Datenschutz bei Doctolib

Eine Aktualisierung zu den rechtlichen und technischen Defiziten

Stand: 28.07.2022

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

Inhalt

Am 11.06.2021 erhielt die Firma Doctolib GmbH, Berlin, den BigBrotherAward in der Kategorie Gesundheit dafür verliehen, dass dessen Plattform bei der Vermittlung von Arztterminen seine Vertraulichkeitsverpflichtung verletzt.[1] Wenige Tage zuvor veröffentlichte das Netzwerk Datenschutzexpertise ein 39seitige Gutachten, in dem im Detail dargestellt wurde, wie das Unternehmen gegen Regelungen zur ärztlichen Schweigepflicht und zum Datenschutz verstößt und ärztliche Einrichtungen zu solchen Verstößen veranlasst.[2]

In Folge der Preisverleihung und der Veröffentlichung des Gutachtens gab es viele Rückmeldungen von betroffenen PatientInnen, von ÄrztInnen, JournalistInnen und Informationstechnischen (IT-) ExpertInnen, welche die Vorwürfe gegenüber dem Unternehmen bestätigten und ergänzten. Eine direkte Rückmeldung von Doctolib erfolgte nicht. Stellungnahmen gegenüber der Presse, in denen das Unternehmen Rechtsverstöße leugnet, blieben im Allgemeinen und gingen nicht substanziell auf die konkreten Vorwürfe ein.

Ein Kritikpunkt gegenüber Doctolib waren die intransparenten, widersprüchlichen und teilweise gesetzeswidrigen Allgemeine Geschäftsbedingungen und Nutzungshinweise (AGB). Ab Februar 2022 veröffentlichte das Unternehmen neue AGB.

Die für Doctolib zuständige Datenschutzaufsichtsbehörde, die bzw. der Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), befasste sich mit dem Angebot von Doctolib – auch auf Grund einer Vielzahl von Eingaben und Beschwerden – und veröffentlichte im Jahresbericht 2019[3] und erneut im Jahresbericht 2021 kritische Bewertungen. Sanktionen wurden bisher nicht ausgesprochen.[4]

Schon Ende 2020 hatte die Berliner Senatsverwaltung für Gesundheit im Rahmen der Impfkampagne gegen das Corona-Virus Doctolib mit der Vergabe von Impfterminen beauftragt. In einem Nachtrag zu diesem Auftrag übernahm Doctolib die gesamte Dokumentation der Impfkampagne der Berliner Senatsverwaltung. Mit Schreiben vom 18.06.2021 beantragte der Autor des vorliegenden Gutachtens gemäß dem Berliner Informationsfreiheitsgesetz Akteneinsicht in die mit Doctolib abgeschlossenen Verträge. Nach Anmahnung und Einschaltung der BlnBDI wurden die eingeforderten Unterlagen mit Datum vom 17.05.2022 zur Verfügung gestellt.

Derweil wirbt Doctolib für seine Dienstleistungen offensiv. Sowohl die Tätigkeit für die Impfkampagne in Berlin wie auch die Aktivitäten für Gesundheitsdienstleister bundesweit werden weitgehend unverändert fortgesetzt. Vor diesem Hintergrund sieht sich das Netzwerk Datenschutzexpertise – unterstützt durch den Organisator des BigBrotherAwards Digitalcourage – veranlasst, eine Aktualisierung der Bewertung des Datenschutzes bei Doctolib zu veröffentlichen.

[1] https://bigbrotherawards.de/2021/gesundheit-doctolib.
[2] Netzwerk Datenschutzexpertise, Arztterminvermittlung über Doctolib, 08.06.2021, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_doctolib.pdf.
[3] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Jahresbericht (JB) 2019, Kap. 6.3 (S. 103 ff.)
[4] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Jahresbericht (JB) 2021, Kap. 1.3.1., 6.5 u. 6.6.

1 Allgemeine Rahmenbedingungen

Im Folgenden wird vorrangig das Angebot zum Terminmanagement im Gesundheitsbereich von Doctolib thematisiert. Doctolib versucht über dieses Angebot in weiteren Bereichen des digitalisierten Gesundheitswesens Fuß zu fassen. Ein wichtiger Schritt hierfür ist, dass Doctolib das Terminmanagement für die Impfkampagne des Berliner Senats übernahm und zusätzlich die gesamte Impfdokumentation für die Verwaltung in Berlin erledigt. Das Unternehmen weitet sein Angebot der **Dokumentation von Gesundheitsdaten** für PatientInnen wie für Heilberufe immer weiter aus.

Mit seinem ärztlichen **Videokonferenzsystem** hat sich Doctolib ein weiteres geschäftliches Standbein geschaffen. Dieses erfolgt nach eigenständigen rechtlichen Rahmenbedingungen, zu denen im Folgenden keine detaillierte Analyse vorgelegt wird. Das Videokonferenzsystem von Doctolib wurde als Telekonsil-Instrument von der Kassenärztlichen Bundesvereinigung (KBV) zugelassen.[5]

Hinsichtlich **Termin-Management-Systemen** gibt es im Gesundheitsbereich in Deutschland viele Anbieter. Gemäß einer im Januar 2021 veröffentlichten Untersuchung der Stiftung Warentest werden in Deutschland monatlich Millionen Arzttermine über Apps und andere digitale Tools gebucht. Dies kann für Patienten sinnvoll sein, da dadurch Aufwand und Wartezeiten vermieden werden können. Für die Praxis der Heilberufe ist dies eine komfortable Möglichkeit zur Entlastung und zur Fokussierung auf die medizinischen Aufgaben sowie zur Optimierung der Praxisauslastung. Bei der Untersuchung durch die Stiftung Warentest erhielt nur der *eTerminservice der Kassenärztlichen Bundesvereinigung* (KBV) in Bezug auf den Schutz persönlicher Daten die Note „sehr gut“. Dieser Dienst steht aber nur für Kassenpatienten und nicht zur Buchung von Zahnarztterminen zur Verfügung. Dem Angebot der Berliner *Dr. Flex GmbH* wurde beim Datenschutz die Note 1,6 bescheinigt. Das Angebot der in anderen Zusammenhängen in der Ärzteschaft nicht unumstrittenen *jameda* erhielt die Note 1,9. Schlechter schnitten insofern die Dienstleister *Arzttermine.de* (3,0) und *Doctena* (3,3) ab. Doctolib landete mit einer 3,6 ganz am Ende nur knapp vor Samedi, das die Note 3,7 erhielt.[6]

2 Neue Erkenntnisse

Ein Team der IT-Webseite mobilsicher.de untersuchte mit Stand vom 18.06.2021 die Version 3.2.26 der Terminvermittlungs-App von Doctolib und stellte fest, dass diese die IP-Adresse, den Buchungsgrund und den Versicherungsstatus eines Nutzers sowie die Facharztbezeichnung der Suche an das **Marketingunternehmen Outbrain sowie an Facebook** gesendet hatte. Auf die Anfrage von mobilsicher.de reagierte Doctolib und entfernte die für die Übermittlung genutzten Cookies.

Eine **Cookie-Übermittlung an Google** wurde nach einer Veröffentlichung von Zeit-online vom 23.06.2021 gestoppt. Im Rahmen der Recherche der IT- und Wissenschaftsjournalistin Eva Wolfangel ergab sich, dass durch Cookies veranlasste Verbindungen mit Google aufgebaut wurden und dadurch

[5] https://www.kbv.de/media/sp/liste_zertifizierte-Videodienstanbieter.pdf.
[6] Ganz schön unsensibel, test 1/2021, 92 ff., https://www.test.de/Arzttermin-Portale-im-Test-Ganz-schoen-unsensibel-5692512-0/; Risiken und Nebenwirkungen von Termin-Management-Systemen, www.zm-online.de 16.10.2021.

Datenübermittlungen „trotz abgelehnter Cookies“ erfolgten, was von Doctolib – jedoch unsubstantiiert – bestritten wurde.[7]

Das Netzwerk Datenschutzexpertise und Digitalcourage wurden über viele Beschwerden hinsichtlich der **Behandlung von Kundenwünschen** informiert. Es dauerte teilweise Monate, bis durch Doctolib angemessene Reaktionen erfolgt waren. Gesundheitsfachkräften wurde u.a. unter Verweis auf den (Beschäftigten-)Datenschutz Login-Information oder zu Sicherheitseinstellungen verweigert, mit denen Arbeitgeber berechtigterweise die dienstliche Nutzung von Doctolib durch ihre Mitarbeiter nachvollziehen wollten. Die Hinzufügung einer Person durch einen Nutzer zur Terminverwaltung führte dazu, dass dessen Daten für den Kontoinhaber umfassend aufrufbar waren.

Schon 2019 nahm die **Berliner Beauftragte für den Datenschutz und die Informationsfreiheit** (BlnBDI) datenschutzrechtliche Ermittlungen in Bezug auf Doctolib auf; die Vorgehensweise des Unternehmens wurde kritisiert.[8] Seitdem wirbt das Unternehmen wie folgt für seinen „Datenschutz“: „Wir arbeiten mit den Behörden, die für den Schutz von personenbezogenen Daten zuständig sind, zusammen.“

In Ihrem Tätigkeitsbericht für das Jahr 2021 thematisierte die BlnBDI erneut die „**Terminverwaltung in Arztpraxen**“ durch Doctolib. Die BlnBDI bekräftigte ihre schon zwei Jahre zuvor erklärte Kritik, dass Terminerinnerungen per E-Mail oder SMS durch „das Terminverwaltungsunternehmen“, über das der Termin nicht vereinbart wurde, unzulässigerweise ohne ausdrückliche Einwilligung der Patienten erfolgen. Nach Ablauf eines Termins müssten die Daten über eine online erfolgte Terminvereinbarung zeitnah gelöscht werden, was „bereits im Auftragsverarbeitungsvertrag festgelegt werden“ solle. Professioneller Rat solle bei einer externen Durchführung der Terminverwaltung eingeholt werden. Problematisch sei es, wenn – wie bei Doctolib – Teile der Datenverarbeitung „außerhalb Deutschlands, insbesondere außerhalb des ‚Geltungsbereichs der DS-GVO stattfinden sollen“.[9] Die BlnBDI berichtet zudem von der Cookie-bedingten Datenübermittlung „an ein US-amerikanisches Unternehmen und damit in einen unsicheren Drittstaat“. Sie weist zudem darauf hin, dass nach Löschung eines Nutzungskontos des Terminverwaltungsunternehmens durch die Patient:innen gemäß Art. 17 DSGVO eine unverzügliche Datenlöschung durch das Unternehmen erfolgen müsse. Die Löschung, die schon nach Erledigung des Termins erfolgen muss, dürfe nicht den Patient:innen selbst aufgegeben werden.[10]

Die BlnBDI thematisiert in ihrem Bericht zudem das **Corona-Impfmanagement des Landes Berlin** und kritisiert, dass das beauftragte Unternehmen bei der Online-Terminbuchung der Schutzimpfungen nicht die Datenschutzregeln der Auftragsverarbeitung einhält. Die Bürger müssten hierfür ein separates Vertragsverhältnis mit dem Privatunternehmen eingehen. Dadurch werde die

[7] Ruhenstroth, https://mobilsicher.de/ratgeber/verstoerend-doctolib-app-teilte-sensible-informationen-mit-facebook-und-outbrain, 21.06.2021; Weiß, Doctolib reicht Gesundheitsdaten an Facebook und Outbrain weiter, https://heise.de/-6114823 22.06.2021; Wolfangel, Ist Ihr Arzttermin sicher? www.zeit.de 23.06.2021; Risiken und Nebenwirkungen von Termin-Management-Systemen, www.zm-online.de 16.10.2021; Schall, Arzt-Termine im Kreis Gießen per App: Sensible Patientendaten missbraucht? www.gießener-allgemeine.de 13.07.2021.
[8] BlnBDI, JB 2019 (Fn. 3), Kap. 6.3 (S. 103 f.).
[9] BlnBDI, JB 2021 (Fn. 4), Kap. 6.5.
[10] BlnBDI, JB 2021 (Fn. 4), Kap. 6.6.

Weisungsabhängigkeit von der Berliner Senatsverwaltung unterlaufen. Nach Zweckerfüllung müssten, so die BlnBDI, in jedem Fall die Nutzungskonten wegen Zweckerfüllung wieder gelöscht werden.[11]

Über einen am 17.06.2021 eingereichten Antrag auf Akteneinsicht nach § 3 Informationsfreiheitsgesetz Berlin erhielt der Autor des vorliegenden Gutachtens nach Mahnungen und Einschaltung der BlnBDI mit Datum vom 17.05.2022 (also nach 11 Monaten!) **Vertragsunterlagen** zwischen der Berliner Senatsverwaltung und Doctolib zu deren Dienstleistungen im Rahmen der Impfkampagne des Landes.

Unter der Überschrift „**Terminverwaltung im Gesundheitswesen**“ veröffentlicht die BlnBDI auf ihrer Webseite Informationen zur Terminorganisation durch externe Unternehmen. Dort werden die Darstellungen im Jahresbericht 2021 vertieft; eine saubere Trennung zwischen eigenverantwortlicher Verarbeitung und Verarbeitung im Auftrag der Gesundheitseinrichtung wird angemahnt.[12] Auf eine Presseanfrage hin erhielt der Autor weitere Informationen über den aktuellen Stand der Bearbeitung des Falls Doctolib durch die Aufsichtsbehörde.

Derweil führt Doctolib teilweise äußerst aggressive **Werbekampagnen** für seine Dienstleistungen durch. Hierbei verschleiert das Unternehmen die für die Wahrung des Datenschutzes wichtige Unterscheidung zwischen seinen informationstechnischen Diensten und den Diensten der medizinischen Leistungserbringer. In seiner Kampagne „Gesucht, Gebucht, Behandelt“ in fünf Großstädten vermittelt das Unternehmen mit 230 Plakaten auf Litfaßsäulen und über Internet-Werbung den Eindruck, in die ärztliche Behandlung einbezogen zu sein. In Webseiten von Ärzten werden Scripte von Doctolib eingebunden.[13]

3 Doctolib – zugleich Verantwortlicher und Auftragsverarbeiter?

Ein zentraler Datenschutzverstoß bei den informationstechnischen Dienstleistungen von Doctolib besteht darin, dass das Unternehmen nominell als Auftragsverarbeiter von Gesundheitseinrichtungen und zugleich als eigenständiger Vertragspartner der Patienten (betroffenen Bürgerinnen und Bürger, Betroffenen) tätig wird, ohne dass eine **klare Trennung** zwischen diesen beiden Funktionen erfolgt. So erlangt Doctolib als „Auftragsverarbeiter“ sensitive Gesundheitsdaten aus dem ärztlichen Vertrauensverhältnis und verarbeitet diese als Verantwortlicher, ohne dass die Betroffenen hierin wirksam eingewilligt haben.[14]

Datenschutzrechtlich **Verantwortlicher** ist gemäß Art. 4 Nr. 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. **Auftragsverarbeiter** ist nach Art. 4 Nr. 8 DSGVO die Stelle, „die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Dabei wird der Zweck ausschließlich vom Verantwortlichen festgelegt; bzgl. der Mittel der Verarbeitung hat ein Auftragsverarbeiter einen Handlungsspielraum, soweit der Verantwortliche keine verbindlichen Vorgaben macht. Der Auftragsverarbeiter muss Weisungen des Verantwortlichen

[11] BlnBDI, JB 2021 (Fn. 4), Kap. 1.3.1.
[12] https://www.datenschutz-berlin.de/infothek-und-service/themen-von-a-bis-z/terminverwaltung.
[13] Z.B. https://contour.de/index.php/referenzen/internet/webseite-mit-einbindung-jameda.
[14] Netzwerk Datenschutzexpertise (Fn. 2), Kap. 4 (S. 13 ff.).

befolgen (Art. 28 Abs. 3 S. 2 lit. a DSGVO). Tut er dies nicht, so wird er gemäß Art. 28 Abs. 10 DSGVO zum Verantwortlichen, ohne dafür i.d.R. eine Berechtigung zu haben.

Der europäische Datenschutzgesetzgeber hat mit Art. 26 DSGVO zur „**gemeinsamen Verantwortlichkeit**“ eine klare Struktur für die Zuordnung der Verantwortungsbereiche beim Datenschutz geschaffen, um der oft komplexen Realität von verschachtelten informationstechnischen Vorgängen gerecht zu werden. Die Verantwortlichkeiten sollen gemäß der DSGVO klar und transparent verteilt sein.[15] Diese Vorgaben wurden durch Entscheidungen des Europäischen Gerichtshofes (EuGH) seit Juni 2018 präzisiert.[16] Gemeinsame Verantwortlichkeit ist demnach gegeben, wenn eine Datenverarbeitung selbständige Entscheidungen verschiedener Stellen voraussetzt, d.h. wenn eine Verarbeitung ohne die aktive Beteiligung jeder Stelle nicht denkbar ist, wenn ein kumulatives Zusammenwirken erfolgt.[17] Eine zeitgleiche und gemeinsam abgestimmte Entscheidung über Zwecke und Mittel ist dafür nicht nötig.[18] Gemeinsame Verantwortlichkeit kann dadurch entstehen, dass im Voraus von einem Anbieter festlegte Zwecke und Mittel von einem anderen Nutzer akzeptiert werden, indem er diese für seine Verarbeitung in Anspruch nimmt.[19] Für die Feststellung der gemeinsamen Verantwortlichkeit kommt es auf die objektiven tatsächlichen Umstände an.[20]

Für eine gemeinsame Verantwortlichkeit ist – in Abgrenzung zur Auftragsverarbeitung (Art. 28 DSGVO) – ausschlaggebend, dass jede Stelle aus Eigeninteresse Einfluss auf die Verarbeitung nimmt und damit an der Festlegung über Zwecke und Mittel dieser Verarbeitung **faktisch mitwirkt**. Dies kann ausdrücklich, aber auch stillschweigend erfolgen.[21] Jeder der Verantwortlichen hat eine rechtliche oder tatsächliche Möglichkeit, Zwecke sowie wesentliche Elemente der Mittel der Verarbeitung zu bestimmen.[22] Eine Gleichrangigkeit der Entscheidungsbefugnis ist nicht nötig, wohl aber muss eine „kooperative Determinierung des Zielzustands“ erfolgen.[23] Die Entscheidungen der gemeinsam Verantwortlichen müssen in der Form erfolgen, dass sie sich zum Zeitpunkt der Datenverarbeitung gegenseitig ergänzen, nacheinander erfolgende Entscheidungen in Bezug auf konkrete Verarbeitungsschritte sind nicht gemeinsam.[24]

Eine **Entscheidung** bzgl. der Datenverarbeitung liegt vor, wenn diese endgültig bestimmt wird und ohne den direktiven, bestimmte Modalitäten der Datenverarbeitung regelnden Input einer Stelle

[15] Specht-Riemenschneider/Schneider MMR 2019, 504; Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, S. 61.
[16] EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = ZD 2018, 357 = NVwZ 2018, 1386 = EuZW 2018, 534 = MMR 2018, 591 = BB 2018, 1480 = DuD 2018, 518;; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), NJW 2019, 285 = NVwZ 2018, 1787 = EuZW 2018, 897; EuGH 29.07.2019 – C-40/17 (Fashion ID).
[17] Weichert DANA 2019, 5.
[18] Doench/Sommerfeld in Kipker/Voskamp, Sozialdatenschutz in der Praxis, 2021, S. 113 m.w.N.; a.A. Kremer CR 2019, 227; Bertermann in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 26 Rn. 10.
[19] Datenschutzkonferenz (DSK), Kurzpapier Nr. 16, Stand 19.03.2018, S. 3.
[20] EuGH 10.7.2018 – C-25/17 (Zeugen Jehovas), Rn. 67, NJW 2019, 285 = NVwZ 2018, 1787 = EuZW 2018, 897; Martini in Paal/Pauly, DS-GVI BDSG, 3. Aufl. 2021, Art. 26 Rn. 18.
[21] EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 68, 80.
[22] European Data Protection Supervisor (EDPS), Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 (2019), S. 23.
[23] Thüsing/Rombey NZA 2019, 10; Martini in Paal/Pauly (Fn. 20), Art. 26 Rn. 21.
[24] Specht-Riemenschneider/Schneider MMR 2019, 504; Thomale in Auernhammer, DSGVO BDSG, 6. Aufl. 2018, Art. 26 Rn. 9; DSK, Kurzpapier Nr. 16 (Fn. 19), S. 3.

potenziell anders ausfallen würde.[25] Fehlt es an der Bestimmungsmöglichkeit über die Zwecke, so ist i.d.R. eine Auftragsverarbeitung gegeben.

Welches **Eigeninteresse** von den Verantwortlichen verfolgt wird, ist unbedeutend. Dieses kann ökonomischer oder altruistischer Art sein; es kann in einem Erkenntnisinteresse liegen oder in Bequemlichkeit bzw. dem Interesse an einer unaufwändigen Abwicklung eines Vorgangs. Einzige faktische Voraussetzung ist, dass sich die von gemeinsam Verantwortlichen verfolgten Zwecke, die sich unterscheiden können, praktisch gegenseitig ergänzen.[26] Die Zwecke müssen nicht übereinstimmen.[27] Die Zwecke müssen auch nicht in einem positiven wirtschaftlichen Bedingungszusammenhang stehen.[28]

Jeder der gemeinsam Verantwortlichen muss für sich die Verarbeitung auf eine **Rechtsgrundlage** stützen können, wobei diese Rechtsgrundlagen nicht zwingend identisch sein müssen.[29] So ist es möglich, dass der eine sich auf eine Einwilligung beruft, der andere auf die Wahrnehmung berechtigter Interessen.

3.1 Gemeinsame Verantwortlichkeit von Doctolib und Gesundheitseinrichtung

Die oben genannten Voraussetzungen einer gemeinsamen Verantwortlichkeit sind bei der Terminverwaltung durch Doctolib für Gesundheitseinrichtungen gegeben. Beide Parteien bestimmen über Zwecke und Mittel der Verarbeitung. Es besteht ein gemeinsames Interesse an der Terminvermittlung; das spezifische Interesse Doctolibs hieran beschränkt sich nicht darauf, für die Gesundheitseinrichtung eine Dienstleistung zu erbringen. Sie erstreckt sich auch auf die Erbringung einer eigenständigen **Dienstleistung für die Kunden**, mit der ein eigenständiges Vertragsverhältnis und eine über eine Gesundheitseinrichtung hinausgehende Kundenbindung aufgebaut wird.

Von einer gemeinsamen Verantwortlichkeit nicht mehr mit umfasst werden vor- und nachgelagerte Vorgänge einer **Verarbeitungskette**, für die weder Zwecke noch Mittel gemeinsam festgelegt werden.[30] Keine gemeinsame Verantwortlichkeit wäre gegeben, wenn die Verarbeitungsschritte bei Doctolib und der Gesundheitseinrichtung nacheinander erfolgen würden, ohne dass Daten für Zwecke des Vorverarbeiters zurückgespielt würden. Bei der Feststellung der gemeinsamen Verantwortlichkeit muss auf den jeweiligen konkreten Verarbeitungsvorgang Bezug genommen werden, wobei ein technisch einheitlicher Prozess evtl. in verschiedene Prozessschritte bzw. Verarbeitungsphasen aufzuteilen ist.[31] Art. 4 Nr. 2 DSGVO umschreibt solche verschiedenen Abschnitte einer „Vorgangsreihe“. Für die Differenzierung bei der Verantwortlichkeit besonders relevant sind die Schritte „Erhebung“, „Speicherung“, „Auswertung“ und „Übermittlung“.[32] Sind einzelne

[25] EDPS (2019), 7; Specht-Riemenschneider/Schneider MMR 2019, 504; Ingold in Sydow, Europäische Datenschutz-Grundverordnung, 2017, Art. 26 Rn. 4; Monreal ZD 2019, 802, Rn. 28.
[26] Golland ZD 2019, 382.
[27] DSK, Kurzpapier Nr. 16 (Fn. 19), S. 2; a.A. Kremer CR 2019, 227.
[28] Golland K&R 2019, 535; anders Hanloser ZD 2019, 123.
[29] Petri in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 26 Rn. 1; Monreal ZD 2019, 805 Rn. 50.
[30] EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74.
[31] EuGH 29.07.2019 – C-40/17 (Fashion ID), Rn. 74; DSK, Kurzpapier Nr. 16 (Fn. 19), S. 2 f.
[32] Golland K&R 2019, 534.

Prozessschritte denklogisch, nicht technisch, miteinander verbunden, so besteht insofern eine einheitliche Verantwortungszuordnung.

Bei der Differenzierung der Verarbeitungsschritte wird zwischen der Mikro- und der Makroebene unterschieden: Bei der Mikroebene wird auf den jeweiligen Verarbeitungsschritt i.S.d. Art. 4 Nr. 2 DSGVO abgestellt, bei der Makroebene auf die Sicht der Betroffenen. Relevant für die Feststellung der gemeinsamen Verantwortung ist die **Mikroebene**, also die Entscheidung über den tatsächlich erfolgenden Verarbeitungsschritt. Um deshalb keine falsche Wahrnehmung der Betroffenen auszulösen, soll für diese über Art. 26 DSGVO Transparenz und Rechtsschutz gesichert werden.[33]

Eine Verarbeitungskette mit getrennten Verantwortlichkeiten besteht bei der Terminvereinbarung durch Doctolib nicht: Vor einer **ärztlichen Terminvermittlung** durch Doctolib wird regelmäßig der Patientendatenstamm an Doctolib transferiert, über den dann ein Abgleich mit den Terminwünschen erfolgt und der dann zu einer Termineintragung führt. Dadurch werden die ärztlichen Patientendaten für die vertragliche Dienstleistung von Doctolib gegenüber dem Kunden verwendet. Doctolib vertritt die Ansicht, dass die Terminhistorie in seinem System als Teil der Patientenakte anzusehen sei. Wie auch bei der Impfvermittlung in Berlin erfolgt bei allen Termineintragungen eine Weiterspeicherung nach Terminablauf. Diese Speicherung ist jedoch für die ärztliche Tätigkeit nicht mehr erforderlich und dient damit ausschließlich den Zwecken von Doctolib im Rahmen der Kundenbeziehung zu seinen Kontoinhabern.

Besteht faktisch eine gemeinsame Verantwortlichkeit, so bedarf es für die Datenverarbeitung einer Rechtsgrundlage bei jedem der Verantwortlichen. Eine solche Rechtsgrundlage besteht für den Arzt durch den Behandlungsvertrag. Hinsichtlich der PatientInnen eines Arztes, deren Daten von Doctolib verarbeitet werden, ohne dass sie dort einen Account haben, besteht für Doctolib **keine Rechtsgrundlage**. Da es sich bei diesen Daten um Gesundheitsdaten i.S.v. Art. 9 Abs. 1 DSGVO handelt, genügt als Legitimation einer Verarbeitung kein irgendwie geartetes „berechtigtes Interesse“ i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO.[34] Eine Legitimation der Verarbeitung durch Art. 9 Abs. 2 DSGVO ist nicht gegeben. Die Datenübermittlung von der Arztpraxis an Doctolib lässt sich insbesondere nicht durch Art. 9 Abs. 2 lit. h DSGVO rechtfertigen: Sie ist nicht erforderlich „für Zwecke der Gesundheitsvorsorge“, „für die medizinische Diagnostik, die Versorgung oder Behandlung“ oder „für die Verwaltung von Systemen und Diensten“ im Gesundheitsbereich. Insofern ist die Einschaltung von Doctolib – die unter dem Label „Auftragsverarbeitung“ erfolgt, tatsächlich aber zur einer gemeinsamen Verantwortlichkeit führt – unzulässig.

Die obige rechtliche Bewertung zur Terminverwaltung ist übertragbar auf das Doctolib-Angebot zur **Videokonsultation**. Auch dieses setzt die Einrichtung eines Doctolib-Accounts voraus, wodurch es zu einer Vermengung von eigener Verantwortlichkeit und Auftragsverarbeitung kommt.

3.2 Medizinrechtliche Bewertung

Gesundheitsdienstleister wie Ärzte oder auch eine Impfangebote machende Gesundheitsverwaltung unterliegen hinsichtlich der erlangten Daten einer medizinrechtlich begründeten

[33] Bertermann in Ehmann/Selmayr (Fn. 18), Art. 26 Rn. 8.
[34] Schantz in Simitis/Hornung/Spiecker (Fn. 29), Art. 6 Abs. 1 Rn. 109.

Vertraulichkeitsverpflichtung. Diese hat ihre zentrale Grundlage in der strafrechtlich geregelten ärztlichen Schweigepflicht (Berufsgeheimnis, speziell: Patientengeheimnis, § 203 Strafgesetzbuch – StGB). Weitere Grundlagen bestehen im spezifischen Medizinrecht und im Standesrecht (z.B. § 9 MBOÄ). Das **Patientengeheimnis** erstreckt sich auf das ärztliche Personal, deren Mitarbeiter als „Gehilfen" sowie auf „Mitwirkende", zu denen Mitarbeitende von externen informationstechnischen Dienstleistern wie Doctolib gehören können.[35]

Für die berufsrechtlich geforderte Vertraulichkeit kommt es auf die datenschutzrechtliche Einordnung nicht an. Die Mitwirkung gemäß § 203 Abs. 3, 4 StGB kann als **Auftragsverarbeitung oder als gemeinsame Verantwortlichkeit** ausgestaltet sein. Erstreckt sich ein Vertrag zur Datenverarbeitung auf Berufsgeheimnisse, egal ob es sich um eine Vereinbarung i.S.v. Art. 26 DSGVO oder einen Auftragsvertrag nach Art. 28 DSGVO handelt, so muss eine rechtliche Bindung zwischen dem Berufsgeheimnisträger und der mitwirkenden Person hergestellt werden. Dies ist im Rahmen eines Vertrags nach Art. 28 Abs. 3 DSGVO wie nach einer Vereinbarung nach Art. 26 DSGVO möglich. Aufgrund eigenständiger Entscheidungsbefugnisse der Handelnden kann die Tätigkeit solcher Personen datenschutzrechtlich als Funktionsübertragung, also als Verarbeitung durch einen externen Verantwortlichen, einzuordnen sein.[36]

Es muss jeweils eine weitergehende Präzisierung der eingebundenen Personen erfolgen, die dann gemäß § 203 Abs. 4 S. 2 Nr. 2 StGB **persönlich zur Geheimhaltung zu verpflichten** sind.[37] Der Berufsgeheimnisträger muss für die Belehrung „Sorge tragen". Es genügt, dass die konkrete Geheimnisverpflichtung nicht durch ihn, sondern durch den Vertragspartner des Gesundheitsdienstleisters, also hier durch Doctolib, erfolgt. Wird die Verpflichtung der mitwirkenden Person zur Geheimhaltung unterlassen, so macht sich der Verpflichtete strafbar, wenn die mitwirkende Person gegen ihre Geheimhaltungspflichten verstößt.[38] Dies gilt auch, wenn der Mitwirkende trotz der unterlassenen Verpflichtung seine eigene Schweigeverpflichtung kannte.[39]

In der Gesetzesbegründung zur Änderung von § 203 Abs. 3, 4 StGB werden **Beispiele für „mitwirkende Tätigkeiten"** genannt. 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".[40] Ein zentraler Anwendungsfall soll die Datenverarbeitung in einer Cloud sein.[41] Der Katalog in der Gesetzesbegründung ist nicht abschließend.

Das Gesetz will „keinen möglichen Rechtsgrund, auf dem eine sonstige Mitwirkung beruhen kann, ausschließen".[42] Typischerweise besteht ein Vertragsverhältnis. Notwendig ist die **Einbindung in die**

[35] Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 81 ff.
[36] Gola/Klug/Körffer in Gola/Schomerus, BDSG, 12. Aufl. § 11 Rn. 11; Pohle/Ghaffari CR 2017, 492; Wronka RDV 2017, 130.
[37] Zu den Anforderungen an die Geheimhaltungsverpflichtung Grosskopf/Momsen CCZ 2018, 100.
[38] Eisele in Schönke/Schröder, Strafgesetzbuch, 30. Aufl. 2019, § 203 Rn. 101, 104; Eisele JR 2018, 86 f.
[39] Kritisch hierzu Eisele JR 2018, 87.
[40] BT-Drs. 18/11936, 22; Härting, MDR 2018, 2.
[41] Zu den weiteren Anforderungen Momsen/Savić KriPoZ 2017, 302.
[42] BT-Drs. 18/11936, 22 f.; Eisele JR 2018, 83.

berufliche Tätigkeit und das Einvernehmen hierüber mit dem Berufsgeheimnisträger. Die Einbindung muss sich nicht auf informationstechnische Aktivitäten beschränken, sondern kann in umfassenden Unterstützungsleistungen bestehen.[43] Bei der helfenden Tätigkeit soll eine weite Auslegung möglich sein. Daher ist eine Mitwirkung der Mitarbeiter von Doctolib bei der medizinischen Tätigkeit einer Gesundheitseinrichtung grundsätzlich in allen Bereichen möglich, in denen Doctolib tätig ist: Terminmanagement, Durchführung von ärztlichen Videoberatungen, Dokumentation von Gesundheitsinformationen. Es genügt, dass die Mitwirkenden „in irgendeiner Weise“ in den Umgang mit den Geheimnissen eingebunden sind.

Es wird zudem nach § 203 Abs. 3 S. 2 StGB rechtlich gefordert, dass die Tätigkeit, bei der ein Geheimnis zur Kenntnis genommen wird oder werden kann, erforderlich ist. Gegen diese Regelung ist aus Bestimmtheitsgründen nichts einzuwenden; eine präzisere Eingrenzung ist angesichts der vielfältigen möglichen Fallgestaltungen, die von der Regelung erfasst werden sollen, nicht möglich.[44] Die **Erforderlichkeit der Dienstleistung** setzt voraus, dass diese nicht ohne Kenntnis der fremden Geheimnisse durchgeführt werden kann. Bei der Feststellung der Erforderlichkeit muss eine Prüfung der konkreten Einbindung erfolgen. Es kann kein strenger Maßstab angelegt werden.[45] Es liegt in der Freiheit des Berufsgeheimnisträgers, seine Methoden selbst festzulegen. Hierzu gehört auch die Einbindung externer Unterstützung. Insofern genügt eine gesteigerte „Dienlichkeit“.[46] Die Dienstleistung ist erforderlich, wenn sie von dem 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 des Geheimnisträgers liegen. Auch das Ziel der Kostenersparnis sowie Qualitäts- und Verfügbarkeitsgründe können eine Erforderlichkeit begründen, wenn diese Gründe erheblich sind.[47] Der Geheimnisträger hat einen weiten Ermessensspielraum.[48]

Es ist zu unterscheiden zwischen der Erforderlichkeit der Dienstleistung generell und der Erforderlichkeit der einzelnen Offenbarung. Hinsichtlich der **Erforderlichkeit der konkreten Offenbarungen** muss 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.[49] Verfügbare technische Mittel der Datenminimierung, etwa der Verschlüsselung oder der Ano- bzw. der Pseudonymisierung sind einzusetzen.[50] Bei der Verarbeitung von Berufsgeheimnissen kommt hinzu, dass möglichst wenige Personen bei einem externen Dienstleister eingebunden werden.

Für eine Offenbarung der gesamten Patientenstammdaten oder von großen Teilen davon besteht zum Zweck der **Terminvereinbarung** keine Erforderlichkeit (siehe auch unten 5.1). Viele Patienten, die im

[43] Grosskopf/Momsen CCZ 2018, 99.
[44] Härting MDR 2018, 3; Eisele JR 2018, 6; a. A. Fechtner/Haßdenteufel CR 2017, 360.
[45] Ruppert K&R 2017, 612, 613.
[46] Strenger Grosskopf/Momsen CCZ 2018, 102.
[47] 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.
[48] Eisele JR 2018, 84.
[49] Dochow, Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen, 2017, S. 1355 ff. m.w.N.
[50] Eisele JR 2018, 84 f.; Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 5 Rn. 48.

Patientenstamm in der Gesundheitseinrichtung aufgeführt sind, vereinbaren keinen Termin. Auch für Terminbestätigungen besteht im Rahmen der ärztlichen Tätigkeit regelmäßig keine „Erforderlichkeit". Sollte ein Patient den Wunsch nach einer Terminbestätigung haben, so kann er diesen Wunsch äußern und evtl. der Einbindung eines Dienstleisters zustimmen.[51] Gegen eine Terminbestätigung bei Patienten, die über Doctolib ihren Termin gebucht haben, ist in Bezug auf § 203 StGB nichts einzuwenden, wenn die Terminbestätigung als Bestandteil der Terminvermittlung für den Betroffenen erkennbar ist.

Durch die Bereitstellung der Stammdaten seiner Patienten an Doctolib verstößt der **Arzt** gegen seine in § 203 Abs. 1 Nr. 1 StGB normierte berufliche Schweigepflicht. Inwieweit der Arzt hierbei schuldhaft handelt, muss im Einzelfall bewertet werden. Dabei ist auch zu berücksichtigen, dass Doctolib – entgegen der Rechtslage – gegenüber seinen Kunden beteuert, dass seine Beauftragung mit § 203 StGB in Einklang stünde.[52] Auf diese Beteuerung kann der Arzt nicht pauschal vertrauen. Vielmehr ist er verpflichtet, zumindest im Zweifelfall sich insofern objektiven rechtlichen Rat einzuholen.

Strafbar machen sich aber auch die **Beschäftigten von Doctolib**, die gegenüber Gesundheitseinrichtungen fälschlich behaupten, die Übermittlung der Patientenstammdaten sei rechtlich unbedenklich. Hierbei kann es sich um eine Anstiftung oder eine Beihilfe zu einer Straftat i.S.v. §§ 26, 27 StGB handeln.

3.3 Zuständige Aufsicht

Doctolib macht geltend, für seine datenschutzrechtliche Aufsicht sei nicht die oder der BlnBDI zuständig, sondern die französische Aufsichtsbehörde, die Commission Nationale de l'Informatique et des Libertés (CNIL). Die CNIL sei die zuständige **federführende Aufsichtsbehörde** gemäß den Art. 56, 60 ff DSGVO. Voraussetzung hierfür ist, dass eine grenzüberschreitende Datenverarbeitung erfolgt und die Entscheidungen über Zwecke und Mittel in der Hauptniederlassung erfolgen. Im Vertrag zur Auftragsverarbeitung Vertrag (AV-Vertrag) unter Nr. 15, der z.B. als Anlage 1 Vertrag zwischen der Senatsverwaltung für Gesundheit Berlin und der Doctolib GmbH von Dezember 2020 beigefügt ist, wird im Kleingedruckten angegeben, dass die für die Doctolib GmbH zuständige Aufsichtsbehörde zwar die BlnBDI sei, federführende Aufsichtsbehörde sei jedoch „die für die Muttergesellschaft Doctolib SAS zuständige französische Aufsichtsbehörde CNIL". Offenbar geht Doctolib generell von dieser rechtlichen Bewertung hinsichtlich der Aufsicht über die Datenverarbeitung in Deutschland aus.

Anknüpfungspunkt für die datenschutzrechtliche Verantwortlichkeit ist die handelnde juristische Person, die den Zweck der Datenverarbeitung vorgibt. Die DSGVO kennt kein Konzernprivileg. Wirtschaftliche Verflechtungen oder faktische Einflussnahmen bleiben grundsätzlich unberücksichtigt. Im Interesse der **Transparenz** gegenüber den Betroffenen, der Aufsicht sowie der weiteren Beteiligten hat sich eine Stelle daran zu orientieren, wie sie diesen gegenüber im Geschäftsverkehr auftritt. Tochtergesellschaften sind auch als hundertprozentige Beteiligungen kein Teil der Muttergesellschaft.[53]

[51] So im Ergebnis auch BlnBDI, JB 2021 (Fn. 4), Kap. 6.5.
[52] Datenschutzcharta, Nr. 7, https://cdn2.hubspot.net/hubfs/5479688/B2B%20-%20Data%20security/Datenschutzgrundsa%CC%88tze%20fu%CC%88r%20A%CC%88rzte.pdf.
[53] Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 4 Rn. 93.

Im Impressum der Webseite wird die deutsche **Doctolib GmbH als Verantwortliche** genannt: Doctolib GmbH**,** Mehringdamm 51, 10961 Berlin. Dort findet sich auch der Hinweis: Die Doctolib GmbH ist ein Tochterunternehmen der Doctolib SAS, 54 quai Charles Pasqua, 92300 Levallois-Perret, Frankreich. Als Vertragspartner der Gesundheitseinrichtungen wird genannt „Doctolib GmbH, Handelsregister AG Berlin HRB 175963 B, Mehringdamm 51, 10961 Berlin".

Sowohl telemedienrechtlich, wettbewerbsrechtlich wie auch datenschutzrechtlich ist die rechtlich unabhängige Doctolib GmbH verantwortlich und nicht das **Mutterunternehmen in Frankreich**. Es gibt keine Hinweise dafür, dass für die Aufsichtszuständigkeit der Sitz des Mutterunternehmens bestimmend ist, dass dieses als Hauptniederlassung (Art. 4 Nr. 16 DSGVO) zu bewerten sei. Es ist die Doctolib GmbH in Berlin, die als solche im Rechtsverkehr auftritt, die Verträge abschließt und hinsichtlich der Datenverarbeitung kommuniziert. Konzerninterne Vorbehalte sind nicht zu berücksichtigen. Doctolib gibt selbst an, dass für das Unternehmen die Aufsichtsbehörde in Berlin zuständig ist.[54] Die Zuständigkeitsregelung der Datenschutzaufsicht in Art. 56 DSGVO ist gesetzlich vorgegeben und kann nicht durch vertragliche Regelungen, schon gar nicht im Kleingedruckten in allgemeinen Geschäftsbedingungen (AGB) festgelegt werden. Ausschlaggebend ist, wo die Entscheidungen über die Datenverarbeitung getroffen werden.[55] Dies erfolgt bei der Doctolib GmbH in Berlin, zumal sich das mit ausschlaggebende nationale Medizinrecht Deutschlands von dem in Frankreich unterscheidet.

Gemäß Art. 56 Abs. 2 DSGVO ist in jedem Fall die örtliche Aufsichtsbehörde zuständig, „wenn der Gegenstand nur mit einer Niederlassung in ihrem Mitgliedstaat zusammenhängt oder betroffene **Personen nur ihres Mitgliedsstaates** erheblich beeinträchtigt" sind. Sowohl die Terminverwaltung für Arztpraxen wie auch sonstige Dienstleistungen für Gesundheitseinrichtungen in Deutschland durch Doctolib einschließlich der Impfdokumentation für die Senatsverwaltung Berlin betreffen ausschließlich Menschen in Deutschland. Eine grenzüberschreitende Datenverarbeitung erfolgt allenfalls als (Unter-) Auftragsverarbeitung. Zuständig für die Doctolib GmbH ist daher ausschließlich der BlnBDI. Mit der Leugnung der Sanktionszuständigkeit des BlnBDI verfolgt Doctolib offensichtlich das Ziel, eine aufsichtliche Sanktionierung seiner unzulässigen Datenverarbeitung zu behindern.

4 Die Änderung des Regelwerks

Im Gutachten des Netzwerks Datenschutzexpertise vom 08.06.2021 wurde das Regelwerk von Doctolib einer ausführlichen Kritik unterworfen, wobei eine Vielzahl von Verstößen gegen das Datenschutzrecht festgestellt wurde.[56] Von Februar bis Mai 2022 erließ Doctolib teilweise völlig überarbeitete Datenschutzhinweise für PatientInnen und für Gesundheitsfachkräfte. Hierbei wurden einige Defizite behoben. Zentrale Kritikpunkte bestehen aber weiterhin. So gesteht Doctolib weiterhin nicht ein, dass bei der Verarbeitung für „Gesundheitsfachkräfte" eine **gemeinsame Verantwortlichkeit** besteht und nicht – wie behauptet – ausschließlich eine Auftragsverarbeitung. Das Unternehmen beachtet nicht die sich hieraus ergebenden Pflichten (s.o. 3.1).

[54] https://media.doctolib.com/image/upload/mkg/file/Impressum_Doctolib_Deutschland.pdf.
[55] Eichler in Wolff/Brink, Datenschutzrecht, 2. Aufl. 2022, Art. 56 DSGVO, Rn. 10.
[56] Netzwerk Datenschutzexpertise (Fn. 2), Kap. 3.2, 3.3, 16.

Doctolib beruft sich weiterhin im Rahmen seines Vertragsverhältnisses mit den PatientInnen sehr umfassend und mit einer langfristigen Speicherung (teilweise unbegrenzt, teilweise 6 Monate für Log, 1 Jahr für IP-Adresse) auf ein „**berechtigtes Interesse**“ für folgende Zwecke: Benutzerverwaltung, Webseitennavigation, Prävention und Bekämpfung von Computerkriminalität.

An der intransparenten **Einbindung von sozialen Netzwerken**[57] hat sich nichts Wesentliches geändert.

Nach der teilweise heftigen Kritik an den Datenschutzregelungen und der Datenschutzpraxis hat Doctolib **Anpassungen** vorgenommen und den Gesundheitsfachkräften bzw. Patienten zusätzliche Wahlmöglichkeiten eröffnet. Hierbei bedarf es aber oft des aktiven Tätigwerdens der Kunden, etwa wenn es um die Identitätsprüfung von Beschäftigten geht, bei der standardmäßig das Hochladen des Personalausweises gefordert wird.

5 Erforderlichkeit

Nach Art. 5 Abs. 1 lit. c DSGVO muss eine Verarbeitung, um datenschutzrechtlich zulässig zu sein, „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung)“. Eine identifizierende Verarbeitung ist nach Art. 5 Abs. 1 lit. e DSGVO nur so lange erlaubt, „wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“ (Speicherbegrenzung). Danach sind diese Daten zu löschen (Art. 17 Abs. 1 lit. a DSGVO).

5.1 Übertragung des Patientenstamms

Im Rahmen der Terminverwaltung erfolgt durch Doctolib regelmäßig eine vollständige Übermittlung des Patientenstamms der Gesundheitsfachkraft. Dieser erfasst auch nicht mehr aktive Patientenbeziehungen sowie PatientInnen, die mit Doctolib keine Vertragsbeziehung eingegangen sind. Es erfolgt in der Regel eine **Synchronisation zwischen dem Terminverwaltungsverfahren** bei Doctolib und der Terminverwaltung im Arztinformationssystem der Praxis. Entsprechende personenbezogene Datentransfers sind nicht für die Erbringung der Terminverwaltung nötig. Dies gilt für sämtliche Patientendaten ohne Doctolib-Konto. Auch soweit diese einen Termin vereinbart haben, bedarf es nicht einer personenbezogenen Datenübermittlung; zur Feststellung belegter Termine genügt eine anonymisierte Übermittlung an Doctolib. Andere Terminverwaltungssysteme kommen ohne entsprechende Übermittlungen aus.

5.2 Terminerinnerung

In ihrem Jahresbericht 2021 bekräftigt die BlnBDI die auch im Gutachten des Netzwerks Datenschutzexpertise ausgeführte rechtliche Bewertung[58], dass eine Terminerinnerung für eine **ärztliche Behandlung** nicht erforderlich ist. Soll ein externer Dienstleister hierzu von einer Arztpraxis beauftragt werden, so setzt dies nicht nur eine Information, sondern die ausdrückliche Einwilligung des Patienten voraus.[59] Diesen Anforderungen genügen die Arztpraxen und ihr Dienstleister Doctolib in der Praxis auch weiterhin weitgehend nicht.

[57] Netzwerk Datenschutzexpertise (Fn. 2), Kap. 12 (S. 29 f.).
[58] Netzwerk Datenschutzexpertise (Fn. 2), Kap. 7.3 (S. 23).
[59] BlnBDI, JB 2021 (Fn. 4), Kap. 6.5 (S. 92 f.).

5.3 Datenlöschung

Der Zweck der Speicherung von Termindaten entfällt, wie auch die BlnBDI feststellte, sobald der **Termin vergangen** ist. Da erfolgte Termine in den Patientenakten dokumentiert sind, ist eine zusätzliche Speicherung im System des Terminverwaltungsunternehmens nach Ablauf des Termins nicht mehr erforderlich und damit unzulässig. Der Terminkalender des Arztes gehört nicht zur arztrechtlich geforderten Patientendokumentation (§ 10 MBOÄ, § 630f BGB). Aus ihm ergeben sich keine den Patienten betreffenden „Feststellungen und getroffenen Maßnahmen". Diese Datenlöschung sollte im Auftragverarbeitungsvertrag ausdrücklich festgelegt sein.[60] Eine Festlegung der entsprechenden Löschpflicht ist im Auftragsvertrag mit Doctolib nicht enthalten. Eine unverzügliche Löschung nach Terminablauf ist auch in der Praxis nicht gewährleistet.

6 Datensicherheit

Datensicherheit, d.h. die Gewährleistung von **Integrität, Verfügbarkeit, Vertraulichkeit, Nichtverkettbarkeit, Intervenierbarkeit und Transparenz**[61] durch technisch-organisatorische Maßnahmen ist angesichts der hohen Sensitivität von Gesundheitsdaten von hoher Relevanz. In Art. 32 DSGVO und ergänzend in § 22 Abs. 2 BDSG werden die Anforderungen hinsichtlich der zu ergreifenden Maßnahmen allgemein benannt und teilweise präzisiert. Einen Baustein-Katalog der Schutzmaßnahmen enthält das von den Datenschutzbehörden entwickelte Standard-Datenschutzmodell.[62]

Das Angebot von Doctolib hat sich in der Vergangenheit immer wieder durch ungenügende Datensicherheitsmaßnahmen ausgezeichnet. Immer wieder bedurfte es einer kritischen öffentlichen Berichterstattung, dass die gesetzlich geforderten Schutzmaßnahmen ergriffen wurden. Die Sicherheitsmaßnahmen werden im Anhang 2 zum Vertrag zur Auftragsverarbeitung mit Doctolib nur abstrakt dargestellt. Deren Umsetzung wird grundsätzlich gegenüber den verantwortlichen Gesundheitsfachkräften **nicht offengelegt**. So müsste z.B. für die Kommunikation Doctolibs mit einem Arztinformationssystem eines Kunden die Firewall auf eine oder wenige Adressen beschränkt sein. Tatsächlich forderte Doctolib hierfür die Freischaltung einer großen Anzahl von Adressen, die sich teilweise sogar im unsicheren Drittausland befinden. Die fehlende Transparenz ändert nichts an dem Umstand, dass die Gesundheitseinrichtung für die Datensicherheit verantwortlich bleibt und sich Lücken bei Doctolib insofern zurechnen lassen muss.

Die Verpflichtung zu Sicherungsmaßnahmen erstreckt sich auch auf Auftragsverarbeiter und Unterauftragsverarbeiter, unabhängig davon, wo diese sich räumlich befinden. Verpflichtet wird somit auch **Amazon Web Services** (AWS) als Unterauftragnehmer. Doctolib gibt an, die Daten würden bei AWS verschlüsselt verarbeitet. Doctolib legte bisher keine technischen Informationen vor, mit denen beurteilt werden kann, ob die Sicherungsmaßnahmen hinreichend sind.

Doctolib setzt zudem **Cloudflare** als Web-Performance und -Sicherheitsunternehmen mit Sitz in den USA ein.[63] Die gesamte Ver- und Entschlüsselung erfolgt browserbasiert. Dadurch hat Cloudflare

[60] BlnBDI, JB 2021, (Fn. 4), Kap. 6.5 (S. 93).
[61] Rost, Die Schutzziele des Datenschutzes, in Schmidt/Weichert, Datenschutz, 2012, S. 353 ff.
[62] https://www.datenschutzzentrum.de/sdm/.
[63] Zur Verarbeitung in den USA Netzwerk Datenschutzexpertise (Fn. 2), Kap. 14.2 (S. 33 f.).

Kontrolle über den an den Browser ausgelieferten Code. Es liegen keine Informationen vor, die eine angemessene Sicherheitsüberprüfung der verwendeten Verfahren ermöglichen würden.

7 Organisation der Impfkampagne in Berlin

Mit Datum vom 04.12.2020 schloss die Berliner Senatsverwaltung für Gesundheit mit Doctolib einen „Vertrag über die Nutzung der Doctolib Services für die **Terminierung von Impflingen** in Corona Impfzentren (CIZ)“[64], wonach das Unternehmen eine webbasierte digitale Lösung „zum Zweck der Terminvereinbarung, -verwaltung und -durchführung mit Patienten“ zur Verfügung stellt.

Mit Datum vom 29.12.2020, versandt am 03.05.2021, schlossen die Gesundheitsverwaltung und Doctolib einen „Vertragsnachtrag Nr. 1 zum Auftragsverarbeitungsvertrag“[65], in dem Doctolib sich verpflichtet, zwecks „Führung der gesetzlichen erforderlichen **Impfdokumentation**“ sowie des „Impfmonitoring einschließlich der von der CoronaImpfV vorgegebenen Übermittlung der vom RKI geforderten Informationen“ u.a. weitere teilweise sensitive Daten[66], u.a. Angaben zu Gesundheitszustand und Krankheitsgeschichte einschließlich Impfstoff, Nebenwirkungen und Priorisierungsgrundlage, zu verarbeiten.

Die Berliner Gesundheitssenatsverwaltung wurde auf die Datenübermittlung mit Hilfe eines **Cookies** der Doctolib-App an Google von mobilsicher.de angesprochen, machte hierzu aber keine Angaben: „Wir haben die Bestätigung von Doctolib, dass alle Applikationen DSGVO-konform betrieben werden. Eine tiefgehende technische Prüfung aller Aspekte der Datensicherheit und des Datenschutzes“ habe es nicht gegeben.[67]

In ihrem Jahresbericht 2021 kritisierte die BlnBDI, dass bei der Auftragserteilung an Doctolib zur Online-Terminbuchung die rechtlichen Anforderungen an eine Auftragsverarbeitung missachtet werden, weil die „Bürger:innen im Rahmen des Online-Terminbuchungsprozesses mit der Anlage eines Nutzungskontos auch zwingend ein eigenes **Vertragsverhältnis mit dem Privatunternehmen** eingehen müssen“. Ein von anderen Ländern genutztes, datenschutzkonformes Online-Terminbuchungssystem der KBV wird in Berlin nicht genutzt. Datenschutzgerecht wäre nur ein Verfahren, das ausschließlich im Auftrag und nach Weisung der zuständigen Senatsverwaltung erfolgt, ohne dass ein eingeschaltetes Unternehmen als „Verantwortlicher“ tätig wird. Die Senatsverwaltung hat, obwohl auf die Rechtswidrigkeit hingewiesen und wiederholt zum Ergreifen „unverzüglicher Maßnahmen“ von der BlnBDI gedrängt, keine Änderung vorgenommen.[68]

In Presseberichten bekräftigte die Dienststelle der BlnBDI Maja Smolczyk, die nach deren Ausscheiden inzwischen kommissarisch von Volker Brozio geleitet wird, ihre Kritik an der Impfterminverwaltung durch die Berliner Senatsverwaltung. Dabei wurde bekannt, dass sich auf die Vermittlung von

[64] Der Nutzungsvertrag (Rahmenvertrag) vom 04.12.2020 mit einem Auftragsverarbeitung Vertrag (AV-Vertrag) als Anlage 1 und 2 Anlagen hierzu (1 Angaben zur Verarbeitung personenbezogener Daten, 2 Technische und organisatorische Maßnahmen), einer Anlage 2 (Service- und Preisliste), einer Anlage 3 (Allgemeine Nutzungsbedingungen – ANB) und einer Anlage 4 (Begriffsbestimmungen), liegt dem Autor vor.
[65] Vertragsnachtrag vom 29.12.2020, liegt dem Autor vor.
[66] § 1 Vertragsnachtrag Nr. 1: Nachweis der Identität und der Impfberechtigung, Führen einer Patientenkarte, Angaben zu Einschränkungen von Impflingen.
[67] Risiken und Nebenwirkungen von Termin-Management-Systemen, www.zm-online.de 16.10.2021.
[68] BlnBDI, JB 2021 (Fn. 4), Kap. 1.3.1 (S. 30 ff.).

Impfterminen fünf interessierte Unternehmen beworben hatten. Den Zuschlag erhielt Doctolib als das „**wirtschaftlichste Angebot**“. Gemäß der Unternehmenssprecherin hat Doctolib seine Impfterminvermittlung „kostenlos“ angeboten: „Es entstehen für die Berliner Zentren und für die Patientinnen und Patienten keine Kosten, lediglich die Kosten von 0,16 Cent für die Erinnerungs-SMS werden dem Senat weiterberechnet.“ Überschlägig verursachte dies nach Presseberechnungen Gesamtkosten für die Senatsverwaltung Berlin bis Ende 2020 in Höhe von ca. 10.000 €.[69]

Der BlnBDI teilte mit, dass Konten erst nach drei Jahren oder auf Antrag der Kontoinhaber gelöscht werden. Er habe Beschwerden erhalten, dass Kunden von Doctolib bei Öffnung ihres Nutzerkontos Zugriff auf personenbezogene, teils sensitive Daten anderer Nutzender hatten. Es sei insofern von einer hohen Dunkelziffer auszugehen. Eine Auskunft, wie viele Nutzerkonten bei Doctolib allein zur Buchung von Terminen für die Corona-Schutzimpfung in Berlin eröffnet wurden, sei unbeantwortet geblieben. Die Gesundheitsverwaltung nannte eine Gesamtzahl von 2,05 Mio. vermittelten Menschen. Hierzu erklärte Volker Brozio: „Doctolib hat den Umstand, dass es als Dienstleister beauftragt wurde, dafür genutzt, eine rechtliche Kundenbindung herzustellen. Das wiederum hätte die Senatsverwaltung verhindern müssen. Wir haben sie mehrmals darauf hingewiesen.“ Vor Beginn der Impfkampagne sei von der BlnBDI erstmals Kontakt in der Sache aufgenommen worden. Die Verwaltung erklärte hierzu, bei der Abstimmung sei die Datenschutzbeauftragte beteiligt gewesen. Nach Darstellung der BlnBDI hat es eine aus **Telefon-, Videokonferenzen sowie mehreren Schreiben** bestehende Korrespondenz gegeben, in deren Verlauf sich die Datenschutzbehörde auf der einen und Gesundheitsverwaltung sowie Doctolib auf der anderen Seite nicht nähergekommen seien. Die im August ergangene Aufforderung, den auf fünf Seiten ausführlich beschriebenen „Datenschutzverstoß“ zu reparieren, sei folgenlos geblieben: „Es wäre die Aufgabe des Auftraggebers – sprich der Gesundheitsverwaltung – gewesen, klare Regeln für die Auftragsverarbeitung zu formulieren. Und es wäre vergleichsweise einfach möglich gewesen, die Terminbuchung mit Kundenkonten in einer neuen Datenbank aufzusetzen. Beides ist leider nicht geschehen“.[70]

Trotz der Datenschutzkritik von Nichtregierungsorganisationen und des BlnBDI teilte die Berliner Senatsverwaltung mit, dass sie den Sommer 2022 auslaufenden Vertrag mit Doctolib ohne wesentliche Änderungen zu **verlängern** beabsichtigt.[71]

Aus dem Vorgehen der Berliner Senatsverwaltung lässt sich hinsichtlich der **Motivation** schließen, dass ihr Kostenersparnis vor Datenschutz ging bzw. weiterhin geht. Für Doctolib ist die Durchführung der Impfkampagne wirtschaftlich interessant, weil sie dadurch neue Kunden gewinnen konnte und kann und die Impfkampagne als Referenz zur eigenen Werbung nutzt.

---

[69] Hoffmann, Berlins offizieller Impftermin-Dienstleister – Warum stellt die Firma Doctolib dem Senat nur ein paar Tausend Euro in Rechnung? www.tagesspiegel.de 28.12.2020.

[70] Kiesel, Profiteur der Berliner Impfkampagne?: Schwere Vorwürfe gegen die Datenkrake Doctolib, www.tagesspiegel.de 22.06.2022; Kritik an Impfterminvergabe über Doctolib, www.morgenpost.de 23.06.2022; Kritik an Impfterminvergabe über Doctolib, https://www.zeit.de/news/2022-06/23/kritik-an-impfterminvergabe-ueber-docotlib u. https://www.t-online.de/region/berlin/id_100021748/kritik-an-impfterminvergabe-ueber-doctolib.html.

[71] Kiesel, Trotz heftiger Datenschutz-Kritik: Berlin plant neuen Auftrag für Doctolib, 01.07.2022, https://plus.tagesspiegel.de/berlin/trotz-heftiger-datenschutz-kritik-berlin-plant-neuen-auftrag-fur-doctolib-525780.html.

8 Wettbewerbsrecht

Bisher gibt es keine Regelungen im Datenschutzrecht, die es verbieten, eine falsche Vorstellung bei den Kunden hinsichtlich der Umsetzung des Datenschutzes in einem Unternehmen zu vermitteln. Wohl aber kann in solchen Darstellungen eine Verletzung des Wettbewerbsrechts liegen. § 3 UWG verbietet **unlautere geschäftliche Handlungen**. Handlungen sind unlauter, wenn sie entgegen der unternehmerischen Sorgfalt geeignet sind, das wirtschaftliche Verbraucherverhalten wesentlich zu beeinflussen. Im Anhang zu § 3 Abs. 3 UWG werden geschäftliche Handlungen aufgeführt, die stets unzulässig sind.

8.1 „Zusammenarbeit mit der Datenschutzbehörde“

Nach Nr. 4 des Anhangs zu § 3 Abs. 3 UWG ist unlauter: „die unwahre Angabe, ein Unternehmer, eine von ihm vorgenommene geschäftliche Handlung oder eine Ware oder Dienstleistung sei von einer öffentlichen oder privaten Stelle bestätigt, gebilligt oder genehmigt worden, oder die unwahre Angabe, den Bedingungen für die **Bestätigung, Billigung oder Genehmigung** werde entsprochen“.

In seiner Datenschutzerklärung behauptet das Unternehmen eingangs: „Doctolib arbeitet mit den europäischen und **nationalen Datenschutzbehörden** sowie den öffentlichen Beteiligten des Gesundheitswesens zusammen, um datenschutzrechtliche Vorgaben einzuhalten und seine Datenschutzprozesse stetig zu verbessern.“[72] Durch diese Äußerung wird Endkunden wie auch Gesundheitseinrichtungen der Eindruck vermittelt, die Datenverarbeitung von Doctolib werde nicht nur von Datenschutzbehörden begleitet, sondern auch gebilligt bzw. im Fall einer aufsichtsbehördlichen Kritik korrigiert. Mit diesem Eindruck soll das Vertrauen in eine datenschutzkonforme Verarbeitung erhöht und damit eine Entscheidung für eine Geschäftsbeziehung mit Doctolib gefördert werden.

Die Behauptung des Unternehmens war tatsächlich von Anfang an und ist weiterhin unzutreffend. Die einzige für Doctolib in Deutschland zuständige Aufsichtsbehörde, die bzw. der BlnBDI, stellte am 22.06.2022 fest, dass trotz der Feststellung von **Datenschutzverstößen** im Rahmen der Impfkampagne seit Anfang 2021 diese von Doctolib **nicht abgestellt** worden sind. Selbst umfangreiche Aufforderungen im August 2021 blieben folgenlos.[73]

Im Hinblick auf die **Terminverwaltung in Arztpraxen** hat die BlnBDI 2019 festgestellt, dass eine Datennutzung von Patientendaten durch Doctolib für Zwecke der Terminerinnerung ohne eine vorherige Terminbuchung bei Doctolib und ohne Einholung einer Einwilligung hierzu unzulässig ist. Im Frühjahr 2022 veröffentlichten Jahresbericht der BlnBDI für das Jahr 2021 beschreibt diese, dass dieser Rechtsverstoß immer noch nicht abgestellt war.

Die Behauptung einer den Datenschutz verbessernden Zusammenarbeit mit der BlnBDI als einzige zuständige Aufsichtsbehörde ist unzutreffend und eine **unlautere Wettbewerbshandlung**. Sie stellt einen Verstoß gegen § 3 UWG dar.

[72] https://info.doctolib.de/datenschutzerklaerung/.
[73] Kiesel, Profiteur der Berliner Impfkampagne?: Schwere Vorwürfe gegen die Datenkrake Doctolib, www.tagesspiegel.de 22.06.2022.

8.2 Werbung mit Zertifikaten

Nach Nr. 2 des Anhangs zu § 3 UWG ist folgende geschäftliche Handlung als irreführend gegenüber Verbrauchern stets unzulässig: die „unerlaubte Verwendung von Gütezeichen und Ähnlichem“ in Form einer „**Verwendung von Gütezeichen**, Qualitätskennzeichen oder Ähnlichem ohne die erforderliche Genehmigung“.

Auf seiner **Webseite** erklärt Doctolib folgende Zertifikate vorweisen zu können:

- ISO/IEC 27001 Zertifizierung der BSI Gruppe
- HDS Zertifizierung (“Health Data Storage”) der BSI Gruppe
- TÜV Saarland (ohne Datumsangabe): geprüfter Datenschutz
- TÜVIT (Stand 2022): Videosprechstunde
- TÜVIT (Stand 2022): Datenschutz

Unterschrieben wird die Darstellung der Zertifikate mit folgendem Text: „Die Zertifizierungen beweisen, dass wir die richtigen Prozesse (basierend auf Risikomanagement) und die besten Verfahren eingeführt haben. Sie beweisen auch unser langfristiges Engagement für den Datenschutz, denn die Zertifizierungen umfassen jährliche Audits und müssen alle drei Jahre erneuert werden.“[74]

In der Datenschutzerklärung von Doctolib heißt es: „Personenbezogene Daten (einschließlich Gesundheitsdaten) von Patient:innen werden von einem Hoster mit physischer Infrastruktur und Managed Services Provider gehostet, der nach europäischen Datenschutzstandards zertifiziert ist.“[75] Mit der werbenden Aussage vermittelt Doctolib den nicht zutreffenden Eindruck, dass das Unternehmen beim Hosting ein **Zertifikat gemäß der europäischen DSGVO** vorweisen könne. Gemäß Art. 42 DSGVO kann nach einem gesetzlich geregelten Verfahren die datenschutzrechtliche Vereinbarkeit nach europäischen Standards nachgewiesen werden. Tatsächlich bezieht sich die Aussage von Doctolib auf eine Zertifizierung der Cloud-Datenverarbeitung bei Amazon Web Services (AWS) nach französischem Recht, ein HDS-Zertifikat (Health Data Services, Health Data Storage). Eine gegenseitige Anerkennung solcher Zertifikate ist in der EU nicht vorgesehen. Inwieweit die Fakten eine DSGVO-Konformität darstellen, die nach deutschem Recht relevant ist, kann nicht beurteilt werden, weil diese Fakten nicht offengelegt werden.[76] Hierin ist ein Verstoß gegen § 3 UWG zu sehen.

Bei den Zertifizierungen der „**BSI-Gruppe**“ handelt es sich nicht um solche des „Bundesamts für die Sicherheit in der Informationstechnik“. Das Kürzel BSI wird in einschlägigen Kreisen in Deutschland für dieses Bundesamt verwendet, das Zertifizierungen zur Datensicherheit anbietet. Die Aussage von Doctolib verweist vielmehr auf eine „British Standards Institution“. Auch bei diesem von Doctolib aufgeführten Zertifikat handelt es sich um ein französisches Zertifikat, das nicht den Datenschutz zum Thema hat, sondern sich allenfalls als Ergänzung hierzu versteht.[77]

Zum Zertifikat des **TÜV Saarland** TK44448, das bis zum 30.11.2022 gültig sein soll, findet sich kein veröffentlichtes Gutachten, das eine Prüfung der Seriosität des Zertifikats erlauben würde.[78]

[74] https://about.doctolib.de/privatsphaere/dna.html.
[75] https://info.doctolib.de/datenschutzerklaerung/; ähnlich Nr. 8 Datenschutzgrundsätze.
[76] So schon Netzwerk Datenschutzexpertise, 08.06.2021 (Fn. 2), Kap. 14.1 (S. 32 ff.).
[77] https://www.bsigroup.com/globalassets/localfiles/fr-fr/hds/ressources/hdh-hds-certification.pdf.
[78] https://www.tuev-saar.de/zertifikat/tk44448/.

Das bis 29.03.2023 gültige Zertifikat des **TÜVIT** 5604.22 wird, anders als das Zertifikat TÜVIT 5704.22, das mit „Videosprechstunde“ beschrieben wird, beworben mit der Bezeichnung „Datenschutz“. Tatsächlich beschränkt es sich aber ausschließlich auf die Doctolib Videosprechstunde.[79] Damit wird fälschlich der Eindruck erweckt, dass das Zertifikat umfassend den Datenschutz bewerten würde. Außerdem enthält das Zertifikat folgende Aussage: „Die Information der Datenschutzaufsichtsbehörde NRW gemäß Art. 43 Abs. 5 DS-GVO ist erfolgt am: 11.03.2022.“ Dadurch wird der nichtzutreffende Eindruck erweckt, dass es sich hierbei um eine Zertifizierung nach Art. 42 DSGVO handeln würde. Auch zu diesem Zertifikat ist kein Auditbericht öffentlich verfügbar. In diesen unzutreffenden Angaben liegt ein weiterer Verstoß gegen § 3 UWG.

Eine frühere Zertifizierung durch **datenschutz cert GmbH** wird nicht mehr von Doctolib aufgeführt.[80] Das Netzwerk Datenschutzexpertise hatte sich an die datenschutz cert GmbH gewendet und von dort die Information erhalten, dass ausschließlich die Videoverbindung peer-to-peer, nicht aber die Terminverwaltung oder sonstige Funktionen geprüft wurden. Ein solcher umfassender Eindruck war bis 2021 fälschlich vermittelt worden.

8.3 Medizinrechtliche Werbebeschränkungen

Mit seinen Werbekampagnen (s.o. 2 am Ende) unterläuft Doctolib zugleich für Ärzte geltende Werbebeschränkungen.[81] Gemäß § 27 Abs. 3 S. 3 MBOÄ ist anpreisende Werbung im **Zusammenhang mit ärztlicher Tätigkeit** unzulässig. Bei einer Arztsuche über Doctolib werden nur solche Gesundheitsfachkräfte angezeigt, die Kunden bei Doctolib sind.

9 Ergebnis

Mehr als ein Jahr nach der Verleihung des BigBrotherAwards 2021 an Doctolib erweist sich das Angebot von Doctolib aus Datenschutzsicht weiterhin als mangelhaft. Das Unternehmen reagierte teilweise auf Mängelfeststellungen, insbesondere im technischen Bereich, nachdem diese eine umfangreiche Medienresonanz gefunden hatten. Die **systematischen materiell-rechtlichen Verstöße** gegen den Datenschutz bestehen weiterhin.

9.1 Rechtswidriges Angebot

Das Unternehmen wirbt aggressiv für seine Terminvermittlung und -verwaltung in der Öffentlichkeit, gegenüber der Ärzteschaft und sonstigen Gesundheitsfachkräften. Dabei nutzt es beschönigende sowie nach Wettbewerbsrecht unzulässige **Falschdarstellungen** zum Thema Datenschutz.

Für das Unternehmen war und ist es ein Coup, die Online-Terminverwaltung für die **Corona-Impfungen** durch die Berliner Senatsverwaltung für Gesundheit vornehmen zu können. Hierbei wird gegen Datenschutzregelungen verstoßen. Wegen des günstigen Preises und der Entledigung von einer technisch anspruchsvollen Aufgabe scheint es für die Senatsverwaltung keine Rolle zu spielen, dass der Datenschutz missachtet wird. Sie macht sich damit zum Komplizen von Doctolib. Ohne erkennbare Not hat die Verwaltung nicht nur die Terminverwaltung, sondern auch die Impfdokumentation dem Unternehmen übertragen. Doctolib kann sich so in der Öffentlichkeit als datenschutzkonformer

79 https://media.doctolib.com/image/upload/v1649341216/tuv%20certifications/doctolib_tuevit_dataprivacy.pdf.
80 Dazu Gutachten Netzwerk Datenschutzexpertise (Fn. 2), Kap. 15 (S. 34 f.).
81 https://mobile.twitter.com/Doctolib_DE/status/1533697698355990528.

Dienstleister für die öffentliche Hand präsentieren. Es ist nicht auszuschließen, dass auch wegen diesem Umstand sich die Berliner Datenschutzaufsichtsbehörde bisher gehindert sah, gegen Doctolib angemessene Sanktionen zu verhängen.

Das Angebot von Doctolib verstößt **materiell-rechtlich** gegen den Datenschutz und gegen das Patientengeheimnis. Weit über die Erforderlichkeit hinaus werden Daten erhoben und gespeichert. Als „Auftragsverarbeiter" beschafft sich das Unternehmen Daten, die es als Verantwortlicher für eigene Zwecke weiternutzt.

Das Doctolib-Angebot zeichnet sich durch **Intransparenz** aus. Hinter einer bunten Fassade ist es für die Stellen, die Doctolib als Dienstleister nutzen, unklar, wie konkret deren Daten verarbeitet werden. Dies hindert die Gesundheitseinrichtungen daran, ihre datenschutzrechtliche, medizinische und strafrechtliche Verantwortung wirksam wahrzunehmen. Doctolib wälzt so die Verantwortung für Verstöße auf seine Kunden ab. Intransparenz besteht auch gegenüber den PatientInnen, für die die verschachtelte Konstruktion von Verantwortlichem und Auftragsverarbeiter noch weniger durchschaubar ist als für die Gesundheitseinrichtungen. Die Betroffenen laufen so Gefahr, dass ihr Gesundheitsdatenschutz und die medizinische Vertraulichkeit auf der Strecke bleiben.

9.2 Was ist zu tun?

Wegen ihres datenschutzwidrigen Angebots im Bereich der Terminverwaltung für Gesundheitseinrichtungen kann und sollte die zuständige Datenschutzaufsicht, der **Berliner Beauftragte für Datenschutz und Informationsfreiheit**, sanktionierend tätig werden. Der Umstand, dass Doctolib von der Berliner Gesundheitsverwaltung „gedeckt" wird, sollte kein Hindernisgrund sein. Angesichts der Hartnäckigkeit der Rechtsverletzungen ist es angebracht, neben einem Bußgeld (Art. 83 DSGVO) eine Beschränkung bzw. ein Verbot der Verarbeitung nach Art. 58 Abs. 2 lit. f DSGVO zu verhängen. Um ein entsprechendes Verbot zur unmittelbaren Wirkung zu bringen, sollte eine zeitnahe Vollziehbarkeit des Verbots angeordnet werden.

Angesichts der Rechtswidrigkeit ihres Vorgehens hat die **Berliner Gesundheitsverwaltung** die Beauftragung von Doctolib im Bereich der Corona-Impfversorgung zu beenden.

Gefordert ist auch die (Zahn-)Ärzteschaft. Die Ärzte verstoßen mit der Beauftragung von Doctolib gegen ihre berufsbedingte Vertraulichkeitsverpflichtung. Damit wird, dem Wortlaut des Gesetzes gemäß, der Straftatbestand des § 203 StGB erfüllt. Es wäre jedoch unangemessen, die Ärzte, die auf die Beteuerung der Rechtskonformität von Doctolib vertrauen, direkt zu sanktionieren. Um dieses unberechtigte Vertrauen zu beseitigen, sollten die **(Zahn-)Ärztekammern** ihre Mitglieder über deren rechtliche Bewertung informieren. Zudem stehen den Kammern weitergehende Sanktionsmöglichkeiten gegenüber ihren Mitgliedern zur Verfügung.

Sollte von Seiten der offiziell zuständigen Stellen kein wirksames Vorgehen erfolgen, so besteht für die **Wettbewerber** von Doctolib (§ 8 UWG) sowie für **Verbraucherverbände** nach § 2 UKlaG die Möglichkeit, wegen der Verletzung des Lauterkeitsrechts und des Datenschutzrechts Abmahnungen auszusprechen und gerichtlich eine Unterlassungsklage gegen Doctolib anzustrengen.

Abkürzungen

a.A.	andere Ansicht
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
Aufl.	Auflage
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BlnBDI	Der/die Berliner Beauftragte für Datenschutz und Informationsfreiheit
BT-Drs.	Bundestags-Drucksache
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift
CR	Computer und Recht (Zeitschrift)
DANA	DatenschutzNachrichten
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f/f.	fort/folgende
i.d.R.	in der Regel
i.S.d./v.	im Sinne des/von
IT	Informationstechnik
JB	Jahresbericht
JR	Juristische Rundschau
Kap.	Kapitel
K&R	Kommunikation und Recht (Zeitschrift)
KriPoZ	Kriminalpolitische Zeitschrift
lit.	Buchstabe
MBOÄ	Musterberufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte
MDR	Monatsschrift des deutschen Rechts
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
RDV	Recht der Datenverarbeitung (Zeitschrift)
RKI	Robert-Koch-Institut
Rn.	Randnummer
S.	Satz oder Seite
s.o.	siehe oben
StGB	Strafgesetzbuch
s.u.	siehe unten
u.	und
UAbs.	Unterabsatz
UKlaG	Unterlassungsklagegesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz