Anhörungsverfahren zur Anpassung der Verfügung gem. § 172 Abs. 2 S. 3 TKG

§ 172 Absatz 2 Satz 3 des Telekommunikationsgesetzes (TKG) überträgt der Bundesnetzagentur die Aufgabe, festzulegen, welche alternativen Verfahren zur Überprüfung der Daten von Anschlussinhabern bei im Voraus bezahlten Mobilfunkdiensten geeignet sind. Diese Verfahren sollen eine Alternative zur unmittelbaren Vorlage der in § 172 Absatz 2 Satz 1 TKG genannten Identitätsdokumente darstellen. Die betroffenen Kreise sind hierzu anzuhören.

Mit dem vorliegenden Entwurf wird die bestehende Festlegung (Verfügung Nr. 94/2021) umfassend überarbeitet. Ziel der Neufassung ist es insbesondere, das Sicherheitsniveau der Identifizierungsverfahren zu erhöhen, technischen Entwicklungen Rechnung zu tragen und die Anforderungen stärker an die europäischen Vorgaben zur Identitätsüberprüfung nach der eIDAS-Verordnung (EU) Nr. 910/2014 und den hierzu erlassenen Durchführungsrechtsakten anzugleichen.

Dies hat zur Folge, dass drei bestehende Verfahren grundlegend überarbeitet werden und ein bisher erlaubtes Verfahren nicht mehr zugelassen wird. Es wird zudem die Möglichkeit eröffnet, bereits im Rahmen einer eIDAS-Konformitätsbewertung geprüfte Anforderungen an die Zugehörigkeitsprüfung (des Identitätsdokuments zu der zu identifizierenden Person) anrechnen zu lassen.

Das Verfahren der anlassbezogenen Vor-Ort-Identifikation durch Dritte wird vor allem durch die Vorgabe des Einsatzes multispektraler Dokumentenprüfgeräte in seiner Sicherheit gestärkt.

Im Bereich der Video-Identifikation wurden umfangreiche Anpassungen zur Stärkung der Sicherheit sowie der Angleichung an die Vorschriften der eIDAS-Verordnung vorgenommen: Da die eIDAS-Durchführungsverordnung (EU) 2025/1566 aufgrund ihres Verweises auf den Standard ETSI TS 119 461 keinen Anwendungsfall für eine vollautomatisierte Prüfung eines **physischen** Identitätsdokuments vorsieht, wird das entsprechende automatisierte Video-Identifikationsverfahren aus der Verfügung herausgenommen. Der vorgenannte ETSI-Standard sieht für physische Identitätsdokumente ausschließlich hybride Verfahren vor, weshalb das bisherige anlassbezogene klassische Video-Identifikationsverfahren durch die Einführung des verpflichtenden Einsatzes technischer Hilfsmittel zu einem solchen hybriden Verfahren weiterentwickelt wurde. Auch verschärfte Anforderungen zur Prüfung der Sicherheitsmerkmale von Identitätsdokumenten sowie zu den technischen Rahmenbedingungen - bspw. zur Mindestauflösung der übertragenen Bilddaten - erhöhen die Sicherheit des Verfahrens.

Grundsätzlich werden Video-Identifizierungsverfahren von der Bundesnetzagentur als Brückentechnologie und Behelfslösung verstanden, da hierbei eine digitale Prüfung manueller Sicherheitsmerkmale erfolgt. Im Rahmen der angestrebten

Neufassung der Identifizierungsverfügung Prepaid-Mobilfunk soll ein solches Verfahren weiterhin als geeignetes Verfahren festgelegt werden, wenngleich perspektivisch der digitalen Prüfung digitaler Identitätsdokumente über kryptographischen Verfahren der Vorzug zu geben sein wird. Dies trägt insbesondere auch den aktuellen gesetzgeberischen Bestrebungen Rechnung, über die derzeit laufende Novellierung des TKG den elektronischen Identitätsnachweis (eID), weitere eIDAS- Identifizierungsmittel mit Sicherheitsniveau hoch, sowie die europäische Brieftasche für die Digitale Identität (EUDI-Wallet) als gesetzliche Identifizierungsmittel gem. § 172 Abs. 2 S. 1 TKG vorzusehen.

Eine vollautomatisierte Prüfung von Identitätsdokumenten wird weiterhin möglich sein, jedoch ausschließlich unter Einsatz eines digitalen Identifizierungsmittels wie der eID oder der EUDI-Wallet – diese Verfahren sind jedoch durch die künftige Aufnahme in Nr. 8-10 des Entwurfs zur Neufassung von § 172 Abs. 2 S. 1 TKG bereits als gesetzliche Identifizierungsmittel vorgesehen und somit nicht in der Identifizierungsverfügung als „andere geeignete Verfahren“ festzulegen.

Das Verfahren des Abgleichs bei anlassunabhängiger Vorabidentifikation wurde im Zuge der ganzheitlichen Überarbeitung und zur Stärkung der Sicherheit der Verfahren im Schwerpunkt dahingehend angepasst, dass das einem solchen Abgleich zugrundeliegende Identifikationsverfahren den Anforderungen der Identifizierungsverfügung Prepaid-Mobilfunk entsprechen muss.

Über alle Verfahren hinweg wurden die Erfordernisse zur Dokumentation der Identifikation überarbeitet sowie damit einhergehende Speicher- und Löschfristen aufgenommen.

Das vorgesehene Inkrafttreten zum 01.08.2027 trägt einerseits der Tatsache Rechnung, dass vorhandenen Verfahren ggfls. eine entsprechende Frist zur Anpassung eingeräumt werden muss, knüpft jedoch auch an das Inkrafttreten der materiellen Vorschriften der EU-Anti-Geldwäscheverordnung zum 10.07.2027 sowie die Tatsache, dass das Gesetzgebungsverfahren zur Novellierung des TKG noch nicht abgeschlossen ist. (Hinweis: Der Verfügungstext basiert auf dem aktuell gültigen Gesetzeswortlaut des TKG – redaktionelle Änderungen infolge der Novellierung des TKG sind entsprechend vorgesehen.) Insgesamt trägt die Neufassung dazu bei, die Sicherheit, Zuverlässigkeit und Nachvollziehbarkeit der Identitätsüberprüfung bei Prepaid-Mobilfunkdiensten zu stärken und die bestehenden Anforderungen an technische und regulatorische Entwicklungen anzupassen.

Es besteht für die betroffenen Kreise die Möglichkeit, **bis zum 07. Dezember 2026** eine schriftliche Stellungnahme abzugeben. Die Stellungnahmen sollten als editierbare Datei per E-Mail an IdentKonform@bnetza.de übersandt werden. Die Bundesnetzagentur behält sich vor, die Stellungnahmen zu veröffentlichen (in einer zusammengefassten Form oder vollständig) Ausführungen, bei denen es sich um Betriebs- und Geschäftsgeheimnisse handelt, sind entsprechend zu kennzeichnen. Gegebenenfalls wird eine Fassung der Stellungnahme veröffentlicht, bei der die als

Betriebs- und Geschäftsgeheimnisse gekennzeichneten Ausführungen nicht enthalten sind.

Ein ergänzender Online-Termin ist nach Sichtung der eingegangenen Stellungnahmen vorgesehen und wird rechtzeitig bekanntgegeben.

Bundesnetzagentur

Referat 216

Canisiusstraße 21

55122 Mainz

E-Mail: IdentKonform@bnetza.de

Nach Fristablauf eingehende Stellungnahmen können nicht berücksichtigt werden.

Verfügung zur Festlegung von Verfahren zur Überprüfung von Anschlussinhaberdaten (Identifizierungsverfahren) gemäß § 172 Absatz 2 Satz 3 Telekommunikationsgesetz

Katalog der Anforderungen für geeignete Verfahren nach § 172 Absatz 2 Satz 3 TKG

I. Allgemeine Anforderungen

1. Jedes Verfahren im Sinne dieser Verfügung muss zum Zweck der Identifikation ein Dokument gemäß § 172 Absatz 2 Satz 1 Nr. 1-7 TKG nutzen. Die Nutzung anderer Identitätsdokumente ist nicht zulässig. Für einzelne Verfahren können Einschränkungen vorgesehen sein.
2. Im Rahmen eines Verfahrens im Sinne dieser Verfügung sind die in § 172 TKG vorgeschriebenen Daten zu erheben und beim Verpflichteten nach § 172 Abs. 2 TKG oder seinem Beauftragten zu speichern.
3. Es ist durch geeignete organisatorische und/oder technische Maßnahmen sicherzustellen, dass Informationen nach § 172 Absatz 2 Satz 6 TKG (Art, Nummer und ausstellende Stelle des Identitätsdokuments) beim Verpflichteten nach § 172 Abs. 2 TKG oder seinem Beauftragten gespeichert werden können. Hierbei ist Folgendes zu beachten:
   In Fällen, in denen die Identitätsdokumente die ausstellende Stelle nicht erkennen lassen, soll ersatzweise die Angabe zum ausstellenden Staat erhoben und gespeichert werden.
4. Anbieter von Verfahren nach dieser Verfügung haben ein Qualitätssicherungssystem einzuführen bzw. aufrecht zu erhalten, welches insbesondere ein Vier-Augen-Prinzip bei internen Kontrollen von Identifizierungsvorgängen beinhaltet.

II. Spezifische verfahrensbezogene Anforderungen

1. Anlassbezogene Vor-Ort-Identifikation durch Dritte

1.1. Anforderungen an das mit der Identifizierung beauftragte Personal

1.1.1. Das mit der Identifikation beauftragte Personal ist vor der erstmaligen eigenständigen Durchführung eines Identifizierungsvorgangs angemessen zu schulen. Die Schulung muss mindestens folgende Inhalte umfassen:

1.1.1.1. die Anforderungen und den Ablauf des Identifizierungsverfahrens nach dieser Verfügung, einschließlich der Erhebung und des Abgleichs der Identifizierungsdaten,

1.1.1.2. den Abgleich des Lichtbilds im Identitätsdokument mit der zu identifizierenden Person (Zugehörigkeitsprüfung), einschließlich

ENTWURF

der für einen zuverlässigen Personenabgleich wesentlichen Merkmale und Einflussfaktoren,

1.1.1.3. die ordnungsgemäße Bedienung des eingesetzten Dokumentenprüfgeräts sowie den Umgang mit dessen Prüfergebnissen, insbesondere bei negativen, uneindeutigen oder technisch nicht verwertbaren Prüfergebnissen

1.1.1.4. Die Schulung kann durch den Verpflichteten nach § 172 TKG, den mit der Identifizierung beauftragten Dritten oder eine fachlich geeignete externe Stelle durchgeführt werden. Eine unternehmensinterne Schulung ist zulässig, sofern die vorgenannten Schulungsinhalte angemessen vermittelt werden.

1.1.2. Eine Nachschulung ist bei wesentlichen Änderungen des Identifizierungsverfahrens, der eingesetzten technischen Systeme oder der maßgeblichen rechtlichen oder sonstigen Anforderungen erforderlich, soweit diese Änderungen für die ordnungsgemäße Durchführung des Identifizierungsverfahrens von Bedeutung sind.

1.1.3. Zu den vorgenannten Schulungsinhalten sowie zur Durchführung der Schulungsmaßnahmen ist eine geeignete Dokumentation anzufertigen und vorzuhalten, die vertraulich zu behandeln ist.

1.2. Anforderungen an den Identifizierungsvorgang

1.2.1. Die Identifizierung im Sinne des in Ziffer A.II.1. festgelegten Verfahrens muss durch einen Dritten erfolgen. Als Dritter gilt nicht, wer als Vertriebspartner, Händler bzw. autorisierte Verkaufsstelle in den Prozess des Erwerbs der SIM-Karte des Anbieters eingebunden wurde.

1.2.2. Der Identifizierungsvorgang hat vor der Freischaltung in persönlicher und räumlich unmittelbarer Anwesenheit der zu identifizierenden Person stattzufinden, wobei diese ein Identitätsdokument im Sinne des § 172 Absatz 2 Satz 1 TKG vorzulegen hat. Das mit der Identifikation beauftragte und geschulte Personal hat das vorgelegte Identitätsdokument neben der Inaugenscheinnahme und haptischen Wahrnehmung zusätzlich mittels eines multispektralen Dokumentenprüfgeräts zu prüfen. Das Gerät muss eine multispektrale Prüfung mit mehr als zwei dokumentenrelevanten Wellenlängenbereichen ermöglichen. Das Identitätsdokument ist auf Echtheit und Unverfälschtheit zu überprüfen.

1.2.3. Die Daten der zu identifizierenden Person sind zu erheben und anhand des vorgelegten Identitätsdokuments zu überprüfen. Die maschinell ausgelesenen Daten sind in den Abgleich einzubeziehen. Ebenfalls zulässig ist das Vor-Ort-Auslesen zum Zwecke der medienbruchfreien Übernahme von Formulardaten unter Anwesenden soweit dies gesetzlich zugelassen ist, vgl. insb. § 18a Personalausweisgesetz und § 13 eID-Karte-Gesetz. Soweit die Daten

mittels des Dokumentenprüfgeräts erhoben werden, ist sicherzustellen, dass diese durch die die Identifizierung durchführende Person nicht verfälscht oder verändert werden können. Es ist sicherzustellen, dass die von den beauftragten Dritten eingesetzten Dokumentenprüfgeräte dem aktuellen technischen Standards für die optische Dokumentenprüfung entsprechen.

1.3. Zugehörigkeitsprüfung

Die Zugehörigkeit des verwendeten Ausweisdokuments zu der zu identifizierenden Person ist durch den Abgleich der zu identifizierenden Person mit dem Lichtbild des verwendeten Identitätsdokuments zu überprüfen.

1.4. Anforderungen an die Dokumentation

1.4.1. Die den Identifizierungsvorgang durchführende Person muss die wesentlichen Punkte des Identifizierungsvorgangs in geeigneter Weise dokumentieren, um eine spätere Nachvollziehbarkeit der Umstände der Identifikation gewährleisten zu können.

1.4.2. Zu den wesentlichen Punkten der Dokumentation gehören:

1.4.2.1. Wann wurde der Identifizierungsvorgang durchgeführt?

1.4.2.2. Wo wurde der Identifizierungsvorgang durchgeführt?

1.4.2.3. Wer ist die den Identifizierungsvorgang durchführende Person?

1.4.2.4. Anschlussinhaberdaten nach § 172 Abs.1 und 2 TKG

1.4.2.5. Welches Identitätsdokument wurde verwendet (vgl. Anforderung in Ziffer A.I.2.)?

1.4.2.6. Welche Art/welcher Typ Dokumentenprüfgerät wurde eingesetzt?

1.4.2.7. Das Ergebnisprotokoll der Prüfung des Dokumentenprüfgeräts.

1.4.2.8. Das Ergebnis der Zugehörigkeitsprüfung nach Ziffer 1.3

1.4.3. Die Dokumentation ist dem Verpflichteten nach § 172 TKG unverzüglich zu übermitteln.

1.4.4. Bei erfolgreicher Durchführung des Identifizierungsverfahrens ist die Dokumentation durch den Verpflichteten nach § 172 TKG für zwei Jahre ab der Durchführung des Identifizierungsvorgangs zu speichern und nach Ablauf zu löschen. Für den Fall, dass die Daten nach § 172 Abs. 1-3 TKG zu einem früheren Zeitpunkt gem. § 172 Abs. 6 TKG zu löschen sind, ist auch die Dokumentation entsprechend mit diesen zu löschen.

1.4.5. Bei abgebrochenen und/oder nicht erfolgreichen Identifizierungsvorgängen ist die Dokumentation durch den Verpflichteten nach § 172 TKG für sechs Monate ab dem Identifizierungsversuch zu speichern und nach Ablauf zu löschen.

2. Anlassbezogene Video-Identifikation

Die Fernidentifikation im Video-Identifikationsverfahren ist nur nach Maßgabe der Anwendungsfälle der jeweils in der Durchführungsverordnung (EU) 2025/1566 aufgeführten und angepassten Norm ETSI TS 119 461 und der folgenden Bestimmungen zulässig und wird durch eine entsprechend geschulte natürliche Person (Operator) durchgeführt.

2.1. Anforderungen an das mit der Identifikation beauftragte Personal

2.1.1. Das mit der Identifikation beauftragte Personal muss vor Aufnahme der Identifizierungstätigkeit mindestens die folgenden Schulungsinhalte angemessen vermittelt bekommen unter Hinweis auf deren Vertraulichkeit:

2.1.1.1. Kenntnis der mittels Videoidentifizierung prüfbaren Sicherheitsmerkmale nach Ziffer 2.2.3

2.1.1.2. Kenntnis der anzuwendenden Prüfverfahren nach aktuellem Stand des Informationssicherheitsmanagements für diejenigen Identitätsdokumente, die im Rahmen des Videoidentifizierungsverfahrens akzeptiert werden

2.1.1.3. Kenntnis über gängige Fälschungs- und Manipulationsmöglichkeiten von Identitätsdokumenten sowie über Maßnahmen zur Betrugsprävention und Betrugserkennung und aktuelle Angriffsszenarien

2.1.1.4. Kenntnis über auf Willensmängeln bei der zu identifizierenden Person sowie über die in solchen Fällen zu ergreifenden Maßnahmen, insbesondere bei Anhaltspunkten für Zwang, Täuschung oder menschliche Manipulationsmethoden

2.1.1.5. Kenntnis typischer Angriffe auf das Identifizierungsverfahren und deren Erkennungsmerkmale, insbesondere der in Ziffer 2.3.9 benannten Manipulationsszenarien

2.1.1.6. Kenntnis der maßgeblichen telekommunikations- und datenschutzrechtliche Vorschriften, sowie die gestellten Anforderungen dieser Verfügung

2.1.1.7. Kenntnis über die Durchführung der Zugehörigkeitsprüfung nach Punkt 2.4.

2.1.1.8. Kenntnis der und Unterweisung in den zur Verfügung stehenden technischen Hilfsmittel zur Durchführung des Identifizierungsvorgangs.

2.1.2. Die Schulung muss in regelmäßigen Abständen (mindestens einmal jährlich) sowie bei Bedarf aktualisiert werden. Ein Aktualisierungsbedarf zur Nachschulung kann z.B. in einer Änderung der gesetzlichen und / oder aufsichtsrechtlichen bzw. datenschutzrechtlichen Anforderungen, bei Anpassung der Identitätsdokumente mit Blick auf verwendete Sicherheitsmerkmale oder im Falle eines Auftretens einer signifikanten Zahl von

Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstiger Fehler im Verfahrensablauf sowie Änderungen und Aktualisierungen der zur Verfügung stehenden technischen Hilfsmittel begründet sein.

2.1.3. Die Beauftragung einer externen Stelle zur Durchführung der Schulungen ist zulässig. Beispielsweise können mit der Echtheitsprüfung von Ausweisdokumenten befasste Stellen beauftragt werden. Die beauftragte Stelle muss über nachgewiesene, aktuelle Fachkunde in den jeweils vermittelten Bereichen verfügen.

2.1.4. Zu den oben genannten Schulungsinhalten sowie zur Durchführung der Schulungsmaßnahmen ist eine geeignete Dokumentation anzufertigen und vorzuhalten, die vertraulich zu behandeln ist. Die Dokumentation muss insbesondere die in Ziffer 2.1.1 genannten Schulungsinhalte in einem ihrer Bedeutung für das Identifizierungsverfahren angemessenen Umfang sowie die Dauer der Schulung beinhalten.

2.2. Anforderungen an geeignete Identitätsdokumente

2.2.1. Für dieses Verfahren zugelassene Identitätsdokumente müssen über ausreichend fälschungssichere und mittels verfügbarer Technik im Verfahren prüfbare Sicherheitsmerkmale und -elemente sowie über eine maschinenlesbare Zone verfügen.

2.2.2. Ein Identitätsdokument verfügt über ausreichend fälschungssichere Merkmale und -elemente sofern eine Prüfung nach Ziffer 2.3.2. unter Einbeziehung der Sicherheitsmerkmale und -elemente in Ziffer 2.2.3., 2.2.4. sowie Ziffer 2.2.5 möglich ist.

2.2.3. Zur Einstufung, ob ein Dokument als geeignet im Sinne dieser Verfügung anzusehen ist, sind folgende Sicherheitsmerkmale heranzuziehen:

- 2.2.3.1. Beugungsoptisch wirksame Merkmale
  - 2.2.3.1.1. Identigram
  - 2.2.3.1.2. Zero-Order-Devices
  - 2.2.3.1.3. 3D-Relief-Effekt
  - 2.2.3.1.4. Achromatische Strukturen
  - 2.2.3.1.5. Chromatische, kinematische Strukturen
- 2.2.3.2. Personalisierungstechnik
  - 2.2.3.2.1. Laserkippbilder
  - 2.2.3.2.2. Taktile Bereiche (Lasergravur)
- 2.2.3.3. Material
  - 2.2.3.3.1. Transparentes Fenster
  - 2.2.3.3.2. Optisch variable Farbe
  - 2.2.3.3.3. Prägung

2.2.4. Es muss mindestens ein Merkmal aus jeder der in Ziffer 2.2.3 genannten Kategorien (2.2.3.1 bis 2.2.3.3) vorhanden und prüfbar

ENTWURF

sein, um als geeignetes Dokument betrachtet werden zu können. Mit „vorhanden“ ist die bloße, physische Existenz des Merkmals gemeint; „prüfbar“ setzt voraus, dass die Qualität und Auflösung der übertragenen Bilder bzw. Videos sowie ggf. der Tonspur ausreichend sind, um die für das jeweilige Merkmal notwendigen Kontrast-, Farb- und Detailunterschiede erkennen zu können.

2.2.5. Aufgrund der Verfügbarkeit guter Fälschungen zu Merkmal 2.2.3.1.5 (chromatische, kinematische Strukturen) gilt: Wenn in dieser Kategorie ausschließlich das Merkmal 2.2.3.1.5 vorhanden ist, müssen ergänzend zu 2.2.4 aus den Kategorien 2.2.3.2 und2.2.3.3 insgesamt mindestens drei Merkmale physisch vorhanden und prüfbar sein .

2.2.6. Als weitere Voraussetzung für die Eignung eines Dokuments müssen ausreichend Merkmale vorhanden sein, die eine sachgerechte Prüfung auf das Angriffsszenario der Verfälschung echter Dokumente ermöglichen. Hierfür sind unter anderem folgende Merkmale erforderlich:

2.2.6.1. Diffractive Optically Variable Image Device, sog. DOVID (d. h. ein Element aus der Kategorie der beugungsoptisch wirksamen Merkmale nach Ziffer 2.2.3.1) im Lichtbildbereich

2.2.6.2. Eine Prägung über den Individualdaten. Diese Bedingung gilt auch als erfüllt, wenn die Prägung ausschließlich über dem Lichtbild angeordnet ist

2.2.6.3. Mindestens ein Sekundärlichtbild zum Abgleich mit dem Primärlichtbild.

2.2.7. Über die in den Ziffern 2.2.3 bis 2.2.6 genannten Merkmale hinaus können weitere Merkmale – insbesondere solche, die einer automatisierten Prüfung zugänglich sind – in den Identifizierungsvorgang einbezogen werden. Hierzu zählen beispielsweise die Prüfung des Schriftbildes oder die Prüfung der Druckbildkonsistenz. Die konkrete Auswahl und Gewichtung dieser ergänzenden Merkmale obliegt dem Verpflichteten nach § 172 TKG im Rahmen seines Qualitätsmanagements.

2.3. Anforderungen an den Identifizierungsvorgang

2.3.1. Allgemeine Anforderungen

2.3.1.1. Die Identifizierung (Dokumentenechtheitsprüfung und Zugehörigkeitsprüfung), die durch das mit der Identifikation beauftragte Personal durchgeführt wird, muss mittels einer Videoübertragung mit sprachlicher Kontaktaufnahme in Echtzeit und ohne Unterbrechung stattfinden.

2.3.1.2. Bei der Zuteilung eines Identifizierungsvorgangs an die im konkreten Fall mit der Identifikation beauftragte Person müssen Mechanismen eingesetzt werden, die einer vorhersehbaren

ENTWURF

Zuteilung von Identifizierungsvorgängen und damit der dadurch bestehenden Möglichkeit einer Manipulation entgegenwirken.

2.3.1.3. Während des Identifizierungsvorgangs muss eine ausreichende Bild- und ggf. Tonqualität der Kommunikation gegeben sein, um eine zweifelsfreie Identifizierung anhand aller in dieser Verfügung geforderten Prüfungen uneingeschränkt zu ermöglichen. Die Auflösung der übertragenen Bilddaten darf hierbei den Wert 720p: 1280 x 720 bei 25 Frames pro Sekunde zu keinem Zeitpunkt des Identifizierungsvorgangs unterschreiten.

2.3.1.4. Der Anlass für die Identifikation ist durch die zu identifizierende Person, ohne Hilfestellung zu benennen um sicherzugehen, dass für diese klar ersichtlich ist, wofür sie sich identifiziert (Freischaltung einer SIM-Karte).

2.3.1.5. Für Identifizierungsvorgänge muss regelmäßig aktualisiertes, geeignetes Referenzmaterial genutzt werden. Das Referenzmaterial ist geeignet, wenn es die Prüfung der nach Ziffer 2.3.6. verwendeten Sicherheitsmerkmale und -elemente ermöglicht.

2.3.1.6. Es sind geeignete Maßnahmen zu ergreifen, um eine Manipulation des Videobildes, des Identitätsdokuments und der zu identifizierenden Person zu erkennen. Hierzu gehören sowohl organisatorische als auch technische Maßnahmen, die durch Interaktion mit dem verwendeten Ausweisdokument oder der zu identifizierenden Person gemäß Anweisung der die Identifikation durchführenden Person, eine Manipulation erkennbar machen. Insbesondere sind Maßnahmen gegen folgende Bedrohungsszenarien zu ergreifen:

2.3.1.6.1. Präsentationsangriffe jeder Art

2.3.1.6.2. Injektionsangriffe (Injection Attacks) jeder Art sowie

2.3.1.6.3. menschliche Manipulationsmethoden (Social-Engineering-Angriffe).

Die eingesetzten Maßnahmen haben sich am Stand der Technik sowie einer risikobasierten Bewertung zu orientieren.

2.3.1.7. Überdies ist die Übereinstimmung der, vorher gemäß § 172 Absatz 2 Satz 1 TKG, erhobenen Daten anhand der auf dem Identitätsdokument aufgedruckten sowie in der maschinenlesbaren Zone enthaltenen Datenzu überprüfen. Eine Datenerhebung im Rahmen des Identifizierungsvorgangs ist ebenfalls zulässig, vgl. Art. 6 Absatz 1 lit. c DSGVO in Verbindung mit § 172 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 TKG.

2.3.1.8. Wird der Identifizierungsvorgang nach Beginn der Prüfung der Sicherheitsmerkmale nach 2.3.2. abgebrochen oder unterbrochen, hat ein erneuter Identifizierungsversuch für dieselbe Person eine vollständige Neuprüfung sämtlicher für den Dokumenttyp vorgesehener Sicherheitsmerkmale zu umfassen. Die im abgebrochenen Vorgang bereits geprüften Merkmale sind hierbei erneut zu prüfen. Es ist technisch und organisatorisch sicherzustellen, dass ein Angreifer durch gezielten Abbruch potenziell entlarvender Prüfungen nicht erreichen kann, dass beim nachfolgenden Versuch nur eine Teilmenge oder andere Merkmale geprüft werden.

2.3.2. Dokumentenechtheitsprüfung

2.3.2.1. Die Echtheit und Unverfälschtheit des Identitätsdokuments ist im Rahmen einer Gültigkeits- und Plausibilitätsprüfung, welche, soweit vorhanden, unter Einbeziehung der maschinenlesbaren Zone sowie der Prüfziffer und der in Ziffer 2.2.3. bis einschließlich Ziffer 2.2.6. genannten Sicherheitsmerkmale und -elemente zu erfolgen hat, zuverlässig zu prüfen.

2.3.2.2. Für eine zuverlässige Prüfung der Sicherheitsmerkmale und -elemente muss eine ausreichende Anzahl bzw. Auswahl der in Ziffer 2.2.3. bis einschließlich 2.2.6. genannten Sicherheitsmerkmale und -elemente überprüft werden, so dass allen bekannten Angriffsszenarien entgegengewirkt wird.

2.3.2.3. Im Rahmen des Dokumentenechtheitsprüfung ist mindestens ein Merkmal aus jeder der in Ziffer 2.2.3 genannten Kategorien (2.2.3.1 bis 2.2.3.3) zu prüfen. In Fällen des 2.2.5 sind mindestens drei weitere Merkmale zu prüfen, wobei diese zwingend aus beiden der übrigen zwei Kategorien (2.2.3.2, 2.2.3.3) stammen müssen.

2.4. Zugehörigkeitsprüfung

2.4.1. Die Zugehörigkeit des verwendeten Ausweisdokuments zu der zu identifizierenden Person, ist durch den Abgleich der zu identifizierenden Person mit dem Lichtbild des verwendeten Identitätsdokuments zu überprüfen.

2.4.2. Zur Durchführung des Abgleichs müssen dem den Abgleich durchführenden Personal geeignete technische Hilfsmittel zur Verfügung stehen.

2.5. Anforderungen an die Dokumentation

2.5.1. Die den Identifizierungsvorgang durchführende Person muss die wesentlichen Punkte des Identifizierungsvorgangs in geeigneter Weise dokumentieren, um eine spätere Nachvollziehbarkeit der Umstände der Identifikation gewährleisten zu können.

2.5.2. Zu den wesentlichen Punkten der Dokumentation gehören:
- 2.5.2.1. Wann wurde der Identifizierungsvorgang durchgeführt?
- 2.5.2.2. Wer ist die durchführende Person?
- 2.5.2.3. Wer ist die zu identifizierende Person?
- 2.5.2.4. Welches Identitätsdokument wurde verwendet (vgl. Anforderung in Ziffer A.I.2.)?
- 2.5.2.5. Welche Sicherheitsmerkmale und -elemente aus Ziffer 2.2.3. und Ziffer 2.2.4. wurden geprüft und mit welchem Ergebnis?
- 2.5.2.6. Das Ergebnis der Zugehörigkeitsprüfung nach Ziffer 2.4
- 2.5.2.7. Welche technischen Hilfsmittel wurden im Zuge des Identifizierungsverfahrens eingesetzt?

2.5.3. Die Dokumentation sowie die nach § 172 TKG zu erhebenden Daten sind dem Verpflichteten nach § 172 TKG unverzüglich zu übermitteln.

2.5.4. Bei erfolgreicher Durchführung des Identifizierungsverfahrens ist die Dokumentation durch den Verpflichteten nach § 172 TKG für zwei Jahre ab der Durchführung des Identifizierungsvorgangs zu speichern und nach Ablauf zu löschen. Für den Fall, dass die Daten nach § 172 Abs. 1-3 TKG zu einem früheren Zeitpunkt gem. § 172 Abs. 6 TKG zu löschen sind, ist auch die Dokumentation entsprechend mit diesen zu löschen.

2.5.5. Bei abgebrochenen und/oder nicht erfolgreichen Identifizierungsvorgängen ist die Dokumentation durch den Verpflichteten nach § 172 TKG für sechs Monate ab dem Identifizierungsversuch zu speichern und nach Ablauf zu löschen.

2.6. Räumliche Anforderungen

Das mit der Identifikation beauftragte Personal muss sich während der Identifizierung in abgetrennten und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.

2.7. Technische Anforderungen

2.7.1. Die audiovisuelle Kommunikation zwischen dem mit der Identifikation beauftragten Personal 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 in der jeweils aktuellen Fassung einzuhalten.

2.7.2. Bei Verwendung einer Anwendungssoftware für mobile Betriebssysteme zum Zwecke der Durchführung des Identifizierungsverfahrens sind Programme einzusetzen, die es nach dem aktuellen Stand der Technik ermöglichen, zu erkennen, ob das Betriebssystem verändert bzw. manipuliert wurde (wie z. B. Jailbreak bzw. Rooting Detection Programme).

2.7.3. Die für die Durchführung dieses Verfahrens erforderliche Kommunikation kann auch mit der erworbenen Mobilfunkleistung selbst aufgebaut werden, wobei die erworbene Mobilfunkleistung vor Freischaltung ausschließlich für diesen Identifizierungsvorgang möglich sein darf, einschließlich der etwaigen vorherigen Datenerhebung.

2.7.4. Für jedes zum Verfahren zugelassene Dokument ist in einer Datenbank ein Katalog von Prüfroutinen zu hinterlegen, der das spezifische Layout, die individuell auf dem Dokument aufgebrachten Sicherheitsmerkmale in ihren Formen, Funktionalitäten und Motiven sowie deren relative Positionierung berücksichtigt. Die Prüfroutinen müssen dabei manipulierte oder nachträglich veränderte genuine Identitätsdokumente, insbesondere deren Personalisierungselemente, zuverlässig erkennen; dies gilt auch dann, wenn dabei aufgebrachte Sicherheitsmerkmale unangetastet bleiben.

2.7.5. Technische Maßnahmen in 2.1 bis 2.5 dürfen nur nachträglich als Assistenzsysteme die einzelnen Prüfschritte des menschlichen Operators unterstützen.

2.7.6. Wenn technische Maßnahmen Verfahren einsetzen, die auf maschinellem Lernen beruhen, ist sicherzustellen, dass diese systematisch gegen Referenzdatensätze getestet und in Bezug auf sich ändernde Risiko- und Bedrohungsszenarien aktuell gehalten werden.

2.8. Abbruch des Identifizierungsvorgangs

2.8.1. Ein Identifizierungsvorgang kann im Ermessen der den Identifizierungsvorgang durchführenden Person abgebrochen werden, etwa aufgrund von schlechten Lichtverhältnissen, schlechter Tonqualität oder einer nicht ausreichenden Bildqualität/-übertragung. Weitere Abbruchsbedingungen können festgelegt werden. Es ist festzulegen, wie oft ein Identifizierungsvorgang wiederholt werden darf. Die maximale Anzahl der Wiederholungen muss dabei einen wirksamen Schutz vor Betrugs- und Missbrauchsversuchen gewährleisten.

2.8.2. Bei Feststellung von Betrugsversuchen ist der Identifizierungsvorgang dennoch in Gänze durchzuführen, um keine Rückschlüsse auf eine Detektion des Betrugsversuchs zuzulassen. Gründe für die nicht erfolgreiche Identifizierung dürfen der zu identifizierenden Person auch im Nachhinein nicht mitgeteilt werden.
Dasselbe gilt, soweit im konkreten Fall die Überprüfung eines vorhandenen Sicherheitsmerkmals scheitert.
Bei einem eindeutig festgestellten Betrugsversuch ist eine Wiederholung des Identifizierungsvorgangs unzulässig.

2.8.3. Eine positive Identifizierungsentscheidung darf weiterhin nicht allein auf intakten Sicherheitsmerkmalen beruhen, wenn Abweichungen zwischen den einzelnen Identifizierungsmerkmalen des Dokuments (beispielsweise Lichtbild, Sekundärlichtbild, maschinenlesbare Zone) oder Hinweise auf eine nachträgliche Veränderung bestehen.

2.9. Anforderungen an ein kontinuierliches Qualitätsmanagement

2.9.1. Es sind geeignete technische und organisatorische Maßnahmen zu treffen, um die Performanz des Verfahrens sicherzustellen. Zwingender Bestandteil sind kontinuierliche Stichprobenüberprüfungen in angemessenem Umfang durch geschultes Personal, das anhand der erhobenen Nachweisdaten die Ergebnisse der Prüfungen überprüft. Die Grundgesamtheit muss hierbei eine Richtigkeitsquote von mindestens 99,999 % aufweisen. Dies entspricht einem maximal zulässigen Fehleranteil von 0,001 %. Der erforderliche Stichprobenumfang ist nach einem geeigneten statistischen Verfahren so zu bestimmen, dass mit einem Konfidenzniveau von mindestens 95 % nachgewiesen werden kann, dass der maximal zulässige Fehleranteil von 0,001 % in der Grundgesamtheit nicht überschritten wird. Die Auswahl der Stichprobe hat nach einem geeigneten, nachvollziehbaren und unverzerrten Verfahren zu erfolgen. Das angewandte Stichprobenverfahren, die Berechnung des Stichprobenumfangs sowie die zugrunde gelegten statistischen Annahmen sind nachvollziehbar zu dokumentieren.

2.9.2. Die Stichprobenüberprüfung hat kontinuierlich unterjährig stattzufinden. Die erhobenen Nachweisdaten sind in der Regel nach Ablauf von 7 Tagen zu löschen. Eine Aufbewahrung darüber hinaus ist nur zulässig, sofern die Stichprobenüberprüfung einen Hinweis auf Betrugsfälle, Betrugsversuche sowie. sonstige Probleme oder Fehler liefert. In diesem Fall ist zur Ermöglichung einer Analyse der Nachweisdaten eine Aufbewahrung bis zum Abschluss der Analyse, in der Regel innerhalb von 4 Wochen zulässig. In besonders begründeten Einzelfällen ist eine Aufbewahrung zu Analysezwecken auch nach Ablauf von 4 Wochen zulässig, jedoch nicht länger als bis zu 8 Wochen nach Beendigung des Identifizierungsvorgangs.

2.9.3. Die Durchführung von Identifizierungsverfahren nach dieser Ziffer ist unverzüglich auszusetzen, wenn die Stichprobenanalyse eine Überschreitung des zulässigen Fehleranteils aufzeigt. Der Verpflichtete nach § 172 TKG ist hierüber unverzüglich zu informieren. Identifizierungsverfahren nach dieser Ziffer dürfen erst wieder aufgenommen werden, wenn entsprechende Maßnahmen erfolgreich durchgeführt wurden, welche die Einhaltung des maximal zulässigen Fehleranteils sicherstellen.

ENTWURF

2.9.4. Für die Qualifikation des mit der Stichprobenüberprüfung beauftragten Personals gilt Ziffer 2.1.1. entsprechend. Ferner ist sicherzustellen, dass die mit der Stichprobenüberprüfung beauftragte Person über entsprechende Kenntnis relevanter Angriffsszenarien verfügt.

2.9.5. Ferner muss sich das mit der Stichprobenüberprüfung beauftragte Personal während der Überprüfung der Identifikationen in abgetrennten mit Zugangskontrolle ausgestatteten Räumlichkeiten aufhalten.

2.9.6. Die Durchführung und Ergebnisse der Stichprobenüberprüfungen sind in geeigneter Weise zu dokumentieren.

3. Abgleich bei anlassunabhängiger Vorabidentifikation

3.1. Anforderungen an den Datenabgleich und den vorherigen Identifizierungsvorgang

3.1.1. Es sind zwei Alternativen für einen Datenabgleich bei Vorabidentifikation zulässig:

a) Prüfung der erhobenen Anschlussinhaberdaten mittels Abgleichs mit Daten, die bei einem Dritten vorgehalten werden und die ihrerseits auf eine vorherige Identifikation mit Identitätsdokumenten im Sinne des § 172 Absatz 2 Satz 1 Nr. 1-7 TKG zurückzuführen sind, entweder im Rahmen der Vorlage des jeweiligen Dokuments oder eines anderen in dieser Verfügung beschriebenen Verfahrens

oder

b) Prüfung der erhobenen Anschlussinhaberdaten mittels Abgleichs mit einem unveränderlichen Datensatz, der bei der identifizierenden Person selbst vorgehalten wird und der auf einer vorherigen Identifikation mit Identitätsdokumenten im Sinne des § 172 Absatz 2 Satz 1 Nr. 1-7 TKG gegenüber einem Dritten zurückzuführen ist, entweder im Rahmen der Vorlage des jeweiligen Dokuments oder eines anderen in dieser Verfügung beschriebenen Verfahrens.

Die vorherige Identifikation muss die Anforderungen des jeweiligen Verfahrens dieser Verfügung erfüllen.

3.1.2. Es ist durch geeignete technische und / oder organisatorische Maßnahmen sicherzustellen, dass die vorgehaltenen Daten in ihrer Integrität geschützt sind. Insbesondere sind Maßnahmen gegen unbefugte Kontoübernahmen (Account Takeover) zu ergreifen.

ENTWURF

3.1.3. Die vorgehaltenen Daten dürfen für eine Freischaltung von im Voraus bezahlten Mobilfunkdiensten nur verwendet werden, sofern die Identifizierung oder die letzte Aktualisierung unter Einhaltung der Vorgaben des entsprechenden Verfahrens nach dieser Verfügung vor nicht mehr als 24 Monaten abgeschlossen wurde, für den Verpflichteten nach § 172 TKG aufgrund äußerer Umstände keine Zweifel an der Richtigkeit der ihm übermittelten Informationen bestehen und das Gültigkeitsdatum eines im Rahmen der Identifizierung oder der letzten Aktualisierung verwendeten Identifikationsdokuments zum Zeitpunkt der Freischaltung noch nicht abgelaufen ist. Vor Verwendung der vorgehaltenen Daten für eine Identifizierung ist die Aktualität und Korrektheit dieser durch die sich identifizierende Person zu bestätigen.

3.1.4. Eine Aktualisierung der vorgehaltenen Daten setzt die erfolgreiche Durchführung eines Identifizierungsverfahrens nach dieser Verfügung voraus.

3.2. Technische Anforderungen

Bei Übermittlungen für Zwecke des Datenabgleichs und -abrufs sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten.

3.3. Anforderungen an die Einwilligung

Bei Alternative a) ist sicherzustellen, dass die Übermittlung der vorgehaltenen Daten an den Verpflichteten nach § 172 TKG nur auf Veranlassung der zu identifizierenden Person erfolgt, d.h. soweit diese nach einem vorgesehenen Verfahren verbunden mit einer Authentifizierung ihrer Person (etwa durch Eingabe einer PIN) zugestimmt hat. In beiden Alternativen bedarf es der Einholung einer Einwilligung der zu identifizierenden Person zu Übermittlungen für Zwecke des Datenabgleichs im Sinne des § 172 TKG, die den datenschutzrechtlichen Anforderungen entspricht.

3.4. Anforderungen an die Dokumentation

Es ist eine Dokumentation zu den wesentlichen Punkten der Datenübermittlung/des Datenabgleichs anzufertigen, in welche auch die Einwilligung nach Ziffer 4.3.2 aufzunehmen ist. Die Dokumentation ist für sechs Monate ab der Datenübermittlung/dem Datenabgleich zu speichern und nach Ablauf zu löschen.

ENTWURF

4. Anerkennung von qualifizierten elektronischen Vertrauensdiensten nach eIDAS

Ein Identifizierungsdiensteanbieter, der gem. Art. 24 Abs. 1a der Verordnung (EU) Nr. 910/2014 für Identifizierungen zertifiziert ist und bei dem Gegenstand der akkreditierten Konformitätsbewertung die Überprüfung der Zugehörigkeitsprüfung nach den Anforderungen des konkreten Identifizierungsverfahrens der im Anhang der Durchführungsverordnung (EU) 2025/1566 aufgeführten und angepassten Norm war, erfüllt im Fall von Punkt 8.4.4 dieser Norm die Anforderungen dieser Verfügung nach II. 2.4.

III. Inkrafttreten, Übergangsfristen und Schlussbestimmungen

Die Regelungen dieser Verfügung treten zum 01.08.2027 in Kraft. Mit Inkrafttreten dieser Verfügung tritt die Verfügung Nr. 94/2021 der Bundesnetzagentur außer Kraft.

Nach der Ziffer 4 erhobene und gespeicherte Daten einer anlassunabhängigen Vorabidentifizierung nach der Verfügung Nr. 94/2021 der Bundesnetzagentur verlieren mit Ablauf des 31.07.2027 ihre Gültigkeit für die Freischaltung von im Voraus bezahlten Mobilfunkdiensten.

Diese Verfügung regelt ausschließlich andere geeignete Verfahren gegenüber den gesetzlich vorgesehenen Regelfällen der Überprüfung von Anschlussinhaberdaten vor Freischaltung gem. § 172 Abs. 2. S. 1 TKG.

Spezialgesetzliche und anderweitige Regelungen und Anforderungen, insbesondere an Konformitätsbewertungen und Zertifizierungen, bleiben unberührt.

Sofern keine speziellen Regelungen in dieser Verfügung getroffen werden, gilt die Datenschutz-Grundverordnung.

ENTWURF