Zeitpunkt der Prüfung

23.11.2010 – 24.02.2012

Adresse des Antragstellers

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

Adressen des/der Sachverständigen

TÜV Informationstechnik GmbH
Prüfstelle für Datenschutz
Leitung:
Monika Wojtowicz, LL.M. (Recht)
Ulrich Heitkötter (Technik)
Langemarckstraße 20
45141 Essen

Kurzbezeichnung des IT-Produktes

E-POSTBRIEF Kern Rel.2.2

Detaillierte Bezeichnung des IT-Produktes

Die Deutsche Post AG (DPAG) stellt mit dem *E-POSTBRIEF* Portal eine Internetplattform zur Verfügung, die den Nutzern, neben Privatkunden auch Geschäftskunden, verschiedene Kommunikations-Möglichkeiten und Mehrwertdienste bietet. Der begutachtete Prüfgegenstand umfasste die Komponenten, die aus Sicht des Anwenders zur alltäglichen Nutzung des *E-POSTBRIEFs* benötigt werden. Hierzu gehören Versanddienst, elektronischer Briefkasten, Adressbuch und öffentliches Adressverzeichnis. Mitbetrachtet wurden ferner die Komponenten zur Unterstützung von Billing- und Support-Prozessen sowie die Sicherheit der Internetpräsenz. Unterstützende Funktionen und Prozesse, wie z.B. die Überprüfung der Identität im Postident-Verfahren, Kundenservice-Funktionalitäten oder die im Rahmen des *E-POSTBRIEF* Portals angebotenen Mehrwertdienste und Besucherwebseiten waren nicht Gegenstand der Prüfung. Die E-Mail- und Fax-Dienste, welche in die Nutzerkonto-Oberfläche des *E-POSTBRIEFs* eingebunden werden können, waren ebenfalls nicht Gegenstand der Prüfung.

Mit dem *E-POSTBRIEF* bietet die DPAG einen Service für die elektronische Kommunikation 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 hinaus besteht die Möglichkeit *E-POSTBRIEFE* zu konvertieren und diese als klassischen gedruckten Brief an einen Empfänger zuzustellen – „*E-POSTBRIEF* mit klassischer Zustellung“ (die klassische Zustellung war nicht Gegenstand der Prüfung).

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.

Die Begutachtung umfasste grundsätzlich das *E-POSTBRIEF* Portal. Weitere, im Folgenden dargestellte Komponenten wurden betrachtet, soweit dies für die Bewertung der Wirksamkeit der technischen Sicherheitsmaßnahmen notwendig war.

Kundenportal: Das Portal beinhaltet alle Funktionalitäten für registrierte bzw. im Registrierungsprozess befindliche Kunden. Hierzu gehören die Erstellung sowie Verarbeitung von *E-POSTBRIEFen*, das Pflegen des eigenen Accounts sowie des Adressverzeichnisses. Die Nutzung des Portals wird sowohl den Privat- als auch den Geschäftskunden eröffnet, wobei für diese Kundengruppen unterschiedliche Registrierungsprozesse gelten.

Geschäftskunden-Gateway: Das Gateway ermöglicht Geschäftskunden und deren Mitarbeitern das Senden und Empfangen der *E-POSTBRIEFe* aus ihrer existierenden E-Mail-Infrastruktur heraus. Über einen Gateway-Zugang wickelt der Geschäftskunde den *E-POSTBRIEF* Verkehr für alle internen Mitarbeiter ab. Der Geschäftskunde hat die Möglichkeit, seinen Zugang beliebigen Mitarbeiter- und Organisationspostfächern zugänglich zu machen. Alle Mitarbeiter- und Organisationspostfächer des Kunden werden über eine oder mehrere Subdomains des Kunden adressiert. Der *E-POSTBRIEF* Service beinhaltet auch das Logging und Auditing der Aktivitäten der Geschäftskunden.

Web-, Publish- und Authoring-Server: Mit diesen Komponenten werden die Webseiten im Rahmen des Kundenportals bereitgestellt.

Administration Backoffice Support-Anwendung (ABS): Diese Komponente dient der Unterstützung der Support- und Billing-Prozesse.

Das *E-POSTBRIEF* **Portal** stellt folgende Funktionen zur Verfügung:

- ***E-POSTBRIEF* Adresse**

Die *E-POSTBRIEF* Adresse für natürliche Personen wird aus dem Vornamen und Nachnamen gebildet. Bei Anmeldungen unterschiedlicher Personen mit gleichem Namen wird nach Vergabe der ersten *E-POSTBRIEF* Adresse für die weiteren zusätzlich eine Nummer mit bis zu vier Ziffern angefügt.
Die *E-POSTBRIEF* Adressen von Geschäftskunden enthalten eine Subdomain, die einen klaren Bezug zum Firmennamen, zum Tätigkeitsbereich oder zu eigenen Websites aufweisen muss.
Vor der Aktivierung des Kontos (Kontoeröffnung) erfolgt obligatorisch eine Identifizierung des Nutzers im Postident-Verfahren. Um eine eindeutige und zuverlässige Identifizierung des Nutzers sicherzustellen, wird ein Abgleich der während der Registrierung angegebenen Pflichtangaben mit den Daten aus dem Postident-Verfahren durchgeführt. Die Begutachtung umfasste nur die Schnittstellen, die für diesen Abgleich verwendet werden. Das Postident-Verfahren selbst war nicht Gegenstand der Prüfung.

Der *E-POSTBRIEF* kann sowohl durch Privat- als auch Geschäftskunden unterschiedlicher Rechtsformen genutzt werden, wobei die unterschiedlichen Identifizierungsprozesse zu beachten sind.

Die Identifikation der Privatkunden erfolgt anhand von Angaben wie: Geburtsname, Name, Vorname, Straße, Nummer, Postleitzahl, Geburtsdatum, Geburtsort und Staatsangehörigkeit.

Der Vertragsabschluss mit den Geschäftskunden setzt eine Identitätsprüfung voraus, die in Abhängigkeit von der jeweiligen Rechtsform und der Ziel-Plattform – Geschäftskunden als Portalnutzer oder Geschäftskunden als Gateway-Nutzer – durch die Vorlage entsprechender Dokumente, wie z.B. Handels-, Genossenschafts-, Vereins- oder Partnerschafts-Registerauszug und die Durchführung des Postident-Verfahrens durch die Vertragsunterzeichner erfolgt.

- **Anmeldung zum Nutzerkonto mit abgestuftem Identitätsnachweis**

Für die Anmeldung am *E-POSTBRIEF* Portal sind zwei Sicherheitsstufen vorgesehen. Die Anmeldung mit normalem Ident-Nachweis erfolgt durch Eingabe der *E-POSTBRIEF* Adresse und des persönlichen Passworts. Diese Art der Anmeldung ermöglicht nur eine eingeschränkte Nutzung der Funktionalitäten bezogen auf den *E-POSTBRIEF*, wie z.B. den lesenden Zugriff auf die versendeten *E-POSTBRIEFe.*

Zum Absenden eines *E-POSTBRIEFs* (mit oder ohne die angebotenen Zusatzleistungen, wie das Einschreiben Einwurf, Einschreiben mit Empfangsbestätigung, *E-POSTBRIEF* persönlich signiert, *E-POSTBRIEF* persönlich verschlüsselt) ist immer ein hoher Ident-Nachweis erforderlich. Zur Erreichung eines hohen Ident-Nachweises wird zusätzlich eine HandyTAN an die in der Online-Registrierung angegebene und von der DPAG verifizierte Mobilfunknummer des Nutzers gesendet, die dann vom Nutzer eingegeben werden muss.

- **Briefkasten**

Der elektronische Briefkasten (Postfach) dient dem Empfangen und Versenden der *E-POSTBRIEFe*.

- **Persönliches Adressbuch**

Die Nutzer können durch die Auswahl und Eingabe von Kontakten ein persönliches Adressbuch anlegen. Die Einträge eines persönlichen Adressbuchs werden vom Nutzer in seiner Herrschaft verwaltet.

- **Öffentliches Adressverzeichnis**

Alle registrierten Nutzer können im Rahmen des öffentlichen Adressverzeichnisses ihre personenbezogenen Daten freischalten und für die anderen registrierten Nutzer einsehbar machen. Jedes Feld erhält bei der Anzeige über den Verzeichnisdienst eine zusätzliche Information, ob die jeweiligen Daten von der DPAG verifiziert wurden.

Das öffentliche Adressverzeichnis dient dem Ziel, die *E-POSTBRIEF* Adressen der Teilnehmer ausfindig zu machen und die Kommunikation mittels *E-POSTBRIEF* zu ermöglichen.
Die in Ziff. 4.2 *Datenschutzhinweise für die Nutzung des E-Postbrief Portals*[1] beschriebene Auskunftserteilung aus dem öffentlichen Adressverzeichnis an die registrierten Geschäftskunden war zum Zeitpunkt der Zertifizierung nicht implementiert und wurde aus

[1] Abrufbar unter: http://www.epost.de/privatkunden/footer/rechtliches/agb.html#KapitelIV

dem Prüfgegenstand ausgeschlossen. Diese Funktionalität soll für den Geschäftskunden in der Zukunft die Voraussetzung schaffen, nach Nennung des Namens und der postalischen Adresse die E-*POSTBRIEF* Adresse des Empfängers bei der DPAG zu erfragen und damit den Versand seiner Nachricht als *E-POSTBRIEF* zu ermöglichen. Die Implementierung dieser Funktionalität wird obligatorisch mit einer Rezertifizierung für den *E-POSTBRIEF* einhergehen.

- **Versand mit Zusatzleistungen**

Das Postfach dient dem Nutzer als elektronischer Briefkasten. Er ermöglicht den Teilnehmern die *E-POSTBRIEFe* zu verschicken und zu empfangen. Die *E-POSTBRIEFe* können zusätzlich mit folgenden optionalen Versandarten versehen werden:

- Einschreiben Einwurf

Der Absender erhält eine vom System generierte Versandbestätigung und eine Zustellbestätigung. Dabei handelt es sich um eine Rückmeldung vom *E-POSTBRIEF* System nach der serverseitigen Annahme zum Versand/Zustellung der Nachricht. Die Versand-/Zustellbestätigung wird dem Absender in einer Nachricht zugesendet, wobei die eigentliche Versand-/Zustellbestätigung als PDF der Nachricht angehängt ist. Die Versandbestätigung ist vom *E-POSTBRIEF* System qualifiziert signiert.

- Einschreiben mit Empfangsbestätigung

Bei Nutzung der Zusatzleistung 'Einschreiben mit Empfangsbestätigung' findet der Empfänger in seinem elektronischen Briefkasten zunächst nur einen Hinweis auf eine Nachricht mit Empfangsbestätigung. Der Hinweis enthält den Absender und den Betreff des *E-POSTBRIEFs*. Beim Öffnen des *E-POSTBRIEFs* wird der Empfänger aufgefordert, den Empfang anzunehmen oder abzulehnen. Für beide Aktionen muss der Empfänger mit hohem Ident-Nachweis angemeldet sein. Wird der *E-POSTBRIEF* angenommen, so erhält der Empfänger einen dauerhaften Zugriff auf die Nachricht. Wird der *E-POSTBRIEF* abgelehnt, so löscht das Portal den *E-POSTBRIEF* aus dem Briefkasten des Empfängers.

Der Absender einer Nachricht mit Empfangsbestätigung erhält sowohl eine Versand- als auch eine Empfangs- bzw. eine Ablehnungsbestätigung. Die Meldung über Annahme bzw. Ablehnung wird als Nachricht zugestellt, wobei die eigentliche Empfangsbestätigung (Annahme oder Ablehnung) als PDF der Nachricht angehängt ist.

Bei Geschäftskunden erfolgt eine automatische Annahme von Nachrichten mit Empfangsbestätigung.
Diese Versandoption kommt dem Auslieferungsnachweis – dem Rückschein – des physischen Einschreibens am nächsten.

- Persönlich verschlüsselt

Nachrichten können vom Nutzer durch ein asymmetrisches Verschlüsselungsverfahren zusätzlich verschlüsselt und/oder signiert werden. Die Ver- bzw. Entschlüsselung, Signaturerzeugung und -prüfung erfolgen dabei auf Systemen der DPAG.
Voraussetzung für die Nutzung der Versandoption 'Persönlich verschlüsselt' ist, dass der Absender selbst ein persönliches Zertifikat besitzt. Dieses Zertifikat beantragt und bezieht der Nutzer über das *E-POSTBRIEF* System.

- Persönlich signiert

Bei ‚Persönlich signiert‘ wird die Nachricht mit dem privaten Schlüssel des Absenders signiert.

Die Signaturerzeugung und -prüfung erfolgt dabei auf Systemen der DPAG.

Tools, die zur Herstellung des IT-Produktes verwendet wurden

- Red Hat Enterprise Linux

Zweck und Einsatzbereich

Der *E-POSTBRIEF* ist ein Angebot der Deutschen Post AG an Unternehmen, Behörden und Privatpersonen für eine verbindliche, vertrauliche und verlässliche elektronische Kommunikation.

Modellierung des Datenflusses

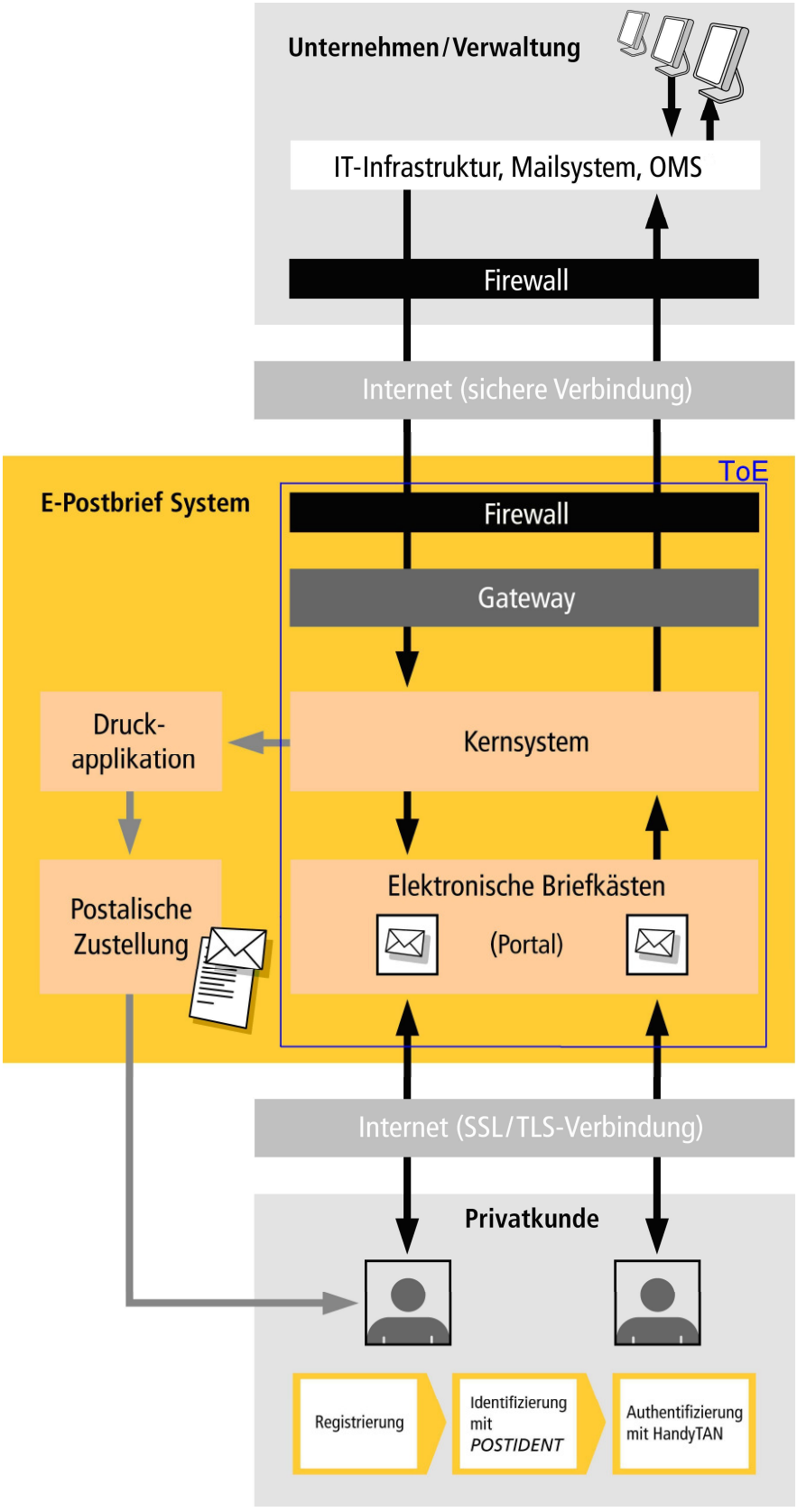

Abbildung 1: Target of Evaluation (ToE)

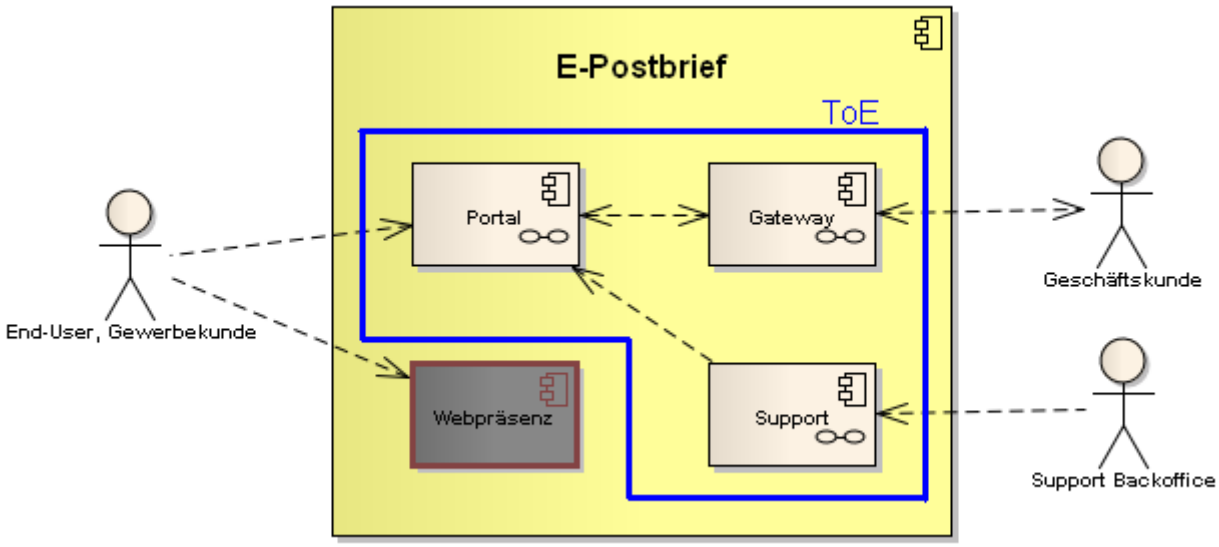

Abbildung 2: *E-POSTBRIEF* Kern mit Portal, Gateway, Support und Webpräsenz

Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Anforderungskatalog v 1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD. Die Einhaltung des De-Mail-Gesetzes wurde nicht geprüft.

Zusammenfassung der Prüfungsergebnisse

Mit dem *E-POSTBRIEF* wird das Ziel verfolgt, eine technische Plattform für die sichere und verbindliche elektronische Kommunikation bereitzustellen. Im Rahmen des *E-POSTBRIEF* Portals werden neben dem *E-POSTBRIEF* als Übertragungsleistung auch – wie oben dargestellt – weitere Funktionalitäten, wie das elektronische Postfach, das persönliche Adressbuch und das öffentliche Adressverzeichnis bereitgestellt.

Diese Funktionalitäten unterliegen zum Teil unterschiedlichen datenschutzrechtlichen Regimen. Bei dem *E-POSTBRIEF* handelt es sich um einen Telekommunikationsdienst i.S.v. § 3 Nr. 24 TKG, der überwiegend in der Übertragung von Signalen über die Telekommunikationsnetze besteht und gemäß § 1 Abs. 1 TMG zugleich ein Telemedium ist. Nach § 11 Abs. 3 TMG unterliegt dieser jedoch den datenschutzrechtlichen Wertungen des Telekommunikationsgesetzes. Das elektronische Postfach und das persönliche Adressverzeichnis fallen dagegen als Telemedien unter die datenschutzrechtlichen Vorschriften des Telemediengesetzes.

Die Überprüfung gemäß dem Prüfschema zur Erlangung eines Datenschutz-Gütesiegels und des hierfür geltenden Anforderungskatalogs hat ergeben, dass die Anforderungen der für den *E-POSTBRIEF* und seine Zusatzfunktionalitäten einschlägigen Datenschutzvorschriften in einer adäquaten bis vorbildlichen Weise umgesetzt wurden. Die Ergebnisse werden im Folgenden dargestellt.

1. Grundsätzliche technische Ausgestaltung des IT-Produkts

Die Inanspruchnahme des *E-POSTBRIEFs* erfolgt in technisch definierten Schritten. Die damit verknüpften Verarbeitungsvorgänge haben jeweils fest definierte Datenkataloge zum Gegenstand, die für die Begutachtungszwecke in folgende Gruppen gefasst wurden:

- Registrierungs- und Accountdaten von Privatkunden
- Registrierungs- und Accountdaten von Geschäftskunden
- Zugangsdaten
- Versanddaten und Nachrichteninhalte
- Billingdaten
- Nutzerdaten im öffentlichen Adressverzeichnis
- Adressbuchdaten
- Protokollierungsdaten

Im Rahmen dieses Abschnitts wurde gemäß dem Anforderungskatalog untersucht, ob die Ausgestaltung des Systems und der Umfang der verarbeiteten Daten den Grundsätzen der Datenvermeidung und Datensparsamkeit genügen, insbesondere, ob das frühzeitige Löschen, die Anonymisierung bzw. Pseudonymisierung, wenn Daten noch erforderlich sind, aber Personenbezug verzichtbar ist, umgesetzt wurden.

Die Prüfung hat ergeben, dass die im Rahmen der einzelnen Teilprozesse verarbeiteten Datenkataloge den Grundsätzen der Datenvermeidung und Datensparsamkeit in adäquater Weise genügen.

Ferner wurde bestätigt, dass Verzicht auf den Personenbezug für die Verarbeitung der Daten im Rahmen der meisten Teilprozesse nicht möglich bzw. nicht zielführend ist. Der Einsatz von Pseudonymisierung kommt in vorbildlicher Weise hinsichtlich der personenbezogenen Daten der Mitarbeiter zur Geltung, welche während der Wahrnehmung ihrer Rollen in den

Bereichen Backoffice, Support und fachlicher Betrieb an dem *E-POSTBRIEF* System anfallen. Diese (Protokollierungs-)Daten werden unter Verwendung von kodierten Nutzerkennungen verarbeitet. Sie lassen keinen direkten Rückschluss auf die Identität der Mitarbeiter zu. Die Dekodierung einer Nutzerkennung ist im definierten Prozess nur bei Verdachtsfällen auf Missbrauch von Kundendaten erlaubt.

Pseudonym erfolgt des Weiteren die Abrechnung in der Billing-Komponente der von Nutzern in Anspruch genommenen Leistungen.

Die *E-POSTBRIEF* Adresse wird in personenbezogener Form vergeben. Eine pseudonyme Vergabe ist gemäß den AGB[2] nicht vorgesehen. Dies ist grundsätzlich mit dem für den *E-POSTBRIEF* einschlägigen Telekommunikationsgesetz vereinbar.

2. Zulässigkeit der Datenverarbeitung

Im Rahmen dieses Abschnitts wurde geprüft, ob die mit dem *E-POSTBRIEF* in Zusammenhang stehenden Verarbeitungsprozesse, die personenbezogene Daten der Nutzer oder Mitarbeiter zum Gegenstand haben, im Einklang mit dem geltenden Datenschutzrecht erfolgen, insbesondere, ob für die Verarbeitungen eindeutige und rechtmäßige Zwecke festgelegt wurden und ob entsprechende Ermächtigungsgrundlagen vorliegen.

An dieser Stelle wurde zuerst die Frage des Verantwortlichen i.S.v. § 3 Abs. 7 BDSG für die Datenverarbeitungen in Bezug auf den *E-POSTBRIEF* untersucht. Die Prüfung hat ergeben, dass zwischen dem Verantwortlichen für die Bereitstellung des Dienstes und dem Verantwortlichen für die Inanspruchnahme des Dienstes zu unterscheiden ist. Der Diensteanbieter (DPAG) verantwortet demnach die Verarbeitung der bei Bereitstellung und dem Betrieb des Dienstes anfallenden Daten, und der Nutzer verantwortet die übertragenen personenbezogenen Inhalte[3].

Des Weiteren wurde überprüft, ob die Zulässigkeit der Weitergabe der Daten an den Diensteanbieter von dem Abschluss entsprechender Vereinbarungen über die Auftragsdatenverarbeitung gemäß § 11 BDSG abhängt. Dies ist insbesondere im Hinblick auf den Regelungsinhalt des § 1 Abs. 2 Nr. 3 BDSG für die Geschäftskunden als *E-POSTBRIEF* Nutzer relevant. In die Bewertung ist die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit als der zuständigen Aufsichtsbehörde für die klassischen Postdienstleistungen eingeflossen. Danach wird die Verarbeitung der Daten im Auftrag nur dann angenommen, wenn die Datenverarbeitung auf den Auftragnehmer (hier: DPAG) übertragen wird, die inhaltliche Verantwortung für die Aufgabenerfüllung (hier: Erbringung der Postdienstleistung) aber beim Auftraggeber verbleibt. Die Aufgabenerfüllung liegt nicht bei dem Kunden, sondern bei der DPAG. Des Weiteren handelt es sich dabei um einen speziell regulierten Bereich, wo die gesetzlichen Rahmenbedingungen, inkl. der Verpflichtung der Mitarbeiter auf das Postgeheimnis, abschließend geregelt sind. Diese Auffassung, auf den *E-POSTBRIEF* übertragen, lässt die Annahme zu, dass eine Auftragsdaten-verarbeitung nur in dem Fall vorliegt, wenn die Anbindung des Geschäftskunden an das *E-POSTBRIEF* Portal über das Massenkommunikations-Gateway erfolgt, da der Nachrichtenversand durch den Kunden selbst, unter dem Einsatz des Schnittstellensystems, betrieben wird. Dieser Sachverhalt wird durch den Abschluss entsprechender Vereinbarungen nach § 11 BDSG mit den Geschäftskunden geregelt.
Die Ermächtigungsgrundlagen für die Datenverarbeitung im Rahmen des *E-POSTBRIEFs* wurden geprüft. Im Gesamtergebnis wurde eine adäquate Umsetzung der sich aus diesem

[2] Abrufbar unter: http://www.epost.de/privatkunden/footer/rechtliches/agb.html
[3] Vgl. Art. 29 Gruppe, WP169, S. 13.

Fragenkomplex ergebenden Anforderungen bestätigt. Insbesondere wurde die Einhaltung folgender Zulässigkeitsnormen bestätigt:

- § 95 Abs. 1 TKG für die Datenverarbeitung zum Zweck der Registrierung, Kontoeröffnung und Anmeldung am Portal,
- § 97 Abs. 2 und 3 TKG für die Abrechnung des Dienstes,
- § 109 TKG für die Umsetzung von technischen Maßnahmen zum Schutze des Fernmeldegeheimnisses und personenbezogener Daten als auch der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe und Störungen,
- §§ 110 ff. TKG für die Umsetzung der Überwachungsmaßnahmen und Einrichtung der Auskunftssysteme nach §§ 112 und 113 TKG,
- § 107 TKG für die Zwischenspeicherung von Nachrichteninhalten im Rahmen der Erbringung des Dienstes *E-POSTBRIEF,*
- § 14 Abs. 1 TMG für die Bereitstellung des Postfachs (Briefkastens) und des persönlichen Adressbuchs,
- § 100 TKG für den Zweck der Erkennung, Analyse und Beseitigung von Störungen des Systems,
- § 95 Abs. 1 TKG für die Zwecke der Qualitätssicherung und des internen Reportings über Performance und Prozessqualität,
- § 95 Abs. 1 TKG für den Zweck der Kundenunterstützung durch den Kundenservice,
- § 95 Abs. 1 TKG für das SLA-Reporting als Nachweis der Leistungserbringung aus dem Service Level Agreement,
- § 28 Abs. 1 Nr. 1 für die Datenverarbeitung im Rahmen der Gewinnspiele,
- Subsidiär die Vorschriften des Bundesdatenschutzgesetzes, insbesondere § 11 BDSG für den Einsatz von Auftragnehmern,
- § 95 Abs. 2 Satz 2 TKG für die Nutzung der *E-POSTBRIEFe* für die Zusendung des Newsletters.

Des Weiteren werden die *E-POSTBRIEFe* beim Eingang in das *E-POSTBRIEF* System vom Malware-Scanner geprüft. Bei einem positiven Befund wird die Annahme durch das System verweigert und dies dem Nutzer mitgeteilt. Eine Prüfung auf Malware erfolgt ebenfalls vor Übermittlung einer Nachricht an den Empfänger. Bei einem positiven Befund werden Absender und Empfänger informiert. Der Zugriff auf die Nachricht bzw. den Anhang, für die der positive Malware-Befund vorliegt, bedürfen einer expliziten Bestätigung durch den Nutzer. Lehnt er dies ab, werden weder der *E-POSTBRIEF* noch die Attachments zugestellt. Bei jedem Öffnen eines Attachments einer Nachricht wird dieses auf Malware geprüft.

Als die datenschutzrechtliche Ermächtigungsgrundlage für den Vorgang wurde § 88 Abs. 3 TKG angenommen. Die Erforderlichkeit des Scannens auf Malware ergibt sich aus der Konzeption des Dienstes als einer sicheren elektronischen Kommunikationsplattform. Für den *E-POSTBRIEF* gelten per se höhere Sicherheitsanforderungen als für die herkömmliche Internetkommunikation, womit aufgrund des automatisierten Zugriffs auf die Nachrichten-Inhalte die Notwendigkeit einhergeht, den Nutzer vor Malware zu schützen.

3. Technisch-organisatorische Maßnahmen

In diesem Komplex wurden insbesondere die technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes untersucht, speziell, ob die getroffenen Maßnahmen angemessen sind.

Die sicherheitstechnischen Anforderungen an das System sind durch geeignete Maßnahmen adäquat erfüllt.

Neben der Prüfung von Dokumenten wurde die Umsetzung der Maßnahmen durch eine sicherheitstechnische Untersuchung geprüft. Voraussetzung zur Planung und Durchführung der sicherheitstechnischen Untersuchung war die Vorlage eines aktuellen Netzplans, passend zu dem zu zertifizierenden produktiven Release. Zentraler Bestandteil und Startpunkt war eine Konfigurations-Analyse, in der mit Hilfe von Tools jeder Server eines Clusters (mehr als 400 Server) überprüft wurde. Dies wurde effektiv durch die Verwendung von entsprechenden Skripten automatisiert durchgeführt.
Bei der stichprobenhaften Überprüfung der Maßnahmen wurden unter anderem die Methoden Interviews, Begehungen, Konfigurations-Analysen, Port-Scans, Penetrationstests, Sourcecode-Analysen und Schwachstellen-Scans eingesetzt.
Als Evidenzen wurden vielfach die Ergebnisse von Tests oder Analysen verwendet, welche von der DPAG oder in deren Auftrag durchgeführt wurden und von den Gutachtern überprüft wurden.

4. Rechte der Betroffenen

Im Rahmen dieses Abschnitts wurde überprüft, wie die im Datenschutzrecht dem Betroffenen gewährten unabdingbaren Rechte auf Auskunft, Berichtigung und Löschung im *E-POSTBRIEF* umgesetzt wurden. Ferner wurden die spezifischen Aufklärungspflichten begutachtet.

Die Ergebnisse der Begutachtung bestätigen die vorbildliche Einhaltung der Betroffenenrechte. Dem Nutzer wird im *E-POSTBRIEF* Portal die Möglichkeit der Einsichtnahme und der Selbstverwaltung von Daten eröffnet. Änderungen bestimmter Daten erfordern jedoch eine erneute Überprüfung im Postident-Verfahren, um das Identitätssicherheitsniveau im *E-POSTBRIEF* Portal aufrechtzuerhalten.

Des Weiteren wurden entsprechende Prozesse zur Bearbeitung von Anliegen zum Datenschutz eingerichtet, die über eine speziell definierte Schnittstelle aus dem Kundenbetreuungssystem regelmäßig zur Bearbeitung an die zuständige Datenschutzabteilung übergeben werden.
Ferner wurde im Rahmen der Begutachtung die adäquate Erfüllung von Informations- und Aufklärungspflichten, die sich für die DPAG als Betreiber des *E-POSTBRIEFs* insbesondere aus § 93 TKG ergeben, bestätigt. Den Transparenzanforderungen hinsichtlich der Angabe von grundlegenden Informationen über Art, Umfang, Ort und Zweck der Erhebung und Verwendung von personenbezogenen Daten wird in Form von *Datenschutzhinweisen für die Nutzung des E-POSTBRIEF* Portals nachgegangen. Diese werden in einer verständlichen und übersichtlichen Form verfasst und als ein separates Dokument im Rahmen der AGB zur Verfügung gestellt. Auf die Hinweise wird von jeder Unterseite des Portals aus verlinkt und sie werden bei Vertragsschluss – während der Registrierung – durch den Nutzer zur Kenntnis genommen und akzeptiert.

Sofern das Produkt einen Teil der Anforderungen nur unzureichend erfüllt: Beschreibung, wie dies ausgeglichen wird

Nicht zutreffend

Beschreibung, wie das IT-Produkt den Datenschutz fördert

1. **Nutzerfreundliche Selbstverwaltung der Daten.** Dem Nutzer wurde die Möglichkeit einer einfach handhabbaren Selbstverwaltung im *E-POSTBRIEF* Portal eröffnet, indem alle ihn betreffenden personenbezogenen Account-Daten von ihm gepflegt werden können (Einschränkungen ergeben sich aus der Verifikationspflicht bestimmter Daten).
2. **Pseudonymisierung.** Die Verarbeitung der personenbezogenen Service-Mitarbeiterdaten, die bei Betrieb und Service des *E-POSTBRIEF* Systems anfallen, erfolgt in pseudonymisierter Form.
3. **Datenvermeidung und Datensparsamkeit.** Der im Rahmen des *E-POSTBRIEFs* verarbeitete Datenumfang wird auf das erforderliche Minimum eingeschränkt.
4. **Unterstützung bei der Erstellung der Datenschutzdokumentation nach DSVO und bei der Durchführung der Vorabkontrollen durch die behördlichen und betrieblichen Datenschutzbeauftragten**. Für die öffentlichen Stellen des Landes Schleswig-Holstein und die sonstigen Nutzer, die den *E-POSTBRIEF* über das Massenkommunikations-Gateway nutzen und somit dem Auftragsdatenverarbeitungs-verhältnis unterliegen, können weitere Informationen zur Verfügung gestellt werden.
5. **Transparenz.** Dem Nutzer wird eine vollständige und verständliche Information bezüglich der grundlegenden Datenverarbeitungen im Rahmen des *E-POSTBRIEF* Portals bereitgestellt. Durch eine Überschriftenstruktur kann er vereinfacht zu den für ihn relevanten Inhalten gelangen. Im Ergebnis des Zertifizierungsverfahrens und der geführten Gespräche wurden weitere Maßnahmen festgelegt, um die Transparenz des Dienstes und die Nutzerfreundlichkeit zu optimieren. Im Rahmen der kommenden AGB-Aktualisierung (2. Quartal 2012) werden folgende Zusatzangaben bzw. Präzisierungen in die *Datenschutzhinweise für die Nutzung des E-Postbrief Portals* aufgenommen:

- Die Angabe bezüglich der Aufbewahrung der Protokollierungsdaten (Logging, Auditing, Reports) über den Zeitraum von 35 Tagen, die zu den Zwecken der Erkennung, Analyse und Beseitigung von Störungen des Systems, der Qualitätssicherung und des internen Reportings über Performance und Prozessqualität, SLA-Reportings für die Nutzer, Nutzerunterstützung durch den Kundenservice verarbeitet werden.
- Die Ziff. IV 2.5 und III 2.5 der AGB werden folgende Formulierung erhalten: Es wird darauf hingewiesen, dass Daten, die in dem Nutzerkonto gelöscht wurden, ggf. zunächst nur gesperrt und dann erst mit zeitlicher Verzögerung von in der Regel mehreren Minuten endgültig gelöscht werden, um versehentlichen Löschungen oder evtl. vorsätzlichen Schädigungen vorzubeugen. Aus technischen und rechtlichen Gründen (vgl. gesetzliche Datenspeicherungspflichten) werden Daten ggf. in Datensicherungsdateien und Spiegelungen von Services dupliziert. Solche Kopien werden ggf. erst mit einer zeitlichen Verzögerung von maximal 28 Tagen gelöscht.
- In die Ziff. IV 2.4 und III 2.4 der AGB wird die Angabe über die 6-monatige Speicherungsfrist für die abrechnungsrelevanten Verkehrsdaten aufgenommen und damit die aktuelle Information hinsichtlich der Löschung dieser Daten nach Ablauf der gesetzlichen Fristen präzisiert.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Essen, 24.02.2012

Ort, Datum Unterschriften der Sachverständigen