Neufassung der Verfügung der Bundesnetzagentur gemäß § 111 Absatz 1 Satz 4 Telekommunikationsgesetz (Stand: 16.12.2020):

In § 111 Absatz 1 Satz 4 des Telekommunikationsgesetzes i.d.F. vom 29.07.2016 (BGBl. I, S. 1822) ist der Bundesnetzagentur die Aufgabe zugewiesen, festzulegen, welche anderen Verfahren als die im Gesetz vorgesehene unmittelbare Vorlage bestimmter Identifikationsdokumente zur Überprüfung der Daten eines Kunden beim Erwerb einer Prepaid-Karte gleichermaßen geeignet sind.

Hiermit wird unter Beachtung der Rechtsauffassung des Verwaltungsgerichts Köln aufgrund der Urteile vom 13.11.2020 - Az. 9 K 573/18, 9 K 574/18 und 9 K 1378/18 - festgelegt, dass folgende Verfahren zur Überprüfung der Kundendaten im Sinne des § 111 Absatz 1 Satz 4 TKG gleich geeignet sind:

1. **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:

   (1) Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass der ausgewählte Dritte die Gewähr dafür bietet, dass die Anweisungen hinsichtlich der Datenerhebung, Identitätsprüfung und Prüfung der Echtheit des Identitätsdokuments eingehalten werden. Dies hat er zu dokumentieren.

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

   (3) 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) 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.

2. **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 gleichzeitigen Abgleich mit der vorzeigenden Person durch den Diensteanbieter oder einen von diesem beauftragten Dritten

Für Verfahren dieser Art gelten folgende Vorgaben:

(1) Der Diensteanbieter hat sich vor der Beauftragung zu vergewissern, dass ausgewählte Dritte die Gewähr dafür bieten, dass die Anforderungen hinsichtlich der Datenerhebung, Identitätsprüfung und Prüfung der Echtheit des Identitätsdokuments eingehalten werden. Dies hat er zu dokumentieren. Die Beauftragung darf nur erfolgen, wenn der Dritte verpflichtend eine jährliche Schulung auf Grundlage neuester Erkenntnisse einer mit Identitätsprüfungen oder der Prüfung von Ausweisdokumenten vertrauten öffentlichen oder allgemein anerkannten Stelle für seine Mitarbeiter durchführt oder durchführen lässt (z.B. durch das Bundeskriminalamt). 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 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 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) 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.

(5) 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.

(6) 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 für die Videoübertragung zur Verfügung stellen.

(0) Bei Verwendung einer 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.

(1) In Bezug auf die Schulung der Mitarbeiter wird mindestens die Kenntnis der mittels Videoidentifizierung prüfbaren Merkmale einschließlich der anzuwendenden Prüfverfahren derjenigen Dokumente vorausgesetzt, die im Rahmen des Videoidentifizierungsverfahrens akzeptiert werden, samt gängiger Fälschungsmöglichkeiten dieser Dokumente, sowie die Kenntnis der maßgeblichen telekommunikations- und datenschutzrechtlichen Vorschriften und der in dieser Verfügung gestellten Anforderungen. Zu den prüfbaren Merkmalen der zugelassenen Identitätsdokumente und den entsprechenden Schulungsmaßnahmen muss eine geeignete Dokumentation vorliegen.
Die vorgenannten Inhalte müssen den Mitarbeitern vor Aufnahme ihrer Identifizierungstätigkeit angemessen vermittelt und nachfolgend in regelmäßigen Abständen (mindestens einmal jährlich) sowie bei Bedarf aktualisiert werden. Ein Bedarf kann z.B. in einer Änderung der gesetzlichen und/oder aufsichtsrechtlichen bzw. datenschutzrechtlichen Anforderungen oder im Falle eines Auftretens einer signifikanten Zahl von Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstiger Fehler im Verfahrensablauf begründet sein.

(2) Die Mitarbeiter müssen sich während der Identifizierung in abgetrennten und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.

(3) Bei der Zuteilung der Identifizierungsvorgänge an die Mitarbeiter müssen Mechanismen eingesetzt werden, die einer vorhersehbaren Zuteilung von Fällen und damit der dadurch bestehenden Möglichkeit einer Manipulation entgegenwirken.

Die Durchführung der Videoidentifizierung muss in Echtzeit und ohne Unterbrechung erfolgen.

Die audiovisuelle Kommunikation zwischen dem Mitarbeiter und der zu identifizierenden Person ist in Bezug auf Integrität und Vertraulichkeit ausreichend abzusichern; aus diesem Grund sind nur Ende-zu-Ende verschlüsselte Videochats zulässig. Es sind hierbei die Empfehlungen der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR-02102 einzuhalten.

Außerdem muss die Bild- und Tonqualität der Kommunikation in einem ausreichenden Maße gegeben sein, um eine zweifelsfreie Identifizierung anhand aller in dieser Verfügung geforderten Prüfungen uneingeschränkt zu ermöglichen. Hierzu zählen insbesondere die Prüfungen der als im Weißlicht visuell prüfbar eingestuften Sicherheitsmerkmale sowie die Prüfung auf Beschädigung und Manipulation des Dokuments. Zur Bewertung der Qualität der Bildübertragung sind geeignete, aussagekräftige Bildelemente zu definieren, bspw. Guillochenstrukturen und Mikroschriften.

(4) Nur Identitätsdokumente, die über ausreichend fälschungssichere, im Weißlicht visuell und bei Bildübertragung mittels verfügbarer Technik ausreichend deutlich erkennbare und damit prüfbare Sicherheitsmerkmale [siehe Auflistung unter (12)] sowie über einen maschinenlesbaren Bereich verfügen, können für die telekommunikationsrechtliche Identitätsüberprüfung im Rahmen eines Videoidentifizierungsverfahrens herangezogen werden.

(5) Um sich über die Identität der zu identifizierenden Person mittels eines zulässigen Identitätsdokumentes zu vergewissern, hat der Mitarbeiter zunächst sicherzustellen, dass das zur Identitätsüberprüfung konkret verwendete Dokument hinsichtlich der darauf enthaltenen, im Weißlicht visuell zu erkennenden optischen Sicherheitsmerkmale mit den bei dieser Art von Dokumenten vorhandenen Merkmalen übereinstimmt.

Zu den optischen Sicherheitsmerkmalen zählen jeweils unter anderem (je nach Dokument):

beugungsoptisch wirksame Merkmale:

- Hologramme
- Identigram
- Kinematische Strukturen

Personalisierungstechnik:

- Laserkippbilder
- Ausfüllschrift

Material:

- Fenster (z.B. personalisiert)
- Sicherheitsfaden (personalisiert)
- Optisch variable Farbe

Sicherheitsdruck:

- Mikroschrift
- Guillochenstruktur

Von einer Übereinstimmung ist auszugehen, wenn die Prüfkriterien von mindestens drei für die Identifizierung zufällig ausgewählten Sicherheitsmerkmalen, aus verschiedenen Kategorien der vorstehenden Liste, die das vorgelegte Identitätsdokument enthält, erfüllt werden.

Der Mitarbeiter hat zudem sicherzustellen, dass das zur Identitätsüberprüfung konkret verwendete Dokument hinsichtlich der sonstigen darauf enthaltenen, im Weißlicht visuell zu erkennenden und einer Kontrolle zugänglichen formalen Merkmale (u.a. Layout, Zeichenzahl, -größe, -abstand und Typographie) mit den bei dieser Art von Dokumenten vorhandenen Merkmalen übereinstimmt.

Es ist durch geeignete IT-Unterstützung sicherzustellen, dass im Rahmen der Videoidentifizierung im Weißlicht visuell zu erkennende optische Sicherheitsmerkmale in Form und Inhalt zu den in dem Identitätsdokument enthaltenen individuellen Merkmalen passen (z.B. Abgleich der auf dem Dokument vorhandenen Primär-und Sekundärlichtbilder wie Identigram, Laserkippbild etc.) bzw. mit Referenzen aus einer Ausweisdatenbank übereinstimmen. Alternativ zu einer IT-Unterstützung muss ein entsprechender Abgleich durch vom Mitarbeiter auszuwählende Standbilder ermöglicht und als Bestandteil des Identifizierungsprozesses zwingend durchgeführt werden.
Der Mitarbeiter muss außerdem stets prüfen, ob das verwendete Identitätsdokument unbeschädigt und nicht manipuliert ist und insbesondere kein aufgeklebtes Bild enthält.

Im Rahmen der visuellen Prüfung muss die zu identifizierende Person das verwendete Identitätsdokument vor der Kamera nach Anweisung des Mitarbeiters horizontal bzw. vertikal kippen und zudem auf Aufforderung des Mitarbeiters bestimmte weitere Bewegungen durchführen. Das Interview mit der zu identifizierenden Person muss mindestens im Hinblick auf dessen Ablauf

variationsreich in Bezug auf Reihenfolge und/oder Art der vom Mitarbeiter gestellten Fragen gestaltet sein.

Einer Substitution/Manipulation von Teilen bzw. Elementen des Identitätsdokumentes ist durch geeignete Maßnahmen entgegenzuwirken. Dazu ist die zu identifizierende Person aufzufordern, an geeigneter (variabler, systemseitig zufällig bestimmter) Stelle z.B. einen Finger vor sicherheitsrelevante Teile des Identitätsdokumentes zu halten und etwa eine Hand vor ihrem Gesicht zu bewegen.

Mittels hierbei gefertigter ausschnittvergrößerter Standbilder ist vom Mitarbeiter zu verifizieren, dass das Identitätsdokument samt im Weißlicht visuell zu erkennender Sicherheitsmerkmale an entsprechender Stelle vollständig überdeckt wird und die Übergänge keinerlei Artefakte erkennen lassen, die auf eine entsprechende Manipulation hindeuten.

Im Rahmen des Videoidentifizierungsverfahrens ist eine Gültigkeits- und Plausibilitätsprüfung der auf dem Identitätsdokument enthaltenen Daten und Angaben vorzunehmen. Dies beinhaltet u.a. die Überprüfung, ob Ausstellungsdatum und Gültigkeitsdatum des Identitätsdokumentes zueinander passen. Das Ausstellungsdatum darf insbesondere nicht in der Zukunft liegen. Ferner darf die Gültigkeitsdauer des vorgelegten Identitätsdokumentes nicht gegen die für Identitätsdokumente dieser Art geltende Norm verstoßen.

Zwingender Bestandteil der Überprüfung ist zudem eine automatisierte Berechnung der in der maschinenlesbaren Zone enthaltenen Prüfziffern sowie ein Kreuzvergleich der in ihr enthaltenen Angaben mit den Angaben im Sichtfeld des Identitätsdokumentes. Außerdem ist die Korrektheit von Ziffernorthographie, Behördenkennziffer und der verwendeten Schriftarten zu überprüfen.

Die zu identifizierende Person hat während der Videoübertragung ferner die vollständige Seriennummer ihres Identitätsdokumentes mitzuteilen.

(13) Der Mitarbeiter muss sich davon überzeugen, dass das Lichtbild und die Personenbeschreibung auf dem verwendeten Identitätsdokument zu der zu identifizierenden Person passen. Lichtbild, Ausstellungsdatum und Geburtsdatum müssen ebenfalls zueinander kohärent sein.

Der Mitarbeiter muss sich durch psychologische Fragestellungen und Beobachtungen während der Durchführung des Identifizierungsvorgangs von der Plausibilität der Angaben im Identitätsdokument, der Angaben der zu identifizierenden Person im Gespräch sowie der vorgegebenen Absicht der zu identifizierenden Person überzeugen. Dabei können z.B. Fragen nach dem Alter der Person für eine Validierung im Hinblick auf das Ausweisbild sowie die Geburtsangaben im Identitätsdokument erfolgen.

Der Anlass für die Identifikation ist durch die zu identifizierende Person zu bestätigen, auch damit für diese klar ersichtlich ist, wofür sie sich identifiziert. Die Mitarbeiter sind dahingehend zu schulen, dass sie zweifelsfrei feststellen, dass die zu identifizierende Person nach eigenem Willen das jeweilige Produkt beim entsprechenden Anbieter erwirbt (Gefährdung durch Phishing, Social Engineering, Verhalten unter Druck durch zweite Person etc.).

(14) Ist die visuelle Überprüfung – etwa aufgrund von schlechten Lichtverhältnissen oder einer schlechten Bildqualität/-übertragung – und/oder eine sprachliche Kommunikation mit der zu identifizierenden Person nicht möglich, ist der Identifizierungsprozess abzubrechen.

Gleiches gilt bei sonstigen vorliegenden Unstimmigkeiten oder Unsicherheiten. In diesen Fällen kann die Identifizierung mittels eines anderen nach dem Telekommunikationsgesetz oder dieser Verfügung zulässigen Verfahrens vorgenommen werden.

(15) Die vorstehenden aufsichtsrechtlichen Anforderungen zum Videoidentifizierungsverfahren gelten unbeschadet der parallel zu beachtenden datenschutzrechtlichen Anforderungen.

3. 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 und Prüfung der Echtheit des Identitätsdokuments 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 einer PIN) zugestimmt hat. Eine Initiierung der Übermittlung zwischen dem Dritten und dem Diensteanbieter durch den Inhaber der Daten unmittelbar kann ebenso möglich sein.

(4) Im Falle der Übermittlung einer opto-elektronischen Kopie, Scan oder entsprechenden 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.

4. **Die Erhebung und Prüfung der Anschlussinhaberdaten kann auch im Wege des elektronischen Identitätsnachweises nach § 18 PAuswG und nach § 78 Aufenthaltsgesetz erfolgen. Auf § 111 Absatz 1 Satz 6 TKG wird hingewiesen.**