TÜVIT

Zertifikat

TÜVIT
TÜV NORD GROUP
Privacy
Trusted Site
2023
tuvit.de ID: 5549.23

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Zertifikatsgültigkeit:
27.06.2023 – 27.06.2025

AOK Niedersachsen. Die Gesundheitskasse
Hildesheimer Straße 273
30519 Hannover

für die Prozesse

Datenschutzrelevante Prozesse innerhalb des Arztportals, Version 2.12

die Erfüllung aller Anforderungen der Kriterien

Trusted Site Privacy, Version 2.1

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

Die Anlage ist Bestandteil des Zertifikats mit der 5549.23 und besteht aus 7 Seiten.

Essen, 27.06.2023

Dr. Christoph Sutter, Leiter Zertifizierungsstelle

Zum Zertifikat

TÜV Informationstechnik GmbH
Am TÜV 1 • 45307 Essen
tuvit.de

TÜVNORDGROUP

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 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- „Trusted Site Privacy – Gutachten Recht – Datenschutzrelevante Prozesse innerhalb des Arztportals, Version 2.12“, Version 1.2 vom 27.06.2023, TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige
- „Trusted Site Privacy – Gutachten Technik – Datenschutzrelevante Prozesse innerhalb des Arztportals, Version 2.12“, Version 1.1 vom 20.06.2023, TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige

Prüfanforderungen

- „Trusted Site Trusted Site Privacy, Version 2.1 Kriterienkatalog“, Dokumentversion 4.0 vom 04.01.2018, TÜV Informationstechnik GmbH

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Der Prüfgegenstand „Datenschutzrelevante Prozesse innerhalb des Arztportals, Version 2.12“ der AOK Niedersachsen. Die Gesundheitskasse ist festgelegt in dem Dokument:

- „Trusted Site Privacy – Target of Audit – Beschreibung des Prüfgegenstandes V1.3, vom 27.06.2023, AOK Niedersachsen. Die Gesundheitskasse

In den Prozessen werden die Kommunikation und der Datenaustausch zwischen Ärzten, Fachärzten und der AOKN vereinfacht, indem analoge Prozesse digitalisiert und neue Prozesse etabliert werden, die in einem einheitlichen Ärzteportal mit einer gemeinsamen Datenbasis zur Verfügung gestellt werden. Folgende Funktionen werden zur Verfügung gestellt:

1. Nutzerverwaltung

Mit Hilfe der Nutzerverwaltung können Arztportal- bzw. CMS Benutzer gemäß einem definierten Rollen-Rechte-Konzept angelegt werden, um ihnen den betreffenden Systemzugriff über eine Anmeldung/Abmeldung zu ermöglichen.

2. Selbstregistrierung

Die Selbstregistrierung gliedert sich in drei Stufen. In Stufe 1 können sich Ärzte zunächst unter https://www.arztportal-niedersachsen.de mit ihren persönlichen Nutzer- sowie Praxisdaten registrieren.

Im Rahmen der Selbstregistrierung Stufe 2 können bereits registrierte Ärzte zudem im AOKN Arztportal Praxismitarbeiter nach Erteilung ihrer Einwilligung registrieren.

In Stufe 3 können Nutzer mit der Rolle "AOK-Mitarbeiter" Registrierungsanfragen vereinfacht bearbeiten.

3. Management von Praxismitarbeitern

Durch das Management von Praxismitarbeitern werden Ärzten zusätzliche Möglichkeiten geboten, die Registrierung von Praxismitarbeitern über das Arztportal Cockpit zu verwalten. Darüber hinaus können registrierte Praxismitarbeiter ihre Zugehörigkeit zu einer Arztpraxis selbstständig beenden.

4. Mitgliedschaftsabfrage / Abrechnungsschein

Ärzte und Praxismitarbeiter können für Patienten, die ohne elektronische Gesundheitskarte in die Praxis kommen, direkt abfragen, ob der Versicherte bei der AOKN versichert ist.

5. Abfrage der Zuzahlungsbefreiung

Durch die Abfrage der Zuzahlungsbefreiung ist es Ärzten und Praxismitarbeitern möglich zu prüfen, ob die AOKN-Versicherten von der Zuzahlung befreit sind oder nicht.

6. DMP-Status Abfrage

Durch die Abfrage des DMP-Status ist es Ärzten und Praxismitarbeitern im Arztportal möglich, den DMP-Teilnahmestatus von AOKN-Versicherten zu prüfen.

7. DMP-Fallführung

Durch die DMP-Fallführung ist es Nutzern möglich, den Dokumentationsstatus ihrer DMP-Patienten einzusehen. Hierzu können sie im Arztportal eine Übersicht der zu erstellenden Dokumentationen all ihrer DMP-Patienten aufrufen und diese nach Fertigstellung als erledigt markieren. Darüber hinaus können sie Rückmeldungen an die AOKN zu einem bestimmten DMP-Fall verfassen und an die AOKN übermitteln. Des Weiteren werden den Nutzern im Arztportal Benachrichtigungen über ausstehende Dokumentationen angezeigt.

8. Arznei- und Heilmittelberichte

Neben den Berichten zur hausarztzentrierten Versorgung (HzV) werden Ärzten Berichte zu Arznei- und Heilmittelverordnungen über eine Schnittstelle zur Verfügung gestellt.

9. Notifications

Durch die Benachrichtigungen im Arztportal-Cockpit werden Ärzte und Praxismitarbeiter über Vorgänge und Neuigkeiten rund um das Arztportal informiert. Die Benachrichtigungen im Arztportal-Cockpit ermöglichen es dem Nutzer, Aktions-Erinnerungen und Benachrichtigungen für alle ihm zugeordneten BSNR bzw. BSNR-LANR-Kombinationen zu erhalten.

10. Arzt- und Praxiskontext

Praxismitarbeiter können Abrechnungsscheine im Kontext eines Arztes in der Praxis ausstellen. Ist ein Praxismitarbeiter in mehreren Praxen tätig, ist es möglich, im wechselnden Kontext von Praxen und Ärzten zu arbeiten. Ist ein Arzt in mehreren Praxen tätig, ist es möglich, im wechselnden Kontext von Praxen zu arbeiten. Die BSNR und LANR wird automatisch ohne manuelle Eingabe in Abrechnungsscheinen ergänzt.

11. Nutzer-Praxen-Beziehung

In der ambulanten Versorgung ist es möglich, dass Ärzte für mehrere Betriebsstätten tätig sind und über diese Leistungen abrechnen. Gleichermaßen können Praxismitarbeiter für mehrere Betriebsstätten und Ärzte, also mehrere BSNR-LANR-Kombinationen, tätig sein. Ein konkretes Beispiel stellen die Praxisgemeinschaften dar, in denen üblicherweise Praxismitarbeiter für unterschiedliche Ärzte mit jeweils eigener BSNR Aufgaben erledigen. Diese Konstellationen werden auch im Arztportal abgebildet. Alle Nutzer (Ärzte, Praxismitarbeiter) können mehreren BSNRs im Arztportal zugeordnet sein können und Funktionen des Arztportals für jede BSNR durchführen.

12. Consent Management

Nutzer des Arztportals müssen den Nutzungsbedingungen zuvor zustimmen. AOK Mitarbeiter können die Nutzungsbedingungen und die Datenschutzerklärung editieren und eine Übersicht aller Versionen sehen, um diese an Änderungen der Funktionalität des Systems oder der gesetzlichen Grundlagen anzupassen und die Nutzer des Arztportals pflichtgemäß über Änderungen zu informieren. Darüber hinaus ist eine Übersicht über alle Versionen der Seiten Nutzungsbedingungen und Datenschutz sichtbar, um nachvollziehen zu können, welche Version für welchen Zeitraum gültig war bzw. ist.

13. Tracking

Das Nutzerverhalten von Ärzten und Praxismitarbeitern kann im Arztportal Cockpit analysiert werden, um anhand der Ergebnisse das Nutzererlebnis zu verbessern. Hierfür werden nach der Einwilligung der Nutzer Cookies gesetzt und pseudonymisierte Daten durch das Trackingtool „Matomo" (Hosting auf eigenen Servern) erhoben.

14. Feedback Funktion

Die Feedback Funktion ermöglicht es, direktes Feedback der Nutzer zu erhalten und schafft so einen Einblick in deren Bedürfnisse, Problemstellungen und Nutzungsanforderungen in Bezug auf das

Arztportal. Auf konkreten Wunsch des Nutzers kann eine Antwort durch die AOKN auf dieses Feedback ermöglicht werden und erfolgen.

15. Kontaktwunsch-Anfrage

Die Kontaktwunsch-Anfrage ermöglicht es den Nutzern des Arztportal Cockpits, eine Kontaktanfrage an die AOKN zu senden, um so bzgl. eines Beratungstermins von der AOKN kontaktiert zu werden.

16. Suchfunktion

Durch die Suche wird den Nutzern die Möglichkeit geboten, Inhalte aus dem Arztportal effizient auffinden zu können.

17. Editierung von Seiten

AOK Mitarbeiter können auf der Arztportal-Website die rechtlichen Hinweise, Datenschutzhinweise, das Impressum, die leichte Sprache, die Erklärung zur Barrierefreiheit und die Gebärdensprache editieren.

Verwendete Abkürzungen:

AOK: Allgemeine Ortskrankenkasse

AOKN: Allgemeine Ortskrankenkasse Niedersachsen

BSNR: Betriebsstättennummer

DMP: Disease-Management-Programm

LANR: Lebenslange Arztnummer

Prüfergebnis

Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Kriterien Trusted Site Privacy, Version 2.1

Hinweise der Zertifizierungsstelle

Das Zertifikat ist kein Zertifikat im Sinne der EU-Datenschutz-Grundverordnung (EU-DSGVO – Verordnung 2016/679).

Eine Zertifizierung nach der EU-DSGVO durch eine akkreditierte Konformitätsbewertungsstelle setzt gemäß Art. 42 Abs. 5 EU-DSGVO voraus, dass die zuständigen Bundes- oder Landesdaten-schutzbehörden oder der Europäische Datenschutzausschuss gemäß Art. 63 EU-DSGVO die Kriterien für die Zertifizierung – also das Zertifizierungsprogramm im Sinne der ISO/IEC 17065 i. V. m. ISO/IEC 17067 – genehmigt haben.

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 Selbstdatenschutz, 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 Datenschutzanforderungen. 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 entsprechen dem Stand der Technik.

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 Risikograde bewertet.