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

Version 1.1

Stand 29. Dezember 2021

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Referat IS14

Canisiusstraße 21

55122 Mainz

Tel.: +49 6131 18-0

Fax: +49 6131 18-5611

E-Mail: IdentKonform@BNetzA.de

Inhalt

Dokumentinformationen 4
Vorwort 4
I. Generelle Erläuterungen 5
1. Begriffsbestimmungen 5
a) „die zu identifizierende Person“ 5
b) „Anschlussinhaberdaten“ 5
c) „Diensteanbieter“ 5
d) „das mit der Identitätsprüfung beauftragte Personal“ 5
e) „Dritter“ 5
f) „Datenerhebung und Datenabgleich“ 5
2. Hinweis zum Anwendungsbereich 6
a) juristische Personen bzw. Personengesellschaften 6
b) Vorlagebegriff 6
3. Konformitätsbewertung und Übergangsregelung 6
a) Erfordernis des Konformitätsnachweises 6
b) Übergangsregelung 6
c) Anwenderkreis 7
d) Kontakt 7
4. Grundsätzliche Änderungen in *Ziffer A. Katalog der Anforderungen für geeignete Verfahren nach § 172 Absatz 2 Satz 3 TKG* 7
a) Anforderungskatalog 7
b) Neue Struktur 7
c) Zulässige Identitätsdokumente 8
5. Streichung des Verfahrens mit elektronischem Identitätsnachweis 9
6. Speicherung von Daten nach § 172 Absatz 2 Satz 6 9
a) Fallgruppe 1: keine erkennbare ausstellende Stelle 10
b) Fallgruppe 2: bei Nutzung des elektronischen Identitätsnachweises kann auf Speicherung der Ausweisnummer verzichtet werden 10
II. Spezifische verfahrensbezogene Erläuterungen 10
1. Änderung der spezifischen verfahrensbezogenen Anforderungen 10
2. Änderung der Dokumentationsanforderungen 10
3. Anlassbezogene Vor-Ort-Identifikation durch Dritte (Ziffer A.II.1.) 11
4. Anlassbezogene klassische Video-Identifikation (Ziffer A.II.2.) 11
zu Ziffer A.II.2.1. Anforderungen an das mit der Identifikation beauftragte Personal 11
zu Ziffer A.II.2.3. Anforderungen an den Identifizierungsvorgang 11
5. Anlassbezogene automatisierte Video-Identifikation (Ziffer A.II.2.) 12

zu Ziffer A.II.3.2. Anforderungen an den Identifizierungsvorgang 12
zu Ziffer A.II.3.2.4. 12
zu Ziffer A.II.3.2.6. 12
zu Ziffer A.II.3.4. Anforderungen an Transparenz und Einwilligung 13
zu Ziffer A.II.3.4.1. 13
zu Ziffer A.II.3.4.2. 13
zu Ziffer A.II.3.6.1. 13
zu Ziffer A.II.3.8. Anforderungen an ein kontinuierliches Qualitätsmanagement 13
zu Ziffer A.II.3.8.1. 14
zu Ziffer A.II.3.8.2. 14
6. Abgleich bei anlassunabhängiger Vorabidentifikation (Ziffer A.II.4) 14
zu Ziffer A.II.4.1. Anforderungen an den Datenabgleich und den vorherigen Identifizierungsvorgang 15
zu Ziffer A.II.4.1.3. 15
zu Ziffer A.II.4.2.1. 16

Dokumentinformationen

Änderungsnachweis		
Versions-Nr.	Datum	Änderung/Bemerkung
1.0	17.12.2021	Basisversion
1.1	29.12.2021	Formatanpassung und klarstellender Hinweis auf Zulässigkeit der Nutzung von eID mit mobilem Endgerät

Vorwort

Am 30. Juni 2016 trat das Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus in Kraft. Dadurch wurde die Regelung des § 111 TKG 2004 angepasst. Die Vorgabe, bestimmte Anschlussinhaberdaten zu erheben, wurde durch die ausdrückliche Pflicht der Diensteanbieter für im Voraus bezahlte Mobilfunkdienste, eine Überprüfung der erhobenen Anschlussinhaberdaten vorzunehmen, ergänzt. Diese Überprüfung muss anhand der Vorlage bestimmter, enumerativ aufgeführter Identitätsnachweise stattfinden.

Neben der direkten Vorlage wurde gesetzlich geregelt, dass die Bundesnetzagentur durch Verfügung im Amtsblatt weitere geeignete Verfahren festlegen kann.

Seitdem gab es insgesamt vier Versionen der Verfügung über geeignete Identifizierungsverfahren.

Am 1. Dezember 2021 trat die Neufassung des TKG in Kraft, welches nun in § 172 Absatz 2 Satz 3 TKG der Bundesnetzagentur die Aufgabe zuweist, eine Festlegung zu treffen, welche anderen Verfahren als die im Gesetz vorgesehene unmittelbare Vorlage der in § 172 Absatz 2 Satz 1 Nr. 1 - 7 TKG genannten Identitätsdokumente zur Überprüfung der Daten des Anschlussinhabers bei im Voraus bezahlten Mobilfunkdiensten geeignet sind.

Entsprechend wird in der mittlerweile fünften und vollständig überarbeiteten Version der *„Verfügung zur Festlegung von Verfahren zur Überprüfung von Anschlussinhaberdaten (Identifizierungsverfahren) gemäß § 172 Absatz 2 Satz 3 Telekommunikationsgesetz“* festgelegt, welche Verfahren geeignet sind und welche Anforderungen an diese Verfahren gelten. Diese ist als Verfügung Nr. 94/2021 im Amtsblatt 23/2021 vom 8. Dezember 2021 erschienen.

Diese Handreichung soll ergänzend zum Verfügungstext weitergehende Informationen bereitstellen. Neben Hintergründen zu Überlegungen im Rahmen der Neugestaltung werden Erläuterungen und punktuelle Konkretisierungen zum aktuellen Verfügungstext dargestellt. Hierbei werden insbesondere klarstellungsbedürftige Punkte berücksichtigt, die im Rahmen des Anhörungsverfahrens seitens betroffener Kreise aufgezeigt wurden.

Soweit im Zuge der Anwendungspraxis der Verfügung weitere Fragestellungen als generell klärungsbedürftig aufgezeigt werden oder sich neue technische oder regulatorische Entwicklungen abzeichnen, behält sich die Bundesnetzagentur eine sukzessive Ergänzung und Überarbeitung dieser Handreichung vor.

Fragen, Ergänzungen oder andere Anliegen bzgl. der Verfügung können an das Postfach IdentKonform@BNetzA.de gerichtet werden.

I. Generelle Erläuterungen

1. Begriffsbestimmungen

a) „die zu identifizierende Person“

Für die Zwecke der Verfügung Nr. 94/2021 ist **die zu identifizierende Person** jede natürliche Person, für die eine Identifizierung durchgeführt wird. Die Begrifflichkeiten in der Verfügung wurden mit der Neufassung neutraler gefasst. So wurde der Begriff des Anschlussinhabers mit dem Begriff der zu identifizierenden Person ersetzt.

b) „Anschlussinhaberdaten“

Sofern die Verfügung auf **Anschlussinhaberdaten** Bezug nimmt, handelt es sich um Daten im Sinne des § 172 Absatz 1 Satz 1 TKG, soweit diese Gegenstand der Überprüfungspflicht in § 172 Absatz 2 Satz 1 TKG sind. Umfasst sind neben dem Namen und der Anschrift des Anschlussinhabers (vgl. § 172 Absatz 1 Satz 1 Nr. 3 TKG) auch dessen Geburtsdatum (vgl. § 172 Absatz 1 Satz 1 Nr. 4 TKG).

c) „Diensteanbieter“

Entsprechend der gesetzgeberischen Vorgabe aus § 172 Absatz 2 Satz 4 TKG wurde der Begriff **Diensteanbieter** für Anbieter von im Voraus bezahlten Mobilfunkdiensten gewählt. An diese ist die Pflicht zur Durchführung einer Überprüfung der Anschlussinhaberdaten in § 172 Absatz 2 Satz 1 ff. TKG gerichtet.

d) „das mit der Identitätsprüfung beauftragte Personal“

Außerdem wurde der Begriff des **mit der Identitätsprüfung beauftragten Personals** ergänzt. Hierbei kann es sich sowohl um Personal handeln, das im Auftrag des Diensteanbieters direkt agiert, oder von Dritten beauftragt wurde.

e) „Dritter“

Nicht als **Dritter** im Sinne der Verfügung und insbesondere des Verfahrens in *Ziffer A.II.1.* zur Vor-Ort-Identifikation bei Dritten gilt, wer als Vertriebspartner, Händler bzw. autorisierte Verkaufsstelle in den Prozess des Erwerbs der SIM-Karte des Diensteanbieters eingebunden wurde. Die Vorlage von Identitätsdokumenten beim Diensteanbieter und von diesem in den Pflichtenkreis einbezogener Dritter ist bereits gesetzlich geregelt, demzufolge ist die Bundesnetzagentur nicht zur Regelung befugt. Damit steht die Verfügung im Einklang mit der Rechtsauffassung des Verwaltungsgerichts Köln im Klageverfahren gegen die Vorgängerversion der Verfügung (VG Köln, Urteile vom 13.11.2020 – Az. 9 K 574/18 und 9 K 1378/18).

f) „Datenerhebung und Datenabgleich“

Bei der Überprüfungspflicht der Anschlussinhaberdaten handelt es sich um eine Verpflichtung, die in engem Zusammenhang zu dem in § 172 Absatz 1 Satz 1 TKG geregelten Vorgang der Datenerhebung steht. Daher werden in der Verfügung Anforderungen an die Tätigkeit der Datenerhebung als den der Datenübermittlung unmittelbar vorausgehenden Teil eines in der Lebenswirklichkeit einheitlichen Vorgangs teilweise mitgeregelt. Soweit dies im Anforderungskatalog vorgesehen ist, kann im Einzelfall auch ein Zusammenfallen von Datenerhebung und Überprüfung, z. B. im Sinne eines Abrufs erfolgen. Die Erhebungsbefugnis ergibt sich aus Art. 6 Absatz 1 lit. c DSGVO in Verbindung mit § 172 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 TKG.

2. Hinweis zum Anwendungsbereich

a) juristische Personen bzw. Personengesellschaften

In der Anhörung vom 12. Mai 2021 (Amtsblatt Nr. 09/2021, S. 534 f.) wurde der Bedarf für ein anderes geeignetes Verfahren spezifisch für **juristische Personen bzw. Personengesellschaften** abgefragt. Aufgrund der weitgehenden Möglichkeiten der gesetzlichen vorgesehenen Überprüfungsmethode in § 172 Absatz 2 Satz 1 Nr. 7 TKG ergab sich im Rahmen der hierzu eingegangenen Stellungnahmen kein zusätzlicher Regelungsbedarf. So kann bereits jetzt seitens der verpflichteten Unternehmen eine Einsichtnahme in Handelsregister sowie die anderen in Nr. 7 genannten Verzeichnisse zu Überprüfungszwecken erfolgen.

b) Vorlagebegriff

Ergänzend ist der Vorlagebegriff in § 172 Absatz 2 Satz 1 Nr. 7 TKG weiter auszulegen, als für die anderen in Satz 1 enthaltenen Fallgruppen Nr. 1 bis Nr. 6. Während hierbei generell eine Vor-Ort-Vorlage durch den Anschlussinhaber verlangt wird, ist dies bei juristischen Personen und Personengesellschaften problematisch, weil diese selbst nur durch vertretungsbefugte natürliche Personen auftreten können. Der bei Vor-Ort-Vorlage eines Identitätsdokuments durch natürliche Personen mögliche Identitätsabgleich ist bei juristischen Personen und Personengesellschaften ohnehin nicht möglich, so dass neben der Vor-Ort-Vorlage auch andere Formen der Vorlage (z. B. Übermittlung per Post oder E-Mail) keinen Bedenken begegnen.

3. Konformitätsbewertung und Übergangsregelung

a) Erfordernis des Konformitätsnachweises

In § 172 Absatz 2 Satz 4 TKG wird geregelt, dass die Feststellung der Übereinstimmung eines konkreten Verfahrens mit der Festlegung der Bundesnetzagentur zukünftig durch eine Konformitätsbewertungsstelle vorgenommen wird.

Die Bundesnetzagentur erteilt keine rechtsverbindlichen Auskünfte zur Konformität von konkreten Identifizierungsverfahren mit den Vorgaben in *A. Katalog der Anforderungen für geeignete Verfahren nach § 172 Absatz 2 Satz 3 TKG.* Die Feststellung der Übereinstimmung obliegt nach dem Willen des Gesetzgebers allein den Konformitätsbewertungsstellen.

Entsprechend der gesetzgeberischen Vorgabe in § 172 Absatz 2 Satz 4 TKG haben Anbieter von im Voraus bezahlten Mobilfunkdiensten ab dem 1. Dezember 2021 vor Nutzung von anderen geeigneten Verfahren die Feststellung der Übereinstimmung eines Verfahrens mit dieser Verfügung durch eine akkreditierte Konformitätsbewertungsstelle nachzuweisen.

b) Übergangsregelung

Gemäß der Ermächtigung in § 230 Absatz 9 TKG legt die Bundesnetzagentur unter *Ziffer A.III. Zeitliche Geltung* eine Übergangsfrist von zwölf Monaten fest.

Die zwölfmonatige Übergangszeit soll ausreichend Zeit gewähren, damit die Verfahrensgrundlagen für Konformitätsüberprüfungen geschaffen werden können und die Diensteanbieter eine Überprüfung ihrer Identifizierungsverfahren durch Konformitätsbewertungsstellen im Sinne des § 172 Absatz 2 Satz 4 TKG durchführen lassen können.

Für Verfahren entsprechend der Vorgaben, die erstmalig durch die Neugestaltung der Verfügung ab dem 1. Dezember 2021 als geeignet angesehen werden (dies betrifft insbesondere

Verfahren nach *Ziffer A.II.3.*), wird darauf hingewiesen, dass ihre Einführung durch die Diensteanbieter im Kontext von im Voraus bezahlten Mobilfunkdiensten auf eigenem unternehmerischen Risiko beruhen. Die Bundesnetzagentur empfiehlt, insbesondere bei Unsicherheiten betreffend die Konformität eines solchen Verfahrens mit den Vorgaben in dieser Verfügung, die Überprüfung durch Konformitätsbewertungsstellen abzuwarten. Erlangt die Bundesnetzagentur Kenntnis von Mängeln in der Umsetzung des Anforderungskatalogs der Verfügung, so behält sie sich vor, Maßnahmen gemäß § 183 Absatz 1 Satz 1 TKG zu treffen. Hierzu kann bei gravierenden Mängeln insbesondere auch die Anordnung einer Neuüberprüfung der mangelhaft überprüften Anschlussinhaberdaten gehören. Auf die Wirksamkeit der Verträge der Diensteanbieter mit den Anschlussinhabern haben Mängel bei der Überprüfung der Daten gemäß § 172 Absatz 2 TKG hingegen keine unmittelbaren Auswirkungen.

c) Anwenderkreis

Grundsätzlich gilt, dass die Diensteanbieter die Anforderungen des Katalogs der Verfügung entweder selbst erfüllen müssen oder hierfür – bei einer entsprechenden Beauftragung Dritter, die Identifizierungsverfahren als Dienstleistung oder Produkt anbieten – diese einbinden können. Bedienen sich die Diensteanbieter eines solchen Dritten für die Durchführung eines Identifizierungsverfahrens, so haben sie sich zu vergewissern, dass die jeweiligen Anforderungen dieser Verfügung, insbesondere hinsichtlich der Datenerhebung, Identitätsprüfung und Prüfung der Echtheit des Identitätsdokuments, eingehalten werden. Dies hat der Diensteanbieter zu dokumentieren. Eine Konformitätsbewertung kann durch Diensteanbieter, aber auch durch Dritte, die Identifizierungsverfahren als Dienstleistung oder Produkt anbieten, veranlasst werden. Sobald ein Konformitätsnachweis für ein Identifizierungsverfahren eines Dritten vorliegt, kann sich der Diensteanbieter, der den Dritten beauftragt hat, vollumfänglich hierauf beziehen.

d) Kontakt

Nähere Informationen zur Konformitätsbewertung werden zu gegebener Zeit auf der Internetseite der Bundesnetzagentur veröffentlicht. Rückfragen hierzu können ebenfalls an das Postfach IdentKonform@BNetzA.de gerichtet werden

4. Grundsätzliche Änderungen in *Ziffer A. Katalog der Anforderungen für geeignete Verfahren nach § 172 Absatz 2 Satz 3 TKG*

a) Anforderungskatalog

Im Zuge der Überarbeitung der Verfügung wurden zahlreiche Änderungen vorgenommen. Insgesamt wurde in Anlehnung an die von der Bundesnetzagentur erlassene, im Bereich der Elektronischen Vertrauensdienste geltende Verfügung gemäß § 11 Absatz 1 Vertrauensdienstegesetz (VDG), die Form eines Katalogs mit Anforderungen gewählt.

Hierbei wurde insbesondere zwischen „anlassbezogenen“ und „anlassunabhängigen“ Identifikationen unterschieden, um diejenigen Identifikationen, die spezifisch zur Erfüllung der Pflichten nach § 172 TKG erfolgen, von solchen abzugrenzen, die zu einem vorherigen Zeitpunkt und aus einem Anlass ohne Bezug zum TKG stattgefunden haben. Im letztgenannten Fall wird lediglich anlässlich von § 172 TKG ein Datenabgleich oder -abruf durchgeführt.

b) Neue Struktur

Des Weiteren wurden bisherige Verfahrensdarstellungen strukturell neu geordnet. Durch die neue Struktur in übergeordnete Kategorien (bspw. *Ziffer 1.1. Anforderungen an den Identifizierungsvorgang*) sowie die neue Nummerierung (bspw. *Ziffer 1.1.1., Ziffer 1.1.2.*), soll vor

allem mehr Übersichtlichkeit, aber auch eine bessere Möglichkeit des Referenzierens einzelner Anforderungen geschaffen werden.

Gerade im Hinblick auf die neue Katalogform soll eine Bewertung durch die Konformitätsbewertungsstellen vereinfacht werden, da nunmehr jede Anforderung eine laufende Nummerierung aufweist und somit auch als Checkliste für die Prüfung verwendet werden kann.

Weiterhin wurden sowohl allgemeine Anforderungen aufgezeigt, die für alle Verfahren gelten, als auch spezifische verfahrensbezogene Anforderungen, die für das jeweilige Verfahren ausschlaggebend sind.

c) Zulässige Identitätsdokumente

In *Ziffer A.I. Allgemeine Anforderungen* der Verfügung wird zunächst darauf eingegangen, welche Identitätsdokumente für die Identifikation zulässig sind. Hierbei wird auf den enumerativen Katalog der Identitätsdokumente in § 172 Absatz 2 Satz 1 TKG hingewiesen.

§ 172 Absatz 2 Satz 1 TKG

„Anbieter von im Voraus bezahlten Mobilfunkdiensten haben die Richtigkeit der nach Absatz 1 Satz 1 Nummer 3 und 4 erhobenen Daten, sofern die Daten in den vorgelegten Dokumenten oder eingesehenen Registern oder Verzeichnissen enthalten sind, vor der Freischaltung zu überprüfen durch

1. *Vorlage eines Ausweises im Sinne des § 2 Absatz 1 des Personalausweisgesetzes,*
2. *Vorlage eines Passes im Sinne des § 1 Absatz 2 des Passgesetzes,*
3. *Vorlage eines sonstigen gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, wozu insbesondere auch ein nach ausländerrechtlichen Bestimmungen anerkannter oder zugelassener Pass, Personalausweis oder Pass- oder Personalausweisersatz zählt,*
4. *Vorlage eines Aufenthaltstitels,*
5. *Vorlage eines Auskunftsnachweises nach § 63a Absatz 1 des Asylgesetzes*
6. *Vorlage einer Bescheinigung über die Aussetzung der Abschiebung nach § 60a Absatz 4 des Aufenthaltsgesetzes oder*
7. *Vorlage eines Auszugs aus dem Handels- oder Genossenschaftsregister oder einem vergleichbaren amtlichen Register oder Verzeichnis, der Gründungsdokumente oder gleichwertiger beweiskräftiger Dokumente oder durch Einsichtnahme in diese Register oder Verzeichnisse und Abgleich mit den darin enthaltenen Daten, sofern es sich bei dem Anschlussinhaber um eine juristische Person oder Personengesellschaft handelt.“*

Weiterhin wird auf die Geltung des § 7 Absatz 2 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) hingewiesen.

§ 7 Absatz 2 TTDSG

„Um dem Verlangen nach Vorlage eines amtlichen Ausweises zu entsprechen, kann der Endnutzer den elektronischen Identitätsnachweis gemäß § 18 des Personalausweisgesetzes, gemäß § 12 des eID-Karte-Gesetzes oder gemäß § 78 Absatz 5 des Aufenthaltsgesetzes nutzen.“

Da § 7 Absatz 2 TTDSG ausdrücklich die Nutzung von Verfahren nach § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes oder § 78 Absatz 5 des Aufenthaltsgesetzes der

Vorlage des amtlichen Ausweises gleichstellt, wird § 172 Absatz 2 Satz 1 Nummer 1 TKG dahingehend ausgelegt, dass die Identifizierung mit dem elektronischen Identitätsnachweis bereits als hiervon umfasst anzusehen ist. Diese Lesart wird durch § 172 Absatz 2 Satz 7 TKG verstärkt, der ausdrücklich ebenfalls auf die Identifizierung anhand eines elektronischen Identitätsnachweises eingeht. In der Zusammenschau der Rechtsgrundlagen in § 172 Absatz 2 TKG sowie § 7 Absatz 2 TTDSG hat der Gesetzgeber selbst bereits die Entscheidung getroffen, dass die Nutzung des elektronischen Identitätsnachweises für die Zwecke der Überprüfung von Anschlussinhaberdaten zulässig ist. Dies gilt sowohl für die Nutzung des elektronischen Identitätsnachweises durch die Übermittlung von Daten aus dem elektronischen Speicher- und Verarbeitungsmediums des Personalausweises (§ 18 Absatz 2 Satz 1 Nr. 1 PAuswG) als auch aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät (§ 18 Absatz 2 Satz 1 Nr. 2 PAuswG). Für eine Berücksichtigung dieser Verfahren im Rahmen der Verfügung besteht damit kein Regelungsbedarf.

5. Streichung des Verfahrens mit elektronischem Identitätsnachweis

Als Konsequenz dieser Auslegung wird das ehemals vierte Verfahren der Verfügung Nr. 132/2020 (*„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.“*) gestrichen.

Damit steht die Verfügung im Einklang mit der Rechtsauffassung des Verwaltungsgerichts Köln im Klageverfahren gegen eine Vorgängerversion der Verfügung (VG Köln, Urteile vom 13.11.2020 – Az. 9 K 573/18 und 9 K 1378/18), das ein Regelungsmandat der Bundesnetzagentur nur für Identifizierungsverfahren vorsieht, die nicht bereits Niederschlag im Gesetz gefunden haben.

Konsequenz dieser Auslegung ist, dass für eine anlassbezogene Identifikation mit einem elektronischen Identitätsnachweis (eID) ebenso wenig die Vorlage eines Konformitätsnachweises gemäß § 172 Absatz 2 Satz 4 TKG erforderlich sein wird, wie für die Vor-Ort-Vorlage von Identitätsdokumenten gegenüber dem Diensteanbieter, sowie dessen Vertriebspartnern, Händlern bzw. autorisierten Verkaufsstellen, die in den Prozess des Erwerbs der SIM-Karte des Diensteanbieters eingebunden wurden.

6. Speicherung von Daten nach § 172 Absatz 2 Satz 6

Außerdem wird in *Ziffer A.I. Allgemeine Anforderungen* der Verfügung auf die Pflicht zur Speicherung von Informationen gemäß § 172 Absatz 2 Satz 6 TKG eingegangen.

§ 172 Absatz 2 Satz 6 TKG

„Bei der Überprüfung ist die Art des eingesetzten Verfahrens zu speichern; bei Überprüfung mittels eines Dokumentes im Sinne des Satzes 1 Nummer 1 bis 6 sind ferner Angaben zu Art, Nummer und ausstehender Stelle zu speichern.“

Zu Klarstellungszwecken wurden Auslegungen, die die Bundesnetzagentur bislang im Rahmen von FAQ zur Verfügung kommuniziert hatte, in die Verfügung aufgenommen und die Auslegung damit verstetigt.

a) Fallgruppe 1: keine erkennbare ausstellende Stelle

So gilt es für alle Fälle, in denen die ausstellende Stelle nicht erkennbar ist (bspw. auf der portugiesischen ID-Card) oder aufgrund von anderen Sprachzeichen nicht erkennbar bzw. lesbar ist, dass ersatzweise der ausstellende Staat erhoben und gespeichert werden soll.

b) Fallgruppe 2: bei Nutzung des elektronischen Identitätsnachweises kann auf Speicherung der Ausweisnummer verzichtet werden

Weiterhin wird eine Regelung für die Fälle der Nutzung eines eID vorgenommen. Der abschließende Datenkatalog des eID in § 18 Absatz 3 Satz 2 PAuswG enthält nicht die Personalausweisnummer, wie sie auf dem verkörperten Personalausweis aufgedruckt ist.

Der Gesetzgeber sieht die Nutzung des eID im Kontext des § 172 Absatz 2 Satz 7 TKG ausdrücklich vor. Deshalb gilt für die Fälle, bei denen die Identifikation mit einem elektronischen Identitätsnachweis vorgenommen wird, dass auf die Speicherung der Ausweisnummer verzichtet werden kann, sofern keine Vor-Ort-Auslesung des eID mit Personalausweis erfolgt und eine Sichtung des verkörperten Personalausweises durch den Dritten nicht erfolgen kann. Die Pflicht zur Erhebung und Speicherung von Informationen zur Art des Ausweisdokuments und zur Art des Verifizierungsverfahrens bleibt unberührt.

II. Spezifische verfahrensbezogene Erläuterungen

1. Änderung der spezifischen verfahrensbezogenen Anforderungen

Die Anforderungen im Abschnitt *A.II. spezifische verfahrensbezogene Anforderungen* beziehen sich auf die jeweiligen Verfahrensarten. Hiervon betroffen sind die Vor-Ort-Identifikation durch Dritte, die anlassbezogene klassische Video-Identifikation, die anlassbezogene automatisierte Video-Identifikation und der Abgleich bei einer anlassunabhängigen Vorabidentifikation. In der Vorversion der Verfügung wurde statt eines Titels eine knappe Verfahrensbeschreibung gewählt. Nunmehr wird der Verfahrensbeschreibung in Form des Anforderungskatalogs ein abstrakter Verfahrensname vorangestellt.

2. Änderung der Dokumentationsanforderungen

Die Dokumentationspflichten wurden in den verschiedenen Verfahren konkretisiert, indem jeweils die wesentlichen Punkte der Dokumentation spezifiziert wurden, um eine spätere Nachvollziehbarkeit der Umstände der Identifikation gewährleisten zu können. Diese ermöglichen eine Fehleranalyse, sowohl im Rahmen von Qualitätssicherungsmaßnahmen der Diensteanbieter selbst, als auch bei Aufsichtsverfahren der Bundesnetzagentur aufgrund von Hinweisen auf Fehler in den überprüften Anschlussinhaberdatensätzen. Eine Ausnahme stellt insoweit das Vorabidentifikationsverfahren in *Ziffer A.II.4. Abgleich bei anlassunabhängiger Vorabidentifikation* dar, welches einen flexibleren Umgang mit den Dokumentationsanforderungen der Verfahren 1 bis 3 zulässt. Dies geschieht mit dem Ziel, die Nutzung von Synergieeffekten zu erleichtern.

3. Anlassbezogene Vor-Ort-Identifikation durch Dritte (Ziffer A.II.1.)

Die Regelung der Vor-Ort-Identifikation durch Dritte ist inhaltlich weitgehend gleichgeblieben. Insbesondere sind unter dem Begriff des „Dritten“ weiterhin nicht Vertriebspartner der Diensteanbieter erfasst, die am Point-of-Sale tätig sind. Insoweit wurde eine klarstellende Erläuterung in *Ziffer A.II.1.1.3.* des Verfügungstextes aufgenommen.

4. Anlassbezogene klassische Video-Identifikation (Ziffer A.II.2.)

Die Anforderungen an die anlassbezogene klassische Video-Identifikation wurden insbesondere durch eine abstraktere Fassung der Vorgaben für den Identifizierungsvorgang sowohl technologieoffener, als auch barrierefreier gestaltet (z. B. Wegfall der regulatorischen Vorgabe zur verpflichtenden Nutzung von Weißlicht oder Eigenhändigkeit von Bewegungsabläufen).

zu Ziffer A.II.2.1. Anforderungen an das mit der Identifikation beauftragte Personal

Die Anforderungen an das mit der Identifikation beauftragte Personal wurden in diesem Punkt gebündelt dargestellt, vor allem in Bezug auf die zu vermittelnden Schulungsinhalte.

Weiterhin wird darauf hingewiesen, dass für die Durchführung der Schulungen eine Beauftragung externer Stellen nicht verpflichtend, sondern lediglich zulässig ist. Die Nennung der in diesem Kontext aufgeführten Stellen (z. B. Bundeskriminalamt) erfolgt beispielhaft und bestimmt damit den Kreis externer Anbieter nicht abschließend.

zu Ziffer A.II.2.3. Anforderungen an den Identifizierungsvorgang

Die Anforderungen an den Identifizierungsvorgang wurden unter Berücksichtigung des abstrakten Ansatzes sowie der Barrierefreiheit überarbeitet. So wurde bspw. der Punkt 2.(3). aus der Vorversion gestrichen, mit dem die Bundesnetzagentur ausdrücklich eine eigenhändige Bewegung des Identitätsdokuments durch die zu identifizierende Person vor der Kamera vorgeschrieben hatte.

Die neuen Vorgaben der Verfügung sehen vor, dass die Prüfung des Identitätsdokuments sowie der Abgleich mit der zu identifizierenden Person durch geeignete technische und organisatorische Maßnahmen gewährleistet wird. Insoweit erhalten die betroffenen Verpflichteten hierbei einen größeren Gestaltungsspielraum, der ihnen unter anderem die Möglichkeit eröffnet, im Einzelfall auf besondere Umstände und Bedürfnisse der zu identifizierenden Personen einzugehen. Regulatorische Barrieren wurden damit abgebaut.

Mit Blick auf „geeignete Maßnahmen“, die bspw. gemäß *Ziffer A.II.2.3.5.* zu ergreifen sind, um eine Manipulation des Videobildes, des Identitätsdokuments und der zu identifizierenden Person zu erkennen, wird den Unternehmen ein Gestaltungsspielraum bei der Auswahl der zur Zweckerreichung geeigneter Maßnahmen gewährt. Eine Orientierung bieten hierfür etablierte Maßnahmenkataloge aus anderen Rechtsbereichen, wie sie bspw. für das Geldwäschegesetz seitens der BaFin in *Rundschreiben 3/2017 (GW) Videoidentifizierungsverfahren* beschrieben werden oder der im Bereich der elektronischen Vertrauensdienste geltenden Verfügung gemäß § 11 Absatz 1 VDG. Die zielorientierte Formulierung im Anforderungskatalog ermöglicht die Berücksichtigung der jeweils zum Begutachtungszeitpunkt aktuellsten technischen Entwicklungen bei der Auswahl von geeigneten Maßnahmen. Entwicklungen sind beispielsweise

denkbar mit Blick auf Sicherungsmaßnahmen im Kontext von Betrugsversuchen durch sog. „Deepfakes“.

Unter *Ziffer A.II.2.3.5.* wurde zudem ein genereller Hinweis auf die Nutzbarkeit von Ausweisdatenbanken aufgenommen, während dies in der Vorgängerversion bisher nur für ausländische Identitätsdokumente – hier aber verpflichtend – vorgesehen war. Wird eine Ausweisdatenbank nicht als Referenz genutzt, so ist im Rahmen der Begutachtung des Identifizierungsverfahrens darzulegen, inwiefern die anderen technischen und organisatorischen Maßnahmen ausreichend erscheinen, gerade auch mit Blick auf die Schulung des bei der Identifikation eingesetzten Personals.

5. Anlassbezogene automatisierte Video-Identifikation (Ziffer A.II.2.)

Im Zuge der Überarbeitung der Verfügung wurde erstmals ein automatisiertes Identifizierungsverfahren, welches video-basiert ist, aufgenommen. Damit wurde zahlreichen Eingaben aus Wirtschaftskreisen entsprochen, die insbesondere auf die Möglichkeit, derartige Verfahren bereits im Bereich der Vertrauensdienste nutzen zu können, hingewiesen hatten.

Dieses Verfahren wurde zunächst in starker Anlehnung an das klassische Video-Identifikationsverfahren gestaltet, jedoch im Rahmen des Anhörungsverfahrens umfassend insbesondere sprachlich überarbeitet, um die technische Praxis besser zu beschreiben und Unklarheiten auszuräumen.

zu Ziffer A.II.3.2. Anforderungen an den Identifizierungsvorgang

Ähnlich wie bei der klassischen Video-Identifikation soll die automatisierte Video-Identifikation durch das IT-System aus einem Ablauf von einzelnen sukzessiven Identifizierungsschritten bestehen bei denen eine Interaktion mit der zu identifizierenden Person stattfindet. Diese kann bspw. unmittelbar textlich z. B. mittels Chat mit einem Chatbot oder auch sprachlich aufgrund von Anweisungen des IT-Systems gegenüber der zu identifizierenden Person erfolgen.

zu Ziffer A.II.3.2.4.

Außerdem müssen geeignete technische Maßnahmen getroffen werden, um eine Manipulation des Identitätsdokuments und der zu identifizierenden Person sowie ihrer Aufnahmen zu erkennen. Ähnlich wie bei der klassischen Video-Identifikation können hierzu bspw. Maßnahmen zählen, um Deepfakes zu erkennen.

zu Ziffer A.II.3.2.6.

Aus Sicherheitsgründen wurde vorgeschrieben, dass die Interaktion mit der zu identifizierenden Person mindestens im Hinblick auf deren Ablauf variationsreich gestaltet werden muss. Entsprechend dieser Vorgabe müssen Vorkehrungen getroffen werden, sodass bspw. Fragestellungen / Art der Fragen / Anweisungen etc. in einer unterschiedlichen Reihenfolge gestellt bzw. gefordert werden, um Manipulationen des Identifizierungsvorgangs bspw. durch (Mehrfach-)Verwendung von Video-Aufzeichnungen entgegenwirken zu können.

zu Ziffer A.II.3.4. Anforderungen an Transparenz und Einwilligung

In der *Ziffer A.II.3.4. Anforderungen an Transparenz und Einwilligung* wurden besondere Vorschriften für die automatisierte Video-Identifikation aufgenommen, um den datenschutzrechtlichen Vorgaben bei der Verwendung eines automatisierten Datenverarbeitungsmechanismus gerecht zu werden.

zu Ziffer A.II.3.4.1.

Voraussetzung für die Nutzung eines solchen Identifizierungsverfahrens ist es, dass die zu identifizierende Person in die Verarbeitung und Entscheidungsfindung durch ein automatisiertes System ausdrücklich einwilligt, vgl Art. 22 DSGVO. Aus diesem Grund muss die Einwilligung in geeigneter Weise dokumentiert werden. Hierzu könnte bspw. die Aufnahme einer Videosequenz zählen, in der die zu identifizierende Person die Einwilligung erteilt. Ebenfalls ist es zulässig, die Einwilligung dadurch einzuholen und zu dokumentieren, dass in einem Formular ein entsprechendes Häkchen gesetzt sein muss, bevor die weiteren Identifizierungsschritte initialisiert werden können. In diesem Fall ist darauf zu achten, dass das Häkchen zum Zustimmen explizit von der zu identifizierenden Person gesetzt wird und es nicht schon vorher ausgewählt ist. Dieser Vorgang muss entsprechend dokumentiert werden.

Sofern die Einwilligung nicht erteilt wird, muss die zu identifizierende Person auf andere Identifizierungsmethoden hingewiesen werden und die Ablehnung des Verfahrens ist entsprechend zu dokumentieren.

zu Ziffer A.II.3.4.2.

Die zu identifizierende Person muss außerdem ihre Einwilligung zur Aufzeichnung der Identifizierungsschritte geben, mit dem Ziel der Ermöglichung von nachträglichen Stichprobenüberprüfungen. Die Einwilligung ist auch hier in geeigneter Weise zu dokumentieren. Die oben zu Ziffer 3.4.1 gemachten Ausführungen zu geeigneten Dokumentationsmöglichkeiten der Einwilligung gelten hier ebenfalls.

zu Ziffer A.II.3.6.1.

Vor der Nutzung eines IT-Systems für Zwecke der Identifizierung im Rahmen der automatisierten Video-Identifikation muss die Gewähr dafür bestehen, dass dieses System mit Blick auf seine Performanz (Korrektheit) hinreichend erprobt ist. Als geeignetes Instrument zur Bewertung der Performanz sind in der Verfügung angemessene Robustheits- und Penetrationstests vorgesehen. Als angemessen werden insbesondere Robustheits- und Penetrationstests anerkannt, die den Maßstäben entsprechen, die in den ergänzenden Bewertungskriterien zu innovativen Identifikationsmethoden im Bereich der eIDAS Verordnung und der elektronischen Vertrauensdienste vorgegeben sind. Insoweit kann ein für diesen Bereich erhaltenes Zertifikat als hinreichender Nachweis der Erfüllung dieser spezifischen Anforderung der hiesigen Verfügung angesehen werden. Die ergänzenden Bewertungskriterien können interessierten Stellen auf Anfrage zur Verfügung gestellt werden.

zu Ziffer A.II.3.8. Anforderungen an ein kontinuierliches Qualitätsmanagement

Da es sich um ein neu in der Verfügung verankertes Verfahren handelt, das den Identifizierungsvorgang im Prinzip ohne direkte menschliche Beteiligung auf Seiten des Diensteanbieters ermöglicht, soll im Rahmen dieser Anforderung eine Erfolgskontrolle erfolgen. Bei der Gestaltung des kontinuierlichen Qualitätsmanagementsystems gewährt die Bundesnetzagen-

tur den Diensteanbietern wiederum einen Gestaltungsspielraum – sie sollen geeignete technische oder organisatorische Maßnahmen vorsehen. In jedem Fall haben die Diensteanbieter die im Praxisbetrieb durchgeführten Identifikationen stichprobenhaft manuell also durch Einsatz von Personal nachträglich zu überprüfen. Deshalb gilt für das mit der Stichprobenüberprüfung beauftragte Personal sogleich die Schulungspflicht wie bei der klassischen Video-Identifikation.

Die Stichprobenüberprüfung soll die Bewertung und Qualität des automatisierten Verfahrens sicherstellen. Anhand der Ergebnisse der Stichprobenüberprüfungen können ggf. Änderungen an den Parametern des Systems angepasst bzw. verändert werden, um eine bestmögliche Qualität der Identifikationen zu erreichen.

zu Ziffer A.II.3.8.1.

Bei der Auswahl der Qualitätssicherungsmaßnahmen kann wiederum auf die ergänzenden Bewertungskriterien zu innovativen Identifikationsmethoden im Bereich der eIDAS Verordnung und der elektronischen Vertrauensdienste Bezug genommen werden. Die darin enthaltenen Performanz- und Robustheitstests können auch im laufenden Betrieb angemessene Sicherheitsmaßnahmen darstellen. Die ergänzenden Bewertungskriterien können interessierten Stellen auf Anfrage zur Verfügung gestellt werden.

Es wird empfohlen dritte Stellen, insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), mit der Durchführung von Robustheits- und Penetrationstest zu beauftragen. Außerdem wird empfohlen, sich an den Praxisleitfäden des BSI zu IT-Sicherheits-Penetrationstest und IT-Sicherheits-Webchecks[1] zu orientieren, um eine größtmögliche Sicherheit des IT-Systems gewährleisten zu können.

zu Ziffer A.II.3.8.2.

Die verpflichtend durchzuführenden Stichprobenüberprüfungen sind innerhalb von sieben Tagen nach Beendigung des Identifizierungsvorgangs durchzuführen. Aus datenschutzrechtlichen Erwägungen wurden konkrete Zeitvorgaben für die Löschung der hierfür erforderlichen Nachweisdaten in der Verfügung festgelegt. Die erhobenen Nachweisdaten (vgl. *Ziffer A.II.3.2.2. der Verfügung*) sind in der Regel nach Ablauf von sieben Tagen zu löschen.

In Ausnahmefällen, wie z.B. bei Aufdeckung von Hinweisen auf Betrugsfälle oder Betrugsversuche sowie bei sonstigen Problemen oder Fehlern bei der Stichprobenüberprüfung, können die Nachweisdaten bis zum Abschluss einer Analyse bis zu vier Wochen aufbewahrt werden. Darüber hinaus kann in besonders begründeten Einzelfällen, wenn bspw. der Analyseaufwand sehr hoch ist oder die Analyse innerhalb dieser vier Wochen nicht stattfinden konnte, aufgrund von z. B. Urlaub oder Krankheit, eine längere Aufbewahrung zulässig sein, jedoch nicht länger als maximal acht Wochen nach Beendigung des Identifizierungsvorgangs.

6. Abgleich bei anlassunabhängiger Vorabidentifikation (Ziffer A.II.4)

Die Regelung zur Vorabidentifikation wurde überarbeitet, mit Blick auf die Anforderungen konkretisiert und an den aktuellen Entwicklungen im Bereich der digitalen Identitäten ausgerichtet.

[1] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html

Zur Abgrenzung von Identifikationen, die spezifisch zur Erfüllung der Pflichten nach § 172 TKG erfolgen und solchen, die zu einem vorherigen Zeitpunkt und aus einem Anlass ohne Bezug zum TKG stattgefunden haben, wurde begrifflich zwischen „anlassbezogenen“ und „anlassunabhängigen“ Identifikationen unterschieden.

zu Ziffer A.II.4.1. Anforderungen an den Datenabgleich und den vorherigen Identifizierungsvorgang

In *Ziffer A.II.4.1.1.* werden zwei Alternativen für einen Datenabgleich bei Vorabidentifikationen aufgezeigt:

Alternative a)

In *Alternative a)* wird das Verfahren beschrieben, wenn die Daten des künftigen Anschlussinhabers aus einer vorherigen Identifikation, die ohne einen Bezug zum TKG durchgeführt wurde, bei einem Dritten vorliegen. Diese Daten müssen mithilfe einer Vor-Ort-Vorlage beim Diensteanbieter oder eines anderen in der Verfügung beschriebenen Verfahrens erhoben worden sein und mithilfe eines Identitätsdokuments im Sinne des § 172 Absatz 2 Satz 1 TKG überprüft worden sein. Die anlassbezogene Prüfung erfolgt dann mithilfe des vorliegenden Datensatzes.

Alternative b)

In *Alternative b)* wird das Verfahren beschrieben, wenn die Daten des künftigen Anschlussinhabers, die ohne einen Bezug zum TKG erhoben wurden, bei der zu identifizierenden Person selbst vorgehalten werden. Diese Daten müssen mithilfe einer Vor-Ort-Vorlage beim Diensteanbieter oder eines anderen in der Verfügung beschriebenen Verfahrens erhoben und mithilfe eines Identitätsdokuments im Sinne des § 172 Absatz 2 Satz 1 TKG überprüft worden sind. Die anlassbezogene Prüfung erfolgt auch hier mithilfe des vorgehaltenen Datensatzes.

Für beide Alternativen gilt, dass die vorherige Identifikation die Anforderungen des jeweiligen Verfahrens in der Verfügung erfüllen muss. Im Fall der beschriebenen Dokumentationspflichten der *Ziffern A.II.1.2.2. und A.II.2.4.2.* können durch andere geeignete Informationen zur Dokumentation ersetzt werden, um Synergieeffekte nutzen zu können. Wichtig ist, dass die Umstände der Identifikation hieraus hervorgehen.

zu Ziffer A.II.4.1.3.

Es soll durch technische und / oder organisatorische Maßnahmen sichergestellt werden, dass die Daten aus der vorherigen Identifikation stets in ihrer Integrität geschützt sind und hierbei einer angemessenen Aktualitätsprüfung unterliegen. Das heißt, die erhobenen und mit Hilfe eines Identitätsdokuments überprüften Daten sollen vor Veränderung und nachträglicher Manipulation stets geschützt sein – sei es beim Dritten oder der zu identifizierenden Person selbst. Die Aktualisierung der Daten insbesondere mit Blick auf Adressinformationen ist hingegen nicht nur zulässig, sondern auch in der Verfügung ausdrücklich vorgeschrieben. Damit wird dem Umstand Rechnung getragen, dass zwischen der ursprünglichen Identifikation und der Verwendung der Datensätze für die Identifikation gemäß § 172 Abs. 2 TKG ein unbestimmt langer Zeitraum liegen kann. Die Verfügung zählt eine Reihe von plausiblen Maßnahmen zur Sicherstellung der Aktualität auf, die jedoch nicht abschließend ist.

Unerlässlich ist, dass die Anpassung unter direkter Einbindung der identifizierten Person stattfindet, die sich hierbei durch erneute Identifikation oder auf andere zuvor festgelegte Art legitimiert (z. B. TAN-Verfahren). Sofern die Aktualisierung eine Namensänderung umfasst, ist stets eine Neu-Identifikation erforderlich.

zu Ziffer A.II.4.2.1.

Sofern die Daten für die Zwecke eines Datenabgleichs oder -abrufs übermittelt werden, sollen stets dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit, insbesondere Vertraulichkeit sowie Integrität gewährleistet werden. Dies kann bspw. durch Verschlüsselung, Abgleich von Hashwerten oder anderen Maßnahmen sichergestellt werden.