbesondere, da Doctolib einen Webdienst anbietet, der ausschließlich im Kontext der Verarbeitung von Berufsgeheimnisträgern steht und über den sensitive Gesundheitsdaten verarbeitet werden. Zwar handelt es sich bei dem Dienst von Doctolib nicht um eine Digitale Anwendung (DiGA) im Sinne von § 33a SGB V. Dessen Dienst ist aber von vergleichbarer Sensitivität. Nutzende der Social-

[76] Specht-Riemenschneider/Scneider MMR 2019, 506 f.

Media-Anwendungen von Doctolib geben über diese Dienste möglicherweise höchstpersönliche Gesundheitsdaten preis. Der Zugang zu diesen Angaben ist für die Social-Media-Betreiber weitgehend unbeschränkt und, z.B. für Werbezwecke, nutzbar. Der Normgeber hat bei DiGA die Einbeziehung von Social Media verboten; ausgeschlossen ist insbesondere eine **Nutzung für Werbezwecke** (§ 4 Abs. 2, 4 DiGAV).

Zudem handelt es sich bei den von Doctolib genutzten Social Media um Anbieter, die ihre Daten u.a. in den USA verarbeiten. Ein zulässiger **Datenaustausch mit den USA** ist nicht gewährleistet (s.u. 14.2). Aus diesem Grund verbietet der Normgeber auch eine solche Übermittlung bei DiGA (§ 4 Abs. 3 DiGAV).

13 Cookies

Docotlib informiert über den Einsatz von Cookies recht detailliert in seiner Cookie-Richtlinie [8]. Darin ist eine Vielzahl von Session-Cookies aufgeführt, die für die Nutzung der Dienst nötig sind bzw. sein sollen. Als längerfristig gespeicherte Cookies werden aufgeführt:

- *cfduid (Cloudflare)* zur Verhinderung von Computerangriffen - einschließlich Denial-of-Service-Angriffen (1 Monat)
- *outbrain_cid_fetch (Outbrain)* Retargeting bestimmter Endnutzer (60 Tage).
- *_gcl_au (Google Adwords)* zum Messen der Effektivität einer Werbekampagne über Google Adwords (3 Monate)
- *cookie_consent (Doctolib)* zur Nachverfolgung Ihrer Einwilligung zur Hinterlegung von Cookies (6 Monate)
- *_ga (Google Analytics)* eindeutige Besucherkennung für für Besucherzahlmessung (6 Monate)
- *euconsent (Doctolib)* zur Feststellung der Zustimmung des Benutzers zur Rohdatenerfassung (1 Jahr)
- *temp_appointment_id (Doctolib)* zum Verfolgen einer Reservierung durch einen Benutzer (13 Monate)
- *anonymous_appointment_id (Doctolib)* zur Verifizierung des Namens (Trigramms) (13 Monate)
- *ssid (Doctolib)* zur Nachverfolgung des Nutzers während der gesamten Zeit auf der Website (13 Monate).

Beim **Einbinden von sozialen Netzwerken** werden offenbar weitere Cookies gesetzt (s.o. 12, DSBest [10]).

Das Setzen von Cookies stellt i.d.R. keine Auftragsdatenverarbeitung dar, so wie dies von Doctolib dargestellt wird. Vielmehr handelt es sich um einheitliche Datenverarbeitungen, bei denen auch Zwecke der Stellen, die Cookies setzen, verfolgt werden. Dies ist z.B. beim Einsatz von Google Analytics der Fall mit der Folge, dass eine **gemeinsame Verantwortlichkeit** gegeben ist, ohne dass die hierfür bestehenden rechtlichen Anforderungen erfüllt sind (s.o. 4.1, 4.6).[77]

[77] DSK v. 11.03.2020, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 2 f.

13.1 Einwilligungserteilung in nicht nötige Cookies

Für Cookies, die nicht zur Erbringung des Dienstes benötigt werden, bedarf es der Zustimmung des Nutzenden. Das Aktivieren und Deaktivieren von Cookies (Audience Mesurement, Analytics, Marketing, Werbung) erfolgt über „Cookie-Einstellungen“ bzw. „Cookie-Verwaltung“.

Bzgl. jeder Datenverarbeitung muss ein konkreter **Zweck angegeben** werden (Art. 13 Abs. 1 lit. c DSGVO). Voraussetzung für eine wirksame Einwilligungserklärung zu Cookies ist es, dass den Betroffenen die Zweckbestimmung der Verarbeitung benannt wird.[78] Zweck ist nicht der Vorgang, sondern die damit verfolgte Intention. Die Benennung der „Verfolgung“ bzw. „Nachverfolgung“ von Reservierungen und der Webseitennutzung lässt nicht erkennen, welche Funktion damit erfüllt werden soll.[79] Es ist auch keine Funktion aus der Art der Datenverarbeitung ableitbar. Die von Doctolib verwendeten Angaben sind unzureichend.

13.2 Speicherdauer und Auslandsübermittlung

Die **Speicherdauer** geht bei einigen Cookies weit über die Erforderlichkeit hinaus. Dies gilt insbesondere für die Cookies zur Verfolgung von Reservierungen und der Webseitennutzung mit 13 Monaten.

Einige der Stellen, über die bzgl. der Cookie-Datennutzung informiert wird, haben ihren Sitz in den USA, etwa Cloudflare oder Google. Dies hat zur Folge, dass mit der Nutzung der Doctolib-Services sensitive Daten **in die USA übermittelt** werden. Insofern wird auf den folgenden Abschnitt (s.u. 14.2) verwiesen.

14 Auslandsdatentransfer

Die Einbindung ausländischer Beteiligter in die Verarbeitung personenbezogener Daten richtet sich nach der DSGVO. Bei Übermittlungen in andere EU-Staaten sowie solche des Europäischen Wirtschaftsraums gelten die allgemeinen Regelungen ohne weitere Einschränkungen (Art. 1 Abs. 3 DSGVO). Übermittlungen in andere Staaten richten sich nach den Art. 44-49 DSGVO.

Unter DHGes [6] heißt es zum **Datentransfer ins Drittausland**: *Zur Erbringung seiner Services kann Doctolib Dienstleister:innen in Anspruch nehmen, die außerhalb der Europäischen Union ansässig sind. Wenn die Übertragung in ein Drittland erfolgt, in dem der Schutz für personenbezogene Daten durch die Gesetzgebung als nicht angemessen beurteilt wurde, stellt Doctolib sicher, dass angemessene Maßnahmen in Übereinstimmung mit dem französischen Gesetz zur Informatik und Freiheiten und der DSGVO getroffen werden und dass, wenn erforderlich, insbesondere Standardvertragsklauseln oder gleichwertige Ad-Hoc-Klauseln in den Auftragsverarbeitungsvertrag aufgenommen werden.*

14.1 Hosting bei AWS

In den „Grundsätzen zum Schutz der Gesundheitsdaten (DChartaG [4],ähnlich DChartaP [5]) heißt es unter 8.: *Ihre personenbezogenen Gesundheitsdaten werden bei zertifizierten Anbietern, sogenannten*

[78] EuGH 01.10.2019 – C-673/17 (Planet49), NJW 2019, 3433 = NVwZ 2019 = 1745; EuZW 2019 = 916; MMR 2019 = 732 = K&R 2019, 705 = CR 2020, 25.
[79] Roßnagel in SHS, Art. 5 Rn. 68.

„Providern von Gesundheitsdaten-Hosting“, gespeichert, sodass ein maximaler Schutz in Bezug auf Vertraulichkeit und Sicherheit gewährleistet ist.

Ohne eine Auslandsdatenverarbeitung anzusprechen heißt es ebenso unter DuS [12]: *Die personenbezogenen Gesundheitsdaten Ihrer Patient:innen werden bei sogenannten „Providern von Gesundheitsdatenhosting“ gespeichert, die nach einem mehrstufigen und gesetzlich geregelten Verfahren zertifiziert sind. … Sie* (ihre Gesundheitsdaten, T.W.) *werden auf der höchsten Sicherheitsstufe geschützt und bei zertifizierten Anbieter:innen, sogenannten „Providern von Gesundheitsdatenhosting”, gespeichert.*

Genaueres zum Hosting findet sich in den Datenschutzhinweisen für Gesundheitskräfte (DHGes [6]): *Personenbezogene Gesundheitsdaten werden von Amazon Web Services gehostet, welches nach europäischen Standards speziell für diesen Zweck zertifiziert ist (französische Zertifizierung “Health Data Services”- HDS). Um die Sicherheit für alle unsere Dienste zu erhöhen, haben wir beschlossen, dort alle personenbezogenen Daten unserer Kund:innen und Gesundheitsfachkräfte ohne Unterscheidung, ob es sich dabei um Gesundheitsdaten oder nicht handelt, zu speichern.* Die Datenverarbeitung erfolgt gemäß den DHGes [6] bei AWS EMEA, also in Europa.

Es bedarf weiterer Recherchen, um Genaueres über die erwähnte Zertifizierung zu erfahren: Bei der **HDS-Zertifizierung** (Hébergeur de Données de Santé) handelt es sich um ein Siegel der französischen Gesundheitsbehörde „Agence du Numérique en Santé“ (ANS). Damit soll die Sicherheit und der Schutz von personenbezogenen Gesundheitsdaten gestärkt werden. Für das Erlangen des Zertifikats erfolgt eine Zusammenarbeit mit einem unabhängigen externen Prüfer.[80] Das Zertifikat gilt jeweils für drei Jahre und bestätigt keine umfassende Konformität mit der DSGVO, sondern hat seine Grundlage im französischen „Gesetz für öffentliche Gesundheit“ (code de la santé publique) mit einem Ausrichtung auf die Datensicherheit, nicht auf die Rechtmäßigkeit der Datenverarbeitung.[81]

Amazon Web Services erlangte das HDS-Zertifikat im Januar 2019.[82] Ein **Zertifizierungsbericht ist nicht veröffentlicht**, lediglich eine allgemeine, sich nicht auf HDS speziell beziehende Darstellung der Sicherungsprozesse bei AWS.[83]

Mit Anträgen seit dem 26.02.2021 forderten medizinische und Bürgerrechts-Organisationen eine **einstweilige Anordnung beim Conseil d´Etat** gegen das französische Gesundheitsministerium. Der Conseil d´Etat ist das oberste französische Gericht und entspricht in etwa dem deutschen Bundesverfassungsgericht. Mit dem Antrag sollte dem französischen Gesundheitsministerium untersagt werden, die Dienste von Doctolib bei der Durchführung des französischen Covid-19-Impfprogramms in Anspruch zu nehmen. Antragsteller waren folgende Verbände bzw. Personen: Association InterHop, Association Constances, Association Actions Traitement, Association les

[80] https://esante.gouv.fr/labels-certifications/hebergement-des-donnees-de-sante.
[81] Explicitation du champ d’application du cadre juridique de l’hébergement de données de santé par le ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d’information de santé v. 16.05.2019, https://esante.gouv.fr/sites/default/files/media_entity/documents/FAQ%20HDS_16052019_V0%2018.pdf.
[82] Hadinger, AWS achieves HDS certification, 31.01.2019, updaten 13.03.2019, https://aws.amazon.com/de/blogs/security/aws-achieves-hds-certification/.
[83] Amazon Web Services: Risk and Compliance, November 2020, https://d1.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf.

Actupiennes, Association Actup santé sud ouest, Syndicat de la Médecine générale(SMG), Union française pour une médecine libre (UFML), Syndicat national des jeunes médecins généralistes (SNJMG), Fédération des médecins de France (FMF), mehrere Einzelpersonen als Nutzender des Conseil de surveillance de l'AP-HP, Fédération SUD santé sociaux und Ligue des droits del' Homme. Ihren Antrag begründeten die Antragsteller damit, dass Doctolib AWS als Hoster nutzt und dadurch der Schutz der bei der Impfaktion erfassten Gesundheitsdaten nicht gewährleistet sei. Durch die Datenverarbeitung bei AWS hätten US-amerikanische Behörden gesetzlichen Zugriff auf die sensitiven Impfdaten. Hierin läge ein Verstoß gegen die auch in Frankreich geltende DSGVO.

In einem Beschluss vom 12.03.2021 stellte der Conseil d´Etat fest, dass die Auftragsverarbeitung für Doctolib mit der Fa. AWS Sarl in Luxemburg erfolgt, eine **Tochter der US-amerikanischen Amazon Web Services Inc**. Die Speicherung der im Auftrag verarbeiteten Daten erfolge in Frankreich und in Deutschland. Ein Datentransfer in die USA sei durch den Vertrag zwischen AWS und Doctolib nicht vorgesehen. Der Beschluss bestätigt, dass eine Tochter von AWS auf der Grundlage von US-amerikanischen Regelungen (FISA, Executive Order 12333) verpflichtet werden kann, verarbeitete Daten herauszugeben.

Dies sei jedoch kein Grund, eine einstweilige Anordnung wegen der Terminvereinbarungen durch Doctolib zu erlassen. Von diesen Vereinbarungen erfasst würden keine „Gesundheitsdaten zu den möglichen medizinischen Gründen für eine Impfberechtigung", sondern nur Daten zur Identifizierung der Betroffenen und zu Terminen und den Umstand der – altersunabhängigen – Impfberechtigung. Die Daten würden drei Monate nach dem Impftermin gelöscht. Die Daten seien bei AWS verschlüsselt gespeichert, wobei der Schlüssel in der Verfügungsmacht eines Treuhänders läge. Zudem bestehe die Möglichkeit für jeden Betroffenen, durch Löschung seines Kontos seine Daten zu löschen. Angesichts dieser Garantien und der Sensitivität der Daten könne das Schutzniveau **nicht als offensichtlich unangemessen** bewertet werden.

Inwieweit diese französische Entscheidung auf die deutsche Situation übertragen werden kann, ist unklar, da weder der insofern bestehende **Unterauftrag** zwischen der Doctolib GmbH und AWS noch die tatsächlich umgesetzten **Garantien** bekannt sind.

14.2 Datenverarbeitung in den USA

Zur **Verwaltung** der Kundenbeziehung zu den Gesundheitskräften nimmt Doctolib als Unterauftragsverarbeiter in den USA die Firmen Salesforce, Talkdesk und Intercom in Anspruch. Für die Verwaltung der Videoübertragung bei der Telekonsultation nutzt Doctolib die Fa. Vonage (Nexmo)/USA. Als Analysetools unterbeauftragt Doctolib in den USA Sentry, Sisense (Periscope) und Didomi. Im Bereich des Marketing werden die Dienste von folgenden US-Firmen genutzt: Hubspot Inc., IQvia**,** Milchimp, Mobile Sphere und Sem Rush. In der wenig spezifischen Rubrik „Finanzen/Recht" nennt Doctolib im DHGes [6] folgende US-Firmen als Dienstleister: unter dem Stichwort „Finanzwesen" Netsuite (Oracle), Zuora, als Zahlungsdienstleister STRIPE und als Anbieter elektronischer Signaturen Docusign. Weitere einbezogene US-Firmen sind Cloudflare (IT-Sicherheit) und Khoros (Managementsoftware für Communities und Social Media).

Durch die Unterbeauftragung von US-Unternehmen erlangen diese **sensitive Gesundheitsdaten**. Dies ist auch der Fall, wenn die Inhaltsdaten verschlüsselt sind und von den Unterauftragnehmern in den USA nicht entschlüsselt werden können. Von hoher Aussagkraft sind z.B. die Metadaten, die bei

Terminvereinbarungen oder bei Telekonsultationen anfallen, da hieraus Schlüsse auf Behandlungsverhältnisse und auf Krankheiten gezogen werden können. Diese Metadaten werden auch durch das Patientengeheimnis nach § 203 StGB geschützt.

Ein Transfer solcher Daten in die USA ist unzulässig. In den USA besteht kein hinreichend angemessenes **Datenschutzniveau**.[84] Es ist nicht erkennbar, dass dieser Mangel durch hinreichende Garantien für die Betroffenen kompensiert wird.

Ein Transfer von Patientengeheimnissen in die USA ist zugleich ein Verstoß gegen das in § 203 StGB normierte Patientengeheimnis. Für eine Unterbeauftragung in einen Staat außerhalb der EU/des EWR zur Verarbeitung von Patientengeheimnissen gelten zunächst die datenschutzrechtlichen Mindestvoraussetzungen an einen Drittstaatsdatentransfer. Darüber hinausgehend müssen die Anforderungen des § 203 Abs. 3, 4 StGB beachtet werden. Dies dürfte bei Unterauftragnehmern in den USA nicht möglich sein, da diese den Weisungen der Gesundheitsfachkraft und Vertraulichkeitsverpflichtungen unterworfen werden müssten, was US-Recht nicht zulässt. Wirksame und durchsetzbare Vertraulichkeitsverpflichtungen nach § 203 Abs. 4 S. 2 Nr. 1 StGB können nicht bei den Mitarbeitern der US-Unternehmen eingeholt werden.

15 Zertifizierung

Unter 19.9 S. 2, 3 ANB [1] heißt es: *Das Hosting von Gesundheitsdaten ist neben deutschen Standards auch nach französischem Recht zertifiziert. Insbesondere besteht eine HDS-Zertifizierung (Health Data Hosting)*. Diese Zertifizierung bezieht sich auf eine Unterbeauftragung an Amazon Web Services (AWS) als Hoster (DHPat [3] Abschnitt 6 Abs. 4; s.o. 14.1). Die **HDS-Zertifizierung** erging nach französischem Recht und hat keine Relevanz nach deutschem Recht. Eine gegenseitige Anerkennung von solchen Zertifikaten in der EU ist nicht vorgesehen. Inwieweit die Fakten, die dieser Zertifizierung zugrunde liegen, nach deutschem Recht bedeutend sind, kann nicht beurteilt werden, da diese Fakten nicht offengelegt werden (s.o. 14.1).

Die **Zertifizierung der Telekonsultation** durch die KBV gemäß § 291g SGB V hat nur begrenzte datenschutzrechtliche Aussagekraft. Die technischen Anforderungen für die Praxis und den Videodienst - insbesondere zur technischen Sicherheit und zum Datenschutz - sind in der Anlage 31b zum Bundesmantelvertrag-Ärzte geregelt. Mit Wirkung zum 20.03.2021 ist eine aktualisierte Vereinbarung in Kraft getreten. Durch die Neufassung sind unter anderem die Anforderungen an die Zertifikate und die ausstellenden Stellen zum Nachweis von IT-Sicherheit und Datenschutz aktualisiert worden. Die Zertifizierung erfolgte nicht durch die KBV selbst, sondern durch das von Doctolib beauftragte Unternehmen datenschutz cert GmbH. Das aktuell erteilte Zertifikat ist gültig bis zum 01.04.2022.[85]

Die Zertifizierung durch **datenschutz cert GmbH** soll die Datenschutzkonformität des Doctolib-Webangebots bestätigen. Die Prüfung erfolgte nach den „internet privacy standards“ (ips), deren

[84] EuGH 06.10.2015 – C-362/14 (Safe Harbor, Schrems I), NJW 2015, 3151 = JZ 2016, 360 = NVwZ 2016, 43 = MMR 2015, 753 = K&R 2015, 710 = DÖV 2015, 1070; EuGH 16.07.2020 – C-311/18 (Privacy Shield, Schrems II), NJW 2020, 2613 = EuZW 2020, 941 = MMR 2020, 597

[85] https://www.kbv.de/media/sp/Liste_zertifizierte-Videodienstanbieter.pdf.

Kriterienkatalog öffentlich abrufbar ist.[86] In der Beschreibung des Auditierungsumfangs wird dargestellt, dass die Datenschutzerklärung und die Cookienutzung geprüft wurden sowie sämtliche Anforderungen von DSGVO, TMG und BDSG. Auch das Datenschutzmanagement sei einbezogen: *So können Sie als Nutzer sicher sein, dass Technik und Mitarbeiter des auditierten Anbieters Datenschutz und Datensicherheit wirklich ernst nehmen - und damit Ihr Persönlichkeitsrecht schützen. … In Abgrenzung zur Datenverarbeitung über das Webportal gehören sonstige Datenverarbeitungsprozesse des Anbieters außerhalb des Webportals / Front-Ends und der Online Video-Sprechstunde nicht zum Auditgegenstand. Nicht auditiert wurden insbesondere das hinter dem Portal liegende Kundenvertrags- und -datenmanagement (CRM), das Kalender- und Terminmanagement sowie Arztinformationssystem für Ärzte, verlinkte fremde Webseiten (wie z.B. info.doctolib.de) oder auf Dienstleister ausgelagerte Services.* In der kurzen Zusammenfassung der Prüfergebnisse werden die in dem hier vorliegenden Gutachten thematisierten Kritikpunkte nicht adressiert.[87] Es kann daher nicht nachvollzogen werden, weshalb die datenschutz cert GmbH meint, Datenschutzkonformität der Doctolib-Services bestätigen zu können.

Das **Zertifikat des TÜV Saarland** wurde am 01.12.2020 mit der Bezeichnung „TÜV geprüfter Datenschutz v5.0“ und der Typangabe „SY Systemzertifizierung“ ausgestellt und gilt bis zum 30.11.2022. Unter der ID TK44448 wird folgender Prüfumfang angegeben: *Die Prüfung und Zertifizierung bestätigt einen datenschutzkonformen Umgang mit personenbezogenen Kundendaten unter Berücksichtigung geltender Gesetze wie der DS-GVO und dem BDSG. Hierzu finden Prüfungen relevanter Dokumente und Auditierungen auch vor Ort statt.*[88] Ein qualifizierter inhaltlicher Zertifizierungsbericht steht öffentlich nicht zur Verfügung. Es handelt sich nicht um ein Zertifikat nach Art. 42 DSGVO. Die Validität des TÜV-Zertifikats ist angesichts der fehlenden Beschreibung des Prüfumfangs und der Prüfergebnisse nicht kontrollierbar. Mangels Transparenz und Vergleichbarkeit fehlt es an Glaub- und Vertrauenswürdigkeit.[89]

16 Ergebnisse

Doctolib weist teils starke, teils weniger gravierende Datenschutzdefizite auf. In der folgenden Zusammenfassung wird in den Klammerzusätzen auf die jeweiligen Kapitel im vorliegenden Gutachten verwiesen.

1. Der umfassende **Import von Patientenstammdaten** von Gesundheitskräften verstößt gegen den Erforderlichkeitsgrundsatz und das Prinzip der Datenminimierung und führt dazu, dass bei Doctolib ein gewaltiger bundesweiter Patientendatenbestand geführt wird (7). Durch die Anforderung des gesamten Patientenstammdatensatzes veranlasst Doctolib die Gesundheitsfachkraft zur Verletzung des Patientengeheimnisses.
2. Die offiziell angegebenen **Löschfristen** Doctolibs gehen teilweise weit über das Zulässige hinaus und führen dazu, dass zu löschende Patientendaten jahrelang unnötigerweise gespeichert bleiben. Die tatsächliche Verantwortung hierfür liegt bei Doctolib, das diese Veratnwortung aber auf die Gesundheitskräfte abwälzt (11).

[86] https://www.datenschutz-cert.de/leistungen/ips-internet-privacy-standards.
[87] https://ips.datenschutz-cert.de/doctolib.
[88] https://www.tuev-saar.de/zertifikat/tk44448/.
[89] Scholz in SHS, Art. 42 Rn. 12; Weichert in DWWS, Art.42 Rn. 14.

3. Die **Informationen für die Nutzenden** durch Doctolib über die Datenverarbeitung sind in verwirrender Weise auf viele Dokumente verteilt, teilweise in sich widersprüchlich, teilweise verzerrend bzw. beschönigend und teilweise falsch und verstoßen damit gegen die datenschutzrechtlichen Transparenzanforderungen (viele Kapitel, 9, 10.1).
4. Mit dem Unterlassen der Information über den Export des Patientenstammdatensatzes sowie dem korrespondierenden Datenimport bei Doctolib wird gegen die **Informationspflicht** gemäß der DSGVO verstoßen.
5. Die Einbindung ausländischer, insbesondere US-amerikanischer Dienstleister und der damit einhergehende **Datentransfer in Drittausland**, ist unzulässig und angesichts der hohen Sensitivität der betroffenen Daten verantwortungslos (14.2).
6. Eine Einbindung **sozialer Netzwerke** sowie der Umfang des **Cookieeinsatzes** und eine **Werbenutzung** von Metadaten ist bei ärztlichen Angeboten verantwortungslos (9, 12, 13).
7. Die Verantwortlichkeiten für die Datenverarbeitung werden von Doctolib teilweise falsch dargestellt mit der Folge, dass das Unternehmen seine Verantwortlichkeit, etwa für die Verarbeitung von Metadaten bei der Inanspruchnahme ärztlicher Services oder für die Nutzung von Social Media, leugnet (4.3 - 4.6, 6, 7).
8. Durch rechtliche Falschinformationen werden **Gesundheitsfachkräfte** veranlasst, selbst gegen Datenschutznormen zu verstoßen (5, 7, 10.2, 11).

17 Abschlussbemerkungen

Die Angebote von Doctolib sind für Gesundheitsberufe wie für Patientinnen und Patienten äußerst verlockend. Diese Verlockungen korrespondieren mit dem Wunsch nach einer Digitalisierung von Angeboten im Gesundheitswesen. Dieser Wunsch geht einher mit der Erwartung an ein **hohes Maß an Vertraulichkeit und Transparenz**. Diese Erwartung wird mit vielfältigen Zusicherungen durch Doctolib bestärkt. Eine Prüfung an Hand verfügbaren Informationen begründet jedoch massive Zweifel an der Seriosität dieser Zusicherungen.

Das Angebot von Doctolib ist nur eines von vielen Tausenden digitalen Services im Gesundheitsbereich. Angesichts dieses großen Angebots ist es praktisch für Nichtregierungsorganisationen wie dem Netzwerk Datenschutzexpertise unmöglich, auch nur die wichtigsten Anbieter auf ihre Datenschutzkonformität hin zu überprüfen. Diese Aufgabe obliegt originär staatlichen Einrichtungen. Für eine valide **Daseinsvorsorge in den Bereichen Gesundheit und Datenschutz** bedürfte es der Etablierung verlässlicher Zertifizierungsverfahren. Eine Selbstzertifizierung oder eine interessierte Fremdzertifizierung, wie sie bisher praktiziert wird, genügt nicht. Die Aufsichtsbehörden müssten zudem personell so ausgestattet werden, dass sie zeitnah qualifiziert Betroffenenbeschwerden bearbeiten, systematische Prüfungen durchführen, „schwarze Schafe“ identifizieren und diese vom Markt ausschließen können. So wichtig eine verstärkte Digitalisierung des Gesundheitswesens im Interesse der Qualität und der Kosteneffizienz ist, so wichtig ist es, dass die strukturellen Voraussetzungen geschaffen werden, damit die Vertraulichkeit der anfallenden Daten gewahrt bleibt.

Ausgewählte Literatur

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-DSGVO und BDSG, 2. Aufl. 2020 (DWWS).

Dochow, Carsten, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017 (Dochow).

Ehmann, Eugen/Selmayr, Martin, DS-GVO, 2. Aufl. 2018 (Ehmann/Selmayr).

Kühling, Jürgen/Buchner, Benedikt, DS-GVO BDSG, 3. Aufl. 2020 (Kühling/Buchner).

Schönke, Adolf/Schröder, Horst/Cramer, Peter u.a., Strafgesetzbuch, 30. Aufl. 2019 (Schönke/Schröder).

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra, Datenschutzrecht, 2019 (SHS).

Abkürzungen

Abs.	Absatz
AGB/N	Allgemeine Geschäftsbedingungen/Nutzer von Doctolib
AIS	Arztinformationssystem
ANB	Allgemeine Nutzungsbedingungen für Patienten von Doctolib
Art.	Artikel
Aufl.	Auflage
AWS	Amazon Webservices
BB	Begriffsbestimmungen von Doctolib
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BT-Drs.	Bundestagsdrucksache
bzw.	beziehungsweise
CCC	Chaos Computer Club
CCZ	Corporate Compliance Zeitschrift
CEO	Chief Enterprise Officer
CookieRL	Cookierichtlinie von Doctolib
CR	Computer und Recht (Zeitschrift)
DANA	DatenschutzNachrichten
DChartaG/P	Datenschutzcharta von Doctolib für Ärzte/für Patienten
d.h.	das heißt
DHGes/Pat	Datenschutzhinweise von Doctolib für Gesundheitsfachkräfte/Patienten
DiGA/V	Digitale Gesundheitsanwendung/en-Verordnung
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DSBest	Datenschutzbestimmungen von Doctolib
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DuS	Datenschutz und Sicherheit von Doctolib
DWWS	Däubler/Wedde/Weichert/Sommer (Kommentar)
ErwGr	Erwägungsgrund der DSGVO
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
e.V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
FAQ	Frequently Asked Questions
f/f.	fort/folgende
FISA	Foreign Intelligence Service Act (US-Gesetz)
Fn.	Fußnote
GmbH	Gesellschaft mit beschränkter Haftung
grds.	grundsätzlich
HDS	Hébergeur de Données de Santé (französische Gesundheitsdaten-Cloudzertifizierung)
i.d.R.	in der Regel
inkl.	inklusive
i.S.d./v.	im Sinne des/von
JR	Juristische Rundschau (Zeitschrift)
Kap.	Kapitel

KBV	Kassenärztliche Bundesvereinigung
K&R	Kommunikation und Recht (Zeitschrift)
KriPoZ	Kriminalpolitische Zeitschrift
Liste	Liste der Verarbeitungen von Doctolib
lit.	Buchstabe
MBOÄ	Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
MDR	Monatsschrift Deutschen Rechts
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
Rn.	Randnummer
S.	Seite/Satz
SAS	Société par action simplifiée (französische Aktiengesellschaft)
SGB	Sozialgesetzbuch
SHS	Simitis/Hornung/Spiecker (Kommentar)
SMS	Short Message Service
s.o.	siehe oben
StGB	Strafgesetzbuch
s.u.	siehe unten
TMG	Telemediengesetz
TÜV	Technischer Überwachungsverein
u.	und
u.a.	unter anderem
USA	Vereinigte Staaten von Amerika
v.	von
vgl.	vergleiche
z.B.	zum Beispiel