Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Deutsche Post AG
Charles-de-Gaulle-Straße 20
53250 Bonn

für das System

E-POST Plattform

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 8 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Privacy TÜViT® 2019 Trusted Site

Certificate ID: 5539.19

21

Zertifikat gültig bis 24.09.2021

Essen, 24.09.2019

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

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 Recht – E-POST Plattform (Stand: Juni 2019)“, Version 1.2 vom 13.09.2019, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige
- „Trusted Site Privacy – Gutachten Technik – E-POST Plattform (Stand: Juni 2019)“, Version 1.2 vom 13.09.2019, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

Prüfanforderungen

- „TÜViT Trusted Site Privacy, Version 2.1”, Dokumentenversion 4.0 vom 04.01.2018, TÜV Informationstechnik GmbH

Prüfgegenstand

Der Prüfgegenstand „E-POST Plattform (Stand: Juni 2019)“ der Deutsche Post AG, ist festgelegt in dem Dokument:

- „Trusted Site Privacy – Target of Evaluation – E-POSTBRIEF Kern, Rel. 2.2 – Deutsche Post AG“, Version 1.0 vom 31.03.2011, TÜV Informationstechnik GmbH, Prüfstelle für Datenschutz

sowie den Ergänzungen in Kapitel 2 „Prüfgegenstand Informationsverbund E-POST-Plattform“ des aktuell vorgelegten Gutachtens Recht und in Kapitel 2 „Gesamtarchitektur“ des aktuell vorgelegten Gutachtens Technik.

Verantwortliche Stelle im Sinne der Datenschutz-Grundverordnung ist die Deutsche Post AG (DPAG).

Der Informationsverbund der E-POST Plattform enthält all diejenigen Prozesse und Systeme, die für die Kernfunktion der E-POST benötigt werden bzw. diese ergänzen oder auf dieser basieren. Mit dem E-POSTBRIEF bietet die DPAG Unternehmen, Behörden und Privatpersonen einen Dienst zur digitalen Schriftkommunikation an, der einen verbindlichen, verlässlichen und vertraulichen Austausch von Nachrichten und Dokumenten eröffnet. Eine Individual-Schnittstelle ermöglicht Geschäftskunden und deren Mitarbeitern das Senden und Empfangen der E-Postbriefe aus ihrer existierenden E-Mail-Infrastruktur heraus. Zusätzlich wird Geschäftskunden eine massentaugliche Schnittstelle zur Verfügung gestellt.

Folgende Funktionen und unterstützenden Prozesse sind Teil des Prüfgegenstandes E-POST Plattform:

- E-POSTBUSINESS API, eine Webservice-Schnittstelle für Geschäftskunden zur Nutzung von E-POSTBRIEF
- E-POSTBUSINESS BOX, eine Lösung für Geschäftskunden für den täglichen Postversand und -empfang
- E-POSTBRIEF END-TO-END, ein Verschlüsselungsdienst für Berufsgruppen mit Geheimhaltungspflicht, der eine Ende-zu-Ende-Verschlüsselung von Dateianhängen zur Wahrung der Geheimhaltungspflicht realisiert. Die Dateianhänge werden in den E-POSTBRIEF integriert.

- E-POST CLOUD, ein Onlinespeicher für Dateien
- DIGITALE KOPIE zum Versenden einer digitalen Kopie ins digitale Postfach eines Empfängers neben einer physischen Briefsendung
- E-POSTNOW für Geschäftskunden zum Versenden von Briefen aus einem Office-Programm heraus mit Ausdruck und Zustellung durch die DPAG

Mitbetrachtet wurden ferner die Komponenten zur Unterstützung von Billing- und Support-Prozessen.

Nicht zum Prüfgegenstand gehören die Informationswebseite (www.epost.de), der E-POSTBRIEF mit klassischer Zustellung und E-POSTSCAN.

Die Datenverarbeitungen zum E-POSTBRIEF erfolgen in redundanten Rechenzentren in Deutschland.

Prüfergebnis

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

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.