

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

**La-Well Systems GmbH**  
**Haßkampstraße 75**  
**32257 Bünde**

für den telemedizinischen Videokonferenzdienst

**eVi elektronische Visite**

die Erfüllung aller Anforderungen der Kriterien

**Trusted Site Privacy, Version 2.1**

der TÜV Informationstechnik GmbH. Die Prüfanforderungen sind in  
der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.



**Certificate ID: 5533.17**

© TÜVIT - TÜV NORD GROUP - [www.tuvit.de](http://www.tuvit.de)

Zertifikat gültig bis  
31.07.2019

Essen, 18.07.2017

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**  
TÜV NORD GROUP  
Langemarckstraße 20  
45141 Essen  
[www.tuvit.de](http://www.tuvit.de)

**Zertifikat**

## Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

## Prüfberichte

- „Trusted Site Privacy – Gutachten Technik – eVi – elektronische Visite v3.0“, Dokumentenversion 1.1 vom 17.07.2017, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige
- „Trusted Site Privacy – Gutachten Recht – eVi – elektronische Visite v3.0“, Dokumentenversion 1.2 vom 17.07.2017, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

## Prüfanforderungen

- „TUViT Trusted Site Privacy, Version 2.1“, Dokumentenversion 2.10 vom 06.02.2014, TÜV Informationstechnik GmbH

## Prüfgegenstand

Der Prüfgegenstand „eVi – elektronische Visite“ der La-Well Systems GmbH ist festgelegt in dem Dokument:

- „Trusted Site Privacy – Target of Audit – eVi – elektronische Visite v3.0“, Dokumentenversion 1.5 vom 11.07.2017, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

Verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist die La-Well Systems GmbH.

Die folgenden Prozesse gehören zum Prüfgegenstand eVi – elektronische Visite:

- Online Registrierung als Arzt/Heilpraktiker
- Versand von Login-Daten mittels SMS an Patienten
- Videosprechstunde in Echtzeit (synchrone Kommunikation) mit
  - Übertragung medizinischer Daten/Vitalparameter in Echtzeit über registrierte Messgeräte vom Patienten zum Arzt/Heilpraktiker
  - Übertragung von Dokumenten und Bildern vom Patienten zum Arzt/Heilpraktiker
  - Konsultationen zwischen Arzt/Heilpraktiker

### **Prüfergebnis**

Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien „TUVIT Trusted Site Privacy, Version 2.1“.

Der Prüfgegenstand erfüllt die Anforderungen an den Videodiensteanbieter aus § 5 Abs. 1 Nr. 1-11 i. V. m. § 5 Abs. 2 der Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß § 291g Abs. 4 SGB V (bekannt gemacht im Deutschen Ärzteblatt, Jg. 113, Heft 51-52, 26.12.2016, Seiten A2391-A2392)

## **Zusammenfassung der Prüfanforderungen**

### **1 Datenschutz-Audit**

#### **Rechtliche Anforderungen**

Auf der Grundlage des festgelegten Prüfgegenstands ist zu überprüfen, welche rechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten zur Anwendung kommen und wie diese in den Anwendungszusammenhang des Prüfgegenstands eingebunden werden. Dabei muss der Datenschutz auch dort genügen, wo Gesetze, Verordnungen und Rechtsprechung Lücken und Gestaltungsspielräume lassen.

#### **Zulässigkeit der Verarbeitung**

Nach Identifikation der prüfungsrelevanten Datentypen wird für jeden Datentyp untersucht, ob die Verarbeitung im Hinblick auf den Zweck der Datenverarbeitung zulässig ist. Dabei werden auch die Anforderungen an die Datensparsamkeit im Hinblick auf den Stand der Technik berücksichtigt.

#### **Betroffenenfreundlichkeit**

Hier wird die Berücksichtigung der schutzwürdigen Belange der Personen, deren Daten verarbeitet werden, überprüft. Die Betroffenen haben ein Recht darauf zu erfahren, was mit ihren personenbezogenen Daten geschieht, wie sie weiterverarbeitet werden und ob es eine Möglichkeit zum Selbstschutz, d. h. eine Einflussnahme auf die Verarbeitung der Daten, gibt.

Die Betroffenen sollten darüber informiert werden, welche ihrer Daten mit welchen Prozessen verarbeitet werden. Den Betroffenen muss transparent gemacht werden, welche Rechte und welche Auskunftsmöglichkeiten sie haben und

wie ihre personenbezogenen Daten gesichert werden. Dabei muss der Datenschutz auch schon bei der Vertragsgestaltung eine wichtige Rolle spielen.

Bei Einsatz eines IT-Produktes muss der Anwender darüber informiert sein, welche Funktionen das Produkt hat, um personenbezogene Daten sicher und datenschutzkonform verarbeiten zu können. Dazu gehören z. B. geeignete Produktbeschreibungen und Installationsanleitungen oder auch entsprechende Einarbeitung bzw. Auskunftsmöglichkeit durch ein Unternehmen, das ein Produkt der Informationsverarbeitung einführt und einsetzt.

### **Transparenz**

Die Datenschutz-Policy, die Datenschutzkonzepte und auch die technischen und organisatorischen Maßnahmen, mit denen der Datenschutz im Unternehmen oder Prozess verwirklicht wird, sollten allen Betroffenen transparent und verständlich gemacht werden. Der Untersuchungsfokus ist darauf ausgerichtet, dass die getroffenen Maßnahmen zur Gewährleistung eines dauerhaften Datenschutzes durchschaubar gestaltet sein müssen.

### **Datenschutz-Qualitätsmanagement**

Veränderungen im Bereich der Informationstechniken und der Rechtsgrundlagen haben in der Regel Auswirkungen auf das Konzept zur Erfüllung der Datenschutzerfordernungen. Sie müssen regelmäßig und rechtzeitig im Hinblick auf die Datenschutzauswirkungen untersucht und umgesetzt werden. Gegebenenfalls sind Analysen und Handlungsmodelle anzupassen. Die darauf aufbauenden Maßnahmen des Qualitätsmanagements sind Gegenstand der Betrachtung.

## **Datensicherheit**

Die eingesetzten Informationssysteme können Datenschutzanforderungen nur dann genügen, wenn entsprechende technische und organisatorische Maßnahmen in Bezug auf Datensicherheit ergriffen wurden. Es müssen entsprechende Konzepte vorliegen und es sollten entsprechende vertrauenswürdige Komponenten beim Aufbau der Systeme eingesetzt werden.

- Zutrittskontrolle

Der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, ist Unbefugten durch geeignete Maßnahmen wirksam zu verwehren.

- Zugangskontrolle

Die Nutzung von Datenverarbeitungssystemen durch Unbefugte ist durch geeignete Maßnahmen wirksam zu verhindern.

- Zugriffskontrolle

Die zur Benutzung eines Datenverarbeitungssystems Berechtigten sollen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Weitergabekontrolle

Personenbezogene Daten dürfen bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Eingabekontrolle

Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Auftragskontrolle

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Ein Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

- Verfügbarkeitskontrolle

Personenbezogene Daten müssen durch geeignete Maßnahmen gegen zufällige Zerstörung oder Verlust geschützt sein.

- Trennungsgebot

Durch geeignete Maßnahmen muss sichergestellt werden, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

## **2 Sicherheitstechnische Untersuchung**

### **Sicherheit der verwendeten Komponenten sowie Netzwerk- und Transport-Sicherheit**

Für alle Teilkomponenten, die Sicherheitsfunktionalitäten realisieren, konnte anhand von bereits durchgeführten formalen Evaluationen und/oder öffentlich zugänglichen Informationen nachvollzogen werden, dass sie als vertrauenswürdig eingestuft werden können.

Die Netzwerk- und Transport-Sicherheit müssen dem Stand der Technik entsprechen.

### **Mittel des Systemmanagements**

Es existieren geeignete Konfigurationsmöglichkeiten, sowie ein angemessenes Monitoring und Logging, die zu einem sicheren Betriebszustand beitragen. Dafür eingesetzte Werkzeuge unterliegen denselben Sicherheitsanforderungen, wie das IT-Produkt / das IT-System selbst.

### **Tests und Inspektionen**

Umfangreiche Penetrationstests auf ausnutzbare Schwachstellen, sowie Analysen der Abwehrmechanismen auf Applikationsebene und Prüfungen der eingesetzten Authentifizierungs-/Autorisierungs-Verfahren werden durchgeführt. Die bei den Tests und den Analysen ermittelten Schwachstellen werden entsprechend ihres Risikogrades bewertet.