

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Deutsche Post AG
Charles-de-Gaulle-Straße 20
53113 Bonn

für den Dienst zur digitalen Schriftkommunikation

E-POSTBRIEF Kern, Rel. 2.2

die Erfüllung aller Anforderungen der Kriterien

Trusted Site Privacy, Version 2.0

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 den zugehörigen
Prüfberichten und ist bis zum 31.07.2013 gültig.



Zertifikat-Registrier-Nr.:
TUVIT-TSP5512.11

13

Essen, 21.07.2011

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuvit.de

Zertifikat

Zertifizierungssystem

TÜV[®]

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produkt-Zertifizierungssystems durch:

- „Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜViT GmbH

Prüfberichte

- „Trusted Site Privacy – Prüfbericht Technik – E-POSTBRIEF Kern, Rel. 2.2 – Deutsche Post AG“, Version 1.00 vom 13.04.2011, TÜViT GmbH, IT Quality, Prüfstelle für Datenschutz
- „Trusted Site Privacy – Gutachten Recht – E-POSTBRIEF Kern, Rel. 2.2 – Deutsche Post AG“, Version 1.01 vom 08.06.2011, TÜViT GmbH, IT Quality, Prüfstelle für Datenschutz

Prüfanforderungen

- „TÜViT Trusted Site Privacy, Version 2.0“, Dokumentenversion 2.5 vom 09.05.2011, TÜViT GmbH

Prüfgegenstand

Der Prüfgegenstand „E-POSTBRIEF Kern, Rel. 2.2“ der Deutsche Post AG ist in folgendem Dokument beschrieben:

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

Die Deutsche Post AG (DPAG) stellt mit dem E-POSTBRIEF-Portal eine Internetplattform zur Verfügung, die den Anwendern, Privatkunden und Geschäftskunden, verschiedene Kommunikations-Möglichkeiten und Mehrwertdienste bietet. Der Prüfgegenstand E-POSTBRIEF Kern, Rel. 2.2 umfasst die Komponenten, die aus Sicht des Anwenders zur alltäglichen Nutzung des E-Postbriefs benötigt werden: Versanddienst, elektronischer Briefkasten, Adressbuch und öffentliches Adressverzeichnis. Mitbetrachtet wurden ferner die Komponenten zur Unterstützung von Billing- und Support-Prozessen.

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. Er wird in zwei Formen angeboten. Der „E-POSTBRIEF mit elektronischer Zustellung“ umfasst den reinen elektronischen Zustellungsweg. Darüber wird den Anwendern angeboten, E-Postbriefe als klassische Briefe an Empfänger versenden zu lassen – „E-POSTBRIEF mit klassischer Zustellung“, der nicht Prüfgegenstand ist.

Bei den Anwendern wird zwischen Geschäfts- und Privatkunden unterschieden. Geschäftskunden können den E-POSTBRIEF für Business-to-Business (B2B) oder Business-to-Consumer (B2C) Kommunikation nutzen. 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 unterstützende Prozesse sind nicht Teil des Prüfgegenstandes:

TÜV[®]

- E-POSTBRIEF mit klassischer Zustellung,
- Überprüfung der Identität im POSTIDENT-Verfahren,
- Kundenservice-Funktionalitäten,
- im E-POSTBRIEF-Portal angebotene Mehrwertdienste.

Prüfergebnis

Mit einer rechtlichen und technischen Prüfung des Prüfgegenstands und der zugehörigen Dokumentation wurde nachgewiesen, dass alle anwendbaren Anforderungen aus den Prüfkriterien erfüllt sind.

Zusammenfassung der Prüfanforderungen

TÜV[®]

1 Datenschutz-Audit

Rechtskonformität

Auf der Grundlage des festgelegten Untersuchungsobjekts ist zu identifizieren, welche Rechtsnormen bei der Verarbeitung personenbezogener Daten zur Anwendung kommen. Diese ergeben sich unmittelbar aus dem Anwendungszusammenhang des Untersuchungsobjektes. Dabei muss der Datenschutz auch dort genügen, wo Gesetze, Verordnungen und die Rechtsprechung Lücken und Gestaltungsspielräume lassen. In einem weiteren Schritt wird geprüft, ob die festgestellten rechtlichen Anforderungen erfüllt sind.

Zulässigkeit der Verarbeitung

Im Datenschutzrecht gilt, dass ohne eine gesetzliche Erlaubnis oder ohne gültige Einwilligung des Betroffenen personenbezogene Daten nicht verarbeitet werden dürfen. 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.

Kundenfreundlichkeit

Hier wird die Berücksichtigung der schutzwürdigen Belange der Personen, deren Daten verarbeitet werden, überprüft. Die Kunden eines Unternehmens 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.

Mitarbeiterfreundlichkeit

Auch die Mitarbeiter eines Unternehmens müssen darüber informiert werden, welche ihrer Daten mit welchen Prozessen verarbeitet werden. Ihnen 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 und Arbeitsplatzbeschreibung eine wichtige Rolle spielen.

Anwenderfreundlichkeit

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 organisatorischen und technischen Maßnahmen, mit denen der Datenschutz im Unternehmen oder Prozess verwirklicht wird, sollte 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 den Datenschutzerfordernungen nur dann genügen, wenn entsprechende organisatorische und technische 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

TÜV[®]

Sicherheit der verwendeten Komponenten

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.

Mittel des Systemmanagements

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

Tests und Inspektionen

Umfangreiche Penetrationstests und technische Schwachstellenanalysen sind bei der Prüfung durchgeführt worden. Die bei den Tests und Analysen ermittelten Schwachstellen sind entsprechend ihres Risikogrades bewertet worden.