

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH  
bescheinigt hiermit dem Unternehmen

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

für den Ende-zu-Ende-Verschlüsselungs-Service für  
Berufsgeheimnisträger auf der E-POST Plattform

**E-POSTBRIEF END-TO-END**

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 zugehörigen  
Prüfbericht bis zum 31.12.2016.



**Voluntary Validation**  
© TÜVIT - Member of TÜV NORD GROUP

Zertifikat-Registrier-Nr.:  
TUVIT-TSP5523.15

16

Essen, 10.03.2015

Dr. Christoph Sutter  
Leiter Zertifizierungsstelle

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

**Zertifikat**

## Zertifizierungssystem

TÜV<sup>®</sup>

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

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

## Prüfberichte

- „Trusted Site Privacy – Gutachten Technik – E-Post Plattform Ende-zu-Ende-Verschlüsselung“, Version 1.00 vom 30.09.2014, TÜV Informationstechnik GmbH, Prüfstelle für Datenschutz
- „Trusted Site Privacy – Gutachten Recht – E-Post Plattform Ende-zu-Ende-Verschlüsselung“, Version 1.00 vom 30.09.2014, TÜV Informationstechnik GmbH, Prüfstelle für Datenschutz

## Prüfanforderungen

- „TÜViT Trusted Site Privacy, Version 2.1“, Dokumenten-version 2.8 vom 24.04.2012, TÜV Informationstechnik GmbH

## Prüfgegenstand

Der Prüfgegenstand „E-Post Plattform Ende-zu-Ende-Verschlüsselung“, kurz E-POSTBRIEF END-TO-END, der Deutsche Post AG, ist festgelegt in den Dokumenten:

- „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

- „Lösungskonzept Berufsgeheimnisträger E-POSTBRIEF“,  
Version 2.0 vom 10.07.2013, Deutsche Post AG

TÜV®

sowie in den aktuell vorgelegten Prüfberichten.

Der Verschlüsselungsdienst E-Post Plattform Ende-zu-Ende-Verschlüsselung realisiert für Berufsgruppen mit Geheimhaltungspflicht für Dateianhänge eine vollständige Ende-zu-Ende-Verschlüsselung zur Wahrung der Geheimhaltungspflicht.

Das E-Mail Anschreiben, die Betreffzeile und Dateinamen verschlüsselter Anhänge werden unverschlüsselt übertragen.

## Prüfergebnis

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

Der Prüfgegenstand stellt aufgrund seiner technischen und organisatorischen Vorkehrungen eine geeignete Möglichkeit für Berufsgeheimnisträger im Sinne von § 203 StGB dar, vertrauliche Inhalte als verschlüsselte Anhänge von E-POSTBRIEFEN zu versenden.

## 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 Datenschutzerfordernungen 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.