

Stellungnahme

Überprüfung der Richtigkeit von Anschlussinhaberdaten im Sinne des § 111 des Telekommunikationsgesetzes (TKG)

30. September 2016

Seite 1

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 900 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet Service Provider-Verband Europas.

Am 30. Juli 2016 trat eine Änderung des § 111 Telekommunikationsgesetz (TKG) in Kraft, die ab dem 1. Juli 2017 strengere Vorgaben für die Datenerhebung und -überprüfung bei im Voraus bezahlten Mobilfunkleistungen vorsieht. Gemäß § 111 Absatz 1 Satz 4 TKG soll die Bundesnetzagentur durch Verfügung im Amtsblatt festlegen, welche anderen Verfahren als das gesetzlich vorgesehene zur Überprüfung der Daten geeignet sind. Bitkom und eco bedanken sich für die Gelegenheit der Kommentierung des Entwurfs der Bundesnetzagentur der geplanten Verfügung gemäß § 111 Absatz 1 Satz 4 TKG und nehmen hierzu wie folgt Stellung:

Zusammenfassung

Schon im Zuge des Gesetzgebungsverfahrens wurde angemerkt, dass insbesondere die Identitätsfeststellung beim Offline-Kauf und Speicherung von Nutzerdaten (z.B. beim Kauf im Discount-Supermarkt oder Tankstelle) die Komplexität des Vertriebs von Prepaid-Sim-Karten erheblich steigert und kostenintensive Prozessimplementierungen bei

**bitkom - Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.**

Nick Kriegeskotte
Bereichsleiter
Telekommunikationspolitik
T +49 30 27576-224
n.kriegeskotte@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

www.bitkom.org

**eco - Verband der Internet-
wirtschaft e.V.**

Nicolas Goß
Referent Telekommunikations-
recht & Regulierung
+49 221 - 70 00 48 - 150
nicolas.goss@eco.de

Französische Str. 48
10117 Berlin

Vorstandsvorsitzender
Prof. Rotert

Geschäftsführer
Harald Summa

www.eco.de

Stellungnahme Überprüfung der Richtigkeit von Anschlussinhaberdaten

Seite 2|5



allen beteiligten Partnern, vom Provider bis zum Händler, voraussetzt. Besonders kleine und mittlere Unternehmen würden belastet, erstens auf Grund der Personalstärke als durch den vorhersehbaren Umsatzrückgang bei Prepaid-Sim-Karten. Dies erkennt grundsätzlich auch der Gesetzentwurf, indem er neben der Vorlage auch „die Überprüfung durch andere geeignete Verfahren“, die nun die Bundesnetzagentur mit ihrem Entwurf festlegen will, erlaubt. Wichtig ist aus Sicht der Verbände, einen Medienbruch zu vermeiden und auch vollständig elektronische bzw. automatisierte Verfahren zu ermöglichen. Mit Blick auf diese Zielsetzung und die praktische Umsetzbarkeit ergibt sich aus Sicht des eco und des Bitkom insbesondere hinsichtlich der erforderlichen Schulung des Personals, der zulässigen Verfahren und der Echtheitsprüfung ein Anpassungsbedarf des vorliegenden Entwurfs. Im Einzelnen:

1. Umsetzungsfrist

- Geschäftsmodelle, die den Verkauf von Prepaid-SIM-Karten außerhalb der Points of Sale (POS) von Telekommunikationsbetreibern vorsehen (bspw. Drogeriemärkte, Tankstellen usw.), können eine Vor-Ort-Prüfung durch eine physische Person gem. Verfügungsentwurf nicht wirtschaftlich abbilden. Damit droht eine signifikante Beeinträchtigung des Prepaid-SIM-Marktes, welcher weder kurz- noch mittelfristig durch den Rückgriff auf Postpaid-Modelle (nicht zuletzt mit Blick auf die Kundenstruktur für den Prepaid-SIM-Markt) substituiert werden wird.
- Die Frist für die Umsetzung der Verfahren nach Veröffentlichung der Verfügung zum 1.1.2017 ist zu kurz bemessen. Den Anbietern blieben nach Veröffentlichung der Verfügung zum 1.1.2017 nur 6 Monate, um die neue Gesetzgebung an den Verkaufsstellen und online umzusetzen. Die Umsetzung der Verfahren hat jedoch weitreichende technische, prozessuale, vertragsrechtliche und personelle Implikationen. Dafür müssen u.a. personelle Kapazitäten aufgebaut und informiert werden.
- Klarstellungsbedürftig ist zudem, dass die Verifizierungsvorgaben nicht für (Prepaid-) IoT-/M2M SIM-Karten gelten (d.h. SIM-Karten, die nicht der zwischenmenschlichen Kommunikation dienen, sondern in Gegenständen, Maschinen, etc. eingebaut sind).

2. Schulungserfordernis

- Aus Sicht der Verbände ist zudem ein Schulungserfordernis nicht Gegenstand der gesetzlichen Verpflichtung, so dass eine Regelungskompetenz nicht gegeben ist. Unabhängig davon sollte aus Sicht der Verbände jedenfalls ausreichend sein, soweit Personen mit dem Verifizierungsprozess betraut werden, mittels eines Merkblatts bzw. einer Checkliste auf wesentliche Elemente echter Ausweisdokumente aufmerksam zu machen. Gleiches gilt für den Vorgang der Datenerhebung und -prüfung. Damit kann eine ausreichende Sicherheit hinsichtlich der vorgelegten Dokumente erreicht werden. Eine tatsächliche Verifizierung der Echtheit kann nicht gefordert werden.

Stellungnahme Überprüfung der Richtigkeit von Anschlussinhaberdaten

Seite 3|5



3. Zulässige Verfahren und Verifizierung durch Vertriebspartner oder Diensteanbieter

- Mit Blick auf die vorstehenden Punkte ist es aus Sicht der Informations- und Kommunikationswirtschaft erforderlich, weitere geeignete Verfahren im Sinne des § 111 Abs. 1 S. 4 TKG zuzulassen. Dazu zählen Videoübertragungsverfahren, bei denen die „prüfende Person“ durch geeignete halb- oder vollständig automatisierte Verfahren ersetzt werden kann. Neben der Abfederung von Spitzenlasten sowie der Lösung der schon jetzt absehbaren personellen Engpässe und der Beeinträchtigung bestehender Geschäftsmodelle würde mit entsprechenden Verfahren ein höheres Sicherheitsniveau bei der Überprüfung der vorgelegten Identitätsdokumente erzielt werden, da schon heute maschinelle Verfahren (jenseits forensischer Echtheitsüberprüfungen, die im Regelungsbereich der Verfügung nicht abgedeckt werden können) ein durchschnittlich höheres Sicherheitsniveau gewährleisten können.
- Im Hinblick auf die Vorgabe, dass der Abgleich notwendigerweise zeitgleich zu erfolgen hat, ist eine unnötige Einschränkung mit signifikant negativen Auswirkungen auf die Kapazitäten erfolgt, die zur Überprüfung vorgehalten werden müssen, auch weil etwa ein zeitversetzter Peak Ausgleich nicht möglich ist. Vielmehr sollte auch die Verwendung eines zeitversetzten Foto-Ident Verfahrens ermöglicht werden. Dabei könnte etwa der Ausweis-Scan zusammen mit einer kurzen Video-Sequenz, in welcher der Anschlussinhaber sein Identitätsdokument zur Überprüfung der Level-1-Sicherheitsmerkmale und der Erfassung seines Lichtbildes sowie der auf dem Dokument aufgetragenen Inhaberdaten bewegt bzw. kippt, elektronisch übertragen und dann überprüft werden. Hinsichtlich der Vorgabe „Bei schlechten Lichtverhältnissen... ist ein sofortiger Abbruch vorzusehen“ ist festzuhalten, dass ein Abbruch nicht in jedem Fall erforderlich ist. Statt eines Abbruchs sollten die Lichtverhältnisse zunächst gemeinsam mit dem Kunden verbessert werden bzw. der Kunde sollte zu einem alternativen Verfahren beraten werden dürfen. Bei der Vorgabe, dass „bei dem Eindruck, dass eine Täuschung oder sonstige Manipulation vorliegt, ist ein sofortiger Abbruch vorzusehen“ ist, sollte der Gedanke berücksichtigt werden, ob dem Sicherheitsgedanken nicht besser damit gedient wäre, die Datenerfassung zunächst abzuschließen und die Daten entsprechend zu melden. Dabei handelt es sich um eine bereits häufig geübte Praxis bei Video-Ident-Anbietern, auch vor dem Hintergrund der Vermeidung zukünftiger Betrugsfälle.
- Es erscheint zweifelhaft, ob in § 111 Abs. 1 S. 4 TKG eine Regelungskompetenz der BNetzA für die Festlegung der Verifizierung durch Vertriebspartner zu sehen ist. Zum einen dürfte es sich bereits nicht um anderes Verfahren im Sinne des § 111 Abs. 1 S. 4 TKG handeln. Denn das Verfahren beschreibt die Vorlage eines Identifikationsdokuments im Rahmen des Verkaufsvorgangs der SIM-Karte und wiederholt damit lediglich das bereits in § 111 Abs. 1 S. 3 TKG definierte Verfahren. Die Einbindung eines Dritten, hier eines Vertriebspartners, ist insoweit nicht als eigenständiges Verfahren festzulegen. Zudem ist hier eigentlicher Regelungsgegenstand die obligatorische Vorhaltung von „Vorkehrungen, die dem Diensteanbieter eine Kontrolle der erfolgten Überprüfung ermöglichen“. Jedoch stellt die Art und Weise der Kontrolle des Diensteanbieters von Dritten, welche in den Prozess der Prüfung einbezogen werden, gerade keine Regelung eines Verfahrens dar. Die Verantwortlichkeit des Diensteanbieters bei der Einbeziehung von Dritten wird vielmehr separat, nunmehr in § 111 Abs. 4 TKG, geregelt. Wie der Diensteanbieter seiner Verantwortung nachkommt, muss allein ihm vorbehalten bleiben. Sofern die Kontrollverpflichtung

Stellungnahme Überprüfung der Richtigkeit von Anschlussinhaberdaten

Seite 4|5



tung für Vertriebspartner wider Erwarten beibehalten bleibt, ist für deren aufwändige Umsetzung eine längere Frist, nämlich von mindestens weiteren 12 Monaten, einzuräumen.

- Nach der gewählten Formulierung *„Die Erhebung der Anschlussinhaberdaten kann auch mittels der eID-Funktion des Personalausweises erfolgen. Diese Funktion stellt jedoch keinen Ersatz für den Abgleich der Person...mit der im Identitätsdokument ausgewiesenen Person dar.“* dürfte die Verwendung der eID nicht den Abgleich des Anschlussinhabers mit der abgebildeten Person im Identitätsdokument ersetzen, d.h. die eID-Funktion dient nur der Erhebung der Anschlussinhaberdaten, es ist weiterhin ein persönlicher Abgleich erforderlich. Dies widerspricht aus unserer Sicht dem originären Zweck der eID-Funktion. Die Verwendung der eID-Funktion als sicheres Legitimationsverfahren sowie weiterer mittelbarer Verfahren, die auf eine bereits erfolgte Verifizierung zurückgreifen (z.B. POSTID) sollten zugelassen werden.
- Wir begrüßen die Möglichkeit, dass auch die erworbene SIM-Karte in die Prüfung eingebunden werden kann. Allerdings sollte diese nicht auf Datenverbindungen beschränkt sein. Vielmehr sollten zur Registrierung und Prüfung auch sonstige Verbindungen zugelassen werden, bspw. den Eingang einer Anbieter-SMS mit Link zum Verifizierungsanbieter oder der Sprach- bzw. Video-Anruf an eine Service-Line. Wir erlauben uns daher, folgenden alternativen Formulierungsvorschlag vorzuschlagen: *„Die Erhebung, Überprüfung und Übermittlung der Identitätsdaten kann auch mit der erworbenen Mobilfunkleistung selbst, bspw. mit der erworbenen SIM-Karte, erfolgen. Die Mobilfunkleistung vor der abgeschlossenen Verifikation darf ausschließlich für die zur Registrierung und Prüfung des Identitätsdokuments notwendige Kommunikation ermöglicht werden.“*

4. Echtheitsprüfung

- Wie die jüngsten Pressemitteilungen zeigen, gelingt es Beamten und Angestellten des Bundes (BAMF) und der Kommunen (Einwohnermeldeämter) anscheinend nicht, ausländische Ausweisdokumente hinsichtlich ihrer Echtheit zuverlässig zu überprüfen. Aufgrund dieser praktischen Erfahrungen mit hinsichtlich der Echtheitsprüfung spezialisiertem staatlichem Personal und der oben aufgezeigten Herausforderungen bei der Personalschulung erscheint das gesetzgeberische Ziel daher besser erreichbar, wenn zusätzlich automatisierte Verfahren zugelassen werden.
- Zudem verstehen Bitkom und eco das Erfordernis der Echtheitsprüfung dahingehend, dass visuell oder auf optoelektronischem Wege erfasste sichtbare_Sicherheitsmerkmale der Dokumente geprüft werden, nicht jedoch Echtheitsmerkmale der Sicherheitsstufe 2, d.h. UV-Kennzeichnungen und weitere verdeckte bzw. nur mit maschineller Hilfe auslesbare Sicherheitsmerkmale. Die bloße Inaugenscheinnahme am Point of Sale (Shop) bzw. die opto-elektronische Erfassung muss ausreichen und die Anschaffung aufwändiger technischer Systeme am PoS darf damit nicht gefordert sein.

Stellungnahme Überprüfung der Richtigkeit von Anschlussinhaberdaten

Seite 5|5



- Nach der Formulierung der Regelung „Die prüfende Person hat vor Eingabe die Richtigkeit der erhobenen Daten ... zu überprüfen“ wird unterstellt, dass die Datenerfassung durch die prüfende Person (z.B. den Händler) erfolgt. Dies muss aber nicht immer der Fall sein. Es sollte die Möglichkeit eröffnet werden, dass auch automatische Erfassungssysteme möglich sind, und die prüfende Person lediglich die erfassten Daten mit dem Identitätsdokument abzugleichen hat. Die Richtigkeit der Daten würde dabei durch das automatische Auslesen der Daten sichergestellt. Eine abschließende Überprüfung durch ein entsprechendes elektronisches System könnte anschließend erfolgen.

5. Ausweisdatenbank

- Nach dem Entwurf der Verfügung soll jeder Diensteanbieter eine Ausweisdatenbank vorhalten, die mindestens jährlich zu aktualisieren ist und aus der sich die entsprechenden Merkmale für ausländische Identitätsdokumente ergeben. Durch diese Forderung werden unbedingt notwendiger Aufwand und Kosten einer solchen Datenhaltung um ein Vielfaches erhöht. Kostensparender und deshalb verhältnismäßiger wäre die konzentrierte Datenhaltung im Sinne einer Referenzdatenbank bei einer nationalen Stelle bzw. die Zulassung entsprechender Drittanbieter. Diese können zugleich dem mit dem Bundesministerium des Inneren, qualifizierten international tätigen Herstellern entsprechender internationaler Ausweisdokumente mit Sitz in Deutschland zusammenarbeiten, so dass mit deren Fachexpertise eine Ausweisdatenbank mit den entsprechenden Hinweisen zur Verfügung gestellt würde. Angesichts des Zwecks der Terrorismusbekämpfung dürfte es sich dabei jedenfalls auch um eine staatliche Aufgabe handeln, die nicht an die Diensteanbieter delegiert werden sollte. Durch den dem Diensteanbieter eingeräumten Datenzugriff auf jeweils aktualisierte und staatlich geprüfte Daten und Identitätsmerkmale würde deren Qualität und Aktualität gesichert und den Verpflichteten vorgegeben.

6. Wiederverwendung bereits erfolgter Legitimationsprüfungen

- Angesichts des Aufwandes und der Kosten der Identitätsprüfung und der hieraus folgenden Auswirkungen auf einzelne Vertriebskanäle und den Absatz von Prepaid-Produkten können Identitätsprüfungen nur dann verhältnismäßig sein, wenn ein Bedürfnis einer (neuen) Identifizierung gegeben ist und die Prüfung nur zwingend in der gesetzlich vorgeschriebenen Weise sicher erfolgen kann. Sofern die Identität des Prepaid-Kunden auch zweifelsfrei ohne erneute volle Identitätsprüfung feststellbar ist, muss den Diensteanbietern die Möglichkeit eingeräumt sein, ein bereits nach den gesetzlichen Kriterien erzielttes Identitätsprüfungsergebnis bei demselben Kunden wiederholt verwerten zu können. Die Verfügung sollte um die Möglichkeit der Wiederverwendung bereits erzielter Legitimationsergebnisse ergänzt werden.