

Transparenzbericht 2014

Willkommen zum Posteo-Transparenzbericht 2014.

Wir möchten, dass Sie wissen, wie häufig Behörden bei Posteo um Kundendaten ersuchen. In diesem Bericht legen wir offen, wie oft Ermittlungsbehörden und Nachrichtendienste sich im Jahr 2014 an uns gewandt haben - und wie oft Posteo tatsächlich Daten herausgeben musste. Der Bericht umfasst alle Behördenanfragen, die Posteo im Jahr 2014 erhalten hat. Sie erfahren außerdem, wie häufig diese Ersuchen formal korrekt waren und wie viele der Anfragen rechtswidrig waren.

Inhalte:

Behördenanfragen bei Posteo (01/2014-12/2014)	Seite 3
Unhaltbare Zustände bei der manuellen Bestandsdatenauskunft	Seite 5
Mangelhafte öffentliche Kontrolle der Auskunftsverfahren	Seite 13
Richtervorbehalt: Offenbar werden alle Anträge bewilligt	Seite 17
Hintergrundinformationen und häufige Fragen	Seite 23

Originaldokumente:

Beispiele rechtswidriger Behördenersuchen	Anhang I
Antworten der Datenschutzbeauftragten zu rechtswidrigen Behördenersuchen	Anhang II
Antworten der Datenschutzbeauftragten zu Kontrollen von Ersuchen nach § 112 TKG .	Anhang III
Antworten der Justizministerien zum Richtervorbehalt	Anhang IV

Posteo veröffentlicht Ersuchen

Da fast alle Behördenersuchen, die Posteo bisher erreicht haben, nicht den gesetzlichen Bestimmungen entsprachen, widmen wir den Auskunftsverfahren einen Schwerpunkt in unserem diesjährigen Bericht. In diesem üben wir Kritik an den chaotischen Zuständen, die insbesondere bei der Bestandsdatenauskunft nach § 113 TKG herrschen. Wir zeigen auf, dass in der Auskunftspraxis gravierende Sicherheitsprobleme bestehen, es regelmäßig zu Rechtsbrüchen kommt und Kontrolldefizite die Situation weiter verschlimmern.

Wir belegen unsere Kritik u.a. mit unserer eigenen Fall-Dokumentation - und veröffentlichen Beispiele rechtswidriger Behördenersuchen. Außerdem veröffentlichen wir unseren Schriftwechsel mit der Bundesdatenschutzbeauftragten, den Landesdatenschutzbeauftragten sowie den Justizministerien der Länder. Sie erhalten so einen Einblick in unsere datenschutzorientierte Arbeit, die bei Posteo ganzjährig stattfindet.

Außerdem beschäftigen wir uns mit dem Kontrollinstrument des Richtervorbehaltes, der unserer Auffassung nach seiner zugeordneten Aufgabe nicht mehr gerecht wird. In der Praxis werden offenbar alle Anträge auf Überwachungsmaßnahmen bewilligt. Obwohl zur Wirksamkeit des Richtervorbehaltes keine Statistiken geführt werden, haben wir Zahlen gefunden, die dies belegen. Und wir erläutern, warum die von uns dargelegten Mängel aufzeigen, warum die Vorratsdatenspeicherung auf keinen Fall wieder eingeführt werden darf.

Unsere Ziele

Im vergangenen Mai hatte Posteo als erster deutscher Telekommunikationsanbieter einen Transparenzbericht veröffentlicht ¹. Zuvor hatten wir mit einem Rechtsgutachten die Zulässigkeit eines solchen Berichtes klären lassen. Mit unserem Vorstoß haben wir erreicht, dass inzwischen auch andere deutsche Anbieter Transparenzberichte veröffentlichen - unter ihnen auch die Deutsche Telekom. Mit unserem diesjährigen Transparenzbericht möchten wir dazu beitragen, dass bestehende Missstände und Rechtswirklichkeiten öffentlich bekannt werden und über sie debattiert werden kann.

Und wir wollen, dass sich etwas ändert: Obwohl die Bundesregierung bereits vor Jahren über einige der Missstände informiert wurde, hat sich die Situation offenbar nicht verbessert. Die demokratische Kontrolle staatlicher Auskunftsverfahren und Überwachungsmaßnahmen in Deutschland muss deshalb gestärkt werden. Hierfür geben wir in unserem Transparenzbericht Anregungen. Zum Beispiel fordern wir eine bessere Ausstattung der Kontrollorgane.

Antworten auf häufige Fragen zu den rechtlichen Grundlagen und Verfahren sowie zum Umgang von Posteo mit Behördenanfragen finden Sie im Bereich „Hintergrundinformationen & Häufige Fragen“.

¹ https://posteo.de/site/transparenzbericht_2013

Auskunftsersuchen 2014:

Vorbemerkung: Posteo verfügt aufgrund eines konsequenten Datensparsamkeitskonzeptes weder über personenbezogene Daten seiner Kunden (Bestandsdaten wie Namen und Adressen), noch über deren dynamische IP-Adressen. Wird Posteo mit einem richterlichen Beschluss dazu verpflichtet, Kundendaten herauszugeben, können den Behörden deshalb lediglich Inhaltsdaten (z.B. E-Mails) übermittelt werden.

Anzahl der Ersuchen	
insgesamt:	22
davon deutsche Behörden:	22
davon ausländische Behörden:	0

Art der Behörde	
Strafverfolgungsbehörden:	22
Nachrichtendienste:	0

Art des Ersuchens	
Bestandsdatenersuchen:	17
Postfachbeschlagnahmen:	1
Verkehrsdatenersuchen:	2
TKÜ (Überwachung eines Postfachs für einen bestimmten Zeitraum):	2

KORREKTHEIT

Zulässigkeit/formale Korrektheit der Ersuchen (Prüfung durch unsere Anwälte)	
Formal korrekte Bestandsdatenersuchen:	2
Formal nicht korrekte Bestandsdatenersuchen:	15
Formal korrekte Beschlagnahme:	1
Formal korrekte TKÜ:	2
Formal korrekte Verkehrsdatenersuchen:	2

ANZAHL DER HERAUSGABEN

Herausgabe von Bestandsdaten: Begründung: Daten nicht vorhanden/anonyme Anmeldung	0
Herausgabe von Bestandsdaten zu vorliegenden Bezahlungen: Begründung: Daten nicht vorhanden/anonyme Bezahlung	0
Herausgabe von Verkehrsdaten: Begründung: Daten (IP-Adressen) nicht vorhanden/betrieblich nicht benötigt	0
Anzahl betroffener Postfächer bei Herausgabe von Inhaltsdaten nach Postfachbeschlagnahme, laufende Übermittlung von Daten nach TKÜ: Begründung: formal korrekter richterlicher Beschluss	2

BESCHWERDEN DURCH POSTEO BEI LANDESDATENSCHUTZBEAUFTRAGTEN

Begründung: rechtswidriges, unsicheres Übermitteln der Behördenersuchen; rechtswidriges Ersuchen nach Verkehrsdaten	15
Zwischenzeitlich durch Posteo abgebrochene TKÜ Begründung: Originalbeschluss nicht fristgerecht an Posteo gesandt	1

Rechtsstaat außer Kontrolle: Unhaltbare Zustände bei der manuellen Bestandsdatenauskunft nach § 113 TKG

Deutsche Politiker argumentieren aktuell gerne, die Risiken beim Datensammeln gingen nicht vom Staat aus, sondern vielmehr von internationalen Konzernen wie Apple, Google und Facebook. Es sei gar besorgniserregend, dass solchen Konzernen mehr vertraut werde als dem Staat. Dem stimmen wir so keineswegs zu. Nicht nur, weil Internetkonzerne massiv in den Ausbau von Verschlüsselungstechnologien investieren, seit Edward Snowden bekannt machte, dass Nachrichtendienste das Internet flächendeckend überwachen. In unserer Eigenschaft als deutsches Telekommunikationsunternehmen können wir belegen, dass öffentliche Stellen im Rahmen von Auskunftersuchen häufig auf eine Art und Weise mit sensiblen Daten umgehen, die ein Sicherheitsrisiko darstellt, rechtswidrig ist und sogar laufende Ermittlungen gefährden kann.

1. Massive Sicherheitsprobleme in der Praxis der Auskunftersuchen nach § 113 TKG

In der Praxis des Auskunftsverfahrens nach § 113 TKG liegen gravierende Sicherheitsprobleme vor, wie wir im Folgenden zeigen. Ersuchen um Bestandsdaten nach § 113 TKG enthalten sensible personenbezogene Informationen. Meist erhalten wir von den Polizeibehörden E-Mail-Adressen oder Namen, die in Verbindung mit einem konkreten Tatvorwurf genannt werden. Manchmal enthalten die Ersuchen sogar vollständige Konto- bzw. Zahlungsdaten einer Person. Posteo erhält regelmäßig solche Bestandsdatenabfragen.

Nun ist es so, dass auch Ermittlungsbehörden u.a. durch das BDSG gesetzlich dazu verpflichtet sind,

„zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.“ (BDSG, Anlage, Satz 4)

Rechtswidrige, unsichere Übertragung sensibler Daten

Die meisten Ersuchen nach § 113 TKG erreichen uns per E-Mail. Und ausnahmslos alle Ersuchen, die wir bisher auf diesem Wege erhalten haben, sind uns durch die Behörden unsicher bzw. unverschlüsselt übermittelt worden. Dieses Vorgehen verstößt gegen die geltenden Datenschutzbestimmungen und ist rechtswidrig. (Siehe u.a. BDSG § 9, Anlage, Satz 4 und 8 sowie die jeweiligen Regelungen zu den „technisch-organisatorischen Maßnahmen“ der Landesdatenschutzgesetze).

Die meisten Ersuchen nach § 113 TKG weisen darüber hinaus weitere Mängel auf, die ebenfalls Verstöße gegen datenschutzrechtliche Bestimmungen oder andere Gesetze darstellen. Dazu zählen:

- Zusenden polizeilicher Ersuchen an den Kunden-Support - und nicht an die zuständigen Personen (Anti-Abuse-Team).
- Verwenden nicht-dienstlicher E-Mail-Postfächer zum Übermitteln von Ersuchen, Angabe solcher Postfächer als Antwortmöglichkeit
- Ersuchen um Informationen und Daten, deren Herausgabe im Rahmen von Abfragen nach § 113 TKG nicht zulässig ist, z.B. um Verkehrsdaten wie IP-Adressen oder um Aktenzeichen anderer Behörden, die ggf. bereits nach dem Postfach gefragt hatten
- fehlende Angabe einer sicheren Antwortmöglichkeit
- fehlende Angabe der Rechtsgrundlage der Abfrage (gesetzlich vorgeschrieben)

Datenschützern ist das Problem bekannt

Die meisten Anfragen nach § 113 TKG erreichen uns auf diese Weise (per unverschlüsselter E-Mail). Der Faxweg wird von den Behörden selten genutzt, auf dem Postweg hat uns bisher nur eine einzige Anfrage erreicht. Gelegentlich erreichen uns per E-Mail auch Ersuchen mit einem unverschlüsselten Dokument im Anhang, das fälschlicherweise als „Telefax-Nachricht“ überschrieben ist. Wir haben uns im Januar

Betreff: Auskunftersuchen/ EILT
Von: [REDACTED]@online.de>
Datum: [REDACTED]
An: support@posteo.de

Sehr geehrte Damen und Herren,

Hier vorliegend Strafanzeige [REDACTED]

zur weiteren Bearbeitung ist es erforderlich die Bestandsdaten bekannt zu machen zum Postach:

[REDACTED]

Wann wurde das Postfach angelegt, mit welcher IP? Wer ist der Inhaber/ Nutzer? Gibt es derzeit weitere Anfragen durch Ermittlungsbehörden (event. Aktenzeichen dieser)?

Aktenzeichen der STA [REDACTED]

mfg

[REDACTED]

E-Mail (Internet): [REDACTED]@polmv.de oder [REDACTED]@online.de

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte

- Verwenden einer nicht-dienstlichen E-Mail-Adresse
 - unzulässige, unsichere Übertragung (unverschlüsselt)

- unzulässiges Zusenden des Ersuchens an den allgemeinen Kunden-Support

- unrechtmäßiges Ersuchen um eine IP-Adresse sowie um Informationen zu evtl. Anfragen anderer Behörden

- fehlende Angabe der Rechtsgrundlage (gesetzlich vorgeschrieben)

- Angabe der nicht-dienstlichen E-Mail-Adresse in der Kontaktsignatur des Beamten

Beispiel für unsicher übermittelte Behördenersuchen (Originaldokumente in Anhang I)

2015 bei den jeweils zuständigen Landesdatenschutzbeauftragten über die unsichere Übertragung sensibler Daten durch Polizeibehörden beschwert. Die Antworten der Datenschützer waren eindeutig: Das Problem der unsicheren Übermittlung sensibler Daten durch Polizeibehörden ist bekannt und immer wieder Anlass für Gespräche und Kontrollen. Die Antworten belegen, dass das unsichere Versenden sensibler Informationen durch Polizeibehörden ein Thema ist, bei dem dringender Handlungsbedarf besteht.

So schrieb uns der nordrhein-westfälische Datenschutzbeauftragte:

„Gegenüber dem Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen (MIK NRW) habe ich wiederholt darauf hingewiesen, dass Anfragen in Ermittlungsverfahren grundsätzlich auf dem Postweg bzw. in begründeten Fällen auch per Fax erfolgen sollten. Wenn im Ausnahmefall eine Anfrage per E-Mail erforderlich sein sollte, so müsste entweder die Nachricht selbst verschlüsselt werden oder zumindest die Übermittlung personenbezogener Daten müsste in einem verschlüsselten Dateianhang erfolgen. Ihre Anfrage werde ich zum Anlass nehmen, diese Thematik nochmals gegenüber dem MIK NRW aufzugreifen und auf eine datenschutzgerechte Ausgestaltung der polizeilichen Ermittlungen hinzuwirken.“

Vollständige Antwort: Siehe Anhang II, Seite 5

Und der bayerische Landesdatenschutzgeber teilte uns mit:

„Nachdem die Übermittlung von personenbezogenen Daten in unverschlüsselten E-Mails durch sonstige Behörden oder durch die Polizei immer wieder Anlass für datenschutzrechtliche Überprüfungen gibt, habe ich mich mit diesem Thema bereits mehrmals in meinen Tätigkeitsberichten befasst. (...) Zudem kann ich Ihnen versichern, dass ich dieses Thema auch unabhängig von meinen konkreten Kontrollen mit den zuständigen Stellen der Polizei regelmäßig erörtere. So stehe ich derzeit mit dem Bayerischen Landeskriminalamt in Kontakt, um die Ausgestaltung des dort betriebenen Abrufverfahrens bei Telekommunikationsdiensten zu überprüfen.“

Vollständige Antwort: Siehe Anhang II, Seite 3

Der mecklenburgische Datenschutzbeauftragte wurde ebenfalls aktiv:

„Ich habe die betreffende Dienststelle kontaktiert und sie auf ihre Umsetzung von datenschutzrechtlichen Maßnahmen hingewiesen, damit Sie in Zukunft Anfragen nach § 113 TKG auf sicherem Wege erreichen und die Rechte des Betroffenen damit nicht verletzt werden. Ebenfalls habe ich das Ministerium für Inneres und Sport Mecklenburg-Vorpommern auf diesen Missstand aufmerksam gemacht. Das Ministerium (...) versicherte mir, die Beamtinnen und Beamten hinsichtlich des richtigen Umgangs mit personenbezogenen Daten und des Umgangs mit TKÜ-Abfragen nach § 113 TKG erneut zu sensibilisieren.“

Vollständige Antwort: Siehe Anhang II, Seite 4

Und der sächsische Datenschutzbeauftragte setzte dem Landespolizeipräsidenten gar ein Ultimatum:

„Wir unterstützen Ihr Anliegen unbedingt. Ich habe deshalb mit heutiger Post den Landespolizeipräsidenten mit der Bitte um Abhilfe angeschrieben und ihn gebeten, bis zum 15.04.2015 mitzuteilen, welche Abhilfemaßnahmen er ergriffen hat.“

Vollständige Antwort: Siehe Anhang II, Seite 6

Die Antworten der Landesdatenschützer an uns belegen, dass die unverschlüsselten Ersuchen ein dort bekanntes Problem sind. Wenn es gängige Praxis sein sollte, dass Polizeibehörden sensible Daten, zum Beispiel im Rahmen von Ersuchen nach § 113 TKG, unverschlüsselt durch das Internet senden, ist dies nicht nur ein Problem aus Datenschutzsicht: Es ist auch rechtswidrig, verletzt die Rechte des Betroffenen und gefährdet möglicherweise laufende Ermittlungen.

In einigen Fällen erleben wir die Bürokratie als sehr schwerfällig. So antwortete uns der Berliner Datenschutzbeauftragte nach fünf Monaten zu einem Fall zurück:

„Leider konnte die Angelegenheit bislang noch nicht abschließend geklärt werden.“

Einige Monate zuvor hatte er uns bereits schriftlich mitgeteilt, dass er die Polizei um Informationen zu allgemeinen Vorgaben zu Auskunftersuchen bzw. zur Versendung personenbezogener Daten gebeten habe.

Fazit: Wir nehmen an, dass insgesamt und flächendeckend Sicherheitsprobleme in der Praxis der manuellen Bestandsdatenauskunft (nach § 113 TKG) bestehen. Bei Posteo ist zumindest per E-Mail noch kein einziges Ersuchen von Polizeibehörden eingegangen, das verschlüsselt gewesen wäre und somit den gesetzlichen Anforderungen an die sichere Übermittlung entsprochen hätte.

Und die Antworten der Datenschützer haben uns bestätigt, dass nicht nur wir betroffen sind.

Die vollständigen Antworten der Landesdatenschutzbeauftragten zu rechtswidrigen Behördenersuchen finden Sie im Anhang II.

Beschwerden führen nicht zu Abhilfe

Wir freuen uns, dass unser Nachhaken in verschiedenen Fällen dazu geführt hat, dass Beamte noch einmal auf die Rechtslage hingewiesen und hinsichtlich des richtigen Umgangs mit personenbezogenen Daten sensibilisiert wurden. Leider haben unsere Beschwerden bisher aber nicht zu einer Abhilfe geführt. Uns wurden auch im Laufe dieses Jahres weiterhin alle Ersuchen, die per E-Mail eingingen, unsicher übermittelt. Auch aus Bundesländern, deren Landesdatenschutzbeauftragte sich besonders engagiert gezeigt hatten. Wir fragen uns deshalb, wie Abhilfe geschaffen werden kann. Wenn Beamte nicht ausreichend auf den sicheren Umgang mit sensiblen Daten und IT-Technik geschult sind, stellt dies ein grundlegendes Sicherheitsproblem in der Polizeiarbeit dar.

Eigeninitiative Beschwerden wie die durch Posteo und die mit ihnen einhergehenden Gespräche und Kontrollen stellen unserer Meinung nach eher die sprichwörtlichen Tropfen auf den heißen Stein dar.

Zu einer flächendeckenden und zeitnahen Abhilfe tragen sie unserer Erfahrung nach nicht bei. Wir werden uns dennoch auch weiterhin über jedes einzelne umverschlüsselt übermittelte Ersuchen bei den Landesdatenschützern beschweren.

Wir sehen die Sicherheit des Verfahrens in der Praxis derzeit nicht gewährleistet. Wir möchten es deshalb nun auch auf anderem Wege versuchen und haben inzwischen die Politik eingeschaltet. Es ist schließlich nicht Aufgabe der Provider, das rechtsstaatliche Handeln der Behörden zu überprüfen oder darauf hinzuwirken. Das muss der Staat selbst leisten und sicherstellen. Anfang Juli haben wir dem Vorsitzenden der SPD-Fraktion, Thomas Oppermann, bei einem Termin im Posteo Lab eine Stellungnahme, u.a. zum unsicheren Versenden sensibler Daten durch Polizeibehörden, übergeben.

2. Unzulässige Ersuchen nach dynamischen IP-Adressen

Um in das nächste Problemfeld einzuführen, das wir in der Praxis von Abfragen nach § 113 TKG sehen, bleiben wir gleich in der Politik: Im Januar 2013 wandte sich der SPD-Abgeordnete Burkhard Lischka mit einer schriftlichen Anfrage an die Bundesregierung. Er fragte, ob der Bundesregierung bekannt sei,

„dass in der Praxis zahllose auf § 113 des Telekommunikationsgesetzes (TKG) gestützte Auskunftersuchen die Herausgabe von Daten zum Gegenstand haben, die keine Bestandsdaten sind (z. B. Log Files, dynamische IP-Adressen, ...)“.

Anfrage an die Bundesregierung (ab Seite 7, Fragen 12, 13 und 14) ¹

Und er fügte hinzu:

„Wenn ja, welche Behörden betreiben diese rechtswidrige Praxis, und was unternimmt die Bundesregierung, um dies abzustellen?“

Der Hintergrund seiner Anfrage: Einige Monate zuvor hatte der Bundesverband der Informationswirtschaft, BITKOM, in einer Stellungnahme an den Rechtsausschuss des Deutschen Bundestages wie folgt auf Missstände bei der Bestandsdatenauskunft aufmerksam gemacht:

„In der Praxis sind zahllose, auf § 113 TKG gestützte Auskunftersuchen bekannt, die die Herausgabe von Daten zum Gegenstand haben, die gerade keine Bestandsdaten sind (z.B. log-files, IP-Adressen, Datum und Uhrzeit des letzten Zugriffs auf einen Account, bekannte E-Mail-Adressen des Betroffenen bei anderen Providern, Identität der Behörden, die bereits nach denselben Bestandsdaten gefragt haben, etc..). Daraus folgt, dass die Anbieter bereits heute mit zahlreichen Anfragen umzugehen haben, die der Ausforschung dienen und weit über den Regelungsgehalt der Norm hinausgehen.“

Stellungnahme des BITKOM vom 17.10.2012 ²

Zur Erklärung: Der BITKOM hatte beanstandet, dass Behörden im Rahmen von Bestandsdatenabfragen (nach § 113 TKG) häufig nach Daten ersuchen, deren Herausgabe bei solchen Abfragen überhaupt nicht rechtmäßig ist. Behörden dürfen bei Abfragen nach § 113 TKG, für die kein Richtervorbehalt existiert, nämlich ausschliesslich um Bestandsdaten ersuchen - also etwa um Namen und Adressen. Nicht aber nach dynamischen IP-Adressen oder Logfiles; diese hochsensiblen Verkehrsdaten unterliegen dem Fernmeldegeheimnis und dürfen nur auf Anordnung eines Richters herausgegeben werden.

In ihrer Antwort vom 28.01.2013 wies die Bundesregierung die Aussagen des BITKOM als „Behauptungen“ zurück:

„Der Bundesregierung sind – abgesehen von der in der Fragestellung zitierten Behauptung in der Stellungnahme des BITKOM – keine derartigen Vorwürfe bekannt.“

Antwort der Bundesregierung (ab Seite 7, Fragen 12, 13 und 14) ³

¹ <http://dip21.bundestag.de/dip21/btd/17/122/1712239.pdf>

² https://www.bitkom.org/Lost-Found/20121015_bitkom_stellungnahme_neuregelung_bestandsdatenauskunft_pdf.pdf

³ <http://dip21.bundestag.de/dip21/btd/17/122/1712239.pdf>

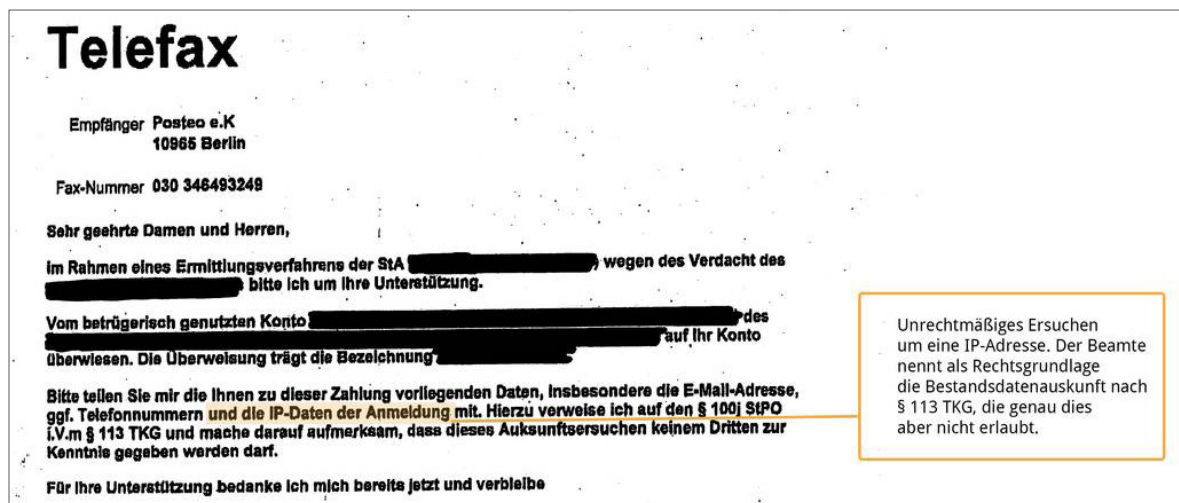
Die Bundesregierung habe die vom BITKOM erhobenen Vorwürfe allerdings zum Anlass genommen, verschiedene Ermittlungsbehörden hierzu zu befragen. Und sie konstatierte:

„Die Ergebnisse der Abfrage haben keine Anhaltspunkte für rechtswidrige Anfragen ergeben.“

Behörden ersuchen rechtswidrig um dynamische IP-Adressen

Wir bestätigen hiermit die „Behauptungen“ des BITKOM: In ca. 30% aller Ersuchen von Polizeibehörden, die uns 2014 im Rahmen von Bestandsdatenabfragen nach § 113 TKG erreichten, fragten Polizeibeamte rechtswidrig nach dynamischen IP-Adressen der Anmeldungen bzw. nach der IP-Adresse des letzten Logins. Dies ist im Rahmen von Abfragen nach § 113 TKG unzulässig.

Um zu belegen, dass dies dennoch (und entgegen der Aussage der Bundesregierung) durchaus Praxis ist, veröffentlichen wir hier Beispiele solcher rechtswidriger Ersuchen (geschwärzt): Die Originale liegen bei Posteo schriftlich vor. In ihnen wird auch deutlich, dass Beamte nicht nur rechtswidrig um die Herausgabe von IP-Adressen ersuchen, sondern sogar gelegentlich verlangen, diese gesondert für ihre Ermittlungen zu erheben und zu speichern. Dies ist ebenfalls nicht zulässig.



Beispiel für unzulässige Behördenersuchen um IP-Adressen (Originaldokumente in Anhang I)

Wir finden es erstaunlich, dass die Bundesregierung sich im Januar 2013 offenbar nicht über den BITKOM an die Unternehmen gewandt hat, denen solche rechtswidrigen Anfragen schriftlich vorliegen. Die Bundesregierung hätte sich unserer Ansicht nach bei den Unternehmen informieren und ggf. geeignete Abhilfemaßnahmen treffen müssen. Dass sie dies unterlassen hat, obwohl sie von einem großen deutschen Branchenverband über rechtswidrige Praktiken von Behörden informiert wurde, ist für uns völlig unverständlich. Stattdessen wurden offenbar lediglich Behörden befragt und die Aussagen des Hightechverbandes wurden als Behauptungen bezeichnet. Wenn Hinweise auf rechtswidrige Praktiken der Exekutive bestehen, sollte diesen in einem Rechtsstaat ernsthafter nachgegangen werden.

Bundesregierung nun erneut befragt

Der Bundestagsabgeordnete Dieter Janecek (der wirtschaftspolitische Sprecher der Fraktion der Grünen), hat die Bundesregierung ganz aktuell erneut zu diesem Thema befragt und wollte wissen, ob sie bei ihrer Einschätzung bleibt. In seiner Frage verwies der Abgeordnete auf die Stellungnahme des BITKOM sowie auf den Posteo-Transparenzbericht 2013. Die Antwort der Bundesregierung ist am Mittwoch, den 19.08.2015, eingegangen.

Das Bundesinnenministerium erklärte:

„Der Bundesregierung liegen weiterhin keine Anhaltspunkte für rechtswidrige Anfragen vor.“ Und es fügte hinzu: „Üblicherweise unterrichten die zuständigen Datenschutzkontrollinstanzen auch die obersten Bundesbehörden über von ihnen festgestellte Verstöße gegen Datenschutzbestimmungen. Darüber hinausgehender Verfahren bedarf es nach Ansicht der Bundesregierung nicht.“

Antwort der Bundesregierung vom 19.08.2015 ⁴

Datenschützer reagierten auf Beschwerden zur IP-Adressen-Problematik nicht

Wir haben uns in allen Fällen, in denen Polizeibeamte unrechtmäßig nach IP-Adressen ersuchten, bei den jeweiligen Landesdatenschutzbeauftragten beschwert. In ihren Antworten ging keiner der Datenschützer auf unsere diesbezüglichen Beschwerden ein. Offenbar wurden unsere Beschwerden auch nicht an die „obersten Bundesbehörden“ weitergegeben, wie es nach Aussage des BMI sonst üblich sein soll. Es handelt sich bei rechtswidrigen Ersuchen um IP-Adressen aber auch nicht um „Verstöße gegen Datenschutzbestimmungen“. Das Ersuchen um IP-Adressen bei Bestandsdatenauskünften ist nach dem Telekommunikationsgesetz (TKG) rechtswidrig. Betroffen sind nicht nur Landespolizeibehörden, von Ermittlungsbehörden des Bundes haben wir zwar weniger Ersuchen erhalten, aber hier waren alle Ersuchen rechtswidrig.

Unser Fazit: Die Bundesregierung interessiert es offenbar überhaupt nicht, ob bei der Bestandsdatenauskunft rechtswidrige Praktiken bestehen. Das Bundesinnenministerium bleibt seit Jahren untätig. Da durch solche Anfragen die Rechte von Bürgerinnen und Bürgern regelmäßig verletzt werden, ist dies unserer Ansicht nach verantwortungslos.

Auseinandersetzungen wegen IP-Adressen-Problematik

Gerade in Fällen, in denen im Rahmen von Abfragen nach § 113 TKG bei Posteo rechtswidrig um Verkehrsdaten ersucht wurde, ist es in der Folge des öfteren zu Situationen gekommen, in denen wir uns unter Druck gesetzt und bedroht sahen. Wir gehen stets so vor, dass wir die Beamten auf die geltende Rechtslage verweisen. Wir weisen sie darauf hin, dass wir uns mit dem Herausgeben von Verkehrsdaten bei Abfragen nach § 113 TKG strafbar machen würden (siehe § 206 StGB) und für die Herausgabe von Verkehrsdaten ein richterlicher Beschluss vorliegen muss. Wir erläutern den Beamten, dass sie im Rahmen einer Abfrage nach § 113 TKG nur anhand einer IP-Adresse, die ihnen bereits bekannt ist, nach Bestandsdaten ersuchen dürfen. Dass die umgekehrte Auskunft nicht zulässig ist, ist Beamten häufig nicht bekannt.

Einige reagieren auf diese Information verwundert bis aufgebracht. Uns gegenüber haben Beamte bereits wiederholt behauptet, bei anderen Verpflichteten problemlos auch im Rahmen von Abfragen nach § 113 TKG IP-Adressen zu erhalten. Ob dies zutrifft oder wir nur verunsichert werden sollten, wissen wir nicht. Was wir aber belegen können: Polizeibeamte ersuchen bei Abfragen nach § 113 TKG regelmäßig und mit einer großen Selbstverständlichkeit schriftlich um Verkehrsdaten (siehe Originaldokumente in Anhang I). Deshalb halten wir es für durchaus möglich, dass die Rechtsvorschriften in der Auskunftspraxis auch von den Verpflichteten (z.B. von Unternehmen) nicht immer beachtet werden.

Ein möglicher Grund hierfür könnte der sein, dass der Kreis der zur Auskunft nach § 113 TKG Verpflichteten sehr groß ist - und nicht auf Telekommunikationsanbieter beschränkt. Viele der Verpflichteten verfügen ggf. nicht über die notwendigen Rechtskenntnisse, um rechtswidrige Abfragen korrekt als solche identifizieren zu können.

Folge: Hohe Anwaltskosten

Unserem Unternehmen sind durch eskalierte, unrechtmäßige Forderungen nach IP-Adressen bereits wiederholt enorme Anwaltskosten und insgesamt ein finanzieller Schaden im mittleren fünfstelligen Bereich entstanden. Zum Beispiel, um „Schutzschriften“ bei Gerichten zu hinterlegen, für die Korres-

⁴ https://posteo.de/transparency_report/Antwort_Bundesregierung_20150819.pdf

pondenz mit Ermittlungsbeamten, Rechtsberatung etc.. In einem Fall haben wir Ermittlungsbeamte, die uns sogar persönlich aufgesucht hatten, angezeigt. Die Staatsanwaltschaft gab unseren Anzeigen allerdings keine Folge - wie unsere Anwälte uns schon vorab in Aussicht gestellt hatten. Sie erklärte, unsere Anzeige sei schlichtweg falsch und stellte das Verfahren gegen die Beamten ohne weitere Ermittlungen gegen diese ein. Stattdessen beantragte sie einen Strafbefehl wegen „falscher Verdächtigung“, den das Gericht auch erlassen hat. Der Geschäftsführer von Posteo, Patrik Löhr, wurde zur Zahlung einer Geldstrafe verpflichtet. Den hohen Anwaltskosten steht gegenüber, dass wir theoretisch für jede Bestandsdatenabfrage nach § 113 TKG achtzehn Euro ⁵ vom Staat für unseren Aufwand zurückerhalten könnten. Von dieser Möglichkeit machen wir jedoch keinen Gebrauch. Wir nehmen als datenschutzorientiertes Unternehmen grundsätzlich kein Geld von Behörden für Abfragen von Kundendaten an.

Abfragen nach § 113 TKG werden mit Wiedereinführung der Vorratsdaten- speicherung an Bedeutung gewinnen

Wir haben aufgezeigt, dass die Sicherheit des Verfahrens derzeit nicht gewährleistet ist und dass Behörden bei Abfragen nach § 113 TKG bei Posteo regelmäßig rechtswidrig um Verkehrsdaten wie dynamische IP-Adressen ersuchen. Außerdem haben wir dargelegt, dass das Problem der unsicheren Übermittlung den Landesdatenschutzbeauftragten bekannt ist. Des weiteren haben wir darauf hingewiesen, dass der Branchenverband BITKOM die Bundesregierung bereits 2012 auf zahllose rechtswidrige Ersuchen bei Abfragen nach § 113 TKG aufmerksam gemacht hatte.

Angesichts der Verfahrensmängel möchten wir hiermit mit Nachdruck darauf aufmerksam machen, dass das Verfahren nach § 113 TKG mit der geplanten Wiedereinführung der Vorratsdatenspeicherung („Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“) an Bedeutung gewinnen wird. Das geplante Gesetz wird eine starke Vergrößerung der für die Bestandsdatenauskunft zur Verfügung stehenden Datenmengen bewirken.

Eine begehrte Auskunft: Mit Abfragen nach § 113 TKG werden Internetnutzer identifiziert

Berechtigte Stellen werden über das Verfahren künftig viel häufiger die Information erhalten können, welcher Person zu einem bestimmten Zeitpunkt eine dynamische IP-Adresse zugewiesen war. Ein Beispiel: Ein Beamter tritt mit einer IP-Adresse an einen Provider heran und möchte wissen, welche Person sich hinter der Adresse verbirgt. Der Provider gleicht die IP-Adresse mit den IP-Daten ab, die in seinen Datenbanken für die Vorratsdatenspeicherung vorgehalten werden. Dies ist dem Provider ohne richterlichen Beschluss erlaubt. Dem Beamten muss er dann mitteilen, welche Person hinter einer IP-Adresse steht (noch einmal: nicht umgekehrt). Eine sehr begehrte Auskunft, für deren Abfrage kein Richtervorbehalt vorgesehen ist und die bereits bei Ordnungswidrigkeiten eingeholt werden kann.

Wir gehen deshalb davon aus, dass sich die Anzahl der Abfragen nach § 113 TKG, und somit auch die Anzahl der unsicheren bzw. rechtswidrigen Abfragen, mit der Einführung des neuen Gesetzes stark erhöhen wird. Für diese Annahme gibt es einen weiteren Grund: Der Abgleich von IP-Daten und die anschließende Herausgabe von Bestandsdaten kann nur über das manuelle Auskunftsverfahren nach § 113 TKG erfolgen. Über das automatisierte Verfahren nach § 112 TKG ist dies nicht möglich.

Anzahl rechtswidriger Abfragen würde sich deutlich erhöhen

Wir sind der Ansicht, dass das Auskunftsverfahren nach § 113 TKG mit seinen derzeitigen offenkundigen Praxismängeln hierfür keinesfalls geeignet ist. Schon heute wird durch das Verfahren eine große Zahl sensibler Bürgerdaten unsicher übertragen und es kommt zu zahlreichen rechtswidrigen Abfragen durch Behörden.

Auch die Kontrolle des Verfahrens ist nicht ausreichend: Es existieren unseres Wissens nach aktuell nicht einmal Statistik-Pflichten für Abfragen nach § 113 TKG. Somit könnte nicht einmal evaluiert werden, wie sich die Einführung des Gesetzes zur Vorratsdatenspeicherung konkret auf die Anzahl der Abfragen auswirkt - und der Öffentlichkeit würde die Anzahl der Abfragen durch staatliche Stellen auch im Nachhinein nicht bekannt werden.

⁵ https://dejure.org/gesetze/JVEG/Anlage_3.html

Bundesregierung muss handeln: Von Einführung der Vorratsdatenspeicherung muss abgesehen werden

Es ist auf keinen Fall hinnehmbar, dass sensible Daten der Bürgerinnen und Bürger weiterhin durch Behörden ungesichert durch das Internet gesendet bzw. abgefragt werden oder dass dynamische IP-Adressen, die dem Fernmeldegeheimnis unterliegen, auf einfache Anfragen nach § 113 TKG ohne richterlichen Beschluss herausgegeben werden. Unserer Ansicht nach dürfen deshalb auch keine neuen Gesetze oder Richtlinien eingeführt werden, die die Anzahl der rechtswidrigen und unsicheren Ersuchen noch einmal erhöhen würden.

Unsere Forderung:

Deshalb fordern wir, dass die Bundesregierung schnellstmöglich Maßnahmen trifft, die dazu geeignet sind sicherzustellen, dass die Abfrage bzw. Übertragung von sensiblen Bürgerdaten durch Behörden nach § 113 TKG grundsätzlich auf einem sicheren Wege (keine proprietären Lösungen) und auch sonst gemäß der gesetzlichen Bestimmungen erfolgt – und wenn sie per E-Mail erfolgt, dann ausschliesslich per verschlüsselter E-Mail. Darüber hinaus fordern wir, dass die Bundesregierung schnellstmöglich Maßnahmen trifft, die sicherstellen, dass im Rahmen von Bestandsdatenabfragen nicht mehr rechtswidrig nach Verkehrsdaten ersucht wird oder um andere Informationen, die weit über den Regelungsgehalt der Norm hinausgehen.

Wir sind der Auffassung, dass hier offenkundiger Bedarf besteht, Prozesse insgesamt in organisatorischer Hinsicht dahingehend anzupassen, dass eine datenschutzgerechte und rechtsstaatkonforme Ausgestaltung des Auskunftsverfahrens in Zukunft sichergestellt werden kann. Hierfür schlagen wir unter anderem das Einführen von Berichtspflichten vor (siehe Abschnitt zur Kontrolle der Auskunftsverfahren).

Unsere Forderung:

Bis diesbezüglich Abhilfe geschaffen wurde, muss von der Wiedereinführung der Vorratsdatenspeicherung („Einführung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“) unserer Ansicht nach alleine schon aus dem Grunde abgesehen werden, dass sich die Anzahl der unsicheren und unzulässigen Datenübermittlungen und der Rechtsbrüche im Rahmen des Auskunftsverfahrens nach § 113 TKG durch die Einführung des Gesetzes noch weiter erhöhen würde.

Unabhängig davon lehnt Posteo die Wiedereinführung der Vorratsdatenspeicherung auch aus zahlreichen weiteren Gründen insgesamt und mit Nachdruck ab, wie z.B. aus Gründen des Datenschutzes und der Datensicherheit sowie aufgrund der mit ihr einhergehenden verdachtsunabhängigen Grundrechtseinschränkungen, die wir für nicht vertretbar halten. Bitte lesen Sie hierzu auch unsere Ausführungen zum Kontrollinstrument des Richtervorbehaltes, das wir in diesem Bericht ebenfalls kritisieren. Die bisherigen Pläne der Bundesregierung sehen zwar vor, E-Mailanbieter von der Vorratsdatenspeicherung auszunehmen. Die Gesetzes Einführung würde E-Mail-Anbieter wie Posteo im Rahmen von Abfragen nach § 113 TKG allerdings mit noch mehr rechtswidrigen Abfragen und den damit einhergehenden Bürokratie- und Anwaltskosten konfrontieren.

Unsere Forderung:

Desweiteren fordern wir, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) als unabhängige Bundesbehörde aus dem Geschäftsbereich des Bundesinnenministeriums (BMI) herausgelöst wird, damit das BSI ein unabhängiger Ansprechpartner in Sicherheitsfragen sein kann.

Mangelhafte öffentliche Kontrolle der Auskunftsverfahren nach § 113 und § 112 TKG

Dass in der Praxis von Auskunftsverfahren regelmäßig Kontrollen stattfinden, ist in einer Demokratie für ein ausgeglichenes Verhältnis zwischen Sicherheit und Freiheit unerlässlich. Durch sie kann einem Missbrauch der Verfahren vorgebeugt oder dieser zumindest im Nachhinein festgestellt werden. Unzulässigen Praktiken kann mit Kontrollen entgegengewirkt werden. Unserer Überzeugung nach weist auch die Kontrolle der Auskunftsverfahren nach § 113 TKG und § 112 TKG gravierende Defizite auf – wenn man denn überhaupt von Kontrolle sprechen kann.

Beispiel § 112 TKG: Millionen automatisierter Abfragen und nur eine Handvoll Kontrollen

Behörden können nicht nur im Rahmen der manuellen Bestandsdatenauskunft nach § 113 TKG um Bestandsdaten ersuchen. Es gibt auch das automatisierte Verfahren nach § 112 TKG, an dem ca. 150 größere Telekommunikationsunternehmen teilnehmen (bei Posteo kann nur nach § 113 TKG um Daten ersucht werden). In Deutschland werden auf diese Weise jährlich mehrere Millionen automatisierte Abfragen nach Bestandsdaten nach § 112 TKG getätigt. Im Jahr 2014 wurden insgesamt 6,92 Mio. Ersuchen bei der Bundesnetzagentur (BNetzA) gestellt, die zusammengekommen zu 34,30 Mio. Abfragen bei Telekommunikationsanbietern führten. Wir haben uns gefragt, wie viele Kontrollen diesen millionenfachen Abfragen durch Behörden eigentlich gegenüberstehen. Deshalb haben wir die zuständigen Stellen angeschrieben.

Aus den Antworten der Datenschutzbeauftragten geht hervor, dass in den vergangenen Jahren offenbar nur eine Handvoll der Abfragen durch die BNetzA und die Bundesdatenschutzbeauftragte (BfDI) kontrolliert wurden. Und das auch meist nur nach konkreten Hinweisen auf Innentäter, die aus den Polizeibehörden selbst gemeldet wurden.

Die Bundesdatenschutzbeauftragte teilte uns hierzu schriftlich mit:

„In den letzten Jahren gab es nur wenige Anfragen zu Auskünften nach § 112 TKG, meist von Polizeibehörden. Diese Fälle wurden zusammen mit der BNetzA überprüft.“

Vollständige Antwort: Siehe Anhang III, Seite 2

Letzte Erwähnung von Kontrollen in zehn Jahre altem Tätigkeitsbericht

Um diese „wenigen Fälle“, die kontrolliert wurden, näher zu erläutern, verwies uns die BfDI allerdings lediglich auf die sehr alten Tätigkeitsberichte der Jahre 2001-2004. Mit dem Zusatz, dass „die durchaus noch aktuell sind“.

Im Bericht 2003-2004 ist konkret von drei Fällen die Rede:

„Während des Berichtszeitraums gab es nur wenige Anfragen von Polizeibehörden wegen des Verdachts auf unberechtigte Abfragen durch Innentäter. In drei Fällen konnten Daten zurückgemeldet werden, die zu einem Ermittlungsverfahren geführt haben.“

Siehe 20. Tätigkeitsbericht des BfDI 2003-2004, Seite 144 ff.¹

Ein Blick in die neueren Berichte zeigt: Kontrollen von Abfragen nach § 112 TKG werden in den Tätigkeitsberichten von 2005-2014 offenbar nicht mehr erwähnt. Ob nach 2004 also überhaupt noch Kontrollen durchgeführt wurden, ist deshalb für die Öffentlichkeit nicht feststellbar. Für uns ein sehr ernüchterndes Ergebnis.

Bevor wir dieses Ergebnis kannten, hatten wir schriftliche Anfragen an alle Landesdatenschutzbeauftragten gerichtet, um Zahlen für die Kontrollen aus den Jahren 2013 und 2014 zu erhalten. Denn

¹ http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/20TB_03_04.pdf?__blob=publicationFile

bei Abfragen nach § 112 TKG haben auch die Landesdatenschützer Kontrollbefugnisse, wenn es um Ersuchen von öffentlichen Stellen ihrer Länder geht. Auch hier Ernüchterung: Alle Datenschützer antworteten uns, dass sie keine Kontrollen von Abfragen nach § 112 TKG durchgeführt haben. Einige der Datenschützer wollen aber aufgrund unserer Anfrage künftig Kontrollen durchführen.

So schrieb uns der Hamburgische Datenschutzbeauftragte:

„Ihre Anfrage wird aber zum Anlass genommen noch in diesem Jahr eine datenschutzrechtliche Kontrolle bei den in § 112 Abs. 2 TKG bezeichneten Stellen durchzuführen.“

Vollständige Antwort: Siehe Anhang III, Seite 3

Und aus Rheinland-Pfalz erhielten wir die Zusage:

„Da im Land allerdings ein Kompetenz-Zentrum für Telekommunikationsüberwachungsmaßnahmen eingerichtet wurde, habe ich diesen Bereich ohnehin auf meinem Prüfplan für das laufende Jahr. In diesem Zusammenhang werde ich auch das Verfahren gem. § 112 TKG und konkret auf dieser Basis erfolgende Abrufe kontrollieren.“

Vollständige Antwort: Siehe Anhang III, Seite 7

Einige Datenschützer waren der Ansicht, sie seien nicht zuständig. Der Datenschutzbeauftragte aus Mecklenburg-Vorpommern wies uns auf ein weiteres Problem hin; die mangelhafte Ausstattung der Datenschutzbehörden:

„Aufgrund einer Vielzahl von Petitionen in verschiedenen Bereichen des Datenschutzes und der Informationsfreiheit ist es uns zeitlich und personell nicht möglich eigeninitiierte Prüfungen über Anfragen nach § 112 TKG vorzunehmen.“

Vollständige Antwort: Siehe Anhang III, Seite 5

Faktisch findet bei dem Verfahren nach § 112 TKG keine Kontrolle statt. Positiv bleibt lediglich zu bemerken, dass bei dem automatisierten Abfrageverfahren nach § 112 TKG immerhin Berichts- und Protokollpflichten bestehen, sodass zumindest in den Jahresberichten der BNetzA eingesehen werden kann, wie häufig das Verfahren von berechtigten Stellen in Anspruch genommen wird.

Die vollständigen Antworten der Landesdatenschutzbeauftragten zu Kontrollen von Auskunftersuchen nach § 112 TKG finden Sie im Anhang III.

Grauzone § 113 TKG: Keine Statistik-Daten verfügbar

Zu der Anzahl der Abfragen nach § 113 TKG liegen keine statistischen Erhebungen öffentlicher Stellen vor. Entsprechende Statistik-Pflichten sind unseren Anwälten nicht bekannt. Sofern Zahlen überhaupt bekannt werden, stammen diese aus den Transparenzberichten von deutschen Telekommunikationsanbietern, die es erst seit 2014 gibt, nachdem Posteo als erster deutscher Anbieter einen Transparenzbericht über Behördenersuchen veröffentlicht hatte. Im Bericht der Telekom für das Jahr 2014 sind 27.957 Ersuchen nach § 113 TKG aufgeführt. Beschwerden über Sicherheitsprobleme und rechtswidrige Abfragen bei den zuständigen Kontrollorganen führten bei den Ersuchen, die uns erreichen, bisher nicht zu einer Abhilfe, wie wir bereits in Teil 1 unseres Schwerpunktes dargelegt haben.

§ 113 TKG: Berichtspflichten zur Verbesserung der öffentlichen Kontrolle einführen

Das Verfahren stellt deshalb in gewisser Weise eine Grauzone dar. Das ist so in keinem Fall hinnehmbar, da es bei der Bestandsdatenauskunft nach § 113 TKG generell einer besseren Kontrolle und Evaluierung bedarf (siehe unser Abschnitt zu den chaotischen Zuständen bei der Bestandsdatenauskunft).

Unsere Forderung:

Unserer Auffassung nach sollten deshalb für Abfragen nach § 113 TKG umgehend Berichtspflichten eingeführt werden. Die Zahlen sollten jährlich veröffentlicht werden, wie es auch bei anderen Arten von Auskunftersuchen wie z.B. bei Abfragen nach § 112 TKG (Veröffentlichung im Jahresbericht der BnetzA) und bei Abfragen nach § 100a StPO (Veröffentlichung auf der Internetseite des Bundesamtes für Justiz) üblich ist.

Protokollierungspflichten sollten außerdem, ähnlich wie im automatisierten Verfahren nach § 112 TKG, sicherstellen, dass zu jeder Abfrage u.a. festgehalten wird, welcher Beamte um welche Daten ersucht hat, um etwaige interne und externe Kontrollen, zum Beispiel durch Datenschutzbeauftragte, im Nachhinein zu erleichtern.

Es ist zu erwarten, dass diese Kontrollmöglichkeiten Missbrauch und rechtswidrigen Abfragen entgegenwirken würden. In diesem Bereich sind Abhilfemaßnahmen dringend notwendig.

§ 113 TKG: Kontrollen ausweiten und Schulung von Ermittlungsbeamten intensivieren

Es ist unserer Ansicht nach darüber hinaus dringend erforderlich, dass die zuständigen Kontrollorgane die Einhaltung der gesetzlichen Anforderungen bei Ersuchen nach § 113 TKG regelmäßig und umfassend kontrollieren, bis die Mängel des Verfahrens flächendeckend beseitigt sind. Ermittlungsbeamte müssen außerdem umfassend auf einen sicheren und rechtskonformen Umgang mit Informationstechnik im Allgemeinen und mit sensiblen Daten im Besonderen geschult werden.

Datenschützer besser ausstatten

Abschließend möchten wir zu dem Thema der fehlenden Kontrollen auch auf den aktuellen Tätigkeitsbericht der Beauftragten für den Datenschutz und die Informationsfreiheit (BfDI) hinweisen.

In ihm warnt sie im Hinblick auf weitere Auskunftsverfahren, dass:

„das System der „Checks and Balances“ im Bereich der Nachrichtendienste in eine massive Schieflage geraten ist. So sind, insbesondere seit dem Jahr 2001, die Aufgaben und Befugnisse der Sicherheitsbehörden sowie deren Personal- und Sachmittel erheblich ausgebaut, die verbundübergreifende Zusammenarbeit von Polizeien und Nachrichtendiensten national und international intensiviert, zentrale Großdatenbanken errichtet und eine neue Sicherheitsstruktur geschaffen worden.(...) Auf Seiten der Kontrollorgane ist keine entsprechende Entwicklung erfolgt, d. h. auch insoweit bestehen gravierende gesetzgeberische Defizite, die im Interesse der Bürgerinnen und Bürger schnellstmöglich beseitigt werden müssen. In Folge dieser Entwicklung ist es mir angesichts der mir zur Verfügung stehenden geringfügigen Personal- und Sachmittel nicht mehr möglich, meine gesetzlich zugewiesenen Beratungs- und Kontrollaufgaben angemessen zu erfüllen. Damit ist es mir auch nicht mehr möglich, die vom Bundesverfassungsgericht in seinem Urteil zum Antiterrordateigesetz betonte Kompensationsfunktion meiner Kontrollen für die betroffenen Bürgerinnen und Bürger sachgerecht zu gewährleisten, d. h. an Stelle der Betroffenen zu überprüfen, ob ihre Rechte bei heimlichen Eingriffen der Sicherheitsbehörden gewahrt worden sind.“

Quelle: Tätigkeitsbericht der Bundesdatenschutzbeauftragten 2013 & 2014, S.36 ²

Diese Aussage ist ein Warnruf der Bundesdatenschutzbeauftragten. Wir sehen dringenden Bedarf, den Forderungen der BfDI dahingehend zu entsprechen, dass ihr schnellstmöglich mehr Personal- und Sachmittel zur Verfügung gestellt werden. Auch, damit sie auf eine sichere und rechtskonforme Praxis von Auskunftsvorgängen, wie z.B. bei Abfragen nach § 113 TKG, drängen und diese mit vermehrten Kontrollen flächendeckend bewirken kann. Dasselbe gilt für die Ausstattung der Landesdatenschutzbeauftragten. Die Kontrollorgane müssen insgesamt besser ausgestattet werden, damit bestehenden Missständen effektiv begegnet werden kann.

² http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf?__blob=publicationFile&v=9

Richtervorbehalt: In der Praxis werden offenbar alle Anträge auf Überwachungsmaßnahmen bewilligt.

Wenn es um Eingriffe in die Grundrechte von Bürgerinnen und Bürgern geht, werden Kritiker häufig mit dem Argument beruhigt, dass diese nur unter strengen Voraussetzungen und nur „mit Richtervorbehalt“ erfolgen dürften. Der Verweis auf den Richtervorbehalt ist ein beliebtes Argument: Denn das Vertrauen der Bürgerinnen und Bürger in die Justiz ist Umfragen zufolge wesentlich größer als das Vertrauen in die Bundesregierung. Auch aktuell wird wieder mit dem Richtervorbehalt argumentiert: Diesmal geht es um die geplante Wiedereinführung der Vorratsdatenspeicherung.

Dem Kontrollinstrument des Richtervorbehaltes wird jedoch schon seit vielen Jahren vorgeworfen, in der Praxis wenig effektiv zu sein. Zu diesem Schluss kamen zum Beispiel zwei groß angelegte Studien, die bereits 2003 von der Universität Bielefeld und dem Max-Planck-Institut für ausländisches und internationales Strafrecht veröffentlicht wurden. Beide Studien belegten damals zahlreiche Mängel des Verfahrens. Das MPI kam beispielsweise zu dem Schluss, dass nur in absoluten Ausnahmefällen einer beantragten Überwachungsmaßnahme nicht stattgegeben wurde.

Die Studie der Universität Bielefeld ¹ konstatierte damals, dass nur ein Viertel der Überwachungen entsprechend den Verfahrensvorschriften angeordnet worden sei. Darüber hinaus würden die Abhörmaßnahmen meist auf Anordnungen beruhen, die vermuten lassen, dass die Richter ihre Entscheidung nicht eigenständig treffen.

Und ein Staatsanwalt, der damals von den Wissenschaftlern des MPI befragt worden war, gab zum Thema E-Mail-Überwachung gar zu Protokoll:

„Im Bereich der E-Mail-Überwachung ist eine Aktualisierung und Klarstellung notwendig, da herrscht Chaos. Es gibt die irrsten Rechtsauffassungen und egal, welchen Antrag ich stelle, der Richter gibt dem in diesen Fällen statt.“

Quelle: Studie des Max-Planck-Institutes für ausländisches und internationales Strafrecht, S.226 ²

Auch wir setzen uns schon seit einiger Zeit mit der Frage auseinander, wie das vom Gesetzgeber bei Überwachungsmaßnahmen vorgesehene Kontrollinstrument des Richtervorbehaltes in Deutschland ausgestaltet ist – und wie seine Wirksamkeit kontrolliert bzw. evaluiert wird. Anlass für diese Auseinandersetzung war unter anderem eine angeordnete Telekommunikations-Überwachung (TKÜ), bei der sowohl wir als auch unsere Anwälte die angegebene Anlassstrafat für nicht ausreichend gehalten hatten. Übrigens: Wenn Sie denken, dass eine Überwachungsmaßnahme (TKÜ) Sie nicht betreffen könnte, weil Sie keine Straftaten begehen - das ist falsch. In der Praxis wird durchaus auch die Kommunikation von Menschen aus dem Umfeld eines Verdächtigen überwacht oder beschlagnahmt. Auch, wenn gegen diese Personen überhaupt kein Tatverdacht besteht.

1. Gesetzgeber evaluiert Wirksamkeit des Kontrollinstrumentes des Richtervorbehaltes nicht ausreichend

Wenn gegen einen Verdächtigen ermittelt wird und Polizeibeamte bei der Staatsanwaltschaft die Beschlagnahmung oder die Überwachung eines E-Mail-Postfaches anregen, ist der Rechtsschutz des Betroffenen durch die Heimlichkeit der Maßnahme stark eingeschränkt. Er kann vor der Entscheidung des zuständigen Ermittlungsrichters nicht angehört werden. Der Richter soll dieses Defizit ausgleichen: Er soll den Fall prüfen und nur wenn er zur Überzeugung gelangt, dass die Telekommunikation des Verdächtigen tatsächlich überwacht oder beschlagnahmt werden sollte, dem Antrag der Staatsanwaltschaft stattgeben. Die Information, wie oft ein Richter eine beantragte Überwachungsmaßnahme ablehnt, ist deshalb ein wichtiger Indikator dafür, wie wirksam das Kontrollinstrument des Richtervorbehaltes tatsächlich ist. Würden in einem Staat beispielsweise allen Anträgen auf Überwachung stattgegeben, wäre

¹ <http://www.spiegel.de/politik/deutschland/telefonueberwachungen-drei-viertel-aller-lauschangriffe-rechtswidrig-a-229958.html>

² http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/telekueberw/rechtswirklichkeit_%20abschlussbericht.pdf

dies ein starker Hinweis darauf, dass sich der Rechtsstaat auf dem Weg in einen Überwachungsstaat befindet.

Wie oft ein Richter einen Antrag auf Überwachung ablehnt, wird statistisch nicht erfasst

Wie oft ein Richter eine Überwachungsmaßnahme ablehnt, wird in Deutschland statistisch jedoch meist nicht erfasst. Im jährlichen Bericht des Bundesamtes der Justiz wird lediglich die Anzahl der erlassenen Beschlüsse aufgeführt, in denen Maßnahmen nach §100a Abs. 1 StPO angeordnet wurden, sowie die Anzahl der durchgeführten Überwachungsmaßnahmen (vgl. § 100b Abs. 5, 6 StPO). Die Länder müssen diese Zahlen an das Bundesamt der Justiz melden. Zahlen darüber, wie häufig einem Antrag auf eine Überwachungsmaßnahme durch einen Richter nicht entsprochen wurde, finden sich in der Statistik hingegen nicht. Der Richtervorbehalt ist also ein Kontrollinstrument, von dem tatsächlich weitgehend unbekannt ist, wie wirksam es ist.

Posteo befragte Justizministerien aller Länder

Wir wollten wissen, ob die entsprechenden Zahlen evtl. doch in den Bundesländern vorliegen. Deshalb haben wir Anfang des Jahres bei den Justizministerien der Länder schriftlich um Auskunft gebeten.

Zunächst fielen die Antworten enttäuschend aus. Wir erhielten immer wieder dieselben Rückmeldungen, in denen uns mitgeteilt wurde, dass keine Statistiken darüber geführt werden, wie häufig eine beantragte Überwachung nicht bewilligt wurde. Daher sei nicht bekannt, in wie vielen Fällen TKÜ-Anträge abgelehnt wurden. Dass die Zahl der abgelehnten Überwachungsanordnungen nicht erhoben werde, habe den Grund, dass hierfür in den Gesetzestexten keine Berichtspflichten existieren.

So erklärte uns unter anderem das bayerische Staatsministerium der Justiz:

„Die Berichtspflicht nach § 100b Abs. 5, Abs. 6 StPo sieht schlicht keine Pflicht zur Erfassung von abgelehnten Anträgen vor, weswegen dazu auch keine Statistik besteht.“

Und das hessische Justizministerium teilte uns mit, dies würde einen manuellen Auswertungsaufwand erfordern,

„der mir unverhältnismäßig erscheint und den Strafverfolgungsbehörden nicht zugemutet werden kann.“

Doch dann erhielten wir die Information, nach der wir gesucht hatten: Aus Berlin erhielten wir die Antwort, dass der Berliner Senat seit dem Jahr 2006 die Anzahl der abgelehnten Überwachungsmaßnahmen erfasst.

Und wir waren schockiert.

Die vollständigen Antworten der Justizministerien finden Sie im Anhang IV.

Nach 2007 wurde kein einziger Antrag auf Überwachung mehr abgelehnt

In Berlin ist nach dem Jahr 2007 kein einziger Antrag auf Telekommunikationsüberwachung mehr abgelehnt worden (siehe die jeweiligen Jahresberichte des Senats ³ über die Praxis der Telefonüberwachung nach §§ 100 a, 100 b StPO).

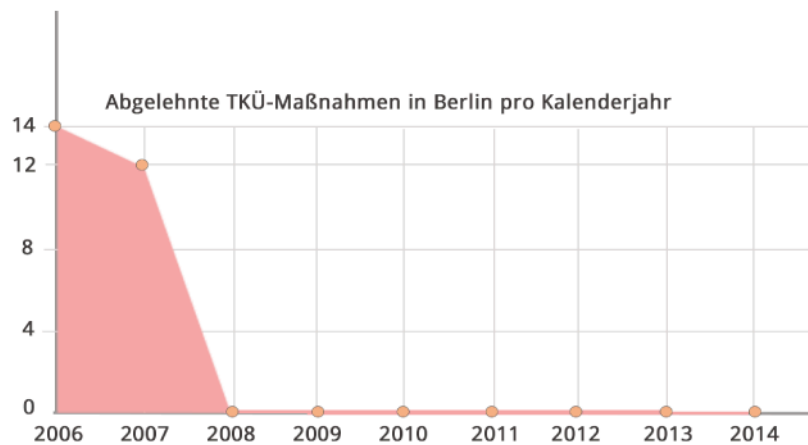
Insgesamt wurden zwischen 2008 und 2014 in Berlin 14.621 Anschlüsse überwacht. Die Anzahl der angeordneten Überwachungen stieg über die Jahre hinweg deutlich an.

Dass zwischen 2008 und 2014 bei 14.621 überwachten Anschlüssen (Festnetz, Mobilfunk und Internet) in Berlin kein einziger Antrag auf Überwachung abgelehnt wurde, verdeutlicht unserer Auffassung nach eindrücklich, dass Zweifel an der Wirksamkeit des Kontrollinstrumentes des Richtervorbehaltes nicht nur berechtigt sind, sondern dass auch Klärungsbedarf besteht. Wie kann es möglich sein, dass Richter über viele Jahre hinweg jedem einzelnen Antrag auf Überwachung einer Bürgerin oder eines Bürgers stattgeben? Was sagen diese Zahlen über den Zustand unseres Rechtsstaates aus? Die Zahlen aus Berlin

³ <http://pardok.parlament-berlin.de/starweb/AHAB/servlet.starweb?path=AHAB/lisshfl.web&id=ahabwebdokfl&format=WEB-VORGAFL&search=ID%3DV-262388>

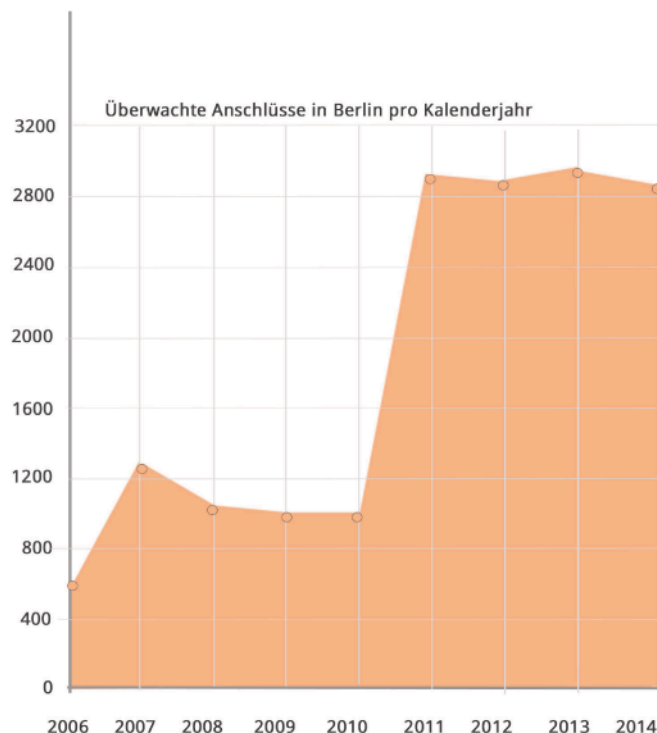
geben einen breiten Überblick über einen großen Zeitraum. Sie belegen unserer Auffassung nach deutlich, dass das Instrument seiner zugeordneten Kontrollaufgabe dort tatsächlich schon lange nicht mehr mit ausreichender Qualität nachkommt und eine Debatte notwendig ist.

Die Situation hat sich im Laufe der Jahre sogar weiter verschlimmert: War die Studie des MPI im Jahr 2003 noch zu dem Schluss gekommen, dass lediglich 0,4% der beantragten Überwachungsmaßnahmen nicht genehmigt wurden, so liegt die Quote in Berlin seit nunmehr sieben Jahren in Folge bei 0,00%. (Quellen: Studie des MPI, Seite 177 bzw. PDF Seite 197 und Jahresberichte aus Berlin) Dass alle Anordnungen entsprechend der Verfahrensvorschriften erfolgten, ist zweifelhaft: Immerhin kam die Studie der Universität Bielefeld 2003 zu dem Schluss, dass 75% der untersuchten Überwachungen nicht entsprechend den Verfahrensvorschriften angeordnet worden waren.



Berichtspflichten nach § 100b Abs. 5, Abs. 6 StPo müssen erweitert werden

Ohne die Berliner Jahresberichte, die das Land seit 2006 freiwillig herausgibt, würden über die Wirksamkeit des Richtervorbehaltes in Deutschland überhaupt keine Zahlen vorliegen. Das ist für uns alleine schon aus Gründen der demokratischen Kontrolle nicht nachvollziehbar. Dass laut den uns vorliegenden Zahlen offenbar jede Überwachungsanordnung bewilligt wird, ist wegen der fehlenden Berichtspflichten weder der breiten Öffentlichkeit bekannt, noch kann der Gesetzgeber die Wirksam-



keit seines eigenen Kontrollinstrumentes evaluieren. Unserer Ansicht nach muss der Gesetzgeber zu Evaluierungs- und Kontrollzwecken unbedingt flächendeckend Statistiken darüber führen, wie häufig beantragten Überwachungsmaßnahmen tatsächlich stattgegeben wird – und wie oft Richter eine TKÜ ablehnen. Nur wenn entsprechende Statistiken vorliegen, ist eine Kontrolle möglich. Bedenkliche Entwicklungen können so frühzeitig erkannt und über sie debattiert werden.

Unsere Forderung:

Wir schlagen deshalb vor, die Berichtspflichten zu Kontroll- und Evaluierungszwecken nach § 100b Abs. 5, Abs. 6 StPO dahingehend anzupassen, dass nicht nur die Anzahl der angeordneten TKÜ-Maßnahmen statistisch erfasst wird, sondern auch die Anzahl der abgelehnten Anträge auf eine TKÜ, um die Wirksamkeit des Richtervorbehaltes zu überprüfen.

Zeit- und Personalmangel in den Gerichten

Studien zufolge trägt seit Jahren auch Zeit- und Personalmangel an den Gerichten zu der Situation bei. Hier sehen wir einen wichtigen Ansatzpunkt, die Kontrolle von Observationsvorgängen zu stärken. Bereits in der Studie des Max-Planck-Institutes aus dem Jahr 2003 erklärte beispielsweise ein Ermittlungsrichter unter Hinweis auf seine hohe Arbeitsbelastung, dass er für das Prüfen eines TKÜ-Beschlusses nur zehn bis maximal 30 Minuten Zeit habe. Ein anderer Richter gab damals an, er setze seine „Überprüfungsprioritäten“ zwangsweise auf schwerwiegendere Eingriffe, etwa auf körperliche Eingriffe oder Haftbefehle. Die Studie stellte darüber hinaus fest, dass regelmäßig polizeiliche Anregungen auf eine TKÜ durch die Staatsanwaltschaft und den Ermittlungsrichter übernommen werden. Die Begründungen von TKÜ-Anordnungen würden „ausweislich der Akten und nach Selbsteinschätzung befragter Kriminalbeamter nahezu ausschließlich durch die Polizei“ geschrieben, nicht etwa durch die Richter selbst.

Im Hinblick auf die Arbeitsbelastung der Richter scheint in den vergangenen Jahren keine Verbesserung eingetreten zu sein:

Aus einer aktuellen Studie, dem Roland Rechtsreport 2014, geht hervor, dass neun von zehn befragten Richtern und Staatsanwälten es für notwendig halten, zusätzliche Richter und Staatsanwälte einzustellen. 85 Prozent der Befragten bewerten die personelle Ausstattung der Gerichte als schlecht. Und mehr als zwei Drittel der Befragten gab an, für ihre Rechtsfälle zu wenig Zeit zu haben. Eine überwiegende Mehrheit der Richter und Staatsanwälte (72 Prozent) vertrat sogar die Ansicht, dass sich die Rahmenbedingungen für die Rechtsprechung in Deutschland aktuell verschlechtern. Dabei ginge es vor allem um zu wenig Personal.

Wir halten es für bedenklich, dass solche Zustände offensichtlich seit Jahren bestehen. Ebenso wie die Tatsache, dass nach den Studien aus dem Jahr 2003 offenbar keine Anstrengungen unternommen wurden, die zu einer tatsächlichen Verbesserung bei der Kontrolle der Überwachungsvorgänge geführt hätten. Dies führt in der Praxis offenbar zu Statistiken wie denen aus Berlin, die unseres Erachtens nach einem Rechtsstaat nicht mehr gerecht werden. Wenn Überwachungsmöglichkeiten in Deutschland immer weiter ausgebaut werden, während diese Mängel fortbestehen, ist dies eine Entwicklung, die der Demokratie nicht zuträglich sein kann.

Unsere Forderung:

Da die Bundesregierung aktuell plant, die Vorratsdatenspeicherung (Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten) wieder einzuführen und diese öffentliche Stellen zu Grundrechtseingriffen berechtigen wird, die mit dem Instrument des Richtervorbehaltes kontrolliert werden sollen, fordern wir den Bundesjustizminister Heiko Maas dazu auf, den Gesetzentwurf zu stoppen. Wenn Überwachungsmöglichkeiten in Deutschland immer weiter ausgebaut werden, während die in unserem Transparenzbericht aufgezeigten Mängel fortbestehen und offenbar jeder Antrag auf Überwachung bewilligt wird, ist dies eine Entwicklung, die der Demokratie nicht zuträglich sein kann. Die Vorratsdatenspeicherung wird öffentliche Stellen zu Grundrechtseingriffen berechtigen, die mit dem Instrument des Richtervorbehaltes kontrolliert werden sollen. Seiner zugeordneten Kontrollaufgabe wird das Instrument ausweislich der von uns dokumentierten Zahlen offenbar schon seit Jahren nicht mehr gerecht. Auch die Kontrolle der Auskunftsverfahren ist mangelhaft. Häufig bestehen nicht einmal Statistik- oder Berichtspflichten. Bei der Bestandsdatenauskunft nach § 113 TKG herrschen in der Praxis chaotische Zustände: Fast alle Ersuchen, die uns erreichen, sind rechtswidrig. Wir befürchten, dass es hier nach der Einführung des Gesetzes zu einem weiteren Anstieg der rechtswidrigen Abfragen kommt.

Allgemein:

Warum veröffentlicht Posteo einmal jährlich einen Transparenzbericht?

Wir wollen, dass unsere Kunden wissen, wie viele und welche Art von Auskunftersuchen wir von Behörden erhalten. Und wir wollen transparent machen, wie Posteo mit solchen Anfragen umgeht. Nach dem Bekanntwerden der massenhaften Überwachung der Bürgerinnen und Bürger durch Geheimdienste ist es wichtiger denn je, dass Provider Transparenzberichte veröffentlichen. Sie stärken die Grundrechte, die informationelle Selbstbestimmung und die Demokratie insgesamt.

Warum hat Posteo 2014 zum ersten Mal einen Transparenzbericht veröffentlicht - und wieso hatte dies bis dahin kein anderer deutscher Telekommunikationsanbieter getan?

Wir haben im Jahr 2013 zum ersten Mal überhaupt Anfragen von Polizeibehörden erhalten. Für uns stand fest: Wir wollen künftig einen Transparenzbericht über Behördenersuchen veröffentlichen - nach dem Vorbild US-amerikanischer Telekommunikationsunternehmen.

Unsere Anwälte wiesen uns allerdings darauf hin, dass die Rechtslage hierzu in Deutschland nicht eindeutig sei und deshalb bisher kein deutscher Provider einen Transparenzbericht veröffentlicht habe. Der Gesetzgeber verpflichtet deutsche Telekommunikationsanbieter zur Verschwiegenheit über Auskunftersuchen, u.a. im TKG¹ und in den G10-Gesetzen². Deshalb haben wir vor der Veröffentlichung im Mai 2014 ein Rechtsgutachten³ erstellen lassen. Wir mussten den Sachverhalt vorab klären, da ein Verstoß gegen die Verschwiegenheitspflichten mit mehrjähriger Haft bestraft werden kann. Das von uns beauftragte Gutachten ergab, dass das Veröffentlichen rein statistischer Angaben, die keine Rückschlüsse mehr auf einzelne Fälle erlauben, zulässig ist. Das bestätigte dann auch das Bundesministerium der Justiz auf eine Anfrage von MdB Christian Ströbele⁴. Daraufhin hat Posteo schließlich am 14.05.2014 den ersten Transparenzbericht eines deutschen Telekommunikationsanbieters veröffentlicht.

Was möchte Posteo mit dem Veröffentlichen seiner Transparenzberichte erreichen?

Wir möchten erreichen, dass es in Deutschland zum Standard wird, dass Telekommunikationsunternehmen Transparenzberichte veröffentlichen. Diese Form der Transparenz stärkt die Möglichkeit der demokratischen Kontrolle und der Evaluation von Überwachungsmaßnahmen. Als wir 2014 den ersten Bericht eines deutschen Telekommunikationsanbieters veröffentlichten, folgte wenige Stunden darauf die Deutsche Telekom. Inzwischen haben auch einige andere deutsche Provider entsprechende Berichte veröffentlicht. Wir bieten anderen Anbietern, die dies für sich in Erwägung ziehen, einen Erfahrungsaustausch an.

Ferner möchten wir anregen, dass die Transparenzberichte durch die deutschen Anbieter in Open-Data-Formaten bereitgestellt werden, sodass ein transparentes Gesamtbild über Auskunftersuchen entstehen kann. Wir veröffentlichen unseren Transparenzbericht in einem offenen, standardisierten Austauschformat (XML und JSON), damit jeder Interessierte die Möglichkeit hat, die von uns bereitgestellten Daten zu verarbeiten und statistisch aufzubereiten. Ein weiteres Ziel unserer Transparenzberichte ist es, Missstände bei den Auskunftsverfahren aufzuzeigen und auf eine Verbesserung hinzuwirken.

¹ http://www.gesetze-im-internet.de/tkg_2004/__113.html

² http://www.gesetze-im-internet.de/g10_2001/__17.html

³ https://posteo.de/Gutachten_Transparenzbericht.pdf

⁴ https://posteo.de/Antwort_Bundesregierung.pdf

Warum veröffentlicht Posteo den Transparenzbericht als Open Data?

Für unsere Transparenzberichte stellen wir die Zahlen ab sofort in maschinenlesbarer Form zur Verfügung. Die Daten dürfen lizenzfrei (CC0) gelesen und weiterverarbeitet werden. So können interessierte Personen oder Organisationen die Daten vielleicht noch in ganz anderer Form aufbereiten als wir - zum Beispiel Analysen und Vergleiche anstellen, wenn auch andere Anbieter diese Form der Datenbereitstellung für die Daten ihrer Transparenzberichte benutzen. Das Stichwort hierzu ist „Open Data“. Eine Zivilgesellschaft kann anhand solcher transparent zur Verfügung stehenden Daten besser debattieren. Im Gegensatz zu persönlichen Daten, die einem hohen Schutzbedürfnis unterliegen, sind solche statistischen Daten nicht schutzbedürftig, sondern sollten allen Interessierten zur Verfügung stehen.

Für die maschinenlesbare Form benutzen wir ein sog. plist/XML-Schema, das auch von anderen Anbietern problemlos genutzt werden und bei Bedarf auch erweitert werden kann. Die Daten für 2014 können hier als JSON ⁵ oder PLIST ⁶ abgerufen werden.

Decken die Posteo-Transparenzberichte alle Ersuchen ab, die Posteo bisher erhalten hat? Und gibt es auch so etwas wie „geheime Ersuchen“, die in der Statistik nicht aufgeführt werden dürfen?

Geheime Ersuchen, über die wir keine statistischen Auskünfte geben dürfen, gibt es in Deutschland nicht. Die Posteo-Transparenzberichte decken daher alle Ersuchen ab, die wir erhalten haben. In den ersten vier Geschäftsjahren (2009-2012) von Posteo haben wir keine Anfragen von Behörden erhalten, Posteo war bis zum Frühjahr 2013 ein sehr kleiner Anbieter. Die Berichte für das Jahr 2013 und das Jahr 2014 liegen vor. Unsere Berichte umfassen sowohl alle Ersuchen von Ermittlungsbehörden, als auch alle Ersuchen von Nachrichtendiensten, die uns erreicht haben.

Warum ersuchen Behörden bei einem E-Mailprovider um Nutzerdaten?

Behörden ersuchen aus verschiedenen Gründen um Nutzerdaten: Zum Beispiel, um Straftaten aufzuklären oder dem Verdacht auf Ordnungswidrigkeiten nachzugehen. Beim Verdacht auf schwere Straftaten sind Strafverfolgungsbehörden unter bestimmten Umständen dazu berechtigt, E-Mails oder Verkehrsdaten von Providern zu erhalten. Allerdings benötigen sie hierfür einen richterlichen Beschluss. Für die Herausgabe von personenbezogenen Daten (z.B. Name und Adresse) ist hingegen weder ein richterlicher Beschluss noch ein Verdacht auf eine schwere Straftat notwendig. Bei Posteo können keine personenbezogenen Daten abgefragt werden, da wir keine Bestandsdaten unserer Kunden erheben.

Was unternimmt Posteo bei Behördenanfragen? Geht Posteo rechtlich gegen unrechtmäßige Ersuchen vor?

Wir lassen jedes Behördenersuchen nach Kundendaten zunächst sorgfältig durch unsere Anwälte prüfen. Wir nehmen den Schutz der Daten unserer Kunden sehr ernst. Ergibt die Prüfung unserer Anwälte, dass ein Ersuchen nicht rechtskonform oder formal falsch ist oder deckt der Umfang eines Beschlusses nicht die Daten ab, um die eine Behörde ersucht, legen wir Beschwerde ein. Posteo wird niemals Daten herausgeben, wenn Zweifel an der Korrektheit oder Rechtmäßigkeit eines Beschlusses bestehen. Wir scheuen hier keine Kosten und Mühen: Wir versichern Ihnen, dass unsere auf Telekommunikationsrecht spezialisierten Anwälte alles tun, um Ihr Recht auf informationelle Selbstbestimmung „im Fall der Fälle“ zu verteidigen. Wir möchten Ermittlungen nicht behindern, wollen aber sicherstellen, dass die ermittelnden Behörden auch tatsächlich berechtigt sind, die angeforderten Daten zu erhalten. Sind Behörden tatsächlich durch einen richterlichen Beschluss dazu berechtigt, Inhaltsdaten (z.B. E-Mails) eines Posteo-Kunden zu erhalten, müssen wir diese übermitteln. Dazu sind wir gesetzlich verpflichtet. Solche Ersuchen sind jedoch sehr selten.

In den meisten Fällen ersuchen Behörden lediglich um Bestandsdaten wie Namen und Adressen - und da wir solche Daten nicht speichern, können wir sie auch nicht herausgeben.

⁵ https://posteo.de/transparency_report/transparency_report_2014_Posteo.json

⁶ https://posteo.de/transparency_report/transparency_report_2014_Posteo.plist

Wie oft musste Posteo bisher Daten an berechnigte Behörden übergeben?

Wir mussten in den Jahren 2013 und 2014 nur in Einzelfällen nach richterlichen Anordnungen (siehe Transparenzberichte für die Jahre 2013 und 2014) Daten an Strafverfolgungsbehörden übergeben. Insgesamt waren 3 Postfächer betroffen, zu denen teilweise mehrere Anordnungen vorlagen (z.B. eine Postfachbeschlagnahme sowie eine TKÜ). Die Behörden hatten jeweils einen formal korrekten Beschluss zur laufenden Überwachung eines E-Mailpostfachs bzw. zu einer Postfachbeschlagnahme vorgelegt. Die Herausgabe der Daten erfolgte erst nach einer sorgfältigen Prüfung durch unsere Anwälte. In den Geschäftsjahren vor 2013 haben wir keine Ersuchen von Behörden erhalten.

Sahen Mitarbeiter von Posteo sich schon einmal bedroht oder wurde versucht, sie rechtswidrig zur Herausgabe von Daten zu bewegen?

Ja. Hierauf gehen wir im Schwerpunkt unseres Transparenzberichtes im Bereich „Behörden ersuchen rechtswidrig um IP-Adressen ein“.

Werden betroffene Kunden durch Posteo informiert?

Nein, wir dürfen betroffene Kunden nicht informieren. Damit würden wir uns strafbar machen. Deutsche Telekommunikationsanbieter werden durch verschiedene Gesetze (u.a. TKG ⁷ und das G10-Gesetz ⁸) zur Verschwiegenheit über die meisten Auskunftersuchen von Behörden verpflichtet. Dies wurde gesetzlich so geregelt, um auszuschließen, dass laufende Ermittlungen gefährdet werden.

Datenarten, Abfragen und rechtliche Grundlagen:

Was sind Bestandsdaten?

Ihre persönlichen Daten (wie Ihr Name, Ihre Adresse oder Ihre Kontonummer) werden in den Gesetzestexten als „Bestandsdaten“ bezeichnet. Werden Sie Kunde eines Telekommunikationsunternehmens, muss das Unternehmen (TKG § 111 ⁹) mindestens folgende persönliche Daten von Ihnen speichern: Ihren Namen, Ihr Geburtsdatum, sowie Ihre Adresse. Bei Anschlüssen müssen darüber hinaus Ihre Telefon- und Faxnummern sowie je nach Anschlussart weitere Daten wie Gerätenummern, Anschlusskennungen oder Daten über den Vertragsbeginn und das Vertragsende gespeichert werden. Für E-Mailanbieter besteht allerdings eine Sonderregelung: Sie dürfen darauf verzichten, Ihre persönlichen Daten zu erheben (TKG § 111) und müssen sie dann auch nicht speichern. Von dieser Regelung macht Posteo Gebrauch. Wir benötigen Ihre persönlichen Daten nicht – auch nicht für Abrechnungszwecke (siehe: anonyme Zahlung bei Posteo ¹⁰). Wenn E-Mailanbieter Ihre persönlichen Daten speichern, müssen sie diese auch herausgeben. Speichern die Anbieter Ihre Bezahlten postfachbezogen, sind auch diese vorliegende Bestandsdaten.

Warum erhebt Posteo keine Bestandsdaten?

Der Gesetzgeber fordert Unternehmen sogar explizit dazu auf (Bundesdatenschutzgesetz § 3a ¹¹), das Speichern von personenbezogenen Daten zu vermeiden, wann immer es möglich ist:

„Datenvermeidung und Datensparsamkeit: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.“

Bundesdatenschutzgesetz §3a

7 http://www.gesetze-im-internet.de/tkg_2004/__113.html

8 http://www.gesetze-im-internet.de/g10_2001/__17.html

9 http://www.gesetze-im-internet.de/tkg_2004/__111.html

10 <https://posteo.de/site/datenschutz#anonymezahlung>

11 http://www.gesetze-im-internet.de/bdsg_1990/__3a.html

An dieser Forderung haben wir uns bei der Konzeption von Posteo orientiert.

Wir arbeiten so datensparsam wie möglich, um unsere Kunden bestmöglich zu schützen: Nur Daten, die nicht erhoben wurden, können mit 100% Sicherheit nicht gestohlen oder missbraucht werden. Inzwischen sind zahlreiche Fälle bekannt geworden, in denen Kriminelle Kundendaten bei Unternehmen gestohlen haben. Zum Beispiel, um an Bankdaten zu gelangen und Betrugsdelikte zu begehen. Unser Konzept setzt auf maximalen Datenschutz: Deshalb erheben wir postfachbezogen keine personenbezogenen Daten und haben auch alle Zahlungsprozesse anonymisiert.

Unter welchen Umständen dürfen Behörden Bestandsdaten bei E-Mailanbietern anfordern? Können Bestandsdaten bei Posteo abgefragt werden?

Bei Posteo können Behörden keine Bestandsdaten erhalten, da wir sie nicht erheben.

Generell dürfen Bestandsdaten schon beim Verdacht auf Ordnungswidrigkeiten (z.B. Falschparken oder Ruhestörung) von zahlreichen Behörden und anderen Berechtigten bei den Providern abgefragt werden. Eine inhaltliche Überprüfung oder einen Richtervorbehalt gibt es nicht. Das Gesetz erlaubt die Identifizierung von Internetnutzern zur Verfolgung von Ordnungswidrigkeiten jeder Art. Anbieter mit mehr als 100.000 Teilnehmern müssen Bestandsdaten automatisiert zur Abfrage bereistellen, wenn sie Daten erheben. Nach Angaben der Bundesnetzagentur wurden auf diese Weise im Jahr 2014 rund 6,92 Millionen Ersuchen mit 34,3 Millionen Abfrageergebnissen durchgeführt. (Quelle: Tätigkeitsbericht Bundesnetzagentur 2014 ¹²)

Fragen Behörden nur nach Daten, die Unternehmen im Rahmen einer Bestandsdatenauskunft auch herausgeben dürfen?

Nein. In der Praxis der Bestandsdatenauskünfte nach § 113 TKG bestehen gravierende Sicherheitsprobleme und Mängel. Lesen Sie hierzu den Schwerpunkt unseres diesjährigen Transparenzberichtes, der sich mit diesem Thema befasst.

¹² http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2015/Jahresbericht14barrierefrei.pdf?__blob=publicationFile&v=6

Was sind Verkehrsdaten?

Verkehrsdaten sind Daten, die bei Telekommunikationsvorgängen entstehen. Sie dokumentieren zum Beispiel, zu welchem Zeitpunkt eine E-Mail zwischen zwei E-Mailpostfächern ausgetauscht wurde. Verkehrsdaten, die bei E-Mailanbietern anfallen, sind z.B.:

- Die Information, wann (Zeitpunkt) eine E-Mail von einer bestimmten E-Mailadresse an eine andere E-Mailadresse versendet wurde
- Die Information, von welcher IP-Adresse diese E-Mail versendet wurde.

Diese Daten werden in den so genannten „Logfiles“ des E-Mailanbieters gespeichert. Verwenden dürfen sie die Daten nur für zwei Zwecke:

1. Zum Erkennen, Eingrenzen und Beseitigen technischer Störungen (§ 100 Abs. 1 TKG), zum Beispiel beim Mailversand oder -empfang.
2. Zum Aufdecken von Missbrauch der Systeme (§ 100 Abs. 3 TKG), z.B. durch Spammer.

Wann dürfen Verkehrsdaten an Behörden herausgegeben werden? Können Behörden verlangen, dass Posteo Verkehrsdaten für die Verfolgung von Straftaten erhebt?

Die Verkehrsdaten unterliegen dem Schutz des Fernmeldegeheimnisses. Es ist deshalb verboten, Verkehrsdaten auf einfache Anfragen von Behörden herauszugeben. Strafverfolgungsbehörden benötigen eine richterliche Anordnung, um Verkehrsdaten bei uns abzufragen. Diese wird nur dann durch einen Richter erteilt, wenn der Verdacht auf eine schwere Straftat besteht. Das deutsche Gesetz erlaubt es auch nicht, dass Verkehrsdaten für den Zweck der Strafverfolgung gesondert gespeichert werden (insb. keine Vorratsdatenspeicherung). Für eine Auskunftserteilung dürfen ausschließlich Daten verwendet werden, die aus betrieblichen Gründen rechtmäßig gespeichert sind. Das bedeutet, dass Behörden von uns nicht einfordern dürfen, zusätzliche Verkehrsdaten unserer Nutzer zu erheben. Wenn Sie unsere Website besuchen und sich in Ihr Postfach einloggen, speichern wir Ihre IP-Adresse z.B. nicht.

Kann Posteo IP-Adressen seiner Kunden herausgeben?

Nein. Wir dürfen diese nicht erheben und speichern, da wir sie betrieblich nicht benötigen. Deshalb verfügen wir nicht über IP-Adressen mit Postfachbezug und können diese auch nicht herausgeben.

Was ist das Fernmeldegeheimnis und wann darf es beschränkt werden?

Das Fernmeldegeheimnis ist ein Grundrecht und steht ebenso wie das Brief- und Postgeheimnis unter dem Schutz von Artikel 10 des Grundgesetzes. Es besagt, dass die Bürgerinnen und Bürger gegenüber dem Staat ein Recht auf Abschirmung ihrer privaten Kommunikation haben, um den unbeobachteten Austausch und die Weitergabe von Tatsachen und Gedanken zu ermöglichen. Dem Fernmeldegeheimnis unterliegen sowohl die konkrete Inhalte (Telefonate, E-Mails) als auch die Verkehrsdaten einer Telekommunikation. Es darf aber auch beschränkt werden: In welchen Fällen das möglich ist, ist z.B. in der Strafprozessordnung (StPO) und im G 10-Gesetz geregelt. Bei Strafverfolgungsmaßnahmen darf eine Überwachung der Telekommunikation für einen bestimmten Zeitraum angeordnet werden, wenn der begründete Verdacht einer schweren Straftat besteht (§ 100a StPO). Die Überwachung muss durch einen Richter oder – bei Gefahr im Verzug – durch die Staatsanwaltschaft angeordnet werden. In Einzelfällen kann nach § 100g StPO auch die Mitteilung der Verkehrsdaten angeordnet werden. Wann Dienste wie die Verfassungsschutzbehörden und das Amt für den Militärischen Abschirmdienst berechtigt sind, Telekommunikation zu überwachen, ist im G10-Gesetz und den Geheimdienstgesetzen geregelt. Wird eine Überwachung angeordnet, muss der Telekommunikationsanbieter eine Kopie des Telekommunikationsvorgangs den berechtigten Behörden zur Verfügung stellen. Der Betroffene einer solchen Überwachung muss über die durchgeführte Maßnahme (von den Behörden) teilweise unterrichtet werden, sobald der „Zweck der Maßnahme“ dies erlaubt. Die Behörden müssen die Daten, die sie erhalten haben, im Anschluss vernichten.

Was sind Inhaltsdaten und unter welchen Umständen können sie bei E-Mailanbietern abgefragt werden?

Inhaltsdaten sind nichts anderes als die „Inhalte“ Ihrer Kommunikation - Ihre E-Mails. Der Gesetzgeber hat die Hürde zur Herausgabe von Inhalten recht hoch gelegt: Ihre E-Mails unterliegen dem Fernmeldegeheimnis. Da wir Postfächer niemals freiwillig herausgeben (§ 94 Abs. 1 StPO), sondern Anfragen stets förmlich widersprechen, muss eine strafrechtliche Beschlagnahme eines Posteo-Postfachs durch einen Richter angeordnet werden (§ 94 Abs. 2 StPO, § 98 Abs. 1 S. 1 bzw. Abs. 2 S. 1 StPO). Eine strafrechtliche TKÜ-Anordnung zur Überwachung eines Postfachs für einen bestimmten Zeitraum kann ausschließlich bei bestimmten schweren Straftaten erwirkt werden. Jeder richterliche Beschluss muss von den Behörden bei uns (dem Provider) vorgelegt werden und wird durch unsere Anwälte auf Umfang und formale Korrektheit geprüft, bevor wir ggf. Daten übergeben. Der betroffene Kunde darf über eine TKÜ-Anordnung nicht informiert werden. Damit würden wir uns strafbar machen.

Bitte lesen Sie hierzu auch den Schwerpunkt unseres diesjährigen Transparenzberichtes, der sich mit diesem Thema auseinandersetzt.

Was ist der Unterschied zwischen einer Postfachbeschlagnahme und einer TKÜ?

Bei einer strafrechtlichen Beschlagnahme eines Posteo-Postfachs (§ 94 Abs. 2 StPO, § 98 Abs. 1 S. 1 bzw. Abs. 2 S. 1 StPO) sind wir dazu verpflichtet, alle E-Mails zu übergeben, die sich zum Zeitpunkt der Beschlagnahme in dem betroffenen E-Mailpostfach befanden und auf die sich der Beschluss bezieht. Bei einer TKÜ-Anordnung zur Überwachung eines Postfachs sind wir dazu verpflichtet, alle E-Mails für die berechtigten Behörden zu kopieren, die ab dem Zeitpunkt der Anordnung in dem betroffenen Postfach ein- und ausgehen. Zuvor gespeicherte E-Mails sind bei einer TKÜ nicht betroffen. Allerdings können beide Maßnahmen, Beschlagnahme und laufende Überwachung, miteinander kombiniert werden.

Häufige Fragen zur Herausgabe: Verschlüsselung, Passwörter und „Abhörschnittstellen“

Ich habe gelesen, dass E-Mailanbieter ab 10.000 Nutzer eine staatliche Abhörschnittstelle aufstellen müssen. Stimmt das und handelt es sich um die so genannte SINA-Box?

Bei Posteo steht bisher keine SINA-Box. Und eine SINA-Box ist auch keine „Abhörschnittstelle“, die Behörden Zugriff auf Daten bei einem Provider verschafft. Mehr Informationen zur SINA-Box und der Art und Weise, wie deutsche E-Mailanbieter Daten an Behörden übermitteln, finden Sie in unserem Blogbeitrag zum Thema ¹³. In der Telekommunikations-Überwachungsverordnung gibt es die Pflicht für Telekommunikations-Anbieter, ab einer Teilnehmerzahl von 10.000 einen speziellen Computer (SINA-Box) aufzustellen. Bei uns ist nicht zweifelsfrei zu sagen, wieviele Teilnehmer unser Dienst hat, da wir keine Bestandsdaten unserer Nutzer erheben. Wir wissen nur die Anzahl der Postfächer. Die Bundesnetzagentur vermutet, dass wir inzwischen zum Kreis der Verpflichteten gehören. Deshalb haben wir uns im vergangenen Jahr intensiv mit dem Thema auseinandergesetzt. Hierbei haben sich verschiedene Fragestellungen ergeben, denen wir nun nachgehen. Sobald es Neues hierzu gibt, werden wir in unserem Blog darüber berichten.

Kann Posteo von Ermittlungsbehörden oder Geheimdiensten dazu gezwungen werden, Verschlüsselung zu brechen?

Nein, das ist in Deutschland, anders als z.B. in den USA oder in Großbritannien, nicht möglich. Hierzulande gibt es keine Gesetze, die uns dazu verpflichten könnten, Verschlüsselung zu brechen. Wir haben dies durch unsere Anwälte prüfen lassen, bevor wir Verschlüsselungsoptionen wie den Posteo-Krypto-Mailspeicher entwickelt haben. Dieser ist technisch z.B. so realisiert, dass Posteo die vom Kunden vorgenommene Verschlüsselung nicht wieder entfernen kann - dies kann nur der Kunde selbst tun.

¹³ <https://posteo.de/blog/posteo-zur-m%C3%A4r-von-der-abh%C3%B6r-schnittstelle>

Versieht ein Kunde Daten mit einer Ende-zu-Ende-Verschlüsselung, kann diese durch den jeweiligen Provider ebenfalls nicht mehr entfernt werden.

Können Behörden oder Dienste Posteo dazu zwingen, Hintertüren o.ä. bei Posteo einzubauen?

Nein. Hierfür gibt es ebenfalls keine rechtliche Grundlage in Deutschland.

Kann Posteo mein Posteo-Passwort an Behörden herausgeben?

Nein. Denn wir speichern Ihr Passwort nicht im Klartext ab, sondern nur als so genannten „gesalteten Hash-Wert“. Wir kennen Ihr Passwort deshalb nicht und können es weder an Sie, noch an Dritte herausgeben. Mehr Informationen zur Verschlüsselung der Passwörter bei Posteo erfahren Sie auf unserer Themenseite Verschlüsselung ¹⁴.

Ich habe eine Mobilfunknummer bei Posteo hinterlegt. Kann diese Nummer an Behörden herausgegeben werden?

Nein. Ihre Handynummer liegt verschlüsselt in unserer Datenbank, ebenfalls als „gesalteter Hash“. Wir kennen Ihre Mobilfunknummer nicht und können sie an Dritte nicht herausgeben. Mehr Informationen zur Verschlüsselung der Mobilfunknummern bei Posteo erfahren Sie auf unserer Themenseite Verschlüsselung ¹⁵.

Kann Posteo meine IP-Adresse herausgeben?

Nein. Seit die Vorratsdatenspeicherung im März 2010 durch das Bundesverfassungsgericht gekippt wurde, dürfen deutsche E-Mail-Anbieter nur dann IP-Adressen speichern, und zwar für maximal 7 Tage, wenn diese aus betrieblichen Zwecken benötigt werden.

Da wir die IP-Adressen unserer Nutzer aus betrieblichen Zwecken aber nicht benötigen, ist es uns folglich auch nicht erlaubt, diese zu speichern. Wir speichern die IP-Adressen unserer Kunden deshalb nicht und können sie deshalb auch nicht herausgeben.

Ist Posteo von der geplanten Wiedereinführung der Vorratsdatenspeicherung betroffen?

Der Gesetzentwurf der Bundesregierung zur geplanten Wiedereinführung der Vorratsdatenspeicherung („Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ ¹⁶) sieht aktuell vor, dass der gesamte E-Mail-Bereich von der Speicherung ausgenommen werden soll. Das bedeutet: Wenn es dabei bleibt, gehört Posteo nicht zum Kreis der Verpflichteten.

Unabhängig davon lehnen wir die Vorratsdatenspeicherung grundsätzlich ab. Wir beobachten die Lage aktuell sehr genau.

Können Ermittlungsbehörden überhaupt an gespeicherte Daten gelangen, wenn ich meine E-Mails mit einer Ende-zu-Ende-Verschlüsselung versehe oder mein Postfach bei Posteo (Krypto-Mailspeicher) verschlüsselt ist?

Wenn wir durch eine richterliche Anordnung zur Herausgabe eines Postfachs verpflichtet werden, müssen wir Inhaltsdaten herausgeben. Und zwar so, wie sie sind. Bei uns gespeicherte E-Mail-Daten, die durch den Kunden verschlüsselt wurden, z.B. mit unserem Krypto-Mailspeicher oder mit Hilfe einer Ende-zu-Ende-Verschlüsselung, können durch Posteo im Nachhinein nicht mehr entschlüsselt werden.

Sind gespeicherte E-Mails verschlüsselt, werden sie also verschlüsselt übergeben.

¹⁴ <https://posteo.de/site/verschuesselung>

¹⁵ <https://posteo.de/site/verschuesselung>

¹⁶ <http://dip21.bundestag.de/dip21/btd/18/050/1805088.pdf>

Anhang I

Beispiele rechtswidriger Behördenersuchen

Betreff: Auskunftersuchen/ EILT

Von: [REDACTED]@online.de>

Datum: [REDACTED]

An: support@posteo.de

- Verwenden einer nicht-dienstlichen E-Mail-Adresse
- unzulässige, unsichere Übertragung (unverschlüsselt)

Sehr geehrte Damen und Herren,

- unzulässiges Zusenden des Ersuchens an den allgemeinen Kunden-Support

Hier vorliegend Strafanzeige [REDACTED]

zur weiteren Bearbeitung ist es erforderlich die Bestandsdaten bekannt zu machen zum Postach:

Wann wurde das Postfach angelegt, mit welcher IP? Wer ist der Inhaber/ Nutzer? Gibt es derzeit weitere Anfragen durch Ermittlungsbehörden (event. Aktenzeichen dieser)?

Aktenzeichen der STA [REDACTED]

- unrechtmäßiges Ersuchen um eine IP-Adresse sowie um Informationen zu evtl. Anfragen anderer Behörden

mfg

- fehlende Angabe der Rechtsgrundlage (gesetzlich vorgeschrieben)

E-Mail (Internet): [REDACTED]@polmv.de oder [REDACTED]@online.de

- Angabe der nicht-dienstlichen E-Mail-Adresse in der Kontaktsignatur des Beamten

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte

Betreff: Polizeiliches Ersuchen [REDACTED]@polizei.sachsen.de)

Von: [REDACTED]

Datum: [REDACTED]

An: support@posteo.de

[REDACTED]@polizei.sachsen.de (nicht angemeldet) schrieb am [REDACTED]

Betreff: Polizeiliches Ersuchen

Sehr geherte Damen und Herren,

im Rahmen der Ermittlungen zu in hiesiger Dienststelle vorliegenden Strafanzeige wegen

[REDACTED] werden Sie ersucht, die Bestandsdaten der Mailadresse
[REDACTED] an den Sachbearbeiter zu übermitteln.

Für Ihre Mitarbeit bedanke ich mich im Voraus.

Mit freundlichen Grüßen

[REDACTED]

[REDACTED]

Kriminalpolizeiinspektion

[REDACTED]

- unsicheres Übermitteln sensibler Daten
per unverschlüsselter E-Mail

- Zusenden an den Kunden-Support

- fehlende Angabe der Rechtsgrundlage

Betreff: Auskunftersuchen

Von: [REDACTED]@polizei.berlin.de>

Datum: [REDACTED]

An: "support@posteo.de" <support@posteo.de>

[REDACTED]

- Unsicheres Übermitteln sensibler Daten per unverschlüsselter E-Mail
- Zusenden des Ersuchens an den Kunden-Support

Fa. Posteo e.K.
Böckhstr. 26,
10967 Berlin

Sehr geehrte Damen und Herren,

bei dem [REDACTED] werden Ermittlungen angestellt, bei dem der Täter ein eMail-Konto genutzt hat, welches offenbar von Ihrem Unternehmen bereitgestellt wurde. Gemäß § 100j StPO i. V. m. § 113 TKG bitten wir im Rahmen des Auskunftsverlangens um die Übermittlung der bei Ihnen bekannten Daten, die beim Anlegen und Nutzen des Kontos entstanden sind.

Die eMail-Adresse des betreffenden Nutzers lautet:

[REDACTED]

Dem Nutzer wird der Tatbestand der/s [REDACTED] zur Last gelegt.
Das staatsanwaltschaftliche Aktenzeichen lautet: [REDACTED]

Wir möchten Sie vorsorglich darauf hinweisen, dass dem Teilnehmer gemäß § 113 TKG keine Auskunft darüber erteilt werden darf, dass diese Daten an eine Ermittlungsbehörde übermittelt wurden. Darunter fällt auch die indirekte Auskunft z.B. durch Sperrung, Löschung oder sonstige unübliche Änderung im bestehenden Vertragsverhältnis

Im Auftrag

[REDACTED]

Betreff: Az. [REDACTED]
Von: [REDACTED]@polizei.bayern.de>
Datum: [REDACTED]
An: "support@posteo.de" <support@posteo.de>

- Unsichere Übermittlung per unverschlüsselter E-Mail
- Zusenden des Ersuchens an den Kunden-Support

Sehr geehrte Damen und Herren,

im Rahmen der Ermittlungen zu einer Anzeige wegen [REDACTED]
benötigen wir den Nutzer einer EMail-Adresse ihrer Firma.
Es handelt sich dabei um die Adresse
[REDACTED]

Bei Bedarf oder zusätzlichen Fragen stehe ich ihnen unter der unten angegebenen Telefonnummer oder per EMail zur Verfügung.

Mit freundlichen Grüßen

- fehlende Angabe der rechtlichen Grundlage, auf deren Grundlage um Daten ersucht wird.



Betreff: Auskunftersuchen zu Bestandsdaten einer Email-Adresse gem. § 100j StPO i.V.m § 113 TKG -

Von: [REDACTED] <[REDACTED]@polizei.nrw.de>

Datum: [REDACTED]

An: <support@posteo.de>

- unsichere Übertragung (unverschlüsselt)
- Zusenden des Ersuchens an den allgemeinen Kunden-Support.

Sehr geehrte Damen und Herren,

im Rahmen eines hier geführten Ermittlungsverfahrens wegen [REDACTED] werden alle Ihnen zur Verfügung stehenden Bestands- und Registrierungsdaten wie Vor-/Nachname, Geburtsdatum/-ort, Anschrift, Telefonnummer(n), IP-Adresse(n), weitere Email-Adresse(n) etc. der folgenden Email-Adresse benötigt (Tatverdächtige(r)):

[REDACTED]

Bitte lassen Sie mir unter Angabe der o.g. Vorgangsnummer die betreffenden Daten per Post, Fax oder E-Mail innerhalb von zwei Wochen an die u.g. Dienststelle zukommen.

Für Ihre Bemühungen bedanke ich mich im Voraus.

Mit freundlichen Grüßen,

[REDACTED]

- Der Beamte bittet ganz selbstverständlich um die Herausgabe von IP-Adressen.

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail ist nicht gestattet.

This e-mail contains confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

Betreff: Polizeiliche Anfrage

Von: [REDACTED] <[REDACTED]@polizei.bayern.de>

Datum: [REDACTED]

An: "support@posteo.de" <support@posteo.de>

- Unsichere Übermittlung per unverschlüsselter E-Mail
- Zusenden des Ersuchens an den Kunden-Support

Siehe Anhang

Mfg

[REDACTED]
[REDACTED]
[REDACTED]@polizei.bayern.de

Tel. [REDACTED]

FAX: [REDACTED]

Ein Beispiel für eine E-Mail, in deren Anhang sich ein Dokument befindet, dass fälschlicherweise als Telefax-Nachricht ausgezeichnet ist. De facto wurde das Ersuchen aber unzulässig per unverschlüsselter E-Mail übertragen.

— Anhänge: —

[REDACTED].pdf

380 KB



Baden-Württemberg


POLIZEIPRÄSIDIUM [REDACTED]
POLIZEIREVIER [REDACTED]

Polizeirevier [REDACTED]

support@posteo.de

- Zusenden des Ersuchens an den allgemeinen Kunden-Support
- unsichere Übertragung (unverschlüsselt)

Datum [REDACTED]
Name [REDACTED]
Durchwahl [REDACTED]
CNP [REDACTED]
Aktenzeichen [REDACTED]
(Bitte bei Antwort angeben)

 Ermittlungsverfahren wegen [REDACTED]

hier: Ermittlung der Bestandsdaten

Es wird gebeten die Bestandsdaten folgender E-Mail Adresse zu übermitteln

[REDACTED]

- fehlende Angabe der Rechtsgrundlage (gesetzlich vorgeschrieben)

Mit freundlichen Grüßen

[REDACTED]

[REDACTED]
ÖPNV-Anschluss:

© 2006 The Authors

[REDACTED]

@polizei.bwl.de>

[REDACTED]

An: "support@posteo.de" <support@posteo.de>

Anbei wird ein Schreiben mit der Bitte übersandt Bestandsdaten festzustellen und hierher zu übermitteln.

Mit freundlichen Grüßen.

[REDACTED]

[REDACTED]

@polizei.bwl.de

@polizei.bwl.de

- unsicheres Übermitteln eines Ersuchens per unverschlüsselter E-Mail
- Zusenden an den Kundensupport und somit an nicht zuständige Personen

Anhänge:

[REDACTED].pdf

149 KB

Polizeipräsidium [REDACTED]

Kriminaldirektion
[REDACTED]

HESSEN



Telefax

Empfänger Posteo e.K.
10965 Berlin

Fax-Nummer 030 346493249

Sehr geehrte Damen und Herren,

Im Rahmen eines Ermittlungsverfahrens der StA [REDACTED], wegen des Verdachts des [REDACTED] bitte ich um Ihre Unterstützung.

Vom betrügerisch genutzten Konto [REDACTED] des [REDACTED] auf Ihr Konto überwiesen. Die Überweisung trägt die Bezeichnung [REDACTED]

Bitte teilen Sie mir die Ihnen zu dieser Zahlung vorliegenden Daten, insbesondere die E-Mail-Adresse, ggf. Telefonnummern und die IP-Daten der Anmeldung mit. Hierzu verweise ich auf den § 100j StPO i.V.m § 113 TKG und mache darauf aufmerksam, dass dieses Auskunftersuchen keinem Dritten zur Kenntnis gegeben werden darf.

Für Ihre Unterstützung bedanke ich mich bereits jetzt und verbleibe

mit freundlichen Grüßen
[REDACTED]

Unrechtmäßiges Ersuchen um eine IP-Adresse. Der Beamte nennt als Rechtsgrundlage die Bestandsdatenauskunft nach § 113 TKG, die genau dies aber nicht erlaubt.

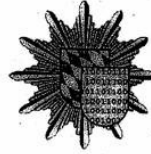
Seitenzahl 1 (mit Deckblatt)
[REDACTED]

Betreff: Behördenauskunft
Von: [REDACTED]@polizei.bayern.de>
Datum: [REDACTED]
An: "support@posteo.de" <support@posteo.de>

Kriminalpolizeiinspektion

[REDACTED]

Kriminalpolizeiinspektion
Posteo.de
Behördenauskünfte



- unsichere Übertragung (unverschlüsselt)
- Zusenden des Ersuchens an das allgemeine Support-Team

Ihr Zeichen
Ihre Nachricht vom

Bitte bei Antwort angeben
Unser Aktenzeichen

Sachbearbeiter

Telefon

[REDACTED]@polizei.bayern.de

i.S. Ermittlungsverfahren wegen [REDACTED]

Sehr geehrte Damen und Herren,

sie werden gebeten gem. § 113 TKG, § 100j StPO folgende Bestandsdaten zu speichern und mitzuteilen:

Benutzerkennung: [REDACTED]

Gegen den bislang unbekannten Benutzer, der genannten E-Mail-Adresse, ermittelt hiesige Dienststelle im Auftrag der Staatsanwaltschaft Ingolstadt.

Für weitere Ermittlungen würden die Daten der Einrichtung des Account und die IP-Adresse mit Zeitangabe der letzten Nutzung des E-Mail-Accounts benötigt.

Für evtl. Rückfragen stehe ich Ihnen jederzeit gerne zur Verfügung. Für Ihre Bemühungen Besten Dank im voraus.

Mit freundlichen Grüßen

[REDACTED]

Ein extremer Fall: Der Beamte bittet völlig selbstverständlich um das rechtswidrige Speichern und Mitteilen von Verkehrsdaten (tatsächlich mind. zwei Verkehrsdaten, nämlich IP-Adresse u. Zeitstempel der letzten Nutzung) und bezeichnet diese als „Bestandsdaten“.

Er bittet um eine gesonderte Speicherung für seine Zwecke, was vollkommen rechtswidrig ist. Berechtigte Auskunft über Verkehrsdaten darf er nur mit richterlicher Anordnung erhalten - und nicht im Rahmen einer Abfrage nach § 113 TKG.

Betreff: Auskunftersuchen zu Bestandsdaten einer Email-Adresse gem. § 100j StPO i.V.m § 113 TKG -

Von: [REDACTED]@polizei.nrw.de>

Datum: [REDACTED]

An: <support@posteo.de>

Unsichere Übermittlung per unverschlüsselter E-Mail.

Zusenden des Ersuchens an den allgemeinen Kunden-Support

Sehr geehrte Damen und Herren,

im Rahmen eines hier geführten Ermittlungsverfahrens wegen [REDACTED] werden alle Ihnen zur Verfügung stehenden Bestands- und Registrierungsdaten wie Vor-/Nachname, Geburtsdatum/-ort, Anschrift, Telefonnummer(n), IP-Adresse(n), weitere Email-Adresse(n) etc. der folgenden Email-Adresse benötigt (Tatverdächtige(r)):

[REDACTED]

Bitte lassen Sie mir unter Angabe der o.g. Vorgangsnummer die betreffenden Daten per Post, Fax oder E-Mail innerhalb von zwei Wochen an die u.g. Dienststelle zukommen.

Für Ihre Bemühungen bedanke ich mich im Voraus.

Mit freundlichen Grüßen,

[REDACTED]

Der Beamte bittet völlig selbstverständlich um das rechtswidrige Mitteilen von Verkehrsdaten. Berechtigte Auskunft über Verkehrsdaten darf er nur mit richterlicher Anordnung erhalten - und nicht im Rahmen einer Abfrage nach § 113 TKG.

Diese E-Mail enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail ist nicht gestattet.

This e-mail contains confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

Anhang II

Antworten der Datenschutzbeauftragten zu rechtswidrigen Behördenersuchen

**Berliner Beauftragter für
Datenschutz und Informationsfreiheit**
Bereich Recht I



Berliner Beauftragter für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin

Posteo e.K.
Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

GeschZ. (bitte angeben)	Bearbeiter(in)	Tel.: (030) 13 889-0	Datum
51.1141.9	[REDACTED]	[REDACTED]	19. Juni 2015

Polizeiliche Auskunftersuchen nach § 100j StPO i. V. m. § 113 TKG an Posteo e.K.
Ihr Schreiben vom 17. Februar 2015

Sehr geehrter Herr Löhr,

leider konnte die Angelegenheit bislang noch nicht abschließend geklärt werden. Wir bedauern die lange Bearbeitungszeit Ihrer Eingabe und bitten um Ihr Verständnis. Sobald uns neue Informationen vorliegen, setzen wir uns mit Ihnen in Verbindung.

Mit freundlichen Grüßen



Sprechzeiten: tgl. 10 - 15 Uhr,
Do. 10 - 18 Uhr
oder nach Vereinbarung
Besuchereingang:
Puttkamerstr. 16-18
auch für Behinderte

U6:
Kochstr.
Bus: M29, 248

Fax: (030) 215 50 50
Elektronische Zugangseröffnung
gem. § 3a Abs. 1 VwVfG:
mailbox@datenschutz-berlin.de
Internet:
<http://www.datenschutz-berlin.de>
<http://www.informationsfreiheit.de>





Der Bayerische Landesbeauftragte für den Datenschutz

Bayer, Datenschutzbeauftragter • PF 22 12 19 • 80502 München

Patrik Lohr
Posteo e.K.
Methfesselstraße 38
10965 Berlin

Ihr Zeichen, Ihre Nachricht vom

Unser Zeichen
DSB/1 - 187 - 57

München, den 27.02.2015

**Vollzug des Bayerischen Datenschutzgesetzes (BayDSG);
Ihre Eingabe vom 17.02.2015 wegen der Übermittlung von Auskunftersuchen
an den Telekommunikationsanbieter Posteo durch die Bayerische Polizei**

Sehr geehrter Herr Lohr,

für Ihren Hinweis über die teilweise per unverschlüsselter E-Mail bei Ihnen eingehenden Bestandsdatenanfragen bayerischer Polizeidienststellen danke ich Ihnen. Soweit Sie dem zustimmen, beabsichtige ich mich in den von Ihnen genannten Fällen – unter der Nennung Ihres Firmennamens – an die zuständigen Polizeipräsidien zu wenden. Insoweit wäre ich Ihnen über eine kurze Rückmeldung dankbar.

Nachdem die Übermittlung von personenbezogenen Daten in unverschlüsselten E-Mails durch sonstige Behörden oder durch die Polizei immer wieder Anlass für datenschutzrechtliche Überprüfungen gibt, habe ich mich mit diesem Thema bereits mehrmals in meinen Tätigkeitsberichten befasst. Zuletzt im aktuellen 26. Tätigkeitsbericht für den Zeitraum 2013/2014 in der Nr. 3.6.6, abrufbar unter <https://www.datenschutz-bayern.de/>.

Zudem kann ich Ihnen versichern, dass ich dieses Thema auch unabhängig von meinen konkreten Kontrollen mit den zuständigen Stellen der Polizei regelmäßig erörtere. So stehe ich derzeit mit dem Bayerischen Landeskriminalamt in Kontakt um

Wagnmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München
Telefon: 089 212672-0
Telefax: 089 212672-50
<https://www.datenschutz-bayern.de>
E-Mail: poststelle@datenschutz-bayern.de

Verkehrsverbindungen:
04/05, Haltestelle Lohr
05/06, Haltestelle Lohr
06/07, Haltestelle Lohr
Haltestelle Nationalmuseum / Haus der Kunst

- 2 -

die Ausgestaltung des dort betriebenen Abrufverfahrens bei Telekommunikationsanbietern zu überprüfen.

Mit freundlichen Grüßen

LA

Ministerialrat

Antwort aus Mecklenburg-Vorpommern



Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern



Der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V
Lennéstraße 1, Schloss · 19053 Schwerin

Posteo e.K.
Herrn Patrik Lühr
Methfesselstr. 38
10965 Berlin

AKTENZEICHEN
1.4.8.039/074/2015-01587

IHR ZEICHEN

IHRE NACHRICHT
vom 17.02.2015

AUSKUNFT

23. Juli 2015

Manuelles Auskunftersuchen nach § 113 TKG Prüfung von automatisierten Auskunftsanfragen nach § 112 TKG

Sehr geehrter Herr Lühr,

Ihre Anfragen vom 17.02.2015 habe ich dankend erhalten.

Ich habe die betreffende Dienststelle kontaktiert und sie auf ihre Umsetzung von datenschutzrechtlichen Maßnahmen hingewiesen, damit Sie in Zukunft Anfragen nach § 113 TKG auf sicherem Wege erreichen und die Rechte des Betroffenen damit nicht verletzt werden.

Ebenfalls habe ich das Ministerium für Inneres und Sport Mecklenburg-Vorpommern auf diesen Missstand aufmerksam gemacht. Das Ministerium für Inneres und Sport Mecklenburg-Vorpommern versicherte mir, die Beamtinnen und Beamten hinsichtlich des richtigen Umgangs mit personenbezogenen Daten und des Umgangs mit TKÜ-Abfragen nach § 113 TKG erneut zu sensibilisieren.

Bezüglich Ihrer Anfrage über die Prüfung bei automatisierten Auskunftsanfragen nach § 112 TKG durch diese Behörde muss ich Ihnen mitteilen, dass eine solche Prüfung bisher nicht erfolgt ist.

Aufgrund einer Vielzahl von Petitionen in verschiedenen Bereichen des Datenschutzes und der Informationsfreiheit ist es uns zeitlich und personell nicht möglich eigeninitiierte Prüfungen über Anfragen nach § 112 TKG vorzunehmen.

Ich hoffe, Ihnen mit dieser Antwort weitergeholfen zu haben, und stehe Ihnen für weitere Fragen gerne zur Verfügung.

Mit freundlichen Grüßen
im Auftrag

POSTANSCHRIFT: Lennéstraße 1, Schloss, 19053 Schwerin

HAUSANSCHRIFT: Johannes-Stelling-Straße 21, 19053 Schwerin

KOMMUNIKATION: Telefon 0385 59494-0, Telefax 0385 59494-58, datenschutz@mvnet.de, www.datenschutz-mv.de, www.informationsfreiheit-mv.de

PGP-Fingerprint: ADB5 030A C111 388C A8FD 92B7 EF40 56E6 71DA 3ABA

**Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen**



LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

Posteo e. K.
Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

07. April 2015
Seite 1 von 2

Alterszeichen
bei Antwort bitte angeben
22.4.2.0-662/15



Datenschutz bei manuellen Auskunftersuchen nach § 113 TKG
Ihre Anfrage vom 17.02.2015

Sehr geehrter Herr Löhr,

für Ihre Anfrage danke ich Ihnen und bitte um Verständnis, dass es mir wegen der Vielzahl der hier eingehenden Zuschriften erst jetzt möglich ist, mich mit Ihrem Anliegen zu befassen.

Ich teile Ihre Einschätzung, dass Anfragen von Ermittlungsbehörden mittels unverschlüsselter E-Mail aus datenschutzrechtlicher Sicht problematisch sind. Dies gilt im Grundsatz für jede Art von Ermittlungen, unabhängig davon, ob sie sich auf Telekommunikationsdaten beziehen. Gegenüber dem Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen (MIK NRW) habe ich wiederholt darauf hingewiesen, dass Anfragen in Ermittlungsverfahren grundsätzlich auf dem Postweg bzw. in begründeten Fällen auch per Fax erfolgen sollten. Wenn im Ausnahmefall eine Anfrage per E-Mail erforderlich sein sollte, so müsste entweder die Nachricht selbst verschlüsselt werden oder zumindest die Übermittlung personenbezogener Daten müsste in einem verschlüsselten Dateianhang erfolgen.

Ihre Anfrage werde ich zum Anlass nehmen, diese Thematik nochmals gegenüber dem MIK NRW aufzugreifen und auf eine datenschutzrechtliche Ausgestaltung der polizeilichen Ermittlungen hinzuwirken.

Zur Frage, welche Maßgaben bei der Erteilung der angeforderten Auskünfte zu beachten sind, weise ich auf Folgendes hin:

Dienstgebäude und Lieferanschrift:
Kavalleriestraße 2 - 4
40215 Düsseldorf
Telefon 0211 35424-0
Telefax 0211 35424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 705, 719
Haltestelle Poststraße

**Landesbeauftragter
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen**



07. April 2015
Seite 2 von 2

Möglicherweise bestehen aufgrund des Telekommunikationsgesetzes für geschäftsmäßige Anbieter von Telekommunikationsdiensten Vorgaben zur Entgegennahme und Beaufkennung von Ersuchen nach § 113 TKG auf gesichertem Wege. Diese Frage entzieht sich jedoch meiner Zuständigkeit. Hierfür ist gemäß § 115 Abs. 1 TKG die Bundesnetzagentur die zuständige Aufsichtsbehörde. Hinsichtlich der Anforderungen an die zur Mitwirkung verpflichteten Telekommunikationsunternehmen zur Beantwortung eines Auskunftsanspruchs sieht § 113 Abs. 5 S. 2 TKG vor, dass Anbieter, die mehr als 100.000 Kunden haben, für die Entgegennahme der Auskunftsverlangen sowie für die Erteilung der zugehörigen Auskünfte eine gesicherte elektronische Schnittstelle nach Maßgabe der Technischen Richtlinie nach § 110 Abs. 3 TKG bereitzustellen haben, durch die eine auch gegen die Kenntnisnahme der Daten durch Unbefugte gesicherte Übertragung gewährleistet ist. Aufgrund des § 110 Abs. 3 TKG hat die Bundesnetzagentur die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten (TR TKÜV) veröffentlicht. Sie sieht optional Vorgaben zu Schnittstelle und Verfahren bei Auskunftersuchen nach § 113 TKG vor.

Ebenso hat die Bundesnetzagentur auf ihrer Homepage einen Antrag für Verpflichtete nach § 113 Abs. 5 TKG auf Teilnahme an einem Verfahren zur gesicherten Übermittlung von Anordnungen und Auskünften mittels Kryptobox und VPN veröffentlicht. Ob Posteo hierzu nach den genannten Vorschriften verpflichtet ist, bitte ich gegebenenfalls bei der Bundesnetzagentur nachzufragen.

Mit freundlichen Grüßen
Im Auftrag





DER SÄCHSISCHE DATENSCHUTZBEAUFTRAGTE

Posteo e. K.
Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

Dresden, 10. April 2015

Az: G-0127/3/10
(Bitte bei Antwort angeben)

Telefon: [REDACTED]

Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG

Ihr Schreiben vom 17.2.2015

Sehr geehrter Herr Löhr,

auf Ihre Frage, ob wir 2013 oder 2014 Fälle nach dem automatisierten Auskunftsverfahren für Bestandstaten nach § 112 TKG kontrolliert oder deren Zulässigkeit überprüft haben, kann ich Ihnen mitteilen, dass wir dies nicht getan haben.

Mit freundlichen Grüßen



Postanschrift: Postfach 120705
01008 Dresden

Hausanschrift: Bernhard-von-Lindenau-Platz 1
01067 Dresden

Besucherverkehr: Devrientstraße 1
01067 Dresden

Telefon: (0351) 49 35 401
Telefax: (0351) 49 35 490

Internet: www.datenschutz.sachsen.de
E-Mail: saechsdsb@stl.sachsen.de

Antwort aus Niedersachsen



Die Landesbeauftragte für den Datenschutz Niedersachsen
Postfach 2 21 • 30002 Hannover

**Die Landesbeauftragte für den Datenschutz
Niedersachsen**

Posteo e.K.
z. Hd. Herrn Patrik Lühr
Methfesselstraße 38
10965 Berlin

Bearbeitet von

Ihr Zeichen, Ihre Nachricht vom

Mein Zeichen (Bitte bei Antwort angeben)

Durchwahl 0511 120-

Hannover,
20.04.2015

**Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG
hier: Ihre Anfrage vom 17.02.2015**

Sehr geehrter Herr Lühr,

zunächst einmal möchte ich mich für Ihre Anfrage vom 17.02.2015 bedanken.

Ich kann Ihnen hiermit mitteilen, dass mir für die Jahre 2013 und 2014 keinerlei Prüfverfahren für getätigte Abfragen gemäß § 112 TKG vorliegen.

Ich hoffe Ihrer Anfrage entsprochen zu haben und stehe für Rückfragen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrage

Besucher
Prinzenstr. 5
30159 Hannover

Telefon:
0511 120-4500

Telefax:
0511 120-4599

Internet: www.lfd.niedersachsen.de
E-Mail: poststelle@lfd.niedersachsen.de

Anhang III
Antworten der Datenschutzbeauftragten zu Kontrollen
von Ersuchen nach §112 TKG

Antwort der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Posteo e.K.
z. Hd. Herrn Patrik Lühr
Methfesselstr. 38
10965 Berlin

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

TELEFON
TELEFAX
E-MAIL
BEARBEITET VON

INTERNET www.datenschutz.bund.de

DATUM Bonn, 02.03.2015

GESCHAFTSZ. VIII-190-2 II#0286

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

BETREFF **Prüfungen des automatisierten Auskunftsverfahrens nach §112 TKG**

BEZUG Ihr Schreiben vom 17.02.2015 an die LDA Brandenburg

Sehr geehrter Herr Lühr,

vielen Dank für Ihr Schreiben, das mir die LDA Brandenburg zuständigkeitshalber
übersandt hat. In den letzten Jahren gab es nur wenige Anfragen zu Auskünften
nach § 112 TKG, meist von Polizeibehörden. Diese Fälle wurden zusammen mit der
BNetzA überprüft. In diesem Zusammenhang möchte ich auf die Beiträge Nr.
11.3.4.2 in meinem 19. Tätigkeitsbericht und Nr. 13.5 in meinem 20. Tätigkeitsbericht
hinweisen, die durchaus noch aktuell sind. Die Tätigkeitsberichte finden Sie auf
<http://www.bfdi.bund.de> in der Infothek. Sollten Sie noch weitere Fragen haben, kön-
nen Sie sich gerne an mich wenden.

Mit freundlichen Grüßen
Im Auftrag



7734/2015

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



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), D – 20095 Hamburg

An
Posteo e.K.
Methfesselstr. 38
10965 Berlin

Klosterwall 6, Block C
D – 20095 Hamburg

Az.: D42 / 2015/6TG

Hamburg, den 03.03.2015

Ihre Anfrage vom 17.02.2015

Sehr geehrter Herr Lühr,

zunächst einmal bestätige ich den Eingang Ihrer Anfrage vom 17.02.2015.

Zu Ihrer Anfrage kann ich Ihnen mitteilen, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in den Jahren 2013, 2014 keine Fälle nach dem automatisierten Auskunftsverfahren überprüft hat.

Ihre Anfrage wird aber zum Anlass genommen noch in diesem Jahr eine datenschutzrechtliche Kontrolle bei den in § 112 Abs. 2 TKG bezeichneten Stellen durchzuführen.

mit freundlichen Grüßen,

Homepage im Internet:
www.datenschutz-hamburg.de

E-Mail Sammelpostfach*:
mailbox@datenschutz.hamburg.de

Öffentliche Verkehrsmittel:
U-Bahnstation Steinstraße (Linie U1)
Busse 112, 120, 124, 34 (Steinstraße)

*Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 53D9 64DE 6DAD 452A 3796 B5F9 1B5C EB0E)



Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Der Landesbeauftragte für den Datenschutz Baden-Württemberg
Postfach 10 29 32 · 70025 Stuttgart

Posteo e.K.
z. Hd. Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

Datum: 13. April 2015
Name: [REDACTED]
Durchwahl: [REDACTED]
Aktenzeichen: F 7510/18
(Bitte bei Antwort angeben)

Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG

Ihr Fax vom 17. Februar 2015

Sehr geehrter Herr Löhr,

für Ihr Fax vom 17. Februar 2015 danken wir Ihnen.

Der Landesbeauftragte für den Datenschutz Baden-Württemberg ist für die Überprüfung von automatisierten Auskunftsverfahren nach § 112 TKG nicht die zuständige Aufsichtsbehörde. Die Einzelfallprüfungskompetenz liegt insoweit gemäß § 112 Absatz 4 Satz 2 TKG bei der Bundesnetzagentur. Soweit eine datenschutzrechtliche Überprüfung der automatisierten Auskunftsverfahren nach § 112 TKG erforderlich ist, obliegt gemäß § 115 Absatz 4 TKG die Prüfungskompetenz der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat daher in den Jahren 2013 und 2014 keine Überprüfung von automatisierten Auskunftsverfahren nach § 112 TKG durchgeführt.

Mit freundlichen Grüßen

Im Auftrag
[REDACTED]

Antwort aus Mecklenburg-Vorpommern



Der Landesbeauftragte
für Datenschutz und Informationsfreiheit
Mecklenburg-Vorpommern



Der Landesbeauftragte für Datenschutz und Informationsfreiheit M-V
Lennéstraße 1, Schloss · 19053 Schwerin

Posteo e.K.
Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

AKTENZEICHEN
1.4.8.039/074/2015-01587

IHR ZEICHEN

IHRE NACHRICHT
vom 17.02.2015

AUSKUNFT

23. Juli 2015

Manuelles Auskunftersuchen nach § 113 TKG Prüfung von automatisierten Auskunftsanfragen nach § 112 TKG

Sehr geehrter Herr Löhr,

Ihre Anfragen vom 17.02.2015 habe ich dankend erhalten.

Ich habe die betreffende Dienststelle kontaktiert und sie auf ihre Umsetzung von datenschutzrechtlichen Maßnahmen hingewiesen, damit Sie in Zukunft Anfragen nach § 113 TKG auf sicherem Wege erreichen und die Rechte des Betroffenen damit nicht verletzt werden.

Ebenfalls habe ich das Ministerium für Inneres und Sport Mecklenburg-Vorpommern auf diesen Missstand aufmerksam gemacht. Das Ministerium für Inneres und Sport Mecklenburg-Vorpommern versicherte mir, die Beamtinnen und Beamten hinsichtlich des richtigen Umgangs mit personenbezogenen Daten und des Umgangs mit TKÜ-Abfragen nach § 113 TKG erneut zu sensibilisieren.

Bezüglich Ihrer Anfrage über die Prüfung bei automatisierten Auskunftsanfragen nach § 112 TKG durch diese Behörde muss ich Ihnen mitteilen, dass eine solche Prüfung bisher nicht erfolgt ist.

Aufgrund einer Vielzahl von Petitionen in verschiedenen Bereichen des Datenschutzes und der Informationsfreiheit ist es uns zeitlich und personell nicht möglich eigeninitiierte Prüfungen über Anfragen nach § 112 TKG vorzunehmen.

Ich hoffe, Ihnen mit dieser Antwort weitergeholfen zu haben, und stehe Ihnen für weitere Fragen gerne zur Verfügung.

Mit freundlichen Grüßen
im Auftrag



POSTANSCHRIFT: Lennéstraße 1, Schloss, 19053 Schwerin

HAUSANSCHRIFT: Johannes-Stelling-Straße 21, 19053 Schwerin

KOMMUNIKATION: Telefon 0385 59494-0, Telefax 0385 59494-58, datenschutz@mvnet.de, www.datenschutz-mv.de, www.informationsfreiheit-mv.de

GPG-Fingerprint: ADB5 030A C111 388C A8FD 92B7 EF40 56E6 71DA 3ABA

ULD



www.datenschutzzentrum.de

ULD - Postfach 71 16 - 24171 Kiel

Posteo e.K.
Herrn Patrik Löhr
Methfesselstraße 38
10965 Berlin

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:

Aktenzeichen:
LD5-74.03/23.006

Kiel, 20. Februar 2015

Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG Ihr Schreiben vom 17. Februar 2015

Sehr geehrter Herr Löhr,

vielen Dank für Ihr oben genanntes Schreiben.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat in den Jahren 2013 und 2014 keine gezielten Prüfungen von Abrufen nach § 112 TKG durchgeführt. Hierzu sind weder Eingaben von Bürgerinnen und Bürgern beim ULD eingegangen, noch hat das ULD diesbezüglich anlasslose Kontrollen durchgeführt. Bestandsdatenauskünfte bei Telekommunikationsdiensteanbietern waren allerdings Gegenstand einiger Strafverfahren, die unter dem Aspekt der nicht individualisierten Funkzellenabfrage nach § 100g Strafprozessordnung in eine Stichprobenprüfung durch das ULD einbezogen wurden. Diese Verfahren wurden jedoch nicht eigenständig erfasst, so dass die Anzahl der Fälle nicht statistisch ermittelbar ist. Nach meiner Erinnerung waren dies nur wenige Fälle (max. fünf).

Mit freundlichen Grüßen

ULD | Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel | Tel. +49 431 988-1200 | Fax +49 431 988-1223
www.datenschutzzentrum.de | E-Mail: mail@datenschutzzentrum.de
PGP-Fingerprint: 042D 0B0E 6D4F F4D3 FB5D 1B6A 318C B401

- 2 -



Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit RLP
Postfach 33 40 | 55020 Mainz

Posteo e.K.
z.H. Herrn Patrick Lohr
Methfesselstr. 38
10965 Berlin

Hinterer Bleichro 34 | 55116 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Ihr Zeichen: _____ Ihre Nachricht vom: _____ Geschäftszahlen: _____ Telefondurchwahl: _____ Datum: 20.02.2015

Prüfung von Bestandsdaten-Auskünften gem. § 112 TKG

Sehr geehrter Herr Lohr,

zunächst ist auf Folgendes hinzuweisen:

Das Verfahren nach § 112 TKG berechtigt folgende Landesstellen zu einer Datenabfrage über die Bundesnetzagentur:

- die Landesgerichte,
- die Strafverfolgungsbehörden des Landes (vor allem also die Staatsanwaltschaften und ihre Ermittlungspersonen, also Polizeibeamte),
- die gefahrenabwehrend tätigen Polizeibehörden,
- den Landesverfassungsschutz,
- die Notrufabfragestellen.

Diese können mittelbar über die Bundesnetzagentur auf folgende Daten von Anschlussinhabern zugreifen:

- Rufnummern und andere Anschlusskennungen,
- Namen und Anschrift des Anschlussinhabers,
- Geburtsdatum,
- bei Festnetzanschlüssen Anschrift des Anschlusses,
- Gerätenummer eines Mobilfunkgerätes, wenn neben einem Mobilfunkanschluss auch ein entsprechendes Gerät überlassen wurde,
- Datum des Vertragsbeginns,
- die Kennungen und Inhaber elektronischer Postfächer bei elektronischer Post (Emails),
- entsprechende Änderungsdaten.

Es handelt sich also um ein Auskunftsverfahren über Bestandsdaten, die gegenüber einem herkömmlichen Telefonbuch um bestimmte Daten (etwa Beginn und Ende eines Vertrags) erweitert sind.

In meiner langjährigen Praxis hat es in diesem Zusammenhang noch keine Beschwerde eines Nutzers wegen unrechtmäßiger Auskunftserteilung gegeben, obwohl solche Auskunftersuchen in zahlreichen Strafverfahren eine Rolle spielen und dann häufig über die Akteneinsicht auch den Betroffenen bekannt werden.

Auch aus sonstigen Gesichtspunkten heraus hat sich bislang für mich kein Anlass ergeben, auf Seiten der abrufberechtigten Landesstellen eine gezielte Kontrolle der über die Bundesnetzagentur erfolgenden Abrufe vorzunehmen. Für die Überprüfung der durch die Bundesnetzagentur erfolgenden Übermittlungen und die entsprechenden Auskünfte der Verpflichteten ist allein die Bundesdatenschutzbeauftragte zuständig (gem. § 115 Abs. 4 Telekommunikationsgesetz).

Da im Land allerdings ein neues zentrales Kompetenz-Zentrum für Telekommunikationsüberwachungsmaßnahmen eingerichtet wurde, habe ich diesen Bereich ohnehin auf meinem Prüfplan für das laufende Jahr. In diesem Zusammenhang werde ich auch das Verfahren gem. § 112 TKG und konkret auf dieser Basis erfolgende Abrufe kontrollieren.

Ich hoffe, Ihnen mit diesen Auskünften weitergeholfen zu haben.

Mit freundlichen Grüßen
in Vertretung





DER SÄCHSISCHE DATENSCHUTZBEAUFTRAGTE

Posteo e. K.
Herrn Patrik Löhr
Methfesselstr. 38
10965 Berlin

Dresden, 10. April 2015

Az: G-0127/3/10
(Bitte bei Antwort angeben)

Telefon: [REDACTED]

Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG

Ihr Schreiben vom 17.2.2015

Sehr geehrter Herr Löhr,

auf Ihre Frage, ob wir 2013 oder 2014 Fälle nach dem automatisierten Auskunftsverfahren für Bestandstaten nach § 112 TKG kontrolliert oder deren Zulässigkeit überprüft haben, kann ich Ihnen mitteilen, dass wir dies nicht getan haben.

Mit freundlichen Grüßen



Postanschrift: Postfach 120705
01008 Dresden

Hausanschrift: Bernhard-von-Lindenau-Platz 1
01067 Dresden

Besucherverkehr: Devrientstraße 1
01067 Dresden

Telefon: (0351) 49 35 401
Telefax: (0351) 49 35 490

Internet: www.datenschutz.sachsen.de
E-Mail: saechdsb@slt.sachsen.de



Die Landesbeauftragte für den Datenschutz Niedersachsen
Postfach 2 21 • 30002 Hannover

**Die Landesbeauftragte für den Datenschutz
Niedersachsen**

Posteo e.K.
z. Hd. Herrn Patrik Löhr
Methfesselstraße 38
10965 Berlin

Bearbeitet von

Ihr Zeichen, Ihre Nachricht vom

Mein Zeichen (Bitte bei Antwort angeben)

Durchwahl 0511 120-

Hannover,
20.04.2015

**Prüfungen bei automatisierten Auskunftsanfragen nach § 112 TKG
hier: Ihre Anfrage vom 17.02.2015**

Sehr geehrter Herr Löhr,

zunächst einmal möchte ich mich für Ihre Anfrage vom 17.02.2015 bedanken.

Ich kann Ihnen hiermit mitteilen, dass mir für die Jahre 2013 und 2014 keinerlei Prüfverfahren für getätigte Abfragen gemäß § 112 TKG vorliegen.

Ich hoffe Ihrer Anfrage entsprochen zu haben und stehe für Rückfragen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Besucher
Prinzenstr. 5
30159 Hannover

Telefon:
0511 120-4500

Telefax:
0511 120-4599

Internet: www.lfd.niedersachsen.de
E-Mail: poststelle@lfd.niedersachsen.de

Anhang IV

Antworten der Justizministerien zum Richtervorbehalt

Die Antwort des berliner Justizministeriums

Senatsverwaltung für Justiz und Verbraucherschutz



Senatsverwaltung für Justiz und Verbraucherschutz
Salzburger Str. 21 - 25 • 10825 Berlin

Posteo e.K.
Z.Hd.
Herrn
Patrik Lühr
Methfesselstraße 38
10965 Berlin

Geschäftszeichen (bitte immer angeben)
III CS 2 – 3133/E/26/2015

Bearb.:

Telefon:

(Vermittlung)

(Intern)

Telefax:

Internet: www.berlin.de/senjust

E-Mail: poststelle@senjust.berlin.de

Elektronische Zugangseröffnung gemäß
§ 3a Abs.1 VwVfG: www.egvp.de

Datum: 22. Januar 2015

Ihre Eingabe vom 9. Januar 2015



Sehr geehrter Herr Lühr,

Ich bestätige den Eingang Ihres vorbezeichneten Schreibens, in dem Sie um Mitteilung der Zahlen bezüglich in Berlin abgelehnter Anträge zur Telekommunikationsüberwachung bitten.

Die von Ihnen gewünschte Information können Sie über die offizielle Seite des Abgeordnetenhauses von Berlin unter dem Stichwort Parlamentsdokumentationen abfragen. Dort ist zu der Drucksache 17/1769 der Jahresbericht 2013 über die Praxis der Telefonüberwachung nach §§ 100a, 100b StPO veröffentlicht. Die von Ihnen erfragten Daten befinden sich darunter.

Die Zahlen für das Jahr 2014 liegen bislang noch nicht vor, mit einer Veröffentlichung ist jedoch im Frühjahr zu rechnen.

Ich hoffe, Ihnen mit diesem Hinweis geholfen zu haben.

Mit freundlichen Grüßen
Im Auftrag

Befugtigt

Beschäftigte



Verkehrsverbindungen: ☎ 104, M 46 bis Rathaus Schöneberg, ☎ 4 bis Rathaus Schöneberg, ☎ 7 bis Bayerischer Platz
Eingang zum Dienstgebäude: Salzburger/Ecke Badensche Straße, 10825 Berlin-Schöneberg
Zahlungen bitte bargeldlos an die Landeshauptkasse Berlin, 10789 Berlin, auf eines der folgenden Konten:

Geldinstitut
Postbank Berlin

IBAN:
DE4710010010000058100

BIC:
PBNKDEFF100

Geldinstitut
Bundesbank, Filiale Berlin

IBAN:
DE53100000000010001520

BIC:
MARKDEF1100

Die Antwort des hessischen Justizministeriums

26-JAN-2015 11:00

Hess.- Min. D. Justiz

+49 611 322868

S.01/01

Hessisches Ministerium der Justiz

HESSEN



Hessisches Ministerium der Justiz
Postfach 31 88 - 65021 Wiesbaden

Posteo e.K.
Herrn Patrik Lühr
Methfesselstr. 38
10965 Berlin

Aktenzeichen:

4104E - III/A 1 - 2015/879 - III/A

Dist.-Nr.:
Bearbeiter:
Durchwahl:
Fax:
E-Mail:



Datum:

21. Januar 2015

Überwachung der Telekommunikation

Zu Ihrem Schreiben vom 9. Januar 2015

Sehr geehrter Herr Lühr,

in Beantwortung Ihres o.g. Schreibens teile ich Ihnen mit, dass mir Zahlen darüber, in wie vielen Fällen einem Antrag auf Überwachung der Telekommunikation nicht stattgegeben wurde, nicht vorliegen.

Eine Ermittlung dieser Daten setzt die händische Auswertung aller infrage kommenden Ermittlungsakten voraus, ein Aufwand, der mir unverhältnismäßig erscheint und den Strafverfolgungsbehörden nicht zugemutet werden kann. Hierfür bitte ich um Verständnis.

Mit freundlichen Grüßen
Im Auftrag



65185 Wiesbaden - Luisenstraße 13
Telefon (0611) 32-0
Telefax (0611) 32 27 63
E-Mail: poststelle@hmdj.hessen.de - www.hmdj.hessen.de

GESAMTSEITEN 01

Die Antwort des bayrischen Justizministeriums

Bayerisches Staatsministerium der
Justiz



Bayerisches Staatsministerium der Justiz • 80097 München

Herrn Patrik Löhrl
Posteo e.K.
Methfesselstraße 38
10965 Berlin

Sachbearbeiter



Ihr Zeichen, Ihre Nachricht vom
9. Januar 2015

Bitte bei Antwort angeben
Unser Zeichen, Unsere Nachricht vom
E7-4101E-II-282/2015

Datum
14. Januar 2015

Ablehnung von beantragten TKÜ-Maßnahmen

Sehr geehrter Herr Löhrl,

mit Ihrem Schreiben vom 9. Januar 2015 baten Sie um Auskunft zur Anzahl der in Bayern in den Jahren 2013 und/oder 2014 beantragten aber nicht bewilligten Beschlüssen für Telekommunikationsmaßnahmen.

Zwar werden in Bayern die erlassenen Beschlüsse und die durchgeführten TKÜ-Maßnahmen zur Erfüllung der Berichtspflicht nach § 100b Abs. 5, Abs. 6 StPO statistisch erfasst. § 100b Abs. 5, Abs. 6 StPO sieht hingegen keine Pflicht zur Erfassung von abgelehnten Anträgen vor, weswegen dazu auch keine Statistik besteht. Zahlen zu abgelehnten Anträgen kann ich Ihnen daher nicht mitteilen.

Die Zahlen zu den erlassenen Beschlüssen sind auf der Webseite des Bundesamtes für Justiz (www.bundesjustizamt.de) veröffentlicht.

Mit freundlichen Grüßen



Ministerialrat

Hausanschrift
Prielmayerstr. 7
Justizpalast
80335 München

Haltestelle
Karlsplatz (Stachus)
S-Bahn, U-Bahn
Trambahn

Telefon
(089) 5597-01
(Vermittlung)

Telefax
5597-2322

E-Mail:
poststelle@stmj.bayern.de
Internet:
<http://www.justiz.bayern.de>

Die Antwort des Justizministeriums aus Mecklenburg-Vorpommern

Justizministerium Mecklenburg-Vorpommern

- Nur per E-Mail -

Herrn
Patrik Löhr
Posteo e.K.
Methfesselstr. 38
10965 Berlin

bearbeitet von:

Telefon:

Geschäftszeichen: III 340/4104E-13
(Bitte bei Antwort angeben.)

Schwerin,

16. Januar 2014

Ablehnungen von TKÜ-Anträgen

Ihr Schreiben vom 09.01.2015

Sehr geehrter Herr Löhr,

auf Ihre vorgenannte Anfrage teile ich mit, dass in Mecklenburg-Vorpommern keine Zahlen
über gestellte oder abgelehnte TKÜ-Anträge vorliegen.

Mit freundlichen Grüßen
Im Auftrag



Hausanschrift:

Justizministerium Mecklenburg-Vorpommern
Puschkinstraße 19-21, 19055 Schwerin

Postanschrift

Justizministerium Mecklenburg-Vorpommern
19048 Schwerin

Telefon: 0385 588-0

Telefax: 0385 588-3453

E-Mail: poststelle@jm.mv-regierung.de

Die Antwort des Justizministeriums aus Baden-Württemberg



Baden-Württemberg JUSTIZMINISTERIUM

Justizministerium Baden-Württemberg • Postfach 103461 • 70029 Stuttgart

Posteo e.K.
Herrn Patrick Löhr
Methfesselstraße 38
10965 Berlin

Datum 19. Januar 2015
Name
Durchwahl
Aktenzeichen
(Bitte bei Antwort angeben)

 Ihr Schreiben vom 9. Januar 2015

Sehr geehrter Herr Löhr,

Ihre oben genannte Anfrage ist beim Justizministerium eingegangen.

Sie bitten um Auskunft, wie vielen Anträgen zu einer TKÜ im Jahr 2014 (oder auch in einem früheren Jahr) in Baden-Württemberg nicht stattgegeben worden ist.

Leider muss ich Ihnen mitteilen, dass diese Zahl uns nicht vorliegt; über die Ablehnung von Maßnahmen zur TKÜ wird hier keine Statistik geführt.

Mit freundlichen Grüßen


Bürgerreferent

Schillerplatz 4 • 70173 Stuttgart • Telefon 0711 279-0 • Telefax 0711 279-2264 • poststelle@jum.bwl.de
www.justiz.baden-wuerttemberg.de • www.service-bw.de

Parkmöglichkeiten: Tiefgarage Commerzbank Einfahrt Dorotheenstraße • VVS-Anschluss: U-Bahn: Schlossplatz S-Bahn: Stadtmitte

Die Antwort des sächsischen Justizministeriums

STAATSMINISTERIUM
DER JUSTIZ



SÄCHSISCHES STAATSMINISTERIUM DER JUSTIZ
Hospitalstraße 7 | 01097 Dresden

Posteo e. K.
Patrik Löhner
Methfesselstr. 38
10965 Berlin

Ihre Ansprechpartnerin

Durchwahl

Ihr Schreiben vom
9. Januar 2015

Aktenzeichen
(bitte bei Antwort angeben)
1410E-ÖR-1/15

Dresden,
21. Januar 2015

Überwachung der Telekommunikation

Sehr geehrter Herr Löhner,

die Länder berichten zu den in ihrem Zuständigkeitsbereich angeordneten Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO aufgrund von § 100b Abs. 5 StPO kalenderjährlich dem Bundesamt für Justiz. Die Berichte haben jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres zu erfolgen. Die Daten für das Berichtsjahr 2014 liegen hier noch nicht vor.

Die Daten zu angeordneten Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO für das Jahr 2013 wurden bereits auf der Internetseite des Bundesamts für Justiz unter

https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/uebersicht_TKUE_2013.pdf?__blob=publicationFile&v=3 veröffentlicht.

Die Fälle, in denen der Erlass einer richterlichen Anordnung zur Telekommunikationsüberwachung nach § 100a StPO abgelehnt wurde, werden statistisch nicht erfasst. Daher können dazu keine Fallzahlen mitgeteilt werden.

Mit freundlichen Grüßen

In Vertretung



Seite 1 von 1



Beglaubigt
Justizangestellte



Hausanschrift:
Sächsisches Staatsministerium
der Justiz
Hospitalstraße 7
01097 Dresden

Briefpost über Deutsche Post
01095 Dresden

www.justiz.sachsen.de/smj

Verkehrsverbindung:
Zu erreichen mit
Straßenbahnlinien
3, 6, 7, 8, 11

Parken und behinderten-
gerechter Zugang über
Einfahrt Hospitalstraße 7

*Zugang für elektronisch signierte sowie
für verschlüsselte elektronische Dok-
umente nur über das Elektronische
Gerichts- und Verwaltungsportal;
nähere Informationen unter
www.egvp.de

Die Antwort des Justizministeriums aus Sachsen-Anhalt



SACHSEN-ANHALT

Ministerium für
Justiz und Gleichstellung

Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt
Postfach 3764 · 39012 Magdeburg

Posteo e.K.
Methfesselstr. 38
10965 Berlin

Beschlagnahme von E-Mails und sonstige Maßnahmen der Telekommunikationsüberwachung

Ihr Schreiben vom 9.1.2015

Sehr geehrter Herr Löhr,

auf Ihre Anfrage vom 9.1.2015 teile ich mit, dass dem Ministerium für Justiz und Gleichstellung des Landes Sachsen-Anhalt keine statistischen Angaben zu (gerichtlich) abgelehnten Anträgen auf Beschlagnahme von auf Mailservern eines Providers gespeicherten E-Mails vorliegen. Ebenso wenig stehen statistische Erhebungen über sonstige abgelehnte Anträge (der Staatsanwaltschaften) auf Durchführung von Maßnahmen der Überwachung der Telekommunikation zur Verfügung.

Mit freundlichen Grüßen

Im Auftrag

Beglaubigt

(Angestellte)

Magdeburg, 20. Januar 2015

Ihr Zeichen/Ihre Nachricht vom:

Az.: 4104 E-401.1217/2015

Bearbeitet von:

Domplatz 2 - 4
39104 Magdeburg
Telefon (0391) 567-01
Telefax (0391) 567-6180
poststelle@mj.sachsen-anhalt.de
www.sachsen-anhalt.de

Landeshauptkasse Sachsen-Anhalt
Deutsche Bundesbank
BIC MARKDEF1810
IBAN
DE21 8100 0000 0081 0015 00

Die Antwort des Justizministeriums aus Schleswig-Holstein



Schleswig-Holstein
Ministerium für Justiz,
Kultur und Europa

Ministerium für Justiz, Kultur und Europa des Landes
Schleswig-Holstein | Postfach 71 45 | 24171 Kiel

Poesteo e.K.
Herrn Patrick Löhr
Methfesselstraße 38
10965 Berlin

Ihr Zeichen: -
Ihre Nachricht vom: -
Mein Zeichen: II 302/4100-185
Meine Nachricht vom: -



3. Februar 2015

Ihr Schreiben vom 9. Januar 2015

Sehr geehrter Herr Löhr,

ich teile Ihnen mit, dass in Schleswig-Holstein keine Statistik über abgelehnte Telekommunikationsüberwachungs (TKÜ) - Anträge der Staatsanwaltschaften geführt wird. Daher ist nicht bekannt, in wie vielen Fällen TKÜ-Anträgen durch die jeweils zuständigen Gerichte nicht entsprochen worden ist.

Mit freundlichen Grüßen



Angestellte



Die Antwort des Justizministeriums aus Bremen

**Der Senator für
Justiz und Verfassung**



Der Senator für Justiz und Verfassung
Richtweg 16 - 22 · 28195 Bremen

Posteo e.K.
Methfesselstraße 38
10965 Berlin

Auskunft erteilt



Datum und Zeichen
Ihres Schreibens

Mein Zeichen
(bitte bei Antwort angeben)
4047-8

Bremen, 16. Januar 2015

Ihr Schreiben vom 09.01.2015

Sehr geehrter Herr Löhr,

die Anzahl der eine Überwachung der Telekommunikation ablehnenden richterlichen Beschlüsse wird in meinem Geschäftsbereich nicht statistisch erfasst. Die gewünschte Information kann ich Ihnen deshalb leider nicht geben.


Mit freundlichen Grüßen

Im Auftrag



 Eingang
Richtweg
28195 Bremen

 Parkhaus
Rövekamp
28195 Bremen

 Bus / Straßenbahn
Haltestellen
Hauptbahnhof

Sprechzeiten
Mo. - Do.:
09:00 - 15:00 Uhr
Fr.:
09:00 - 13:30 Uhr

Die Antwort des Justizministeriums aus Brandenburg



LAND BRANDENBURG

**Ministerium der Justiz
und für Europa
und Verbraucherschutz**

Ministerium der Justiz und für Europa und Verbraucherschutz des Landes Brandenburg | Heinrich-Mann-Allee 107 | 14473 Potsdam

Posteo
Herrn Patrik Löhr
Methfesselstraße 38
10965 Berlin

Heinrich-Mann-Allee 107
D-14473 Potsdam

Bearbeiterin: 
Telefon: 
Nebenstelle: 
Fax: (03 31) 
E-Mail: Poststelle@mdjev.brandenburg.de
Internet: www.mdjev.brandenburg.de
Aktenzeichen (bei Antwort bitte angeben)
1410 - E III.005/15 (II.5)

Potsdam, 16. Januar 2015

Anordnungen zur Telekommunikationsüberwachung (TKÜ)
hier: Anzahl der Ablehnungen

Ihr Schreiben vom 9. Januar 2015

Sehr geehrter Herr Löhr,

für Ihre Anfrage vom 9. Januar 2015 bedanke ich mich.

Eine Auskunft über die Anzahl der Ablehnungen zur Anordnung einer Telekommunikationsüberwachung kann Ihnen auf der Grundlage Ihrer Anfrage aber nicht erteilt werden.

Mit freundlichen Grüßen
Im Auftrag

