KURZGUTACHTEN

ZUM ZERTIFIKAT

TRUSTED SITE DATA PRIVACY

Vorgangsnummer:	5604.22
Prüfgegenstand:	Doctolib Videosprechstunde
Betreiber:	Doctolib GmbH Mehringdamm 51 10961 Berlin
Prüfinstitution:	TÜV Informationstechnik GmbH TÜV NORD GROUP Am TÜV 1 45307 Essen
Prüfzeitraum:	20.09.2021 bis 23.03.2022
Version:	1.0
Verfasser:	Alexander Taubitz, Tobias Mielke
Erstellungsdatum:	23.03.2022

…….……..……

Tobias Mielke

Auditor Technik

…….……..……

Alexander P. Taubitz

Auditor Recht

Inhalt

1 Einleitung

Die Doctolib GmbH hat die TÜV Informationstechnik GmbH (TÜViT) mit einer Datenschutzzertifizierung nach Artikel 42, 43 DSGVO gemäß dem Trusted Site Data Privacy-Prüfverfahren (TSDP) für die „Doctolib Videosprechstunde“ beauftragt.

Ziel war die Erteilung eines Zertifikates, mit der Zertifizierungs-ID: 5604.22, mit der Berechtigung zur Verwendung eines Prüfzeichens TÜViT Trusted Site Data Privacy.

Die Doctolib GmbH bietet auf Basis einer Mobile App sowie eines Webmoduls für privat und gesetzlich Versicherte eine Konsultation per Video an. Im Rahmen dieser sog. Videosprechstunde kann von in Deutschland approbierten Ärzten gesundheitlicher Rat eingeholt werden.

2 Bezeichnung des Prüfgegenstandes

Bei dem zur Zertifizierung Prüfobjekt handelt es sich um die Doctolib Videosprechstunde mit folgenden Versionsnummern:

- Webanwendung Doctolib (v4628f32561751f5ec53b2985ea83c3ebe2810e32)
- Webanwendung Doctolib Pro (v4628f32561751f5ec53b2985ea83c3ebe2810e32)
- iOS Applikation Doctolib (v.3.4.6)
- Android Applikation Doctolib (v3.4.6)

Im Konkreten wird eine Zertifizierung einer Online-Videosprechstunde in Echtzeit im Rahmen einer synchronen Kommunikation zwischen einem Vertragsarzt und einem Patienten (Peer-to-Peer), ggf. unter Assistenz z.B. durch eine Bezugsperson des Assistenten, vorgenommen.

3 Beschreibung des Prüfgegenstandes

Videosprechstunden sind grundsätzlich definiert als synchrone Kommunikation zwischen einem Arzt und einem ihm bekannten Patienten, über die dem Patienten zur Verfügung stehende technische Ausstattung (Peer-to-Peer), ggf. unter Assistenz, z. B. durch eine Bezugsperson, im Sinne einer Online Videosprechstunde in Echtzeit, die der Arzt dem Patienten anbieten kann.

Gegenstand der Prüfung ist hierbei die telemedizinische Funktion der Doctolib Videosprechstunde (Durchführung von Online-Videosprechstunden). Hierbei erstreckt sich der Prüfbereich auf die Zertifizierung, die Durchführung der Videosprechstunde (ärztliche Konsultation) und die Beendigung dieser.

Zudem unterfallen nachfolgende Dienste nicht dem Zertifizierungsscope:

- Terminvereinbarungssystem von Doctolib

Die Wahrnehmung einer Videosprechstunde mit der Anwendung Doctolib kann in zwei Varianten erfolgen. Der Anwender kann sich entweder in der Doctolib Videosprechstunde registrieren oder Ärzte können Patienten zu einer Videosprechstunde einladen (Nutzung ohne Registrierung).

Sowohl die Durchführung mit als auch ohne Registrierung/ Accounterstellung (Nutzung mit Gast-Account) ist für App-Nutzer möglich und ist Gegenstand der Zertifizierung.

Aus dem Wortlaut des § 5 Abs. 1 Nr. 3 Anlage 31b des BMV-Ä *„Patienten und Pflegekräfte müssen den Videodienst nutzen können, ohne sich vorher registrieren zu müssen. […]"* ist zu entnehmen, dass die Vorhaltung eines accountfreien Anmeldeprozesseses das alternative Angebot der Nutzerkonto-Einrichtung als weiteren Anmeldeweg nicht ausschließt, sodass Gegenstand der Zertifizierung ebenso die accountbasierte Nutzung der Anwendung ist.

Gegenstand der Prüfung ist somit die Videosprechstunde Doctolib,

- Webanwendung Doctolib (v4628f32561751f5ec53b2985ea83c3ebe2810e32)
- Webanwendung Doctolib Pro (v4628f32561751f5ec53b2985ea83c3ebe2810e32)
- iOS Applikation Doctolib (v.3.4.6)
- Android Applikation Doctolib (v3.4.6)

sowie die dazugehörigen Schnittstellen zur Verarbeitung von personenbezogenen Daten im Rahmen einer Videosprechstunde.

Dazu gehören:

- Schnittstellen zum Streaming-Anbieter (Vonage Holdings Corp.)
- Schnittstellen zu den genutzten Servern (Amazon Web Services EMEA Sarl)
- Schnittstellen zu den genutzten SMS-Providern (Calade Technologies und Balthazar et compagnie)
- Schnittstellen zum Verschlüsselungs-Service (Tanker SAS)

Im Kontext dieser Videosprechstunde sind die folgenden Module maßgeblich zur Gewährleistung der Dienstleistungen:

- die App als Patientenoberfläche (im Browser sowie als Anwendung für iOS und Android)
- das Portal Doctolib Pro als Weboberfläche für Ärzte zur Durchführung der Videosprechstunde

Bei der Betrachtung des Produkts präsentieren sich grundsätzlich zwei verschiedene Komponenten:

1. Komponente: Anwendung mit Erstellung eines Doctolib Nutzeraccounts durch den Patienten
2. Komponente: Anwendung ohne Erstellung eines Nutzeraccounts durch den Patienten

Die Wahrnehmung einer Videosprechstunde mit der Anwendung Doctolib kann wie vorstehend ausgeführt auf zwei unterschiedliche Arten erfolgen.

4 Prüfzeitraum und Prüfgrundlage

Die Prüfung wurde im Zeitraum vom 20. September 2021 bis 23.03.2022 remote bei der TÜViT, Am TÜV 1 in 45307 Essen durchgeführt.

Die Prüfung wurde auf Grundlage des Kriterienkatalogs Trusted Site Data Privacy, Version 2.4 vom 15.12.2021[1] durchgeführt.

Die Prüfung der Videosprechstunde in der Anwendung Doctolib erfolgte zum einen auf Grundlage von Dokumenten, die den Gutachtern zur Verfügung gestellt worden sind und zum anderen auf Basis einer Sicherheitstechnischen Untersuchung (SU). Für die Sicherheitstechnische Untersuchung wurde die Anwendung Doctolib jeweils auf einem iOS sowie Android Endgerät (Smartphone) auf Schwachstellen untersucht.

Zudem wurde ein Remote-Audit durchgeführt. Hierbei wurde im Rahmen von Interviews das Datenschutzmanagement und die Sicherheit der Verarbeitung überprüft. Hierbei wurden die konkreten Systeme und Prozesse im Kontext des Prüfgegenstandes einbezogen. Inkludiert war auch die Demonstration der in Kontext des Prüfgegenstandes einbezogenen Systeme.

Dieses TSDP-Verfahren wird im Geltungsbereich der kassenärztlichen Videosprechstunde durchgeführt. Ergänzend zu diesem Verfahren gibt es ein korrespondierendes TSVC-Verfahren, indem die Informationssicherheit der Videosprechstundenlösung analysiert und bewertet wird.

5 Rechtliche Rahmenbedingungen

Es werden die bereichsspezifischen und einschlägigen Regelungen zum Datenschutz beschrieben, die ausschlaggebend für die Prüfung des Prüfgegenstands sind.

Folgende Gesetzgebung wird der Begutachtung zugrunde gelegt:

- **Datenschutz-Grundverordnung (DSGVO)**: VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

- **Bundesdatenschutzgesetz (BDSG):** Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist
- **Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)**: vom 23. Juni 2021 (BGBl. I S. 1982), das zuletzt durch Artikel 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544) geändert worden ist

6 Prüfergebnis

Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus der EU Verordnung 2016/679 (DS-GVO) und des Kriterienkatalogs Trusted Site Data Privacy, Version 2.4.

7 Referenziertes Dokument

[1] Trusted Site Data Privacy Kriterienkatalog für Prüfungen der Konformität einer IT-Lösung zur Europäischen Datenschutzgrundverordnung, Version 2.4 (15.12.2021)