Kurzbegründung Kategorie Gesundheit, Laudator Dr. Thilo Weichert

Den BigBrotherAward 2021 in der Kategorie Gesundheit erhält die Firma Doctolib GmbH, Berlin. Doctolib bietet insbesondere die Vermittlung von Arztterminen über ihre Plattform an. Diese Daten werden unter Missachtung der Vertraulichkeitsverpflichtung verarbeitet und laut Datenschutzvereinbarung auch im Rahmen kommerzieller Marketingzwecke genutzt.

BigBrotherAward 2021 - Kategorie Gesundheit – Laudator Dr. Thilo Weichert

Der BigBrotherAward in der Kategorie „Gesundheit“ geht an

die Firma Doctolib in Berlin für ihr Terminvermittlungsportal für Ärzte.

Doctolib verarbeitet mit diesem Portal unter Missachtung der ärztlichen Vertraulichkeit die Daten von zigtausenden Patient.innen.

Das Angebot für Gesundheitsfachkräfte, also vor allem für Ärzte, und deren Patienten, ist genial: Die Ärzte schließen einen Vertrag mit Doctolib ab, erteilen Zugriff auf ihre Patientendaten und können dann über eine Internetseite Behandlungs-, Beratungs- oder Impftermine verbindlich verabreden lassen. Und schon können die Patient.innen online Termine buchen. Kein Warten in einer Telefonwarteschleife, keine gestressten Mitarbeiter.innen, selbst das Erinnern der Patient.innen an den Termin übernimmt Doctolib – und für das alles zahlen die Praxen nur etwas mehr als 100 € im Monat. Für die Patient.innen ist alles unentgeltlich. Und nicht nur das. Doctolib verspricht:

„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.“

Na, dann ist ja alles in Butter. Auf dem Bildschirm.

Funktionsweise

In der Realität sollten Ärzt.innen schnell stutzig werden, denn wenn ein Arzt Doctolib für seine Praxis in Anspruch nehmen will, erscheint ein Mitarbeiter des Unternehmens und bittet zunächst einmal um Zugriff auf den gesamten im Arztinformationssystem gespeicherten Patientenstammdatensatz.

Und damit nicht genug: Nach dem Import der Patientenliste ist ein regelmäßiger Datenabgleich der Termintabelle des Arztsystems mit dem Vermittlungssystem von Doctolib nötig.

Da stellen sich unsere Stacheln auf. Trotzdem beteiligen sich Praxen an diesem Dienst. Wir vermuten: Die meisten Ärzt.innen verstehen von den technischen Vorgängen wenig und vertrauen auf die Expertise von Doctolib sowie das Versprechen, Patientengeheimnis und Datenschutz zu beachten.

Als Zusatzangebot für die Patient.innen bietet Doctolib zur Orientierung eine bundesweite Ärzteliste sowie zur Telekonsultation einen Videodienst an. Und seit Beginn der Corona-Pandemie vermittelt Doctolib auch Impftermine, für das französische Gesundheitsministerium ebenso wie für die Gesundheitsverwaltung in Berlin.

Und tatsächlich funktioniert dann auch alles. Doctolib rühmt sich einer Kundenzufriedenheit von 97%. Nach eigenen Angaben nutzen 150.000 Ärzte und Gesundheitsfachkräfte in Deutschland und Frankreich und 50 Millionen Patient.innen den Dienst. Dass dies alles in Ordnung geht, dafür sollen gleich drei unterschiedliche Gütesiegel bürgen.

Intransparenz

Ein qualifizierter Blick ins Kleingedruckte aber belehrt ein geschultes Auge eines Schlechteren: Verwirrend ist zunächst die Vielzahl der Dokumente: Während es bei anderen Diensten einmal Allgemeine Geschäftsbedingungen (AGB) gibt, gibt es hiervon bei Doctolib ein Dutzend: Nutzungsbedingungen, Datenschutzhinweise, Grundsätze zum Schutz von Gesundheitsdaten (jeweils unterschieden nach Patient.innen und den sog. Gesundheitsfachkräften), zusätzlich eine Cookie-Richtlinie, eine Verarbeitungsliste, Hinweise zu Datenschutz und Sicherheit, FAQs, einen Auftragsverarbeitungsvertrag und Begriffsbestimmungen. Das ist für einen einheitlichen Dienst zu viel. Die Dokumente sind verwirrend und unklar, teilweise widersprüchlich. Die meisten sind nicht durchnummeriert, was eine Berufung darauf zusätzlich erschwert.

Der Teufel steckt im Detail: Doctolib trennt formaljuristisch zwischen einer Auftragsverarbeitung für die Gesundheitsfachkraft und einer eigenen Doctolib-Verantwortung für sein eigenes Webangebot. Soweit so gut und richtig. Doch dann maßt sich Doctolib an, die im Auftrag des Arztes verarbeiteten Daten in den eigenen Datenbanken zur Terminvergabe zusammenzuführen. Für Ärzt.innen wie Patient.innen und auch für uns bleibt unklar, wie die Daten dann weitergenutzt werden.

Besonders sensible Gesundheitsdaten

Es sollte unstreitig sein, dass ärztliche Terminvereinbarungen ebenso wie die

Metadaten von Videosprechstunden sensitive Gesundheitsdaten sind, die unter dem besonderen Schutz der Datenschutzgrundverordnung stehen, und die zudem der beruflichen Schweigepflicht unterliegen. Das Vertrauen des Patienten gegenüber dem Arzt verbietet es, dass Namen, Termine, Behandlungen in die Hände Dritter gelangen und für andere als Behandlungs- und Beratungszwecke in der Praxis des Vertrauens genutzt werden. Juristisch dürfen Ärzte dafür Auftragsverarbeitungsverträge abschließen, ohne dass ihre Patient.innen zustimmen müssen. Aber dieses Vertrauensverhältnis wird spätestens dann in strafbarer Weise verletzt, wenn sich Doctolib aus dem Arztsystem Daten von Patient.innen beschafft, die keine Termine vereinbaren und nicht einmal ein Konto bei Doctolib haben, und wenn die Betroffenen über diese Datenweitergabe nicht informiert werden.

Werbung, Tracking, Analysen – wer ist verantwortlich?

So vollmundig sich Doctolib zum Datenschutz und zum Patientengeheimnis bekennt, so sehr müssen wir diese Versprechen nach Lektüre des Kleingedruckten in Frage stellen:

In der Cookie-Liste von Doctolib taucht z.B. Google auf mit Analytics und Adwords bzw. Ads. Als Zwecke werden das „Verfolgen“ oder „Nachverfolgen“ der Webseitennutzung angegeben. Ads dient für nichts Banaleres als Werbung. Stimmt man den Datennutzungen für Werbung und Meinungsumfragen einmal zu, dann hat dies bei allen weiteren Terminvereinbarungen offenbar zur Folge, dass die Daten z. B. auch zu Google gelangen. Das gleiche Problem stellt sich bei der Einbindung von sozialen Netzwerken wie Twitter, Instagram, Facebook, LinkedIn, Medium und YouTube schon auf der Startseite von Doctolib. Wofür das alles gut sein soll, weshalb zum Beispiel eine Terminvergabe-Seite einen YouTube-Button braucht, muss Doctolib sich ernsthaft fragen lassen. Bei den dortigen Cookieeinstellungen wird jeweils „alle akzeptieren“ angeboten. Und Doctolib erklärt dann unschuldig, dass es für die Verarbeitung von Daten bei diesen Diensten nicht verantwortlich sei.

Hier irrt Doctolib: In jüngster Zeit hat der Europäische Gerichtshof gleich in drei völlig unabhängigen Verfahren festgestellt, dass bei einer solchen Datenverarbeitung eine Mitverantwortlichkeit des Seitenanbieters, also hier von Doctolib, besteht. Wir meinen: Kommerzielle Social Media-Firmen haben in der Arzt-Patientenbeziehung nichts zu suchen, schon gar nicht, wenn diese ihren Sitz in einem unsicheren Drittstaat wie den USA haben.

Schweigepflicht

In Doctolibs „AGB Nutzer“ von 2019 kann der Patient lesen, dass er seine Ärzte mit seiner Zustimmung von der gesetzlichen Schweigepflicht entbindet. Wofür und weshalb, wird dem Patienten und wurde auch uns auf Anfrage nicht erklärt. Es sollte klar sein, dass eine solche Entbindung im Kleingedruckten unwirksam

ist.

Tatsächlich beginnt die Verletzung der Schweigepflicht früher und hat eine gewaltige Dimension: Einem Arzt ist es zwar nach einer neuen gesetzlichen Regelung aus dem Jahr 2017 explizit erlaubt, technische Dienstleister wie Doctolib in Anspruch zu nehmen. Voraussetzung ist aber, dass die hierfür offenbarten Patientengeheimnisse für den Dienst erforderlich sind. Definitiv nicht erforderlich ist der gesamte Import der Patientenliste eines Arztes durch Doctolib. Dem Unternehmen würde es für seine Terminvermittlung genügen, vom Arzt die freien Termine zu erfahren, um dann diese gegenüber dem Arztsystem zu vermitteln.

Mandantentrennung

Als Mitwirkender eines Arztes und als dessen Auftragsverarbeiter ist Doctolib verpflichtet, die sog. Mandantentrennung einzuhalten. Das heißt, Doctolib darf die Patientendaten von verschiedenen Ärzten bei sich nicht zusammenführen. Doch das genau scheint das Unternehmen zu tun. Auf dem Chaos Computer Congress 2020 wurde berichtet[1], dass dem Chaos Computer Club eine Doctolib-Datenbank zugespielt worden sei. Über die beschriebene Lücke sei der Zugriff auf ca. 150 Millionen Terminvereinbarungen möglich gewesen, die wohl auf eine Synchronisierung mit den Terminkalendern der Arztpraxen zurückzuführen waren und die bis ins Jahr 1990 zurückreichten.[2] Wie die Daten verarbeitet wurden und werden, was Doctolib mit dieser Sammlung tut und weshalb alte Daten nicht gelöscht wurden, bleibt das Geschäftsgeheimnis unseres Preisträgers.

Die angeblich verliehenen Gütesiegel haben entgegen der Firmenbehauptung keine Grundlage in der DSGVO. Was hier gesiegelt wurde und weshalb, bleibt weitgehend das Geheimnis von Doctolib. Bekannt ist u.a., dass Doctolib ein in Frankreich zertifiziertes Cloudangebot von Amazon Web Services – mit Rechnern in Europa – nutzt.[3]

Was tut Doctolib wirklich?

[1] Video-Mitschnitt der CCC-Veranstaltung: https://media.ccc.de/v/rc3-11342-tut_mal_kurz_weh_neues_aus_der_gesundheits-it (der Bericht über die Doctolib-Daten beginnt bei 1:00:00)

[2] Wasner, Datenpanne bei Online-Terminbuchungsportal, 19./25.01.2021, https://www.medical-tribune.de/praxis-und-wirtschaft/praxismanagement/artikel/datenpanne-bei-online-terminbuchungsportal/; 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.

[3] Datenschutzhinweise für personenbezogene Daten – Gesundheitsfachkräfte https://info.doctolib.de/datenschutzerklaerung/.

Unsere Nachfragen beim Unternehmen wegen des millionenfachen Herunterladens von Patientendaten, zur Mandantentrennung und vieles mehr, blieben unbeantwortet.

Uns bleiben insofern nur Spekulationen, was auf den Servern von Doctolib und AWS passiert.

Spekulieren tun übrigens auch Wagniskapitalgeber, die dem 2013 gegründeten Unternehmen 2016 23 Mio. €, 2017 weitere 35 Mio. € und 2019 nochmals 150 Mio. € bereitstellten. Doctolib zählt inzwischen zu den sog. Unicorns, also den Firmen, die auf dem Kapitalmarkt mit mehr als einer Milliarde € bewertet werden.[4]

Der Markt der Gesundheitsdaten ist, nachdem der globale und auch der europäische Markt von Internetnutzungsdaten zwischen Facebook und Google aufgeteilt ist, ein neues Spielfeld für IT-Konzerne und Spekulanten. Bisher ist es halbwegs gelungen, hier in Europa US-Unternehmen draußen zu halten unter Verweis auf die ärztliche Vertraulichkeit. Doctolib arbeitet daran, sich einen großen Teil dieses Kuchens einzuverleiben mit dem vollmundigen Bekenntnis zu dieser Vertraulichkeit, ohne sich daran wirklich zu orientieren.

Die Digitalisierung unseres Gesundheitssystems ist wichtig, um die Gesundheitsversorgung der Bevölkerung zu verbessern und auf einem hohen Niveau zu halten. Dies darf aber nicht auf Kosten der Vertraulichkeit zwischen Patient.innen und Heilberufen passieren. Dafür, dass Doctolib diese Vertraulichkeit seinem Expansionsstreben unterordnet, dafür erhält das Unternehmen den BigBrotherAward 2021 in der Kategorie „Gesundheit“.

Herzlichen Glückwunsch, Doctolib.

[4] Haak, Doctolib wird zum Einhorn, 20.03.2019, https://www.businessinsider.de/gruenderszene/health/doctolib-einhorn/.