



KURZGUTACHTEN ZUM ZERTIFIKAT TRUSTED SITE DATA PRIVACY

Vorgangsnummer: 5603.22

Prüfgegenstand: Doktor.de Videosprechstunde

Betreiber: Doktorde GmbH
Cicerostr. 2
10709 Berlin

Prüfinstitution: TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen

Prüfdatum: September 2021 bis März 2022

Version: 1.0

Erstellungsdatum: 14.03.2022

Verfasser: Stefanie Fischer, Tobias Mielke

.....
Tobias Mielke
Auditor Technik

.....
Stefanie Fischer
Auditorin Recht



Inhalt

1	EINLEITUNG	3
2	BEZEICHNUNG DES PRÜFGEGENSTANDES	3
3	BESCHREIBUNG DES PRÜFGEGENSTANDES	3
4	PRÜFZEITRAUM UND PRÜFGRUNDLAGE	5
5	RECHTLICHE RAHMENBEDINGUNGEN	5
6	PRÜFERGEBNIS	5
7	REFERENZIERTES DOKUMENT	6

1 Einleitung

Die Doktorde 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 „Doktor.de Videosprechstunde“ beauftragt.

Die Doktorde GmbH bietet auf Basis einer Mobile App 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 Prüfobjekt handelt es sich um die Doktor.de Videosprechstunde Versionsnummer: iOS 1.0.0 (44), Android 0.1.8 (10000) sowie Carealot.de 1.0. 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 sind hierbei die telemedizinische Funktion der Doktor.de Videosprechstunde (Durchführung von Online-Videosprechstunden). Hierbei erstreckt sich der Prüfbereich auf die Zertifizierung, die Durchführung der Videosprechstunde (ärztliche Konsultation) und die Beendigung dieser.

Nicht Teil des zu betrachtenden Zertifizierungssscopes ist die zertifizierte Praxissoftware RED medical sowie der Videosprechstundenlösung RED connect der Red Medical Systems GmbH.

Zudem sind nachfolgende Dienste nicht Gegenstand der Zertifizierung:

- Appsflyer zur Überwachung von Performance-Marketing-Kampagnen gegenüber App-Nutzern
- Braze zur Durchführung von Marketingkampagnen
- Google Firebase, um die App-Nutzung zu tracken
- Dienst Datadog zum Monitoring der Systeme

- Mitarbeiterportal Quinyx, welches für die Planung der Verfügbarkeiten der Ärzte genutzt werden kann
- Abrechnung der Videosprechstunde über die Ärztliche Verrechnungsstelle Büdingen GmbH

Die Nutzung der Anwendung Doktor.de Videosprechstunde kann in zwei Varianten erfolgen. Der Anwender kann sich entweder in der Doktor.de 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 Anmeldeprozesses das alternative Angebot der Nutzerkonto-Einrichtung als weiteren Anmeldeweg nicht ausschließt, so dass Gegenstand der Zertifizierung ebenso die accountbasierte Nutzung der Anwendung ist.

Gegenstand der Prüfung ist somit die Anwendung Doktor.de Videosprechstunde, Versionsnummer: iOS 1.0.0 (44), Android 0.1.8 (10000), Carealot.de 1.0, sowie die dazugehörigen Schnittstellen zur Verarbeitung von personenbezogenen Daten im Rahmen dieser Anwendung. Dazu gehören:

- Schnittstellen zum Streaming-Anbieter (Vonage Holdings Corp.)
- Schnittstellen zu den genutzten Servern (AWS)
- Schnittstellen zu verschiedenen Datenbanken

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

- die App als Patientenoberfläche
- Carealot als Weboberfläche für Ärzte zur Durchführung der Videosprechstunde
- Carealot als Weboberfläche für Administratoren/Backoffice zur Administration der Carelot Plattform, Einsichtnahme in Statistiken und Verwaltung von Bewertungen

Die Doktor.de Videosprechstunde bietet 2 Varianten bzgl. der Erstellung des Nutzeraccounts:

1. Erstellung eines Nutzeraccounts durch den App-Nutzer
2. Erstellung eines Nutzeraccounts durch den Doktorde-Nutzer

4 Prüfzeitraum und Prüfgrundlage

Die Prüfung wurde im Zeitraum vom September 2021 bis März 2022 remote mit 38 Personentagen bei der TÜV Informationstechnik GmbH, Am TÜV 1 in 45307 Essen durchgeführt.

Die Prüfung wurde auf Grundlage des Kriterienkatalogs Trusted Site Data Privacy, Version 2.0 vom 05.05.2021^[1] durchgeführt.

Die Prüfung der Doktor.de Videosprechstunde erfolgte zum einen auf Grundlage von Dokumenten, die den Gutachtern zur Verfügung gestellt worden sind und zum anderen auf Basis einer sicherheitstechnischen Untersuchung. Die Informationssicherheit der Doktor.de Videosprechstunde (iOS sowie Android App) wurde 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.

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 [1].

7 Referenziertes Dokument

- [1] Trusted Site Data Privacy Kriterienkatalog für Prüfungen der Konformität einer IT-Lösung zur Europäischen Datenschutzgrundverordnung, Version 2.0