[BNetzA]

Verfügung

gemäß § 111 Absatz 1 Satz 4 Telekommunikationsgesetz

- Auswertung der Stellungnahmen –

(Dezember 2016)

Inhaltsverzeichnis

Einleitung

Am 30. Juli 2016 trat das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus in Kraft, das auch eine Änderung des § 111 Telekommunikationsgesetz (TKG) vorsieht. Nun wird ausdrücklich eine Prüfpflicht des Diensteanbieters in Bezug auf die zu erhebenden Anschlussinhaberdaten normiert. Der Diensteanbieter ist verpflichtet, bei im Voraus bezahlten Mobilfunkdiensten vor der Freischaltung die Richtigkeit der Anschlussinhaberdaten zu prüfen. Dies hat ausgehend vom Gesetzeswortlaut durch Vorlage von bestimmten Identitätsdokumenten beim Diensteanbieter zu geschehen. Gemäß § 111 Absatz 1 Satz 4 TKG erhält die Bundesnetzagentur die Aufgabe, nach Anhörung der betroffenen Kreise andere geeignete Verfahren im Rahmen einer Verfügung im Amtsblatt der Bundesnetzagentur festzulegen. Ausgehend von der Gesetzesbegründung sind dabei gleichermaßen geeignete Verfahren festzulegen, bei denen vor Freischaltung eine unmittelbare Identifikation anhand eines Identitätsdokuments stattgefunden hat (BT-Drucks. 18/8702, S. 23).

Die Bundesnetzagentur hat auf Grundlage dieses Auftrages am 31. August 2016 einen Entwurf der Verfügung zur Anhörung gestellt. Die Frist zur Stellungnahme war auf den 30. September 2016 datiert.

Mit dem vorliegenden Dokument werden die eingereichten Stellungnahmen zusammengefasst dargestellt und anschließend von Seiten der Bundesnetzagentur bewertet. Die Reihenfolge der Auswertung und Bewertung orientiert sich dabei an der Reihenfolge des zur Anhörung gestellten Verfügungsentwurfs.

Für die Bewertung wurde der gesetzliche Auftrag zugrunde gelegt, Verfahren festzulegen, die im Verhältnis zur Vorlage beim Diensteanbieter gleichermaßen geeignet sind, um eine Prüfung der Anschlussinhaberdaten im Sinne des § 111 Absatz 1 Satz 1 TKG anhand gesetzlich vorgesehener Identitätsdokumente durchzuführen. Wesentlich war dabei die Überlegung, dass eine Vorlage eine fundierte und selbstbestimmte Prüfung des vorgelegten Identitätsdokuments durch den Diensteanbieter ermöglicht. Die Festlegung beinhaltet neben der Benennung von Verfahren jeweils auch einzelne Vorgaben. Diese stellen sicher, dass das jeweilige Verfahren tatsächlich als gleichermaßen geeignet bewertet werden kann und keine zusätzlichen Unwägbarkeiten entstehen. So ist es nach Ansicht der Bundesnetzagentur erforderlich, beispielsweise auch datenschutzrechtliche Aspekte zu beachten. Ebenso sind Vorgaben des Personalausweisgesetzes (PAuswG) zu beachten. Dies gilt umso mehr als gleichermaßen geeignete Prüfverfahren auch eine Beauftragung Dritter beinhalten können und so eine Übermittlung von Daten und Dokumenten an den Diensteanbieter erfolgen muss. Die Gesetzesbegründung nennt dementsprechend beispielhaft Identitätsnachweise durch Web-Ident oder Post-Ident-Verfahren.

Der Grundfall in § 111 Absatz 1 Satz 3 TKG geht von einer Vorlage des Identitätsdokuments beim Diensteanbieter aus, der die Prüfung durchzuführen hat. Gemäß § 111 Absatz 4 TKG ist es dem Diensteanbieter möglich, die Erhebung der Daten durch einen Dritten durchführen zu lassen. Zur Prüfung der durch den Dritten erhobenen Daten sagt Absatz 4 des § 111 TKG nichts. Daraus ergibt sich, dass der Gesetzgeber die Prüfung der Daten jedenfalls nicht vollständig auf einen Dritten übertragen lassen wollte. Mit Blick auf die Wertung von Verfahren wie beispielsweise dem PostIdent- oder einem Web-Ident-Verfahren als gleichermaßen geeignet wie die Vorlage kann eine Prüfung der Richtigkeit der erhobenen Anschlussinhaberdaten aber zumindest in Teilen sinnvollerweise nur durch den Dritten erfolgen. Aus diesem Grunde sieht die Verfügung vor, dass im Falle der Beauftragung eines Dritten mit der Datenerhebung und einer teilweisen Prüfung immer eine Übermittlung von Kopien, Scans o.ä. an den Diensteanbieter erfolgt. Nur so ist es diesem möglich, die ihm weiterhin obliegende Prüfpflicht zumindest in Teilen zu erfüllen. Die Prüfung der Echtheit des Identitätsdokuments sowie der Abgleich der Person des Anschlussinhabers mit der im Dokument ausgewiesenen Person kann in Fällen der Dirttbeauftragung in aller Regel nur durch den Dritten erfolgen, der Dokument und Person tatsächlich vor Augen hat. Dieses Verständnis bedingt eine Aufteilung der einzelnen Prüfschritte zwischen Diensteanbieter und Dritten, die sich in den Vorgaben widerspiegelt.

Konkret werden mit dieser Verfügung Verfahren festgelegt, die bereits in anderen Bereichen zu Identifizierungszwecken angeboten und angewendet werden. Es handelt sich dabei weitgehend um etablierte Produkte und Anbieter. Daher geht die Bundesnetzagentur davon aus, dass ihre Implementierung innerhalb der gesetzlichen Umsetzungsfrist bis zum 1. Juli 2016 möglich sein wird.

Auf eine mündliche Anhörung der betroffenen Kreise wurde verzichtet, da aufgrund der schriftlichen Stellungnahmen bereits eine umfassende Bewertung möglich war. Von der Veröffentlichung der eingereichten Stellungnahmen wird abgesehen, da wesentliche Inhalte der Stellungnahme wegen Betriebs- und Geschäftsgeheimnissen sowie erhobenen Widersprüchen in Bezug auf eine Veröffentlichung nicht publiziert werden können. Eine nur teilweise Veröffentlichung würde die der Auswertung und Bewertung zugrundeliegenden Aspekte nur unzureichend abbilden.

Teilnehmer:

Im Rahmen der Anhörung sind insgesamt 17 Stellungnahmen von den betroffenen Kreisen eingegangen. Die Stellungnahmen stammen von Seiten der Diensteanbieter, Anbietern von Verfahren zur Verifikation der Identität sowie von betroffenen oder fachkundigen Landes- und Bundesbehörden. Im Einzelnen waren dies:

bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Bundesministerium des Innern

Deutsche Post AG

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

eco – Verband der Internetwirtschaft

freenet AG

IDnow GmbH

Lebara Limited

Landeskriminalamt Nordrhein-Westfalen

Medion AG

Ministerium für Inneres und Sport Mecklenburg-Vorpommern

PVD – Prepaid Verband Deutschland

Senatsverwaltung für Inneres und Sport, Berlin

sipgate GmbH

Telefónica Germany GmbH & Co. OHG

VATM - Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V.

Zollkriminalamt

Die Stellungnahmen zeigen zum Teil stark divergierende Ansichten bzw. Interessen zwischen den Anbietern einerseits und den Sicherheitsbehörden andererseits. Diese gilt es, im Sinne des neugefassten § 111 TKG in Ausgleich zu bringen.

Wegen teilweise betroffener Betriebs- und Geschäftsgeheimnisse wird darauf verzichtet, die Urheber der jeweiligen Stellungnahme namentlich zu erwähnen. Zudem werden inhaltlich gleiche Stellungnahmen zusammengefasst dargestellt.

Stellungnahmen zum Verfügungsentwurf und Bewertung durch die Bundesnetzagentur

A. Grundsätzliche Anmerkungen zum Inhalt des Entwurfs

1. Geltung für Internet of Things (IoT)- und Machine-to-Machine (M2M)-Anwendungen ausschließen

Von Seiten der Diensteanbieter wurde vorgetragen, dass die Geltung der Verfügung für Prepaid-SIM-Karten, die für IoT- und M2M-Anwendungen eingesetzt werden, ausgeschlossen werden solle.

Bewertung durch die BNetzA:

Der § 111 TKG selbst unterscheidet nicht nach der konkreten Verwendungsart der vergebenen Telekommunikationsanschlüsse. Demnach kann auch die Verfügung, die lediglich Verfahrensarten zur Identitätsprüfung regeln darf, keine Einschränkung des gesetzlichen Regelungsumfangs vornehmen.

2. Regelungen zum Missbrauchsschutz ergänzen

Um beispielweise massenhafte Registrierungen durch dieselbe Person erkennbar zu machen, wurde vorgeschlagen, Regelungen zum Schutz vor Missbrauch zu ergänzen. Dabei sollte auch das konkret vorgelegte Identitätsdokument in allen Überprüfungsverfahren in geeigneter Weise gesichert und an den Diensteanbieter übermittelt werden. Der Diensteanbieter sollte dadurch in die Lage versetzt werden, die erfolgte Überprüfung zu kontrollieren.

Bewertung durch die BNetzA:

Diesem Vorschlag kann nicht entsprochen werden. Sofern es darum geht, Massenregistrierungen zu verhindern, handelt es sich nicht um eine Regelung eines gleichermaßen geeigneten Verfahrens. Vielmehr würde es darum gehen, ganz allgemein die Kontrahierungsfreiheit eines Diensteanbieters einzuschränken. Dies stellt jedoch eine wesentliche Entscheidung mit eingreifendem Charakter dar, die der Gesetzgeber selbst in § 111 TKG hätte formulieren müssen.

Sofern es um die Kontrolle der tatsächlich durchgeführten Prüfung des vorgelegten Identitätsdokuments geht, liegt dies bereits im Eigeninteresse der Diensteanbieter. Die Diensteanbieter sind gemäß § 111 Absatz 4 TKG nämlich auch dann für die Richtigkeit der erhobenen Anschlussinhaberdaten verantwortlich, wenn sie die Erhebung durch einen Dritten durchführen lassen.

3. Dokumentation der konkret prüfenden Person

Es wurde vorgetragen, dass die konkrete, die Identitätsprüfung durchführende Person in geeigneter Weise dokumentiert werden sollte**.**

Bewertung durch die BNetzA:

Mit diesem Vorschlag wird zwar eine Regelung eingeführt, die in § 111 Absatz 1 Satz 3 TKG für die Vorlage beim Diensteanbieter nicht ausdrücklich vorgesehen ist. Dennoch ist es nach Ansicht der Bundesnetzagentur erforderlich, insbesondere für Verfahren, in denen externe Dritte in den Erhebungs- und Prüfprozess einbezogen werden, eine Pflicht zur Dokumentation der die Daten erhebenden und prüfenden Person vorzusehen. Damit soll sichergestellt werden, dass die Vorgaben für das jeweilige Erhebungs- und Prüfverfahren auf Seiten des Dritten auch tatsächlich beachtet und umgesetzt werden. Dabei ist es nicht erforderlich, Klarnamen zu verwenden. Es genügt, wenn Kürzel, Nummern oder Pseudonyme verwendet werden, mit denen auch im Nachhinein ein Bezug zu der verantwortlichen Person eindeutig hergestellt werden kann.

Dementsprechend wird für die Verfahren 1 bis 3 jeweils folgende Vorgabe ergänzt:

Der Diensteanbieter hat dafür zu sorgen, dass die Person, die die Erhebung der Daten, die Echtheitsprüfung des Ausweises und den Identitätsabgleich durchführt, in geeigneter Weise dokumentiert wird.

Für das Verfahren 1 bedarf es einer weiteren Ergänzung. Hier stellt die Identitätsprüfung nicht eine eigens beauftragte Dienstleistung dar, sondern nur eine Nebentätigkeit neben dem Verkauf der SIM-Karte. Es könnte somit ein wirtschaftliches Eigeninteresse seitens des in den Vertrieb eingebundenen Dritten bestehen, das die Gewähr für eine korrekte Datenerhebung möglicherweise einschränkt. Deshalb ist es aus Sicht der Bundesnetzagentur erforderlich, dass eine Kennung der erhebenden und prüfenden Person an den Diensteanbieter mit übermittelt wird. Daher wird für Verfahren 1 die Mitteilung an den Diensteanbieter hinzugefügt:

Der Diensteanbieter hat dafür zu sorgen, dass die Person, die die Erhebung der Daten, die Echtheitsprüfung des Ausweises und den Identitätsabgleich durchführt, in geeigneter Weise dokumentiert wird. Dem Diensteanbieter ist eine eindeutige Kennung dieser Person mit zu übermitteln.

4. Benachteiligung von Diensteanbietern ohne Ladengeschäfte

Der Entwurf der Verfügung benachteiligt nach Ansicht einiger Prepaid-Anbieter diejenigen Diensteanbieter, die nicht über ein eigenes Ladengeschäft verfügen. Für diese stelle eine unmittelbare Identitätsprüfung mittels persönlicher und physischer

Anwesenheit am Point of Sale keine realistische Option dar, da dies aufgrund des hohen Aufwands der manuellen Datenerhebung rein wirtschaftlich momentan noch nicht tragbar sei. Daher seien kostengünstige Alternativen notwendig, die evtl. erst zukünftig entwickelt werden. Auch diese Verfahren sollten in der Verfügung abgebildet werden.

Bewertung durch die BNetzA:

Der Gesetzgeber geht in § 111 TKG zunächst von einer Vorlage beim Diensteanbieter aus. Somit ist im Gesetz bereits angelegt, dass in irgendeiner Form eine persönliche Kontrolle durchgeführt wird, und damit besteht die angesprochene „Benachteiligung“ bereits durch das Gesetz selbst. Die mit der Verfügung festzulegenden Verfahren bezwecken gerade, marktgängige Vertriebswege im Rahmen der aktuellen gesetzlichen Vorgaben zu ermöglichen. Dabei sind Alternativen verfügt, die auch Anbietern ohne Ladengeschäft offen stehen. Gerade die Einschaltung eines in den Vertrieb eingebundenen Dritten oder eines Anbieters von Identifizierungsverfahren steht jedem Anbieter offen, unabhängig davon, ob ein Ladengeschäft unterhalten wird oder nicht.

B. Zu den Verfahren

1. Verfahren Nr. 1 des Entwurfs

Überprüfung der Richtigkeit der Daten durch einen von dem Diensteanbieter in seinen Vertrieb eingebundenen Dritten anhand eines der aufgeführten Identitätsdokumente mit Vorkehrungen, die dem Diensteanbieter eine Kontrolle der erfolgten Überprüfung ermöglichen (z.B. mittels obligatorischer Übermittlung einer opto-elektronisch erfassten Kopie des Identitätsdokumentes an ihn)

Stellungnahmen:

Von Seiten der Diensteanbieter, ebenso wie von Seiten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wurden Zweifel an der Regelungskompetenz für das unter Nummer 1 dargestellte Verfahren geäußert. Das Gesetz regle bereits die Vorlage des Identitätsdokuments, dieses Verfahren werde nicht zu einem neuen Verfahren, nur weil ein Vertriebspartner eingeschaltet werde. Der § 111 Abs. 4 TKG regele insoweit auch die Verantwortlichkeit des Diensteanbieters. Wie dieser seiner Verpflichtung nachkomme, solle ihm überlassen bleiben. Eine Vermischung von Fragen der Verantwortlichkeit und der Regelung zusätzlicher Prüfverfahren solle vermieden werden. Sollte diese Vorgabe dennoch in der Verfügung enthalten bleiben, müsse die Umsetzungsfrist der Diensteanbieter auf mindestens 12 Monate verlängert werden.

Bewertung durch die BNetzA:

In § 111 Absatz 4 Satz 1 und § 111 Absatz 1 Satz 3 TKG trennt der Gesetzgeber zwischen der Erhebung von Anschlussinhaberdaten einerseits und der Überprüfung der Richtigkeit der erhobenen Daten andererseits. Die Überprüfung der Richtigkeit der erhobenen Daten besteht wiederum aus einer Identitätsprüfung, einer Echtheitsprüfung des vorgelegten Identitätsdokuments sowie einem Abgleich der erhobenen mit den im Identitätsdokument enthaltenen Anschlussinhaberdaten. Dem Diensteanbieter wird ermöglicht, die Datenerhebung durch einen Dritten vornehmen zu lassen. Die Überprüfung der Richtigkeit der erhobenen Daten ist jedoch gemäß § 111 Absatz 1 Satz 3 TKG durch Vorlage eines der dort genannten Identitätsdokumente beim Diensteanbieter vorzunehmen, ohne dass ihm dafür die Einschaltung eines Dritten erlaubt wird. Somit handelt es sich immer dann um ein über das bloße Erheben hinausgehendes Verfahren, wenn neben der in § 111 Absatz 4 TKG erwähnten Datenerhebung Teile der Identitätsprüfung durch einen Dritten durchgeführt werden sollen. Dies ist auch der Fall bei einem in den Vertrieb eingebundenen Dritten, der im Rahmen des unmittelbaren Kundenkontaktes die Person des Erwerbers sowie das Identitätsdokument vor Augen hat.

Vor diesem Hintergrund ist schon rein faktisch davon auszugehen, dass vor allem der in den Vertrieb eingebundene Dritte, der die Anschlussinhaberdaten erheben darf, auch derjenige sein wird, der der Person des Erwerbers tatsächlich gegenübersteht. Somit ist dieser am besten, wenn nicht gar als einziger dazu in der Lage, die Echtheit des vorgelegten Identitätsdokuments zu prüfen und einen Abgleich der ihm gegenüber stehenden Person mit der im Identitätsdokument ausgewiesenen Person (= Identitätsprüfung) vorzunehmen. Somit ist dieser Teil der Prüfung der angegebenen Anschlussinhaberdaten schon aus faktischen Gründen sinnvollerweise nur durch den Dritten vorzunehmen.

Nach der gesetzlichen Wertung darf der Diensteanbieter die Prüfpflicht jedoch nicht vollständig auf den Dritten verlagern, sondern muss weiterhin selbst seiner Prüfpflicht nachkommen. Dies geschieht mit der vorgeschlagenen Verfahrensvariante dadurch, dass er vom Dritten eine Kopie, einen Scan oder vergleichbare Abbildungen zugesandt erhält und jeweils selbst die Prüfung der Angaben anhand der ihm zugeleiteten Kopie, des Scans etc. durchführt. Erst dann darf gemäß § 111 Absatz 1 Satz 3 TKG die Freischaltung des Anschlusses erfolgen. Für die Behandlung der Kopie etc. findet § 95 Absatz 4 TKG Anwendung. Die Prüfung seitens des Diensteanbieters hat dabei in jedem Falle zu erfolgen, nicht nur stichprobenartig. Entsprechend ist in jeden Fall eine Kopie oder entsprechendes an den Diensteanbieter zu übermitteln.

Hierbei wird zwar die Identitätsprüfung tatsächlich durch den in den Vertrieb eingebundenen Dritten durchgeführt. Der Diensteanbieter kann somit überhaupt nur den Abgleich zwischen den erhobenen und den im vorgelegten Identitätsdokument enthaltenen Anschlussinhaberdaten vornehmen. Dabei befähigt ihn die Kopie aber nicht nur zur Prüfung der Daten in dem ihm möglichen Umfang, sondern sie

ermöglicht als Nebeneffekt zugleich eine „Kontrolle“ über die tatsächlich erfolgte Vorlage eines Identitätsdokuments. Würde man die Übermittlung einer Kopie hier für entbehrlich halten, läge kein gleich geeignetes Verfahren vor, da der Diensteanbieter nicht einmal eine (reduzierte) Prüfung der erhobenen Anschlussinhaberdaten durchführen könnte.

Diese Verfügung hat die Aufgabe, im Verhältnis zu § 111 Absatz 1 Satz 3 TKG gleichermaßen geeignete Verfahren festzulegen. Dazu zählen auch konkrete Vorgaben zum jeweiligen Verfahren. Jede Abweichung vom gesetzlich vorgesehenen Ablauf, mithin jedes weitere Verfahren birgt die Gefahr einer unzureichenden Umsetzung der gesetzlichen Vorgabe bzw. konkret einer geringeren Zuverlässigkeit der Datenprüfung. Dieser Gefahr kann jedoch dadurch begegnet werden, dass die Alternativverfahren durch geeignete Vorgaben so gestaltet werden, dass sie ein entsprechendes Niveau erreichen und dadurch als gleich geeignet bewertet werden können.

Zur Klarstellung wird folgender neuer Wortlaut für die Verfahrensvariante 1 aufgenommen:

Erhebung der Anschlussinhaberdaten durch einen von dem Diensteanbieter in seinen Vertrieb eingebundenen und unmittelbar anwesenden Dritten mit Prüfung der Echtheit des Identitätsdokuments sowie der Übereinstimmung des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person.

Für Verfahren dieser Art gelten folgende Vorgaben:

(1) Die prüfende Person ist hinsichtlich der Prüfung der Identitätsdokumente sowie des Ablaufs der Datenerhebung und -prüfung umfassend zu schulen.

Stellungnahmen:

Von Seiten der Sicherheitsbehörden wird zu diesem Punkt ergänzend gefordert, den erforderlichen Schulungsumfang in der Verfügung deutlich zu bestimmen, Infomaterial ausdrücklich nicht ausreichen zu lassen und eine Dokumentationspflicht hinsichtlich der Schulung sowie der Einhaltung der Vorgaben zu ergänzen.

Die Diensteanbieter akzeptieren das Erfordernis der Schulung zum Teil, wobei jedoch um Klarstellung gebeten wird, dass auch unternehmensinterne Schulungen ausreichen. Überwiegend wird jedoch die Regelungskompetenz für das Schulungserfordernis angezweifelt bzw. angemerkt, dass es keine sachliche Begründung für die Differenzierung zwischen Mitarbeitern des Diensteanbieters bzw. diesen selbst einerseits und durch diesen beauftragten Dritte gebe. Die Pflicht zur Prüfung treffe jeden, der zu diesem Zwecke tätig werde, unabhängig davon, ob es der Diensteanbieter selbst ist oder ein durch ihn beauftragter Dritter. Es handele sich

um eine unzulässige Verschärfung der gesetzlichen Regelung. Für Verkäufe im Point of Sale sei der Schulungsaufwand aufgrund der Vielzahl des Personals viel zu hoch. Allenfalls reiche eine Checkliste bzw. ein Merkblatt aus. Vorteil davon wäre zudem, dass das Informationsmaterial vor Ort vorläge.

Bewertung durch die BNetzA:

Mit dem Erfordernis, jede mit der Prüfung betraute Person hinsichtlich der Datenerhebung und Datenprüfung zu schulen, wird im Rahmen der Verfügung eine Regelung aufgenommen, die nicht über das in § 111 Absatz 1 TKG für den Diensteanbieter selbst vorgesehene Prüfverfahren hinausgeht. Der gesetzliche Zweck der Prüfung kann sinnvollerweise nur dann erfüllt werden, wenn die Prüfenden wissen, was sie prüfen, wie die Prüfung vonstattengeht und worauf zu achten ist. Somit ist nach Ansicht der BNetzA auch schon im Grundfall des § 111 Absatz 1 TKG(also der Prüfung ausschließlich durch den Diensteanbieter) selbstverständlich vorauszusetzen, dass die mit der Prüfung beauftragten Personen für die Prüfung entsprechend befähigt sind. Sollte dies nicht der Fall sein und es daraufhin zu Falscherhebungen kommen, liegt der Schluss nahe, dass das Fehlen einer ausreichenden Schulung Ursache für den falschen Datenbestand ist. Somit läge diese grundsätzlich im Verantwortungsbereich des Diensteanbieters. Der Diensteanbieter müsste in einem solchen Fall auch nachweisen, dass die Falschdatenerhebung nicht auf eine mangelnde Befähigung des Prüfenden zurückgeht.

Hinsichtlich des Umfangs der vorgesehenen Schulung sieht es die Bundesnetzagentur als Verantwortung der Diensteanbieter an, diese so zu gestalten, dass eine ausreichend fundierte Prüfung der Echtheit des Dokuments stattfinden kann. Da der Diensteanbieter auch bei Einbindung Dritter weiterhin die Verantwortung für die Erhebung richtiger Anschlussinhaberdaten trägt, liegt es in seinem Eigeninteresse, die Schulung ausreichend zu gestalten. Dabei ist es nach hiesiger Ansicht nicht erforderlich, dass der in dieser Hinsicht fachfremde Dritte alle Sicherheitsmerkmale der aufgeführten Identitätsdokumente kennt und einem Experten gleich überprüfen kann. Vielmehr kann es dabei nur auf augenscheinliche oder ohne weiteres ertastbare Merkmale ankommen. Dazu zählen etwa Beschädigungen, erkennbar unautorisierte Beklebungen sowie offensichtliches Fehlen von vorgesehenen optischen und/oder haptischen Sicherheitsmerkmalen. Eine verpflichtende externe Schulung durch Fachleute würde die Grenzen der Verhältnismäßigkeit dieser Verfügung überschreiten.

Dennoch sollte der Diensteanbieter im Sinne der vorzunehmenden Prüfung dafür sorgen, dass die Echtheit des Identitätsdokuments durch enthaltene Sicherheitsmerkmale insoweit geprüft werden kann, wie diese Merkmale offensichtlich nach angemessener Einweisung erkennbar sind. Dies kann unter anderem durch eine intensive externe oder interne Schulung erfolgen, aber auch durch ausführliche schriftliche Hinweise, die nachweisbar und verpflichtend zu beachten sind. Um weitere Unklarheiten zu vermeiden, wird der Begriff der Schulung

ersetzt durch den Begriff der Unterweisung. Somit hat der Diensteanbieter die mit der Prüfung betrauten Personen hinsichtlich der Prüfung und der Datenerhebung in geeigneter Form zu unterweisen.

Demnach wird eine neue Formulierung gewählt:

Der Diensteanbieter hat den Dritten hinsichtlich der Prüfung der Echtheit der Identitätsdokumente sowie des Ablaufs der Datenerhebung in geeigneter Weise, zum Beispiel durch eine Schulung der prüfenden Personen oder schriftliche Instruktion, zu unterweisen.

Zudem wird folgende Vorgabe als Ziffer (2) zusätzlich eingefügt:

Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass der ausgewählte Dritte die Gewähr dafür bietet, dass die Anweisungen hinsichtlich der Datenerhebung, Identitätsprüfung, Prüfung der Echtheit des Identitätsdokuments, der Fertigung der Kopien u.ä. sowie deren Übermittlung an ihn eingehalten werden. Dies hat er zu dokumentieren.

(2) Die prüfende Person hat sich von der Echtheit des vorgelegten Identitätsdokumentes zu überzeugen.

Stellungnahmen:

Nach Ansicht der Diensteanbieter kann sich eine Überprüfung nur auf offensichtliche Manipulationen und Fälschungen bzw. auf sichtbare Sicherheitsmerkmale beziehen. Die Anforderungen dürften nicht über das Vorhandensein bestimmter wesentlicher Merkmale wie beispielsweise das holografische Portrait hinausgehen. Eine ausreichende Sicherheit sei vielmehr auch dann gewährleistet, wenn auf wesentliche Elemente echter Ausweisdokumente aufmerksam gemacht würde. Demzufolge würde die Vorgabe so verstanden, dass nur Merkmale der Sicherheitsstufe 1 visuell oder auf opto-elektronischem Wege erfasst werden, Merkmale der Sicherheitsstufe 2 hingegen nicht. Aufwändige technische Systeme oder Hilfsmittel am Point of Sale dürften nicht gefordert werden.

Zur Durchführung wurde angegeben, dass die Prüfung der Echtheit durch Kippen oder Drehen des Identitätsdokuments und die Erfassung visueller oder opto-elektronischer Sicherheitsmerkmale geschehen könne.

Dazu wurde von einem Diensteanbieter folgender konkreter Formulierungsvorschlag gemacht: „[Die prüfende Person hat] das vorgelegte Identitätsdokument anhand der wesentlichen Merkmale durch Inaugenscheinnahme zum Ausschluss offensichtlicher Fälschungen zu prüfen."

Daneben wurde vorgebracht, dass auch automatisierte Erfassungssysteme möglich sein sollten und die prüfende Person nur die so erfassten Daten mit dem

Identitätsdokument abgleichen müsse. Die Richtigkeit der Daten werde durch das automatisierte Auslesen der Daten sichergestellt. Eine abschließende Prüfung durch ein entsprechendes elektronisches System könnte zudem anschließend erfolgen.

Bewertung durch die BNetzA:

Der alternative Formulierungsvorschlag spiegelt mit einer Ergänzung das nach Ansicht der Bundesnetzagentur erforderliche Maß für die Echtheitsprüfung wider.

Ziel des § 111 TKG ist es, eine sichere Datenlage für die Abrufe nach den §§ 112, 113 TKG zu schaffen. Dafür mag es zwar wünschenswert sein, eine Prüfung von Identitätsdokumenten, besonders hinsichtlich des deutschen Personalausweises, auf Expertenniveau einzuführen. Im Verhältnis zu den in § 111 Absatz 1 TKG aufgeführten Identitätsdokumenten, die gar keine oder geringe bzw. unsichere Sicherheitsmerkmale aufweisen, wäre eine derart tiefgründige Ausbildung für Dokumente, die über Sicherheitsmerkmale verfügen, jedoch überzogen. Das Ziel der Identitätsprüfung erschöpft sich auch bei den weniger sicheren Dokumenten naturgemäß in einer Anscheinskontrolle. Anderenfalls dürften diese Dokumente für die Identitätsprüfung schon nicht zugelassen werden. Daher reicht es für den Zweck des § 111 TKG aus, die Echtheit des vorgelegten Identitätsdokuments anhand augenscheinlicher oder unmittelbar wahrnehmbarer Merkmale zu prüfen.

Zudem ist zu berücksichtigen, dass § 111 TKG hinsichtlich der verpflichtenden Prüfung von Identitätsdokumenten zwischen Prepaid- und Postpaid-Mobilfunkanschlüssen unterscheidet. Während für Postpaid-Anschlüsse keine Prüfung aufgrund von Identitätsdokumenten vorgeschrieben wird, soll dies bei Prepaid-Anschlüssen zwingend erfolgen. Dabei ist gemessen am Gesetzeszweck des § 111 TKG für alle Anschlussarten die Erhebung richtiger und somit geprüfter Anschlussinhaberdaten erforderlich. Während demnach also für Postpaid-Anschlüsse die in Einzelverfahren entwickelten Vorgaben der Bundesnetzagentur ausreichen (Bankverbindung, postalische Zusendung, postalische Zusendung von PIN zur Freischaltung, Welcome Letter etc.), müsste für Prepaid-Anschlüsse faktisch ein Experten-gleiches Kenntnisniveau erreicht werden. Dies ist mit Blick auf die gleiche Relevanz von Prepaid- und Postpaid-Mobilfunkverträgen für die gesicherte Datenlage in der Kundendatei nach § 112 TKG nicht zu begründen.

Absolute Gewähr für ein Erkennen von Fälschungen wird vom Gesetz nicht verlangt. Der Faktor Mensch als Ursache für Fehler und Unsicherheit ist in § 111 Abs. 1 TKG bereits angelegt, wenn die Gesetzesformulierung auf eine Prüfung durch den Diensteanbieter mittels Vorlage der Dokumente abstellt. Es wird gerade kein automatisiertes Auslesen der Identitätsdokumente verlangt und wäre bei einigen der aufgeführten Identitätsdokumente (einige ausländische Reisepässe) auch nicht oder zumindest nicht mit einem Mehrwert für die Echtheitsprüfung möglich.

Die vorgeschlagene Formulierung wird demnach mit folgender Ergänzung übernommen:

Die erhebende Person hat das vorgelegte Identitätsdokument anhand der wesentlichen Merkmale durch Inaugenscheinnahme und haptische Wahrnehmung zum Ausschluss offensichtlicher Fälschungen zu prüfen.

Zudem erscheint es als nicht zu beanstanden, dass auch eine automatisierte Erhebung der Daten erfolgt, sofern dabei die datenschutzrechtlichen Vorgaben für das Auslesen und Übermitteln von Daten aus Identitätsdokumenten (z.B. PersAuswG) eingehalten werden und lediglich die manuelle Erhebung der Daten ersetzt wird. Mithin dürfen nur die Daten automatisiert erhoben werden, die im Rahmen des § 111 TKG erforderlich sind. Dies erfolgt, indem etwa nur bestimmte Bereiche oder Zeilen des Identitätsdokuments automatisiert für das Erheben erfasst werden.

Für ein Verfahren im Sinne der Nummer 1 ist es nicht möglich, den Abgleich zwischen der Person des Erwerbers und der im Identitätsdokument ausgewiesenen Person mithilfe automatisierter Verfahren durchzuführen.

(3) Die prüfende Person hat vor der Eingabe die Richtigkeit der erhobenen Daten anhand des Identitätsdokuments zu überprüfen, soweit diese darin enthalten sind. Zudem hat sie sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

Stellungnahmen:

Von Seiten der Diensteanbieter wird angeregt, keine Vorgaben zur Reihenfolge der Datenerhebung und Prüfung zu machen. Auch sollte die Formulierung nicht einschränken, dass auch mehrere Personen an der Prüfung bzw. an den erforderlichen Schritten zur Datenerhebung und Prüfung beteiligt sein können. Dies sei zum Beispiel der Fall, wenn ein Mitarbeiter/beauftragter Dritter das Übereinstimmen von Bild und Person durchführt, während eine weitere Person die Daten erfasse.

Ferner sollte nach Ansicht einiger Diensteanbieter eine Formulierung gewählt werden, die keinen Zweifel daran ließe, dass auch automatisierte Erfassungssysteme oder die Eingabe durch den Kunden selbst möglich seien und die prüfende Person lediglich die Daten mit dem Identitätsdokument abgleiche.

Von Seiten einiger Prepaid-Diensteanbieter wurde zudem angemerkt, dass nur der Diensteanbieter selbst bzw. dessen Ladengeschäfte prüfen könnten, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimme. Es sei letztlich unklar, ob die kaufende Person tatsächlich die Person des Anschlussinhabers ist bzw. sein wird.

Als Alternative zur händischen Erfassung der Daten wurde konkret vorgeschlagen, dass der Verkäufer die eindeutige Seriennummer der SIM-Karte einscannen und anschließend das vom Käufer vorgelegte Identitätsdokument mittels Scan oder am Kartenlesegerät elektronisch erfassen könne. Dies könne zusammen mit der Seriennummer gespeichert werden. Datenschutzrechtliche Bestimmungen sowie § 20 Personalausweisgesetz wären zu beachten. Automatisierte Verfahren zur Datenerfassung und –übertragung sollten einbezogen werden , eine Übersendung der so erhobenen Daten sollte dabei ausreichen. Eine Übermittlung der Kopie des Identitätsdokuments wäre in dem Falle entbehrlich.

Bewertung durch die BNetzA:

Die Reihung der Handlungsschritte in diesem Punkt der Verfügung folgt einer denkbaren logischen Vorgehensweise, schließt jedoch nicht aus, dass tatsächlich eine andere zeitliche Abfolge gewählt wird. Wesentlich ist, dass der Prüfende insgesamt jeden Schritt durchführt.

Der Begriff der prüfenden Person als im Singular formulierte Vorgabe schließt nicht aus, dass Arbeitsschritte unter mehreren Personen aufgeteilt werden. Dabei wäre jede von ihnen prüfende Person, die jedoch nur Teilaufgaben wahrnimmt.

Eine Eingabe durch den Anschlussinhaber selbst wird nach dem Wortlaut des § 111 TKG nicht zwingend ausgeschlossen. So ist es etwa im Rahmen eines Online-Chats möglich, die Daten durch den Anschlussinhaber selbst eingeben und an den Dritten übermitteln zu lassen. Dabei macht es keinen Unterschied, wer die Daten in eine Maske oder Ähnliches eingibt. Dies ist jedenfalls der Fall, wenn ein Abgleich der Angaben anhand des vorgelegten Identitätsdokuments durch den in den Vertrieb eingebundenen Dritten erfolgt, sofern die Angaben in diesem Dokument enthalten sind.

Anders ist es unter Umständen zu bewerten, wenn nur eine handschriftliche Erhebung erfolgt. Hier ist zu berücksichtigen, dass das Schriftbild deutlich lesbar und eindeutig sein muss, da ein Erheben logisch voraussetzt, dass der Erhebende ein tatsächliches Verständnis von den aufzunehmenden Angaben erhält. Da dies bei handschriftlichem Ausfüllen eines Formulars zu erheblichen Mängeln führen kann und die Datenprüfung beeinträchtigt werden könnte, sollte von dieser Möglichkeit Abstand genommen werden.

Grundsätzlich ist anzumerken, dass das Gesetz seinem Wortlaut nach von einer Erhebung durch den Diensteanbieter oder den beauftragten Dritten ausgeht.

Variante 1 betrifft gerade den Vertrieb mittels sogenannten „Points of Sale“. In jeder Variante besteht die Frage, ob die kaufende Person tatsächlich Nutzer ist und bleiben wird. Sollte der Kunde die SIM-Karte für einen Dritten erwerben und dies mitteilen, ist es dem Diensteanbieter stets möglich, um persönliche Vorsprache des zukünftigen Anschlussinhabers zu bitten bzw. auf einen alternativen Registrierungsweg aufmerksam zu machen, auf dem sich der bis dahin unbekannte

tatsächliche Anschlussinhaber registrieren und die SIM-Karte freischalten lassen kann.

Das im vierten Absatz der Zusammenfassung vorgestellte Vorgehen (Einscannen der Seriennummer der SIM-Karte sowie des Identitätsdokuments) widerspricht dem möglichen Ablauf eins nach Variante 1 dieser Verfügung gestalteten Verfahrens nicht. Insbesondere ist eine automatisierte Erhebung der Daten vom Gesetz nicht ausgeschlossen, sofern in gleichwertiger Weise gewährleistet ist, dass keine zusätzlichen Fehlerquellen entstehen können. Eine Übermittlung der Ausweiskopie oder eines Scans o.ä. an den Diensteanbieter wird dadurch jedoch nicht entbehrlich. Anderenfalls könnte dieser seiner ihm obliegenden Prüfpflicht nicht nachkommen. Die Verknüpfung mit der Seriennummer der SIM-Karte würde diesen Mangel ebenfalls nicht heilen und stellt mit Blick auf § 111 TKG ein nicht erforderliches zusätzlich erhobenes Datum dar. Dies entspricht nicht dem Gebot der Datensparsamkeit.

Zur Klarstellung hinsichtlich der konkreten Pflichtenverteilung zwischen dem in den Vertrieb eingebundenen Dritten und dem Diensteanbieter wird der Wortlaut wie folgt angepasst:

Der Dritte hat die Daten des Anschlussinhabers zu erheben. Zudem hat er sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

(4) Bei der Erhebung, Überprüfung und Übermittlung der Daten an den Diensteanbieter zur Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

Ergänzung und Anpassung durch die Bundesnetzagentur:

Den an anderer Stelle geäußerten Bedenken hinsichtlich der sich aus dem Personalausweisgesetz (PAuswG) ergebenden Beschränkungen der zu erhebenden und damit der zulässigerweise zu kopierenden Angaben im deutschen Personalausweis sind nach Maßgabe der Vorgabe Rechnung zu tragen.

Zur Klarstellung in Bezug auf die konkreten Pflichten des Diensteanbieters wird der Wortlaut der Vorgabe entsprechend obigen Ausführungen wie folgt geändert:

Bei der Erhebung und Übermittlung der Daten an den Diensteanbieter zur Prüfung und Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben und Beschränkungen nach dem PAuswG zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

(5) Die Kontrolle muss es dem Diensteanbieter ermöglichen, die tatsächlich erfolgte Vorlage des Identitätsdokuments zu prüfen. Dazu kann der Diensteanbieter den Dritten beispielsweise anweisen, ihm eine opto-elektronisch erfasste Kopie des Identitätsdokuments zu übermitteln.

Stellungnahmen:

Einzelne Diensteanbieter bezweifeln die rechtliche Kompetenz der Bundesnetzagentur zur Regelung einer Kontrollpflicht des Diensteanbieters. Es solle vielmehr dem Diensteanbieter selbst obliegen, wie er seiner Pflicht nachkomme. Auch seien Kopien, wie auch Scans, besonders bei einer flächendeckenden Ausstattung aller Points of Sale sehr aufwändig und kostenintensiv. So werde es erforderlich, mehrere 10.000 Points of Sale auszustatten. Für eine Übergangsfrist von mindestens 12 Monaten sollte vielmehr eine Erklärung der prüfenden Person zur Inaugenscheinnahme ausreichen. Diese könne z.B. durch Bestätigung der Erklärung in Aktivierungssystemen erfolgen.

Unter Datenschutzaspekten wird die Anfertigung von opto-elektronischen Kopien als problematisch angesehen. Auch bei einer Pflicht zur sofortigen Löschung oder Vernichtung der Kopien könne man nicht sicher sein, ob die Kopien tatsächlich unverzüglich gelöscht würden.

Insgesamt solle man den Umgang mit opto-elektronischen Kopien restriktiv regeln. Eine Kopie sollte als solche erkennbar sein, nicht benötigte Ausweis-/Passdaten seien zu schwärzen und der Betroffene sei auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen. Es sei eine unverzügliche und dauerhafte Löschung nach Erreichen des mit der Kopie verfolgten Zwecks vorzuschreiben. Auch wurde vorgeschlagen, in der Verfügung zu klären, ob Kopien zu Kontrollzwecken aufzubewahren oder sofort nach erfolgter Registrierung zu vernichten sind (§ 95 Abs. 4 TKG). Ferner wurde darauf hingewiesen, dass die Nutzung der Ausweisdaten zum automatisierten Abruf personenbezogener Daten unzulässig sei.

Seitens einiger Diensteanbieter wurde bemängelt, dass die Pflicht zur Vernichtung der Kopie durch den Vertriebspartner nicht geregelt werde. Dem Diensteanbieter sei es jedoch weder möglich zu überprüfen, noch könne er dafür verantwortlich gemacht werden, dass sein Vertriebspartner die von ihm erstellte Kopie des Identitätsdokuments nicht vernichte bzw. dauerhaft lösche. Das Beispiel der Anfertigung einer Kopie sei daher zu streichen. Stattdessen könne eine Kontrolle der Vorlage durch Videoübertragung zwischen Diensteanbieter und Vertriebspartner entsprechend Nr. 3 des Entwurfs oder durch eine unmittelbare Übermittlung eines Scans ohne dauerhafte Kopie des Ausweisdokuments beim Vertriebspartner vorgesehen werden.

Bewertung durch die BNetzA:

Die Übermittlung der opto-elektronischen Kopie oder eines digital zu übermittelnden Scans erfolgt zum Zwecke der Prüfung durch den Diensteanbieter. Dieser ist gemäß § 111 Absatz 1 TKG verpflichtet, die erhobenen Daten anhand der ihm zugeleiteten Kopie des Identitätsdokuments vor der Freischaltung zu prüfen (s.o.). Ist dieser Zweck erreicht, ist die Kopie entsprechend § 95 Absatz 4 TKG unverzüglich zu löschen. Dies gilt in jedem Einzelfall, da sich auch die Prüfpflicht des Diensteanbieters auf jeden Einzelfall erstreckt. Dabei dürfen keine Kopien oder sonstige Vervielfältigungen des vorgelegten Identitätsdokuments beim Dritten verbleiben. Den Bedenken hinsichtlich der sich aus dem Personalausweisgesetz (PAuswG) ergebenden Beschränkungen im Hinblick auf die zu erhebenden und damit zulässigerweise zu kopierenden Angaben im deutschen Personalausweis wird Rechnung getragen. Dies hat der Diensteanbieter entsprechend anzuweisen.

Zur Klarstellung wird der Wortlaut dementsprechend wie folgt abgeändert:

Der Diensteanbieter dafür zu sorgen, dass der Dritte in jedem Einzelfall eine opto-elektronische Kopie, Scan oder entsprechende Abbildung anfertigt und zum Zwecke der Prüfung unter Beachtung datenschutzrechtlicher und personalausweisrechtlicher Vorgaben an ihn übermittelt. Opto-elektronische Kopien, Scans oder entsprechende Abbildungen sind als solche zu kennzeichnen und dürfen nicht beim Dritten verbleiben. Für die beim Diensteanbieter vorgelegten Kopien gilt § 95 Absatz 4 TKG.

Die durch diese Regelung entstehende Kostenlast betrachtet die Bundesnetzagentur als unmittelbare Folge der verpflichtenden Umsetzung des gesetzlichen Auftrags. Auf Seiten der Diensteanbieter werden in jedem geeigneten Verfahren zur Identitätsprüfung weitere Kosten zu bewältigen sein – mit Ausnahme für die Diensteanbieter, die bereits jetzt die gesetzliche Vorgabe des § 111 TKG umsetzen oder ein gleich geeignetes Verfahren im Sinne dieser Verfügung anwenden. Die in der Verfügung aufgezeigten Alternativen sollen dabei im Rahmen des gesetzlich Möglichen Auswahlmöglichkeiten je nach Leistungsfähigkeit und technischer sowie personeller Machbarkeit darstellen.

Da der Gesetzgeber die Frist für die Umsetzung der nach § 111 TKG geforderten Prüfverfahren zweifelsfrei definiert hat, besteht keine Möglichkeit, innerhalb der Verfügung von dieser Frist abzuweichen.

Eine weitere Ergänzung erfolgt aufgrund von Stellungnahmen zum Video-Identverfahren. Es wurde vorgeschlagen, zu regeln, dass das Erhebungsverfahren fortzusetzen ist, wenn ein Täuschungsverdacht besteht. Ebenso soll eine Kennzeichnung der so erhobenen Daten als Täuschungsversuch erfolgen.

Aufgrund des Vorschlags wird von Seiten der BNetzA entsprechend klargestellt, dass die an den Diensteanbieter zu übermittelnden und aufgrund eines Täuschungsverdachts entsprechend markierten Daten nicht in die Kundendatei im

Sinne des § 112 TKG aufgenommen werden dürfen. Ferner darf keine Freischaltung der SIM-Karte erfolgen.

Dementsprechend wird folgende Vorgabe auch für diese Verfahrensform eingefügt:

Bestehen Anhaltspunkte für eine Täuschung oder sonstige Manipulation, hat der Dritte das Erhebungs- und Prüfverfahren fortzusetzen. Die so erhobenen Daten sind entsprechend gekennzeichnet an den Diensteanbieter zu übermitteln. Diese Daten dürfen nicht in der Kundendatei im Sinne des § 112 TKG gespeichert werden. Eine Freischaltung der Prepaid-SIM-Karte darf in diesem Fall nicht erfolgen.

2. Verfahren Nr. 2 des Entwurfs

Überprüfung der Daten durch einen vom Diensteanbieter eigens mit der Identitätsprüfung beauftragten Dritten anhand eines der aufgeführten Identitätsdokumente mittels persönlicher und räumlich unmittelbarer Anwesenheit des künftigen Anschlussinhabers (z.B. Post-Ident-Verfahren, IdentService von Hermes u.v.m.)

Stellungnahmen:

Hierzu gab ein Diensteanbieter an, es handele sich um eine gute Verfahrensvariante, die bereits von Teilen des Marktes umgesetzt werde.

Anpassung durch die BNetzA:

Zur Klarstellung der beim Diensteanbieter verbleibenden Prüfpflicht wird der Wortlaut wie folgt geändert:

Erhebung der Daten durch einen vom Diensteanbieter mit Teilen der Identitätsprüfung beauftragten Dritten anhand eines der aufgeführten Identitätsdokumente mittels persönlicher und räumlich unmittelbarer Anwesenheit des künftigen Anschlussinhabers (z.B. Post-Ident-Verfahren, IdentService von Hermes).

Für Verfahren dieser Art gelten folgende Vorgaben:

Ergänzung durch die BNetzA:
Die Vorgaben sind aus Gründen der Gleichwertigkeit der Verfahren um folgenden Punkt (1) zu ergänzen:

Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass der ausgewählte Dritte die Gewähr dafür bietet, dass die Anforderungen hinsichtlich der Datenerhebung, Identitätsprüfung, Prüfung der Echtheit des

Identitätsdokuments, hinsichtlich der Fertigung der Kopien u.ä. sowie deren Übermittlung an ihn eingehalten werden. Dies hat er zu dokumentieren.

(1) Die prüfende Person hat sich von der Echtheit des vorgelegten Identitätsdokumentes zu überzeugen.

Stellungnahmen:

Hierzu wird auch auf die unter Punkt 1. (2) wiedergegebenen Stellungnahmen verwiesen.

Bewertung durch die BNetzA:

Hierzu gilt das unter Verfahren 1 Vorgabe (2) Gesagte.

(2) Die prüfende Person hat vor der Eingabe die Richtigkeit der erhobenen Daten anhand des Identitätsdokuments zu überprüfen, soweit diese darin enthalten sind. Zudem hat sie sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

Anpassung durch die BNetzA:

Entsprechend der Anpassung in Verfahren 1 Vorgabe (2) wird der Text wie folgt angepasst:

Der Dritte hat die Daten des Anschlussinhabers zu erheben. Zudem hat er sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

Um klarzustellen, das auch in dieser Variante eine Übermittlung von Scans oder opto-elektronischen Kopien an den Diensteanbieter zum Zwecke der Prüfung durch ihn zu erfolgen hat, wird folgende weitere Vorgabe eingefügt:

Der Diensteanbieter hat dafür zu sorgen, dass der Dritte in jedem Einzelfall eine opto-elektronische Kopie, Scan oder entsprechende Abbildung anfertigt und zum Zwecke der Prüfung unter Beachtung datenschutzrechtlicher und personalausweisrechtlicher Vorgaben an ihn übermittelt. Opto-elektronische Kopien, Scans oder entsprechende Abbildungen sind als solche zu kennzeichnen und dürfen nicht beim Dritten verbleiben. Für die beim Diensteanbieter vorgelegten Kopien gilt § 95 Absatz 4 TKG.

(3) Bei der Erhebung, Überprüfung und Übermittlung der Daten an den Diensteanbieter zur Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben zu beachten. Geeignete Maßnahmen zur

Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

Anpassung durch die BNetzA:

Entsprechend der in Verfahren 1. vorgenommenen Änderungen wird die Formulierung wie folgt geändert:

Bei der Erhebung und Übermittlung der Daten an den Diensteanbieter zur Prüfung und Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben und Beschränkungen nach dem PAuswG zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

(4) Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass der zu beauftragende Dritte die vorstehenden Vorgaben einhält und seine Mitarbeiter entsprechend schult. Dies ist zu dokumentieren.

Stellungnahmen:

Es wurde vorgetragen, dass aufgrund von Sicherheitsaspekten sämtliche Anbieter verpflichtet werden sollten, das überarbeitete/aktualisierte Post-Ident-Verfahren zu nutzen. Anbieter, die dieses Verfahren nicht übernähmen, dürften nicht zugelassen werden.

Von Seiten der Diensteanbieter wurde angeregt, dass die BNetzA eine Liste von Anbietern von in Betracht kommenden Identifizierungsverfahren veröffentlichen und regelmäßig aktualisieren solle. Ferner könnte Anbietern auf freiwilliger Basis eine Bestätigung im Sinne eines „Zertifikats“ erteilt werden.

Bewertung durch die BNetzA:

Es besteht keine Möglichkeit, von Seiten der BNetzA bestimmte Drittanbieter zu verpflichten, bestimmte Vorgaben einzuhalten. Dies kann nur durch „faktischen Zwang“ erreicht werden, soweit die Diensteanbieter verpflichtet sind, gleichwertige Verfahren anzuwenden. Eine entsprechende Vorgabe ist nun in Ziffer (1) enthalten. Daher kann die bisherige Ziffer (4) gestrichen werden.

Die Gesetzesbegründung verweist ausdrücklich auf das Post-Ident-Verfahren als eines der als gleich geeignet zu betrachtenden Verfahren. Dabei wurde das bei Verfassen der Amtlichen Begründung des Gesetzes angewandte Post-Ident-Verfahren zu Grunde gelegt, das in der zu diesem Zeitpunkt bestehenden Ausgestaltung somit als gleich geeignet bewertet wurde. Durch Verbesserungen oder Änderungen an diesem Verfahren, die nach dieser Bewertung erfolgen, könnte das konkrete Produkt der Deutschen Post AG zwar noch besser geeignet werden. Dies darf aber nicht dazu führen, dass alle weiteren Drittanbieter, deren Produkte bereits

nach dem gegenwärtigen Stand gleichermaßen geeignet wären, sich an Änderungen des Produktes der Deutschen Post AG orientieren müssen.

In Bezug auf die Frage nach einer von der BNetzA veröffentlichten Liste aller als geeignet angesehenen Drittanbieter sowie der Möglichkeit, diese zu zertifizieren, weist die BNetzA darauf hin, dass der gesetzgeberische Auftrag darin besteht, mit dieser Verfügung gleich geeignete Verfahren festzulegen - nicht hingegen, bestimmte Produkte oder Anbieter zu benennen. Die Bundesnetzagentur erachtet die Benennung von Verfahrensarten und wesentliche Vorgaben für jede Verfahrensart als ausreichend, um die gesetzlichen Anforderungen zu erfüllen. Auf diese Weise ist es den Diensteanbietern, etwa im Fall von Video-Ident-Verfahren, möglich, selbst aktiv zu werden. Ebenso wird der Markt für Drittanbieter von Identifizierungsverfahren nicht eingeschränkt, sondern nur darauf verwiesen, für Produkte im Rahmen des § 111 TKG bestimmte erforderliche Verfahrensweisen und Vorgaben einzuhalten.

Eine Ergänzung erfolgt aufgrund von Stellungnahmen zum Video-Identverfahren. Es wird vorgegeben, dass das Erhebungsverfahren fortzusetzen ist, wenn ein Täuschungsverdacht besteht. Ebenso soll eine Kennzeichnung der erhobenen Daten als Täuschungsversuch erfolgen.

Darüber hinaus ist von Seiten der BNetzA klarzustellen, dass die so an den Diensteanbieter zu übermittelnden Daten nicht in die Kundendatei im Sinne des § 112 TKG aufgenommen werden dürfen. Ferner darf keine Freischaltung der SIM-Karte erfolgen.

Dementsprechend wird folgende Vorgabe (6) eingefügt:

Bestehen Anhaltspunkte für eine Täuschung oder sonstige Manipulation, hat der Dritte das Erhebungs- und Prüfverfahren fortzusetzen. Die so erhobenen Daten sind entsprechend gekennzeichnet an den Diensteanbieter zu übermitteln. Diese Daten dürfen nicht in der Kundendatei im Sinne des § 112 TKG gespeichert werden. Eine Freischaltung der Prepaid-SIM-Karte darf in diesem Fall nicht erfolgen.

3. Verfahren Nr. 3 der Anhörung

Überprüfung der Daten im Rahmen einer Videoübertragung mit sprachlicher oder unmittelbarer textlicher Kontaktaufnahme (z.B. Chat) durch Sichtung und Prüfung eines der aufgeführten Identitätsdokumente und <u>zeitgleichen Abgleich</u> mit der vorzeigenden Person durch den Diensteanbieter oder einen von diesem beauftragten Dritten

Stellungnahmen:

Von Seiten der Diensteanbieter wird vorgebracht, der zeitgleiche Abgleich stelle eine unnötige Einschränkung dar. Gerade für Spitzenlastzeiten sollte vielmehr auch die

Verwendung eines zeitversetzten Foto-Ident-Verfahrens ermöglicht werden – dabei würde ein Ausweisscan zusammen mit einer kurzen Videosequenz an den Diensteanbieter übermittelt.

Andererseits wird - ausgehend von Sicherheitsinteressen - die Fernidentifizierung per Videoübertragung als nicht ausreichend bewertet, um die Echtheitsprüfung für die Ausweisdokumente zu gewährleisten. Die Prüfmerkmale seien für eine unmittelbare visuelle bzw. manuelle Prüfung konzipiert, daher seien die Vorgaben Nr. 3 und 4 des Verfahrens in diesem Verfahren praktisch nicht umsetzbar.

Es sollte explizit angeordnet werden, dass eine zeitversetzte Identifikation (also Aufzeichnung eines Videos und erst anschließende Sichtung durch einen Mitarbeiter) nicht zulässig ist. Dies widerspräche dem gesetzlich angeordneten Merkmal „unmittelbar".

Von Seiten der Diensteanbieter wurde vorgeschlagen, die Datenverbindung für die Verifikation für alle Beteiligten kostenlos zu halten, dem Mobilfunknetzbetreiber sollte ferner ein Entschädigungsanspruch gegenüber der Bundesrepublik Deutschland zustehen, da staatliche Aufgabe der Terrorismus- und Verbrechensbekämpfung zum Zwecke des Gemeinwohls der Terrorismus- und Verbrechensbekämpfung übernommen würden.

Ein Diensteanbieter bewertet das vorgeschlagene Verfahren als gute Verfahrensvariante, die bereits am Markt umgesetzt werde.

Bewertung durch die BNetzA:

Ziel dieser Verfügung ist es, im Verhältnis zur Vorlage beim Diensteanbieter gleichermaßen geeignete Verfahren festzulegen. Mit dem Erfordernis einer Vorlage in § 111 TKG soll der Diensteanbieter in die Lage versetzt werden, die erhobenen Daten vor der Freischaltung zu überprüfen. Dabei dient die Vorlage, im Gegensatz zum bloßen Vorzeigen, dazu, das Dokument nicht nur optisch zur Kenntnis nehmen zu können, sondern durch optische oder haptische Wahrnehmung tatsächlich zu überprüfen, inhaltlich ausreichend zur Kenntnis nehmen und es in der Regel selbstbestimmt so lange betrachten und ggf. prüfen zu können, wie dies erforderlich ist, um sich von der Echtheit zu überzeugen. Bei Unsicherheit auf Seiten des Prüfenden muss eine Nachfrage bzw. eine Wiederholung bestimmter Prüfschritte, z.B. im Rahmen der Inaugenscheinnahme, möglich sein.

Beim Video-Identverfahren gibt es im Vergleich zu den bisher behandelten Verfahren Unsicherheitsfaktoren: Eine haptische Echtheitsprüfung des Identitätsdokuments ist nicht möglich und durch das Medium Technik sind Täuschungsmöglichkeiten unter Umständen leichter nutzbar. Nach Ansicht der BNetzA erscheint es jedoch vertretbar und angemessen, mit Hilfe bestimmter Vorgaben die Sichtprüfung und den Personenabgleich auch im Rahmen eines Video-Ident-Verfahrens zu ermöglichen.

Diese Bewertung ergibt sich bereits aus der Gesetzesbegründung zum neuen § 111 TKG, in der der Gesetzgeber das WebIdent-Verfahren ausdrücklich als ein gleichermaßen geeignetes Verfahren bewertet hat.
Die Ansicht der BNetzA stützt sich darüber hinaus aber auch auf den Umstand, dass die in § 111 TKG aufgeführten Identitätsdokumente nicht in Gänze über haptisch wahrnehmbare Echtheitsmerkmale verfügen. Daher kann sich der Kern der Echtheitsprüfung bei gleich zu behandelnden Dokumentenarten lediglich auf eine optische Kontrolle beziehen.

Zudem ist festzuhalten, dass die Personen, die für oder im Auftrag des Diensteanbieters die Echtheit des Dokuments prüfen, diese Prüfung nur als Randtätigkeit erfüllen. Es handelt sich nicht um Personen mit Expertenwissen, wie dies beispielweise bei Zollbeamten der Fall sein dürfte. Demnach kann auch nicht verlangt werden, dass die durchzuführende Prüfung über das hinausgeht, was gemeinhin von einer fundierten, aber dennoch jedermann ohne weiteres möglichen Prüfung offensichtlich erkennbarer Veränderungen oder Mängel umfasst wird. Dies wird im § 111 TKG für den Diensteanbieter selbst nicht verlangt und kann somit auch im Rahmen der vorliegenden Verfügung nicht Maßstab für ein gleichermaßen geeignetes Verfahren sein.

Ausgehend von den im betreffenden Markt etablierten Video-Ident-Verfahren dürfte das Niveau der Sach- und Fachkenntnis in Bezug auf die optische Ausweisprüfung und den Personenabgleich der für den Drittanbieter agierenden Person indes sehr fundiert und umfassend sein.

Mit Blick auf die Parallelität zur Akzeptanz des Video-Verfahrens im Geschäftsbereich der BaFin ist zudem darauf hinzuweisen, dass angesichts der Unterschiede zwischen TKG und GWG keine Notwendigkeit besteht, die Vorgaben der BaFin gleichlautend vorzugeben oder weitere Entscheidungen der BaFin diesbezüglich abzuwarten. Die für die BaFin verbindlichen Vorgaben im GWG, insbesondere § 6 Absatz 2 Nr. 2 GWG, legen den Normadressaten besondere Sorgfaltspflichten auf, sofern die zu identifizierende Person nicht persönlich anwesend ist. Auf dieser Grundlage und mit bestimmten Vorgaben hat die BaFin auch mit Blick auf im europäischen Recht getroffenen Wertungen Video-Ident-Verfahren für eine Prüfung „unter Anwesenden“ ausreichen lassen. Grundlage war also immer das gesetzliche Erfordernis der gleichzeitigen Anwesenheit bei der Identitätsprüfung im Rahmen des GWG.

Dieses Erfordernis existiert im TKG nicht. Dies zeigt sich deutlich daran, dass der Gesetzgeber es dem Diensteanbieter in § 111 Absatz 4 TKG gerade erlaubt, einen Dritten für die Erhebung zu beauftragen. Dabei geht das Gesetz mangels Regelung offensichtlich weiterhin davon aus, dass die Prüfung der Daten anhand des vorgelegten Identitätsdokuments durch den Diensteanbieter selbst erfolgen soll. Tatsächlich verfügt aber nur der mit der Erhebung beauftragte Dritte über die Möglichkeit, den künftigen Anschlussinhaber in persona zu sehen und mit der im Identitätsdokument abgebildeten Person abzugleichen. Ebenso hat auch nur der

Dritte in diesen Fällen das Identitätsdokument vor Augen. Dies ist bei den in der Gesetzesbegründung bereits als gleich geeignet aufgeführten Verfahren des PostIdent oder des WebIdents ebenfalls der Fall.

Zwar hat der Gesetzgeber mit den §§ 111-113 TKG die Anschlussinhaberdaten als so wesentlich für Sicherheitsbehörden bewertet, dass diese kostenträchtig zu speichern und abrufbar sein müssen. Dabei ist jedoch schon allein aufgrund der Möglichkeit, eine erworbene SIM-Karte frei an einen (ggf. unbekannten) Dritten weiterzugeben, zu akzeptieren, dass es zu unrichtigen Daten kommen kann. Dies ist bei der Eröffnung eines Kontos nicht der Fall, da dieses rechtlich an den Inhaber gebunden ist.

Kostenregelungen sowie Entschädigungsansprüche sind kein Bestandteil der Regelung gleich geeigneter Verfahren und daher kein zulässiger Gegenstand dieser Verfügung.

Für Verfahren dieser Art gelten folgende Vorgaben:

(1) Die prüfende Person ist hinsichtlich der Prüfung des Identitätsdokuments sowie des Ablaufs der Datenerhebung und -prüfung umfassend zu schulen.

Stellungnahmen:

Von Seiten der Sicherheitsbehörden wird, wie unter Punkt 1. (1), zu diesem Punkt ergänzend gefordert, den erforderlichen Schulungsumfang in der Verfügung deutlich zu bestimmen, Infomaterial ausdrücklich nicht ausreichen zu lassen und eine Dokumentationspflicht hinsichtlich der Schulung sowie der Einhaltung der Vorgaben zu ergänzen.

Bewertung durch die BNetzA:

Es wird auf die Stellungnahme unter Verfahren 1 Punkt (1) verwiesen. Zur Gleichbehandlung mit den Verfahren 1 und 2 ist der Wortlaut entsprechend anzupassen. Um sicherzustellen, dass Anbieter derartiger Identifizierungsverfahren bzw. deren erhebenden Mitarbeiter ausreichende Gewähr dafür bieten, dass die Echtheitsprüfung tatsächlich durch spezielle befähigte Mitarbeiter geschieht, ist die Vorgabe der Schulung ausdrücklich aufgenommen worden. Hier erscheint es angesichts der Bedenken der Sicherheitsbehörden angemessen, über das für Verfahren 1 und 2 verlangte Maß an Anweisung hinauszugehen. Dadurch wird der Unsicherheitsfaktor des nur medial vermittelten Gegenüberstehens nach Ansicht der BNetzA ausreichend ausgeglichen.

Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass ausgewählte Dritte die Gewähr dafür bieten, dass die Anforderungen hinsichtlich der Datenerhebung, Identitätsprüfung, Prüfung der Echtheit des Identitätsdokuments, der Fertigung der Kopien u.ä. sowie deren Übermittlung

an ihn eingehalten werden. Die Beauftragung darf nur erfolgen, wenn der Dritte verpflichtend eine jährliche Schulung auf Grundlage neuester Erkenntnisse einer mit Identitätsprüfungen oder der Prüfung von Ausweisdokumenten betrauten öffentlichen oder allgemein anerkannten Stelle für seine Mitarbeiter durchführt oder durchführen lässt (z.B. durch das BKA). Dies hat der Dritte zu dokumentieren. Erfolgt die Erhebung und Prüfung durch den Diensteanbieter selbst, gelten das Schulungserfordernis sowie die Dokumentationspflicht für ihn entsprechend.

(2) Es ist eine Ausweisdatenbank vorzuhalten und mindestens jährlich zu aktualisieren, die entsprechende Merkmale für ausländische Identitätsdokumente enthält und für den Abgleich von der prüfenden Person bei Vorlage eines ausländischen Identitätsdokuments heranzuziehen ist.

Stellungnahmen:

Von Seiten der Diensteanbieter wird angeregt, eine konzentrierte Datenhaltung im Sinne einer Referenzdatenbank bei einer nationalen Stelle einzurichten bzw. entsprechende Drittanbieter für diese Zwecke zuzulassen. Auch von Seiten der Sicherheitsbehörden wurde gefragt, ob die Möglichkeit einer Referenzdatenbank bestünde.

Vereinzelt wurde vorgeschlagen, nur solche Identitätsdokumente für die Identifizierung heranzuziehen, die in einer Ausweisdatenbank vorzuhalten sind. Dabei solle es dem Diensteanbieter obliegen, zu entscheiden, mithilfe welcher Ausweisdokumente (!) eine Überprüfung möglich sein soll.

Eine Ermittlungsbehörde schlägt vor, diesen Punkt auch für die anderen Verfahrensvarianten zu ergänzen.

Bewertungen durch die BNetzA:

Der Vorschlag einer Referenzdatenbank ist nach Ansicht der Bundesnetzagentur sehr sinnvoll, kann jedoch nicht im Rahmen der hiesigen Verfügung thematisiert werden. Insoweit wird die Formulierung dahin angepasst, dass sowohl eine vom Diensteanbieter selbst erstellte also auch eine von Drittanbietern oder öffentlichen Stellen herangezogene Datenbank zugrunde gelegt werden darf.

Einem Diensteanbieter steht es grundsätzlich frei, zu bestimmen, welche der in § 111 Absatz 1 TKG aufgeführten Identitätsdokumente er konkret zur Prüfung zulässt. Insoweit ist auf den Grundsatz der Vertragsfreiheit hinzuweisen. Dem Diensteanbieter steht es frei, zu entscheiden, ob und mit wem er in Bezug auf Prepaid-SIM-Karten einen Vertrag abschließt.

Umgekehrt bedeutet das aber auch: Kann er bestimmte in § 111 Absatz 1 TKG aufgeführte Identitätsdokumente nicht prüfen bzw. nicht auf Echtheit prüfen lassen, darf auf Grundlage einer Vorlage dieser Dokumente keine Freischaltung erfolgen.

Die Regelung der Datenbank wird in Verfahren 3 aufgeführt, da hier schon aufgrund des zwischengeschalteten Mediums die Verfügbarkeit und Nutzbarkeit einer Datenbank einfach und ohne zeitliche Verzögerung oder besonderen Aufwand im Rahmen des Erhebungs- und Prüfverfahrens möglich ist. In den Verfahren 1 und 2 ist dies nicht der Fall und muss dort durch alternative Quellen ersetzt werden. Selbstverständlich ist auch in diesen Verfahren die Nutzung einer Datenbank möglich und sinnvoll.

Aufgrund der dargestellten Bewertung wird folgende neue Formulierung eingefügt:

Es ist eine regelmäßig aktualisierte Ausweisdatenbank zu nutzen, die Prüfmerkmale für ausländische Identitätsdokumente enthält und vom Dritten bei Vorlage eines ausländischen Identitätsdokuments für den Abgleich heranzuziehen ist.

(3) Die prüfende Person hat sich von der Echtheit des vorgelegten Identitätsdokuments zu überzeugen.

Stellungnahmen:

Nach Ansicht der Diensteanbieter kann sich eine Überprüfung nur auf offensichtliche Manipulationen und Fälschungen bzw. auf sichtbare Sicherheitsmerkmale beziehen. Die Anforderungen dürften nicht über das Vorhandensein bestimmter wesentlicher Merkmale wie beispielsweise dem holografischen Portrait hinausgehen. Eine ausreichende Sicherheit sei vielmehr auch dann gewährleistet, wenn auf wesentliche Elemente echter Ausweisdokumente aufmerksam gemacht würde. Demzufolge würde die Vorgabe so verstanden, dass nur Merkmale der Sicherheitsstufe 1 visuell oder auf opto-elektronischem Wege erfasst werden (Anm. BNetzA: gemeint sind vermutlich Merkmale, die ohne Hilfsmittel und geringen Vorkenntnissen visuell, taktil oder auditiv wahrnehmbar sind). Merkmale der Sicherheitsstufe 2 seien hingegen nicht umfasst (Anm. BNetzA: gemeint sind vermutlich Merkmale, die nur unter Hinzuziehung technischer Hilfsmittel wie z.B. UV-Lampe wahrnehmbar sind). Aufwändige technische Systeme oder Hilfsmittel am Point of Sale dürften nicht gefordert werden.

Zur Durchführung wurde angegeben, dass die Prüfung der Echtheit durch Kippen oder Drehen des Identitätsdokuments und die Erfassung visueller oder opto-elektronischer Sicherheitsmerkmale geschehen könne.

Dazu wurde von einem Diensteanbieter folgender konkreter Formulierungsvorschlag gemacht: „[Die prüfende Person hat] das vorgelegte Identitätsdokument anhand der wesentlichen Merkmale durch Inaugenscheinnahme zum Ausschluss offensichtlicher Fälschungen zu prüfen."

Bewertung durch die BNetzA:

Es wird auf die Bewertungen zur Verfahren 1 Vorgabe (2) verwiesen. Im Sinne einer einheitlichen Regelung werden Vorgabe (3) und (4) in zusammengefasst und dem überarbeiteten Wortlaut angepasst. Daher ergibt sich folgender neuer Wortlaut:

Die erhebende Person hat das vorgelegte Identitätsdokument anhand der wesentlichen Merkmale durch Inaugenscheinnahme zum Ausschluss offensichtlicher Fälschungen auf äußerlich erkennbare Manipulationen zu überprüfen. Die Person des zukünftigen Anschlussinhabers ist zu diesem Zweck aufzufordern, das Identitätsdokument vor der Kamera entsprechend zu bewegen und zu positionieren (Kippen, Drehen etc.).

(4) Das zur Identifizierung vorgezeigte Identitätsdokument ist von der prüfenden Person auf äußerlich erkennbare Manipulationen zu überprüfen. Die Person des zukünftigen Anschlussinhabers ist zu diesem Zweck aufzufordern, das Identitätsdokument vor der Kamera entsprechend zu bewegen und zu positionieren (Kippen, Drehen etc.).

Stellungnahmen:

Hierzu schlägt eine Ermittlungsbehörde vor, diese Vorgabe bei den Verfahren 1 und 2 zu ergänzen.

Bewertung durch die BNetzA:

Dies ist in entsprechender Form in den Verfahren 1 und 2 umgesetzt. Da hier die Prüfung auf eine Inaugenscheinnahme reduziert ist, bedarf es in Verfahren 3 konkreterer Vorgaben in Bezug auf den genauen Ablauf der Echtheitsprüfung. Dies wird gemeinsam mit der Vorgabe aus Ziffer (3) behandelt.

Der Wortlaut ergibt sich aus der Bewertung der BNetzA zu Vorgabe (3). Die Reihung nachfolgenden Vorgaben wird entsprechend angepasst.

(5) Die prüfende Person hat vor der Eingabe die Richtigkeit der erhobenen Daten anhand des Identitätsdokuments zu überprüfen, soweit diese darin enthalten sind. Zudem hat sie sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

Anpassung durch die BNetzA:

Entsprechend der Anpassung in Verfahren 1. Vorgabe (2) wird der Text wie folgt angepasst:

Der Dritte hat die Daten des Anschlussinhabers zu erheben. Zudem hat er sich zu vergewissern, dass die Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

Um klarzustellen, dass auch in dieser Variante eine Übermittlung von Scans, Screenshots oder opto-elektronischen Kopien an den Diensteanbieter zum Zwecke der Prüfung durch ihn zu erfolgen hat, wird folgende weitere Vorgabe unter Ziffer (6) eingefügt (die Ziffern der folgenden Vorgaben sind entsprechend anzupassen):

Der Diensteanbieter hat dafür zu sorgen, dass der Dritte in jedem Einzelfall eine opto-elektronische Kopie, Scan oder entsprechende Abbildung anfertigt und zum Zwecke der Prüfung unter Beachtung datenschutzrechtlicher und personalausweisrechtlicher Vorgaben an ihn übermittelt. Opto-elektronische Kopien, Scans oder entsprechende Abbildungen sind als solche zu kennzeichnen und dürfen nicht beim Dritten verbleiben. Für die beim Diensteanbieter vorgelegten Kopien gilt § 95 Absatz 4 TKG.

(6) Bei schlechten Lichtverhältnissen oder dem Eindruck, dass eine Täuschung oder sonstige Manipulation vorliegt, ist ein sofortiger Abbruch vorzusehen.

Stellungnahmen:

Von Seiten der Diensteanbieter wie auch der Anbieter entsprechender Verifikationsverfahren wird vorgeschlagen, bei einem Verdacht auf Täuschung und/oder Manipulation die Datenerfassung zunächst abzuschließen und durch die prüfende Person dokumentieren oder kennzeichnen zu lassen, damit künftige Täuschungsversuche schneller erkannt werden. Auch könne gegenüber dem Diensteanbieter eine Meldung der Daten bzw. eine Kennzeichnung als „Betrugsverdacht“ erfolgen. Dies sei bereits geübte Praxis für Video-Ident-Verfahren.

Von anderer Seite wurde vorgeschlagen ein Abbruch sei nicht in jedem Fall erforderlich, vielmehr sollte man die prüfende Person und den Kunden gemeinsam

versuchen lassen, die Lichtverhältnisse zu verbessern. Ebenso sollte der Kunde zu alternativen Verfahren beraten werden können.

Von Seiten einer Ermittlungsbehörde wurde angeregt, diesen Punkt auch für die Verfahren zu Nr. 1 und 2 zu ergänzen.

Bewertung durch die BNetzA:

Der Vorschlag der Fortführung des Erhebungsverfahrens wird aufgenommen und in den Verfahren 1 und 2 ergänzt. Ebenso die Kennzeichnung der so erhobenen Daten als Betrugsfall.

Darüber hinaus ist klarzustellen, dass die so an den Diensteanbieter zu übermittelnden Daten nicht in die Kundendatei im Sinne des § 112 TKG aufgenommen werden dürfen. Ferner darf keine Freischaltung der SIM-Karte erfolgen.

Dementsprechend wird der Wortlaut wie folgt geändert:

Bestehen Anhaltspunkte für eine Täuschung oder sonstige Manipulation, hat der Dritte das Erhebungs- und Prüfverfahren fortzusetzen. Die so erhobenen Daten sind entsprechend gekennzeichnet an den Diensteanbieter zu übermitteln. Diese Daten dürfen nicht in der Kundendatei im Sinne des § 112 TKG gespeichert werden. Eine Freischaltung der Prepaid-SIM-Karte darf in diesem Fall nicht erfolgen.

(7) Bei der Erhebung, Überprüfung und Übermittlung der Daten an den Diensteanbieter zur Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

Anpassung durch die BNetzA:

Zum Zwecke der einheitlichen Regelung wird der Wortlaut wie folgt angepasst:

Bei der Erhebung und Übermittlung der Daten an den Diensteanbieter zur Prüfung und Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben und Beschränkungen nach dem PAuswG zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

(8) Die Datenverbindung kann auch mit der erworbenen Mobilfunkleistung selbst, beispielsweise mit der erworbenen SIM-Karte aufgebaut werden, wobei die erworbene Mobilfunkleistung vor der abgeschlossenen

Verifikation ausschließlich die zur Registrierung und Prüfung des Identitätsdokuments erforderliche Datenverbindung ermöglichen darf.

Stellungnahmen:

Von Seiten der Diensteanbieter sowie einzelnen Anbietern dieser Verifikationsverfahren wird darum gebeten, auch sonstige Verbindungen zuzulassen, bspw. den Eingang einer SMS des Anbieters, ggf. mit Link zum Verifizierungsanbieter, oder einen Sprach- bzw. Video-Anruf an eine Service-Line. Dazu wurde von einigen Teilnehmern folgender konkreter Formulierungsvorschlag eingereicht:

> „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."

Ergänzt werden sollte nach Ansicht eines Anbieters von Video-Ident-Verfahren darüber hinaus, dass die Datenverbindung auch den Zugriff auf den App Store beinhalten sollte. Die zur Identifizierung notwendige App müsse in den meisten Fällen aus dem App Store geladen werden können.

Aus Gründen des Datenschutzes wurde verlangt, einen datenschutzrechtlichen Hinweis bei einem Video-Chat-Dienst aufzunehmen. Der Kunden dürfen nicht gezwungen werden, außereuropäische Diensteanbieter für die Videoübertragung zu nutzen. Des Weiteren werden eine Aufzeichnung des Chats sowie Screenshots abgelehnt.

Von Seiten der Sicherheitsbehörden wird angeregt, ähnlich wie unter Variante 1 eine nachträgliche Übermittlung einer opto-elektronischen Kopie zu fordern.

Bewertung durch die BNetzA:

Auf Grundlage und nach Bewertung der eingereichten Stellungnahmen kommt die Bundesnetzagentur zu dem Ergebnis, dass die Initiierung der Kommunikation mithilfe der erworbenen Mobilfunkleistung auf vielfältige Weise möglich ist. So ist denkbar, dass mit Einlegen der SIM-Karte und Starten des Endgeräts eine Kommunikation mittels einer SMS erfolgt, die den link zu einer Webseite enthält. Ferner ist denkbar, dass der Erwerber zunächst in einen Store für Anwendungssoftware für mobile Betirebssysteme oder entsprechendes geleitet wird.

Die besondere Eingriffsanfälligkeit einer Anwendungssoftware für mobile Betriebssysteme ist nicht in gleicher Weise relevant für die Vorlage gemäß § 111 TKG wie dies in anderen Sachverhalten der Fall sein könnte. Es ist nicht zu erwarten, dass jemand für eine erfolgreiche Täuschung beim Prepaid-SIM-Karten-Kauf den dafür erforderlichen technischen Aufwand in Kauf nimmt. Es handelt sich um den

Erwerb eines alltäglichen, jederzeit und frei zugänglichen Gegenstands. Dabei bestehen wesentlich einfachere Möglichkeiten die Datenerhebung und – prüfung des § 111 TKG zu umgehen. Aus diesem Grund besteht nach Ansicht der Bundesnetzagentur keine Erforderlichkeit, die App-Funktion außen vor zu lassen. Dennoch soll den Bedenken der Sicherheitsbehörden insoweit Rechnung getragen werden, dass in Anlehnung an das Rundschreiben der BaFin Nr. 4 aus 2016 zusätzliche Sicherungen für die Kommunikationsverbindung über eine App gefordert werden.

Den datenschutzrechtlichen Bedenken hins. des möglichen faktischen Zwangs, eine dem deutschem bzw. europäischen Datenschutzstandard nicht unterliegende Kommunikationsverbindung zu nutzen, wird in der geänderten Formulierung Rechnung getragen.

Die nachträgliche Übermittlung der Daten und Nachweise an den Diensteanbieter ist auch für das Verfahren 3 erforderlich, damit der Diensteanbieter seiner Prüfpflicht nachkommen kann.

Darauf basierend wird der Wortlaut wie folgt geändert:

Die für die Erhebung und Übermittlung der Daten erforderliche Telekommunikation kann auch mit der erworbenen Mobilfunkleistung selbst aufgebaut werden, wobei die erworbene Mobilfunkleistung vor Freischaltung ausschließlich für diesen Kommunikationsvorgang möglich sein darf. Der Diensteanbieter darf dabei nicht ausschließlich außereuropäische Anbieter zur Verfügung stellen.

Zudem wird folgende Vorgabe ergänzt:

Bei Verwendung von Anwendungssoftware für mobile Betriebssysteme für den Aufbau der Telekommunikationsverbindung zum Zwecke der Datenerhebung sind Jailbreak bzw. Rooting Detection Programme einzusetzen, die dem aktuellen Stand der Technik entsprechen.

4. Hinweis auf eID-Funktion des deutschen Personalausweises

Die Erhebung der Anschlussinhaberdaten kann auch mittels der eID-Funktion des Personalausweises erfolgen. Diese Funktion stellt jedoch keinen Ersatz für den Abgleich der Person des künftigen Anschlussinhabers mit der im Identitätsdokument ausgewiesenen Person dar.

Stellungnahmen:

Sowohl von Seiten der Diensteanbieter als auch von Seiten der Sicherheitsbehörden besteht die Überzeugung, dass die eID-Funktion des Personalausweises als sicheres Legitimationsmittel zugelassen werden sollte. Zusammen mit der PIN, welche nur

dem Inhaber bekannt sein sollte, werde ein Abgleich zwischen der Person des künftigen Anschlussinhabers und dem Personalausweis vor Ort entbehrlich. Demnach sei der letzte Satz dieses Absatzes zu streichen.

Nach Hinweis von Seiten der Sicherheitsbehörden soll folgender Passus ergänzt werden:

> "Der elektronische Identitätsnachweis nach §§ 8 PAuswG und nach 78 Aufenthaltsgesetz kann die Identitätsprüfung unter Anwesenden auf einem hohen elektronischen Vertrauensniveau ersetzen.
>
> Dafür gelten folgende Vorgaben:
>
> (1) Der elektronische Identitätsnachweis weist die Korrektheit der übermittelten Daten nach. Nicht aus dem Ausweis übermittelte Daten müssen auf anderem Wege verifiziert werden.
>
> (2) Die Dokumentationspflichten bleiben unberührt.
>
> (3) Auf §111 (1) Satz 6 TKG wird verwiesen."

Bewertung durch die Bundesnetzagentur:

Die eID-Funktion wird als zusätzliches viertes Verfahren in die Verfügung aufgenommen, ohne auf einem persönlichen Abgleich zwischen der Person des Nutzers des Identitätsnachweises und des berechtigten Inhabers des Identitätsdokuments zu bestehen.

Die konkret vorgeschlagenen Vorgaben dazu werden insoweit aufgenommen, als der Verweis auf § 111 Absatz 6 TKG betroffen ist. Diese enthält eine deklaratorische Wiederholung des geltenden Rechts und ist daher nicht zu beanstanden. Die weiteren Vorschläge für konkrete Vorgaben werden jedoch nicht übernommen, da in Bezug auf die erstgenannte Ziffer zum einen eine reine Tatsachenbeschreibung enthalten ist und zum zweiten eine weitere Verifikationspflicht eingeführt würde, die in § 111 TKG in der Form nicht enthalten ist. Aus diesem Grunde ist es nicht möglich, die zusätzliche Regelung im Rahmen dieser Verfügung zu gleich geeigneten Verfahren aufzunehmen.

Die in § 111 Absatz 1 TKG ausdrücklich normierten Dokumentationspflichten bedürfen keiner Regelung in der Verfügung mehr. Darüber hinausgehende Dokumentationspflichten sind für dieses Verfahren nicht vorgesehen.

Daraus ergibt sich folgender zu ändernder Wortlaut des Verfahrens 4:

Die Erhebung und Prüfung der Anschlussinhaberdaten kann auch im Wege des elektronischen Identitätsnachweises nach § 8 PAuswG und nach § 78 Aufenthaltsgesetz erfolgen. Auf § 111 Absatz 6 TKG wird hingewiesen.

5. Verweis auf qualifizierte elektronische Signatur

Für Identifizierungsverfahren, die auf Grundlage der Vorgaben für die qualifizierte elektronische Signatur nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) seitens der nach § 18 Absatz 1 SigG anerkannten Prüf- und Bestätigungsstellen bereits geprüft und zertifiziert wurden, werden die genannten Vorgaben bereits als eingehalten betrachtet.

Stellungnahmen:

In Ergänzung zum Hinweis auf die qualifizierte elektronische Signatur wurde von Seiten der Sicherheitsbehörden ausgeführt, dass die Identitätsprüfung anhand einer Qualifizierten Elektronischen Signatur die Identitätsprüfung unter Anwesenden ersetzen könne, wenn die erforderlichen Identitätsdaten über einen sicheren Kanal untrennbar von der Signatur übertragen werden. Dieses Erfordernis sei klar in der Verfügung zu definieren und als erforderlich anzuordnen. Die Identitätsfunktion der elektronischen Signatur ermögliche durch die Identitätsprüfung des Zertifizierungsdienstleisters an Hand eines Personalausweises oder Passes eine aus der Gültigkeit und Unversehrtheit der Signatur abgeleitete Identitätsprüfung. Die für die Identitätsprüfung zusätzlich erforderlichen und im Signaturzertifikat nicht enthaltenen Personendaten, ggf. eine foto-elektronische Kopie des Dokuments seien zusätzlich zur Übermittlung der Signatur gesichert zu übertragen, zweckmäßiger Weise als signiertes Dokument.

Andererseits wurde vorgetragen, dieser Absatz erschiene zumindest in seiner Pauschalität nicht zweckmäßig. Verfahren nach SigG würden immer im Kontext der Ausgabe eines qualifizierten Zertifikates bzw. einer Signaturerstellungseinheit bestätigt. Dadurch würden ggf. durch weitere Prozessschritte Sicherheitsleistungen erbracht (z.B. Adressverifikation durch Versand der Signaturerstellungseinheit), die das Identifizierungsverfahren als solches nicht erbringe, die aber für die Sicherheit des Verfahrens erforderlich seien. Darüber hinaus wurde darauf hingewiesen, dass das SigG durch die eIDAS-Verordnung abgelöst werde. Ein Verweis auf das SigG mit der hinterliegenden Bestätigungssystematik liefe mit Außerkrafttreten des SigG ins Leere. Daher wurde vorgeschlagen, diesen Absatz zu streichen.

Ein Anbieter von online-Zertifizierungsverfahren schlägt vor, in Ergänzung zur Signatur auch Identifizierungsverfahren anzuerkennen, die durch anerkannte Prüf- und Bestätigungsstellen im Rahmen der TR der eIDAS-VO bereits geprüft und zertifiziert wurden.

Bewertung durch die BNetzA:

Der Anregung, eine qualifizierte elektronische Signatur unter bestimmten Vorgaben als Ersatz für die Identitätsprüfung zu akzeptieren, kann nur eingeschränkt gefolgt werden.

Durch die Signatur kann die nach zahlreichen Vorschriften erforderliche eigenhändige Unterschrift im Rahmen des elektronischen Rechtsverkehrs ersetzt werden. Sie lässt dabei lediglich den Namen des Urhebers erkennen, soweit kein Synonym verwendet wird. Erfolgt eine Übermittlung der nach § 111 TKG zu erhebenden Anschlussinhaberdaten versehen mit einer von diesen Angaben untrennbaren qualifizierten elektronischen Signatur, wird durch die Signatur gegenüber dem Diensteanbieter nur nachgewiesen, dass der Absender auch tatsächlich die Person dieses Namens bzw. die Person des Anschlussinhabers ist. Nicht geprüft werden kann jedoch, ob die weiteren Angaben aus dem Identitätsdokument, das bei der Identitätsprüfung für die Signaturerteilung vorgelegt wurde, mit den Angaben übereinstimmen, die mittels des mit der Signatur versehenen Dokuments übermittelt wurden und nach § 111 TKG zu erheben sind. Einsicht in die Angaben, die bei der Identitätsprüfung für die Signaturerteilung gemacht und geprüft wurden, wird durch die Nutzung der qeS nicht ermöglicht. Demnach müssten alle Daten aus dem Identitätsdokument, die nicht mit der Signatur belegt werden, namentlich alle Angaben neben dem Namen, auf gesondertem Wege geprüft werden. Daher ist die Nutzung einer qeS nur als Ergänzung im Rahmen der Datenprüfung nach § 111 Absatz1 TKG denkbar und kann mithin nur neben einem Prüfverfahren im Sinne dieser Anordnung bzw. der Vorlage beim Diensteanbieter verwendet werden.

Als alleiniges Verfahren stellt die qeS mithin kein gleich geeignetes Verfahren wie die Vorlage eines Identitätsdokuments beim Diensteanbieter dar. Gleichwohl kann die Verwendung eines mit einer qeS versehenen Dokuments als Prüfung des Anschlussinhabernamens ausreichen und in Kombination mit einem der aufgeführten Verfahren ergänzend herangezogen werden.

Der Verweis auf das SigG ist aufgrund der unmittelbar anwendbaren eIDAS-VO, die das SigG ersetzt, nicht mehr tragfähig. Somit wird darauf insgesamt verzichtet. Zukünftig könnte ein Verweis auf die Verfahren nach § 24 der eIDAS-VO in Verbindung mit entsprechenden nationalen Vorgaben in Betracht kommen, soweit dabei die nach § 111 TKG benötigten Daten entsprechend zur Verfügung gestellt werden können. Die Technische Richtlinie, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfasst, stellt nur eine Empfehlung dar, die neben anderen Standards herangezogen werden kann. Die Entscheidung über die Anwendung oder das Heranziehen eines anderen Standards obliegt den Konformitätsbewertungsstellen und der Bundesnetzagentur.

C. Vorschläge zu weiteren Verifikationsverfahren

1. Videoübertragung mit halb- oder vollständig automatisierten Prüfverfahren

Ein Vorschlag von Seiten der Diensteanbieter sieht ein (teil-) automatisiertes Verfahren zur Prüfung der Identitätsdokument-Daten vor, bei dem bspw. das Auslesen von Ausweisdaten mit Hilfe eines Scanners mit einem automatischen Abgleich mit einer Ausweisdatenbank kombiniert wird und möglicherweise auch die Identitätsprüfung automatisiert erfolgen würden. Dies solle gerade zum Abfedern von Spitzenlastzeiten helfen, die Kunden schnellstmöglich zu bedienen.

Vorteile davon seien mehr Sicherheit, Schnelligkeit und Nutzerfreundlichkeit. Dabei würden die Kosten für den Identifizierungsvorgang gesenkt, der Fehlerfaktor Mensch reduziert und moderne Techniken unterstützen. In Spitzenlastzeiten sei eine Bearbeitung mit geschultem Personal hingegen nur mit Wartezeiten für die Kunden möglich.

Bewertung durch die BNetzA:

Nach Ansicht der Bundesnetzagentur ist ein automatisiertes Erheben der Anschlussinhaberdaten in Kombination mit einer durch eine Person vorgenommenen oder automatisierten Echtheits- sowie Identitätsprüfung unter dem Vorbehalt der Einhaltung bestimmter Vorgaben grundsätzlich eine ebenso geeignetes Mittel wie die Vorlage beim Diensteanbieter, § 111 Abs. 1 TKG.

Ein automatisiertes Erheben der Daten ist als Ergänzung zu einer Echtheits- und Identitätsprüfung durch eine Person ohne weiteres gleich geeignet. Dabei sind allerdings in besonderem Maße die datenschutzrechtlichen Anforderungen und Vorgaben nach dem PAuswG oder Aufenthaltsgesetz zu beachten.

Ein vollständig automatisierter Ablauf für die Datenerhebung sowie für die Prüfung der Dokumentenechtheit und der Identität des Erwerbers kann derzeit jedoch nur unvollständig bewertet werden. Daher sieht die BNetzA davon ab, dieses auf zukünftige Entwicklungen gerichtete Verfahren schon zum hiesigen Zeitpunkt zu regeln. Hier bestünde Potential, zukünftige Entwicklungen gegebenenfalls im Rahmen einer erneuten Anhörung und eventuellen Aktualisierung der Verfügung abzubilden.

Abstrakt dürfte ein automatisiertes Verfahren ist im Rahmen des § 111 TKG grundsätzlich umsetzbar sein. Anders als im Finanzsektor besteht im TK-Bereich kein Erfordernis einer gleichzeitigen Anwesenheit von Personen. Auch der Begriff der Vorlage verlangt nicht, dass diese unmittelbar von Hand zu Hand geht. Anderenfalls würde auch die eID-Funktion des deutschen Personalausweises nicht als Vorlage ausreichen, was aber sogar nach Ansicht der Sicherheitsbehörden ausreichen soll. Ebenso wird auf die Ausführungen zu Verfahren 3 verwiesen.

Eine hinreichend gestaltete automatisierte Prüfung könnte dabei nach klar definierten Kriterien und objektivierten Bewertungsmaßstäben erfolgen und so die Ungenauigkeiten und Unzulänglichkeiten einer „persönlichen“ Prüfung beseitigen. Das Niveau eines Video-Ident-Verfahrens könnte dabei gemessen am Regelungsziel des § 111 TKG ebenfalls erreicht werden.

Dennoch ist in dieser Abstraktheit unklar, welche Möglichkeiten zur Prüfung, welche Datenbanken, Systeme und Tools verfügbar und ausreichend sein könnten und welche Anforderungen an die Datenverbindung und die automatisierte Prüfung zu stellen wären.

2. Foto-Ident-Verfahren/zeitversetztes Video-Ident-Verfahren

Der Vorschlag zu einem Unterfall eines Foto-Ident-Verfahren sieht zum Teil vor, dass ein Foto des Ausweises und sowie eine vorab aufgezeichnete kurze Videosequenz des Kunden aufgenommen und über eine gesicherte Verbindung an geschultes Personal übermittelt wird (vgl. hierzu Variante A) mit einer automatisierten Prüfung und Erfassung. Nach erfolgter Prüfung werden die Daten und ggf. Aufzeichnungen an den Diensteanbieter übergeben.

Ein zeitversetztes opto-elektronisches Verfahren würde nach den vorliegenden Äußerungen von Seiten der Diensteanbieter nicht zu einer geringeren Validität der erhobenen Daten und der zu prüfenden ID-Dokumente führen. Es würde jedoch eine erhebliche Entlastung auch in finanzieller Hinsicht für den Diensteanbieter bedeuten. Durch die Übermittlung einer opto-elektronischen Kopie müsste die Prüfung nicht mehr am Point of sale stattfinden. Dabei gestalten sich die Varianten, auf welchem Wege bzw. mithilfe welcher technischer Kanäle (Smart Phone, PC, Tablet) eine Übermittlung stattfinden kann, sehr zahlreich.

Ein anderer Vorschlag basiert hingegen nur auf die Zusendung von Fotos, wobei der künftige Anschlussinhaber sich selbst und sein Identitätsdokument fotografieren soll. Das Verfahren, welches jedoch keine Videosequenz der Bewegung des Identitätsdokumentes enthalten soll, wird wie folgt beschrieben:

> (1) Der zukünftige Anschlussinhaber erwirbt die SIM-Karte und ruft die Webseite des Diensteanbieters auf. Auf einer Registrierungsseite gibt er die Rufnummer und die SIM-Kartennummer (zusammen „SIM-Daten“) ein. Diese SIM-Daten werden durch den Diensteanbieter oder einen beauftragten Dritten validiert.
>
> (2) Nach erfolgreicher Validierung der SIM-Daten nimmt der zukünftige Anschlussinhaber ein Foto von sich selbst mit seinem Mobilfunkgerät, Computer, digitalen Kamera o.ä. auf. Ebenso fotografiert er sein Identitätsdokument. Beide Fotoaufnahmen übermittelt er an den Diensteanbieter. Dieser überprüft – ggf. durch

einen beauftragten Dritten, der über entsprechende Verifikationssysteme verfügt – die Echtheit des Identitätsdokuments und die Übereinstimmung des übermittelten Fotos mit dem Foto auf dem übermittelten Identitätsdokument. Diese Validierung des Ausweises erfolgt – i.d.R. automatisiert – anhand zuverlässiger Verifikationssoftware, die u.a. in der Lage ist, die Echtheit des Identitätsdokuments anhand vorgegebener Kriterien zu überprüfen, die Klarangaben auf dem Identitätsdokument mit den maschinenlesbaren Angaben auf dem Identitätsdokument abzugleichen und das Foto des zukünftigen Anschlussinhabers mit dem Foto auf dem Identitätsdokument unter Berücksichtigung von Altersunterschieden und Änderung des Aussehens (z.B. anderer Haarschnitt) zu vergleichen. Nur im Falle fehlender Anzeichen dafür, dass das Identitätsdokument unecht ist, und einer hohen Übereinstimmung der beiden Fotos ist die Validierung des Identitätsdokuments erfolgreich.

(3) Bei erfolgreicher Validierung der SIM-Daten und des Identitätsdokuments werden dem zukünftigen Anschlussinhaber die Registrierungsdaten gemäß § 111 Abs. 1 Satz 1 Nrn. 1, 2 und 3 TKG auf der Webseite angezeigt und er muss diese bestätigen. Nach Bestätigung wird die SIM-Karte freigeschaltet und die ermittelten Anschlussinhaberdaten werden beim Diensteanbieter gespeichert. Die übermittelten Fotos des Anschlussinhabers und des Identitätsdokuments werden gelöscht (§ 95 Abs. 4 Satz 4 TKG).

(4) Bei der Erhebung, Überprüfung und Übermittlung der Daten zwischen Anschlussinhaber und Diensteanbieter sind die datenschutzrechtlichen Vorgaben zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

(5) Die Daten- und Telekommunikationsverbindung zur Übermittlung des Fotos des Anschlussinhabers und des Identitätsdokuments sowie für das Verifikationsverfahren kann auch mit der erworbenen Mobilfunkleistung selbst, beispielsweise mit der erworbenen SIM-Karte erfolgen, wobei die erworbene Mobilfunkleistung vor der abgeschlossenen Verifikation ausschließlich die zur Registrierung und Prüfung des Identitätsdokuments erforderliche Daten- und Telekommunikationsverbindung ermöglichen darf.
Diese Daten- und Telekommunikationsverbindung hat hierbei für alle Beteiligten kostenfrei zu sein (vgl. hierzu die vorstehenden Ausführungen unter Ziffer 3).

Bewertung durch die BNetzA:

Ein Verfahren, bei dem lediglich ein Foto des Identitätsdokuments zusammen mit einem Foto der Person des SIM-Karten-Erwerbers an den Diensteanbieter übermittelt wird, genügt den Anforderungen an eine Vorlage im Sinne des § 111 TKG nach Ansicht der Bundesnetzagentur nicht. Ebenso genügt es nicht, eine vorab durch den zukünftigen Anschlussinhaber aufgezeichnete Videosequenz zusammen mit einem Foto des Identitätsdokuments an den Diensteanbieter zu übermitteln.

Mit dem Erfordernis einer Vorlage in § 111 TKG soll der Diensteanbieter in die Lage versetzt werden, die erhobenen Daten vor der Freischaltung zu überprüfen. Dabei dient die Vorlage, im Gegensatz zum bloßen Vorzeigen, dazu, das Dokument nicht nur optisch zur Kenntnis nehmen zu können, sondern durch optische oder auch haptische Wahrnehmung tatsächlich zu überprüfen, inhaltlich ausreichend zur Kenntnis nehmen und es in der Regel selbstbestimmt so lange betrachten und ggf. prüfen zu können, wie dies erforderlich ist, um sich von der Echtheit zu überzeugen. Diese eingehende Prüfmöglichkeit ist mit Ausnahme der eID-Funktion in allen Verfahren, die diese Verfügung festlegt, gewährleistet.

Diese Möglichkeiten bestehen bei einem reinen Foto-Ident-Verfahren bzw. einem zeitversetzen Verfahren nicht. Das Identitätsdokument wird in einer starren Abbildung wiedergegeben, ohne dass der Prüfende/Erhebende z.B. eine schlechte Bildqualität rügen und auf eine bessere Sicht und Erkennbarkeit bestimmter optischer Sicherheitsmerkmale hinwirken kann. Eine eingehende Echtheitsprüfung durch Neigen, Drehen, Hin- und Her-Bewegen und weitere Veränderungen von Position oder Umgebung ist nicht möglich. Diese ausführliche und dem Einzelfall anpassbare Prüfmöglichkeit ist nach Ansicht der Bundesnetzagentur jedoch Grundlage dafür, dass das Video-Ident-Verfahren überhaupt als gleichermaßen geeignet akzeptiert werden kann. Ein Verfahren, das ausschließlich starre Abbildungen oder rein durch den Erwerber gesteuerte Aufnahmen beinhaltet, kann somit mangels ausreichender Möglichkeit einer Echtheits- sowie Identitätsprüfung nicht als gleich geeignet bewertet werden.

Aufgrund dieser Mängel reicht es nicht aus, dass ein Foto-Identverfahren im Vergleich zu den anderen aufgeführten Verfahren eher kostengünstig einzuführen und umzusetzen wäre und voraussichtlich sehr marktgängig sein dürfte.

Das Foto-Ident-Verfahren wird nicht in die Verfügung aufgenommen.

3. Rückgriff auf bereits erfolgte Verifizierungen anhand eines Identitätsdokuments

Von Seiten der Diensteanbieter wird angeregt, auch „mittelbare“ Verfahren ausreichen zu lassen, die auf eine bereits erfolgte Verifizierung zurückgreifen. So könne eine einmal erfolgte Verifikation bei einem entsprechenden Anbieter im Bedarfsfalle herangezogen werden. Diese Wiederverwendung einer einmal erfolgten Verifikation bzw. einer Datenverifikation „auf Vorrat“ könne gewährleisten, dass die Prüfung des initialen Vorgangs erhalten bliebe und somit auch das ursprüngliche Sicherheitsniveau erhalten bliebe.

Bewertung durch die Bundesnetzagentur:

Nach Auffassung der BNetzA besteht kein Zwang, für jeden Vertrag erneut eine eigene Datenverifikation durchzuführen. Dies widerspräche dem Gebot der Datensparsamkeit. Dies gilt insbesondere für Erwerber, die bereits Inhaber von Anschlüssen des jeweiligen Diensteanbieters sind und deren Daten bei einer vorangegangenen Erhebung aufgrund einer in § 111 Absatz 1 Satz 3 TKG vorgesehenen Vorlage oder eines Verfahrens im Sinne dieser Verfügung geprüft wurden und sich nicht geändert haben.

Darüber hinaus sind auch Verfahren von Drittanbietern als gleich geeignet anzusehen, die auf eine bereits erfolgte Prüfung der Anschlussinhaberdaten anhand von Identitätsdokumenten im Sinne des § 111 Absatz 1 TKG zurückgreifen und eigens zu dem Zweck der Abfrage der so geprüften Identitätsdaten verwendet und beauftragt werden. Die Akzeptanz derartiger „Vorrats-Verfahren“ setzt jedoch voraus, dass bei der ursprünglichen Erhebung und Prüfung der Daten zwingend Dokumente im Sinne des § 111 Absatz 1 TKG vorgelegt wurden oder dass die Richtigkeit der Angaben im Wege eines in dieser Verfügung festgelegten Verfahrens geprüft wurde und die Person des Erhebenden und Prüfenden auf geeignete Weise dokumentiert wird. Für den konkreten Abruf der so geprüften Daten ist eine Dokumentation jedoch entbehrlich.

Dieses Vorgehen würde den Schritten der Verfahrensvariante 2 entsprechend, die der beauftragte Dritte anstelle des Diensteanbieters durchführt. Dass dieser Prüfabschnitt eventuell mit größerer zeitlicher Diskrepanz als in Variante 2. zugrunde gelegt durchgeführt wurde, hat keine ersichtlichen Auswirkungen auf die Qualität der so geprüften Daten sowie der Prüfung an sich.

Dabei wäre, wie in allen Verfahren vorausgesetzt, eine Übermittlung einer Kopie oder eines Scans oder entsprechender Abbildungen erforderlich, damit der Diensteanbieter seiner Prüfpflicht nachkommen kann.

Zudem muss der Abruf der so geprüften Daten durch den Diensteanbieter bzw. die Anweisung des Sim-Karten-Erwerbers/Inhabers des Identitätsdokuments, die so geprüften Daten samt Kopie, Scan o.ä. an den Diensteanbieter zu übermitteln zweifelsfrei von dem Inhaber der so geprüften Daten vor Übermittlung entweder aktiv bestätigt bzw. selbst initiiert werden. Dies ist auf geeignete Weise sicherzustellen, etwa durch eine Registrierungsnummer und PIN, die der Drittanbieter an den Inhaber des so geprüften Identitätsdokuments zu dessen ausschließlicher Verfügung herausgegeben hat.

Dementsprechend wird folgendes Verfahren als Verfahren 4. ergänzt:

Prüfung der erhobenen Anschlussinhaberdaten durch den Diensteanbieter mittels Abgleichs mit Daten, die bei einem eigens mit einer Identitätsprüfung beauftragten Dritten zum Zwecke des Abrufes vorgehalten werden und die ihrerseits anhand der Vorlage eines Identitätsdokuments im Sinne des § 111

Absatz 1 Satz 3 TKG oder eines gleich geeigneten Prüfverfahrens geprüft wurden (Vorabverifikation).

Für Verfahren dieser Art gelten folgende Vorgaben:

(1) Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass der ausgewählte Dritte die Gewähr dafür bietet, dass die Anforderungen aus dem jeweils angewandten Verfahren aus dieser Verfügung, insbesondere hinsichtlich der Datenerhebung, Identitätsprüfung, Prüfung der Echtheit des Identitätsdokuments, hinsichtlich der Fertigung der Kopien u.ä. sowie deren Übermittlung an ihn eingehalten werden. Dies hat er zu dokumentieren.
(2) Der Diensteanbieter hat sich zu vergewissern, dass der Abruf der vorgehaltenen Daten bei dem Dritten nur in dem Umfang erfolgt, wie er sich in Ansehung der zu erhebenden Anschlussinhaberdaten nach § 111 Absatz 1 TKG aus dem ursprünglich vorgelegten Identitätsdokument ergibt.
(3) Der Diensteanbieter hat sich zu vergewissern, dass die Übermittlung der vorgehaltenen Daten durch den Dritten an ihn nur erfolgt, soweit der Inhaber der Daten nach einem vorgesehenen Verfahren verbunden mit einer Authentifizierung der Person des Dateninhabers (etwa durch Eingabe eines PIN) zugestimmt hat. Eine Initiierung der Übermittlung zwischen dem Dritten und dem Diensteanbieter durch den Inhaber der Daten unmittelbar kann ebenso möglich sein.
(4) Der Diensteanbieter hat dafür zu sorgen, dass der Dritte jeweils eine opto-elektronische Kopie, Scan oder entsprechende Abbildung zum Zwecke der Prüfung unter Beachtung datenschutzrechtlicher und personalausweisrechtlicher Vorgaben an ihn übermittelt. Für den Diensteanbieter angefertigte opto-elektronische Kopien, Scans oder entsprechende Abbildungen sind als solche zu kennzeichnen und dürfen nicht beim Dritten verbleiben. Für die beim Diensteanbieter vorgelegten Kopien gilt § 95 Absatz 4 TKG.
(5) Im Falle der Übermittlung einer opto-elektronischen Kopie, Scan oder entsprechende Abbildung durch den zukünftigen Anschlussinhaber selbst hat der Diensteanbieter diesen auf die datenschutzrechtlichen und personalausweisrechtlichen Beschränkungen für Kopien, Scans oder entsprechende Abbildungen hinzuweisen. Für die beim Diensteanbieter vorgelegten Kopien gilt § 95 Absatz 4 TKG.
(6) Bei der Erhebung und Übermittlung der Daten an den Diensteanbieter zur Prüfung und Speicherung in der Kundendatei sind die datenschutzrechtlichen Vorgaben und Beschränkungen nach dem PAuswG zu beachten. Geeignete Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität der Daten sind hierbei einzusetzen.

4. Zusendung einer Ausweiskopie (übergangsweise)

Von Seiten eines Diensteanbieterverbands wurde für den Cash- and Carry - Vertrieb vorgeschlagen, übergangsweise auch die Zusendung von Ausweiskopien, - Scans oder – Bildern durch den Kunden selbst an den Diensteanbieter zu akzeptieren.

Bewertung durch die BNetzA:

Dieses Vorgehen entspräche nach Ansicht der Bundesnetzagentur nicht einem gegenüber der Vorlage gleichermaßen geeigneten Verfahren. Eine Vorlage oder ein gleich geeignetes Verfahren beinhaltet nicht nur eine irgendwie gestaltete Abbildung eines Identitätsdokuments, sondern die Möglichkeit, die Echtheit dieses Dokuments zu prüfen und einen Abgleich zwischen der Person des Erwerbers und der des im Identitätsdokument ausgewiesenen Person vorzunehmen. Somit würde dieses Verfahren ganz offensichtlich nicht das mit der Gesetzesänderung bezweckte Niveau an Gewissheit hins. der Identität des Anschlussinhabers erreichen.

Auch würde die Identifikation anhand des Identifikationsdokuments nicht unmittelbar erfolgen (vgl. amtl. Begründung zum Gesetzesentwurf BT Drucks. 18/8702, S. 23). Maßgeblich dabei ist, dass die zu identifizierende Person tatsächlich und im Rahmen der Vorlage bzw. im Rahmen des in dieser Verfügung festgelegten Prüfverfahrens mit der im Identitätsdokument ausgewiesenen Person abgeglichen werden kann. Dies ist bei bloßen Einreichen einer Kopie ohne vorherigem Abgleich mit der Person des Einreichenden nicht ausreichend.

D. Stellungnahmen zum Verfahren und zum weiteren Vorgehen

1. Umsetzungsfrist

Von Seiten einiger Diensteanbieter wurde kritisiert, dass die gesetzliche Umsetzungsfrist aufgrund der mit der Verfahrensumstellung einhergehenden technischen, prozessualen, vertragsrechtliche und personellen Implikationen zu kurz bemessen sei. Eine Verlängerung sei daher angezeigt.

Bewertung durch die BNetzA:

Die gesetzliche Frist kann durch eine behördliche Verfügung nicht abgeändert werden.

2. Außerachtlassen von Postpaid-Verträgen

Von Seiten einer Sicherheitsbehörde auf Landesebene wird kritisiert, dass die gesetzliche Regelung zu kurz greife. Es wären ebenso auch die Vertragskunden (Postpaid) zu verpflichten. Zudem sollten auch andere Erbringer von TK-Diensten (elektronische Post-Geschäftsmodelle) eine Erhebungspflicht erfüllen müssen. Diese Dienste sind derzeit anonym nutzbar.

Bewertung durch die BNetzA:
Eine Verfügungsbefugnis, die gesetzliche Regelung auf weitere Vertragsformen auszudehnen, existiert für die Bundesnetzagentur nicht.

3. Zukünftige Fortentwicklung

Ein Diensteanbieter schlägt vor, in der Verfügung Verfahren mitzuteilen, wie zukünftige Fortentwicklungen mitgeteilt und diskutiert werden könnten. Dies sei aufgrund von möglichen technischen Neuerungen geboten.

Bewertung durch die BNetzA:
Eine Prüfung und Überarbeitung der Verfügung wird erfolgen, wenn konkrete technische, wirtschaftliche, faktische und/oder rechtliche Entwicklungen eine Neubewertung erforderlich machen und den Änderungen nicht durch eine sinngemäße Auslegung und Anwendung der Verfügung entsprochen werden kann.

(Stand: Dezember 2016)