



Die Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

**Andrea Voßhoff**

Bundesbeauftragte für den Datenschutz  
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,  
Postfach 1468, 53004 Bonn

Posteo e.K.  
Herrn Patrik Lühr  
Methfesselstraße 38  
10965 Berlin-Kreuzberg

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn  
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) [REDACTED]  
TELEFAX (0228) [REDACTED]  
E-E-MAIL [REDACTED]@bfdi.bund.de

INTERNET [www.datenschutz.bund.de](http://www.datenschutz.bund.de)

DATUM Bonn, 30.12.2016

GESCHÄFTSZ. [REDACTED]

Bitte geben Sie das vorstehende Geschäftszeichen bei  
allen Antwortschreiben unbedingt an.

BETREFF **Beratungs- und Kontrollbesuch E-Mail Posteo**  
HIER **Bericht**

Sehr geehrter Herr Lühr,

am 24. November haben meine Mitarbeiter [REDACTED] und [REDACTED]  
[REDACTED] einen Beratungs- und Kontrollbesuch gemäß § 115 Abs. 4 Tele-  
kommunikationsgesetz (TKG) i.V.m. §§ 24 Abs. 1, 26 Abs. 3 Bundesdatenschutzge-  
setz (BDSG) durchgeführt.

Gegenstand des Besuches waren datenschutzrechtliche Fragen bei der Verarbeitung  
von Verkehrsdaten (§§ 96 bis 97 und 99 bis 101 TKG) und Inhalten (§ 107 TKG) im  
Umfeld des Posteo-E-Mail-Angebots. Betrachtet wurden Dauer und Zweck der Spei-  
cherung sowie die Realisierung des Spam- und Virenschutzes sowohl bei eingehenden  
als auch bei ausgehenden E-Mails und die Erkennung von Störungen.

Für die besonders freundliche und offene Zusammenarbeit im Rahmen der Vorberei-  
tung und der Durchführung des Beratungs- und Kontrollbesuchs möchte ich mich  
bedanken. Die Ergebnisse fasse ich wie folgt zusammen:

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn  
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße



## 1. Datenschutz

Posteo ist ein Unternehmen mit weniger als 20 Mitarbeitern, das werbefreie, gebührenpflichtige Postfächer anbietet. Der Datenschutzbeauftragte (DSB) erfüllt die Vorgaben des § 4 BDSG. Seine weitere Tätigkeit im Support erlaubt ihm, datenschutzbezogene Anfragen von Nutzern direkt zu beantworten. Datenschutzaufgaben werden von ihm vorrangig behandelt. Die Mitarbeiter werden aufgabenbezogen vom Datenschutzbeauftragten regelmäßig in Datenschutzfragen unterwiesen.

Hier möchte ich besonders anerkennen, dass Posteo trotz seiner geringen Größe die Rolle des Datenschutzbeauftragten personell nicht mit anderen teilweise potentiell konfliktbehafteten Rollen vereinigt.

## 2. Bestandsdaten

In der Regel werden von Diensteanbietern bei der Einrichtung eines Kundenkontos Bestandsdaten für die inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben.

Posteo kann dagegen einen E-Mail-Dienst anbieten und betreiben, ohne auf Bestandsdaten zurückgreifen zu müssen, obwohl grundsätzlich nur gebührenpflichtige Konten möglich sind. Nach Einrichtung eines Kontos kann ein Kunde von seinem 14-tägigen Widerrufsrecht Gebrauch machen. Auch die Kündigungsfrist beträgt 14 Tage. Die Gebühren richten sich ausschließlich nach dem bestellten Festplatzspeicher und hinzubuchbaren Optionen. Im Rahmen des Registrierungsvorgangs sind nur Benutzername und Passwort, beide frei wählbar, notwendig. Nur wenn der Kunde in dieser Zeit sein Konto auflädt, bleibt es bestehen.

Es gibt mehrere Bezahl-Möglichkeiten: per Überweisung, per PayPal, per Kreditkarte, direkt im Laden oder per Post. Die Bezahl-daten werden nicht mit den E-Mail-Postfächern verknüpft, sondern getrennt gespeichert. Hierfür hat Posteo bereits 2009 ein eigenes System zur Anonymisierung der Zahlungsvorgänge entwickelt, das in 2015 den neuen gesetzlichen Vorgaben zur länderspezifischen Mehrwertsteuer angepasst wurde.

Der anonyme Zahlungsvorgang nutzt einen Einmal-Code, der zur temporären Zuordnung von Postfach und der Zahlung generiert wird. Ein Kunde stößt einen Bezahlvorgang an und erhält einen achtstelligen Einmal-Code per E-Mail. Im Posteo-System werden jedoch nur die ersten 5 Zeichen des Einmal-Codes gespeichert. Tref-



SEITE 3 VON 8

fen die Überweisung oder das Bargeld ein, werden die ersten 5 Zeichen des Einmal-Codes ausgewertet und dem Postfach zugeordnet. Die Zuordnung zwischen Finanzkonto und E-Mail-Konto findet nur während einer flüchtigen Millisekunde auf dem verarbeitenden Server statt, es erfolgt keine dauerhafte Speicherung der Zuordnung.

Die letzten 3 Zeichen des Einmal-Codes chiffrieren die Landesbestimmung und dienen dazu, die abzuführende Umsatzsteuer für das jeweilige EU-Land zu berechnen. Die ersten 5 Zeichen bilden mit Hilfe eines mathematischen Verfahrens eine Checksumme über die letzten drei Zeichen, um Manipulationen der Landesbestimmungen auszuschließen. Passen die letzten 3 Zeichen mathematisch nicht zu den ersten 5 Zeichen, ist ein Zahlungscode „kaputt“ - und die Zahlung wird zurückgesendet. Die Landeskodierungen werden ebenfalls nicht gespeichert. Damit wird vermieden, dass bis zum Abschluss der Zahlung das E-Mailpostfach einem Land zugeordnet werden kann. Dadurch kann auch das Land, in dem ein Kunde lebt, als Bestandsdatum im Rahmen einer Bestandsdatenabfrage bei Posteo nicht abgefragt werden.

Zahlungen über ein Paypal-Konto oder mittels Kreditkarte werden direkt nach dem Start des Bezahlvorgangs abgeschlossen. Der Einmal-Code ist in diesen Fällen nicht notwendig. Die Informationen zur Landesbestimmung werden umgehend ausgewertet und auch nicht temporär gespeichert. Auch bei Paypal- und Kreditkartenzahlungen werden die Landeskennungen nicht mit den Postfächern verknüpft.

Mit dem Abschließen der Registrierung wird das Kundenkonto eingerichtet, Passwörter können in den Einstellungen im Postfach geändert werden. Ein Kunde kann in den Konto-Einstellungen zusätzliche Dienste aktivieren, wie die Verschlüsselung des Adressbuchs und des Kalenders. Er kann seinen Kontostand einsehen, den Speicherplatz anpassen, den Posteo-Newsletter bestellen bzw. kündigen. Dieses Vorgehen entspricht der Regelung in § 95 Abs. 2 TKG.

Kunden können einen Umzugsservice beantragen, dabei werden die vom Kunden ausgewählten E-Mailpostfächer automatisch zu Posteo umgezogen. Posteo berücksichtigt ausschließlich Anbieter, auf deren Server ein Zugriff verschlüsselt möglich ist. Dabei bieten alle größeren E-Mail-Dienste-Anbieter TSL-Verschlüsselung an, während kleinere oder ausländische Anbieter hier noch nicht so weit sind.

Befürchtet ein Kunde, dass er sein Passwort vergisst, kann er seine Handynummer zur Legitimation und Ausstellung eines neuen Passwortes hinterlegen. Diese wird mittels einer Hashfunktion verschlüsselt gespeichert. Die Besonderheit der Verschlüsselung kleiner Wertebereiche wie Telefonnummern wird dabei berücksichtigt. So wird jedem Kunden ein individueller 128 Bit langer Salt zugeordnet und zusammen mit dem Postfach auf den Server gespeichert. Wählt ein Kunde die Funktion



SEITE 4 VON 8

„Handynummer hinterlegen“ an, wird ein kleines Programm in den Browser geladen, das die Handynummer lokal auf dem Kundenrechner mit dem individuellen Salt in mehreren Iterationen hasht und nur den Hashwert auf dem Posteo-Server hinterlegt. D.h., obwohl Posteo die Hasfunktion und den Salt kennt, ist selbst für Posteo eine Brute-Force Attacke ohne immensen, auch finanziellen Aufwand nicht möglich und müsste zudem für jeden Kunden individuell durchgeführt werden. Angriffe mittels Rainbow-Tabelle lassen sich ausschließen.

Posteo hat ein Gutachten in Auftrag gegeben zu der Frage, ob es sich bei dem persistent gespeicherten gesalteten Hashwert um ein Bestandsdatum im Sinne des § 95 TKG handelt. Dieses Gutachten liegt mit vor. Auch aus meiner Sicht ist der gespeicherte gesaltete Hashwert kein personenbeziehbares Datum.

Nutzer, die über einen Browser auf ihr Postfach zugreifen, können zusätzlich eine Zwei-Faktor-Authentifizierung einrichten und erhöhen damit die Sicherheit des Zugriffs auf das Postfach. Der erste Faktor ist wie bisher das Passwort, der zweite ist ein Einmal-Passwort, das sich alle 30 Sekunden ändert. Es wird von einem zusätzlichen Endgerät, z.B. dem Handy, mit einem speziellen Programm (App) berechnet. Gelangt das reguläre Passwort in die Hände von Dritten, haben diese keine Möglichkeit, über das Webinterface auf das Kundenkonto zuzugreifen.

Wenn das Posteo-Postfach nicht mehr aufgeladen ist, erhalten die Nutzer regelmäßige Erinnerungen.

Da keine Werbung erfolgt, muss keine Werbeeinwilligung im Sinne von § 95 Abs. 2 TKG eingeholt werden.

Das Posteo-Postfach ist monatlich mit einer Kündigungsfrist von 14 Tagen kündbar. 14 Tage nach dem Kündigungstermin wird das Postfach gelöscht.

Zusammenfassend stelle ich fest, dass Posteo im Sinne des § 95 TKG keine Bestandsdaten erhebt.

### 3. Verkehrsdaten

Auf eine genauere Darstellung der für die Erbringung des Dienstes erforderlichen Systeme kann hier verzichtet werden, da es sich im Aufbau nicht grundlegend von





einem Standard-E-Mailsystem mit Firewall, E-Mail-Exchange-Server und Proxy unterscheidet.

Auf verschiedenen Systemen werden Log-Daten generiert. Es werden nur die IP-Adressen der kontaktierenden E-Mailserver anderer Anbieter protokolliert, sowie der Zustellstatus einer E-Mail. IP-Adressen von Kunden sind in den internen Systemen von Posteo nicht verfügbar und können daher auch nicht gespeichert werden. Innerhalb der Posteo-Server werden ausschließliche interne IP-Adressen verwendet, d.h. kein interner Server sieht eine externe IP-Adresse.

Die Logdaten werden u.a. vom Support genutzt, um Kundenanfragen zu beantworten, die eine E-Mail vermissen. Anfragen, die sich auf Kommunikationsvorgänge beziehen, die älter als 7 Tage sind, gibt es nur sehr selten.

Ausgehende E-Mails von Nutzern werden nicht geloggt, da der Absender selbst ein Feedback erhält, falls die E-Mail nicht zugestellt werden konnte.

Zur **Störungserkennung** werden zwei Faktoren ankommender und ausgehender E-Mail genutzt:

[REDACTED]

Gem. § 109 TKG ist der Anbieter verpflichtet, die Sicherheit seiner Systeme zu gewährleisten. Es findet eine klassische Missbrauchs-, Spam- und Virenprüfung statt.

Um einen **Missbrauch** der E-Mail-Postfächer, insbesondere für den Versand von Spam, zu verhindern bzw. zu begrenzen, wird die Anzahl der Adressaten pro Tag limitiert (Rate-Limiting). Neue Kunden, die noch keine Gebühren überwiesen haben, unterliegen dabei größeren Versand-Einschränkungen. Positiver Nebeneffekt ist die Glättung des E-Mail-Aufkommens und damit die gleichmäßige Auslastung der Server auch bei starkem Newsletter-Aufkommen. Weiterhin werden Beschwerden zu Spam-E-Mails durch das Abuse-Team bearbeitet und ggf. Postfächer von Spammern gesperrt.

Im Zuge der Eingangsprüfung wird eine E-Mail auf syntaktische Korrektheit und gegen eine Blacklist mit bekannten Spammern geprüft. Posteo bezieht dazu in regelmäßigen, kurzen Abständen Blacklists verschiedener Anbieter, speichert diese lokal und prüft lokal auf den eigenen Servern gegen die Blacklists ab. Somit muss keine E-Mail von Posteo aus an einen weiteren Dienste-Anbieter übermittelt werden. Weiter wird die E-Mail auf bekannte technische Muster des Inhalts geprüft, [REDACTED]



Bei negativer Prüfung wird die E-Mail abgelehnt, bei positiver Prüfung wird die E-Mail angenommen, dem Absender wird der entsprechende Status zurückgemeldet.

Zur Virenschutzprüfung wird ein lokal implementiertes Opensource-Programm eingesetzt.

Bei der Nutzung des Web-Interface zum Zugriff auf das E-E-Mail-Konto werden zu Beginn der Eingabe der E-Mail-Adresse Vorschläge für Adressen gemacht. Hierbei wird ausschließlich auf die im Adressbuch gespeicherten Adressen zurückgegriffen.

Zusammenfassend stelle ich fest, dass Posteo keine auf Kunden beziehbare IP-Adressen und damit keine Verkehrsdaten nach § 96 TKG zur Dienstleistung benötigt und speichert. Auch zur Entgeltermittlung werden keine Verkehrsdaten benötigt (§ 97 TKG). Die Daten zur Störungserkennung nach § 100 TKG werden für maximal 7 Tage gespeichert. Dies halte ich für den maximal vertretbaren Zeitraum. Die Maßnahmen sind zur Missbrauchs-, Spam- und Virenerkennung geeignet und angemessen.

#### **4. Speicherdauer der E-E-Mails**

Die Speicherdauer der E-Mail ist grundsätzlich durch den Kunden und dessen Postfachgröße bestimmt.

Verschiebt ein Kunde E-Mail in den Papierkorb, so verbleibt sie dort, bis der Kunde den Papierkorb löscht. Ob eine aus dem Papierkorb gelöschte E-Mail über das 7 Tage Backup wiederherstellbar ist, hängt von verschiedensten Faktoren ab. Je nach Abrufprotokoll (IMAP oder POP3) oder Hardware verbleibt von der abgerufenen E-Mail keine Kopie auf dem Server. Wird eine neu eingetroffene E-Mail vor dem nächsten Backup abgerufen und verbleibt keine Kopie zurück, oder wird die E-Mail aus dem Papierkorb direkt gelöscht, so kann die E-Mail auch nicht wieder hergestellt werden. Der Wiederherstellungsservice wird von den Kunden nachgefragt.

Das BackUp liegt im elementaren Geschäftsinteresse von Posteo.

Das BackUp-Verfahren und der Wiederherstellungsservice sind angemessen.



## **5. Verschlüsselung**

Jeder Nutzer kann eine TLS-Versand-Garantie einschalten. Diese stellt sicher, dass die E-Mail über eine sichere, verschlüsselte Verbindung gesendet wird. Dazu versucht Posteo vor jedem E-Mailversand, eine verschlüsselte Verbindung mit anderen E-Mailservern aufzubauen. Die E-Mail wird nur ausgeliefert, wenn sie sicher an den Empfänger gesendet werden kann. Ist ein sicherer Versand nicht möglich, wird die E-Mail nicht versendet und Posteo benachrichtigt den Absender per E-Mail.

Gegen physischen Diebstahl sind alle Festplatten verschlüsselt, wobei Posteo im Besitz dieses Schlüssels ist.

Zusätzlich kann der Nutzer den Posteo-Krypto-E-Mailspeicher nutzen, um seine E-Mail mit einem eigenen Schlüssel zu verschlüsseln.

Posteo unterstützt zusätzlich die Ende-zu-Ende-Verschlüsselung basierend auf PGP und S/MIME.

Eine E-Mail kann also dreimal unabhängig voneinander verschlüsselt sein.

## **6. Datenschutzbestimmungen**

In den Datenschutzbestimmungen sind alle Informationen zum E-Mail-Dienst enthalten. Die Hinweise zum Datenschutz sind – wie das Impressum – auf den Posteo-Webseiten zu finden, nicht direkt aus dem Postfach heraus. Dies betrachte ich als ausreichend, da Nutzer verschiedene E-Mail-Interfaces nutzen können. Zusätzlich stellt Posteo ausführliche Hintergrundinformationen zum Datenschutz bereit, in dem z.B. die Datensparsamkeit, -sicherheit und der Vorteil der Werbefreiheit erläutert wird.

Unter den Hilfe-Seiten im Postfach finden sich ausführliche Informationen zu einzelnen Datenschutz- und Sicherheitsthemen. Hierzu zählen Themen rund um die Verschlüsselung und aktuelle Sicherheitsthemen.

## **7. Bestandsdatenauskunft nach § 113 TKG**

Wie im Posteo-Transparenzbericht veröffentlicht, hatten Sie in der Vergangenheit datenschutzrechtliche Mängel auch bei Anfragen aus dem Bereich der Bundespolizei



SEITE 8 VON 8

festgestellt. Hierzu hatte ich die Behörden, die meiner Aufsicht unterliegen, angeschrieben; erfreulicherweise konnten Sie eine deutliche Verbesserung beobachten.

Gleichzeitig haben Sie mir von einem Formular der Bundespolizei berichtet, bei dem Sie das datenschutzkonforme Erfragen einer IP-Adressen-Auskunft prüfen lassen möchten. Sie haben mir die Übermittlung des Formulars, bereinigt um die personenbezogenen Daten, zugesagt. In Anschluss an die Prüfung werde ich Sie vom Ergebnis unaufgefordert verständigen.

Ergänzend haben Sie mir berichtet, dass [REDACTED]

[REDACTED]  
[REDACTED] Bitte informieren Sie mich über das Ergebnis.

## 8. Zusammenfassung

Posteo berücksichtigt den Grundsatz der Datensparsamkeit sehr umfassend. Obwohl die Konten gebührenpflichtig sind, hat Posteo einen Weg gefunden, keine Bestandsdaten erheben zu müssen.

Die Gewährleistung der Sicherheit der Systeme nach § 109 TKG ist ohne Erhebung von personenbeziehbaren Verkehrsdaten sicher gestellt.

Bitte übermitteln Sie mir das Formular der Bundespolizei. (Abschnitt 7)

Bitte informieren Sie mich über den Ausgang [REDACTED]  
[REDACTED]

Ich darf Sie bitten, mir Ihre Stellungnahme zu meinem Bericht innerhalb von sechs Wochen zukommen zu lassen.

Mit freundlichen Grüßen  
[REDACTED]