ePrivacyseal

Z e r t i f i k a t

Nr. 291/20

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Deutschland

bestätigt* hiermit, dass

als Ergebnis der Zertifizierungsentscheidung am 6. August 2020

LifeTime GmbH
Felicitas-Kukuck-Straße 14, 22765 Hamburg, Deutschland

das Produkt oder die Dienstleistung
„LifeTime“
Version 08.04.2020
betreibt, wie in Anhang 1 definiert und unter Ausschluss der Verarbeitungstätigkeiten in Anhang 2 dieser Bescheinigung

in Übereinstimmung mit dem Kriterienkatalog der ePrivacyseal GmbH, Version 2.1. vom Mai 2018.

Letzter Audittag: 03.08.2020
Nächste geplante Überprüfung bis 01.07.2022
Gültigkeitsdauer: 02.07.2020 – 01.07.2022

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

Anhang 1 zum Zertifikat Nr. 291/20

Beschreibung der Verarbeitungstätigkeiten

Kunden der LifeTime sind Health Facilities, welche die LifeTime Desktop Applikation nutzen, um Daten mit Patienten oder anderen medizinischen Einrichtungen auszutauschen. Kunden der LifeTime können über die Website die Desktop Applikation bestellen und diese herunterladen. Der Patient nutzt hierfür die LifeTime App. Beim ersten Versand einer Health Facility an einen Patienten findet eine zwei Faktor Authentifizierung via SMS und Versichertennummer statt.

Nach erfolgter Authentifizierung können Patient und Health Facility Dokumente austauschen und Benachrichtigungen übermitteln. Der Arzt nutzt hierfür die LifeTime Desktop Anwendung. Der Patient nutzt die LifeTime App auf seinem Smartphone. Das besondere hierbei ist, dass Lifetime keinen Account für den Patienten anlegt. Es wird lediglich eine sogenannte Storage-ID generiert, zu der außer einem Verschlüsselungsschlüssel keine Daten gespeichert werden.

Diese ID ist eindeutig für die Kombination aus Handynummer und der Versichertenkarte. Schickt eine Health Facility ein Dokument an eine Mobilnummer, so erkennt LifeTime, dass diese Mobilnummer über eine eingerichtete LifeTime-App verfügt und verschlüsselte Dokumente empfangen kann. Die Versichertennummer bzw. TAN dient als zweiter Faktor, so dass bei Zahlendrehern bei der Nummerneingabe sichergestellt ist, dass nur die berechtigte Person die Daten auch lesen (d. h. entschlüsseln) kann.

Die Kommunikation zwischen Health Facilities erfolgt auf beiden Seiten über die Desktop Anwendung. Sowohl die App als auch die LifeTime Desktop Anwendung kommunizieren gesichert über das LifeTime Storage. LifeTime Web hält Kundendaten der angemeldeten Health Facilities, prüft den Login der Kunden und verwaltet die Berechtigung des Kunden entsprechend des von ihm gewählten Abos. LifeTime Web ist nicht Teil des Produkts „Lifetime“.

Datenverarbeitungen bei Nutzung der Desktop-App zur Überprüfung der Systemzuverlässigkeit sowie Mobile-App für die App-Absturzberichte sind entsprechend in die Begutachtung einbezogen.

Innerhalb der Begutachtung wurden drei verschiedene Anwendungsfälle berücksichtigt:

- Die Health Facility will dem Patienten Daten über die LifeTime Desktop Anwendung zusenden
- Der Patient möchte der Health Facility etwas zusenden
- Eine Health Facility möchte einer anderen Health Facility Daten zusenden

Anhang 2 zum Zertifikat Nr. 291/20

Ausgeschlossene Verarbeitungstätigkeiten

Die Bewertung bezieht sich auf das in Anhang 1 genannte Produkt und damit ausschließlich auf Prozesse, an denen LifeTime GmbH und ihre Kunden beteiligt sind.

Optional können Daten an Health Facilities, die noch keine LifeTime Kunden sind, per Fax versendet werden. Das Empfangen von Daten in einer Health Facility ist erst möglich, nachdem die Faxnummer von der Health Facility verifiziert wurde. Um Dokumente von Patienten empfangen zu können ist zusätzlich eine manuelle interne Überprüfung der Praxis und der angegebenen Faxnummer erforderlich. Der mögliche Faxversand ist für LifeTime-Kunden nicht notwendig und zählt nicht zum zu überprüfenden Produkt.