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

## A. 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 TKG nutzen. Auf die Geltung von § 7 Absatz 2 TTDSG wird hingewiesen. Die Nutzung anderer Identitätsdokumente ist nicht zulässig. Für einzelne Verfahren können Einschränkungen vorgesehen sein.
2. 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 Diensteanbieter gespeichert werden können.
   Hierbei ist folgendes zu beachten:
   2.1. In Fällen, in denen die Identitätsdokumente die ausstellende Stelle nicht erkennen lassen, soll ersatzweise die Angabe zum ausstellenden Staat erhoben und gespeichert werden.
   2.2. Bei Identifikation mit dem elektronischen Identitätsnachweis kann auf die Erhebung und Speicherung der Ausweisnummer in den Fällen verzichtet werden, in denen keine Vor-Ort-Auslesung des eID mit Personalausweis erfolgt und eine Sichtung des verkörperten Personalausweises durch den Dritten nicht erfolgen kann.

### II. Spezifische verfahrensbezogene Anforderungen

#### 1. Anlassbezogene Vor-Ort-Identifikation durch Dritte

**1.1. Anforderungen an den Identifizierungsvorgang**

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

1.1.2. Die Daten der zu identifizierenden Person sind zu erheben und anhand des vorgelegten Identitätsdokuments zu überprüfen. Sofern die Daten bereits erhoben wurden, ist ein Abgleich vorzunehmen. Zudem muss sich vergewissert werden, dass die vorstellige zu identifizierende Person mit der im Identitätsdokument ausgewiesenen Person übereinstimmt.

1.1.3. Nicht als Dritter im Sinne des in *Ziffer A.II.1.* festgelegten Verfahrens gilt, wer als Vertriebspartner, Händler bzw. autorisierte Verkaufsstelle in den Prozess des Erwerbs der SIM-Karte des Anbieters eingebunden wurde.

### 1.2. Anforderungen an die Dokumentation

1.2.1. 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.

1.2.2. Zu den wesentlichen Punkten der Dokumentation gehören:

1.2.2.1. Wann wurde der Identifizierungsvorgang durchgeführt?

1.2.2.2. Wo wurde der Identifizierungsvorgang durchgeführt?

1.2.2.3. Wer ist die den Identifizierungsvorgang durchführende Person?

1.2.2.4. Wer ist die zu identifizierende Person?

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

## 2. Anlassbezogene klassische Video-Identifikation

### 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:

2.1.1.1. Kenntnis der mittels Videoidentifizierung prüfbaren Sicherheitsmerkmale

2.1.1.2. Kenntnis der anzuwendenden Prüfverfahren für diejenigen Identitätsdokumente, die im Rahmen des Videoidentifizierungsverfahren akzeptiert werden

2.1.1.3. Kenntnis über gängige Fälschungsmöglichkeiten der Identitätsdokumente

2.1.1.4. Kenntnis über Hinweise bzw. Maßnahmen zur Feststellung von Willensmängeln bei der zu identifizierenden Person (bspw. Zwang, Social Engineering o.Ä.)

2.1.1.5. Kenntnis über maßgebliche telekommunikations- und datenschutzrechtliche Vorschriften, sowie die gestellten Anforderungen dieser Verfügung.

2.1.2. Die Schulung muss in regelmäßigen Abständen (mindestens einmal jährlich) sowie bei Bedarf aktualisiert werden. Ein Aktualisierungsbedarf 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.

2.1.3. Die Beauftragung einer externen Stelle zur Durchführung der Schulungen ist zulässig. Beispielsweise können mit Identitätsprüfungen oder der Prüfung von Ausweisdokumenten vertraute öffentliche Stellen oder allgemein anerkannte Stellen beauftragt werden (z. B. Bundeskriminalamt).

2.1.4. Zu den oben genannten Schulungsinhalten sowie zur Durchführung der Schulungsmaßnahmen muss eine geeignete Dokumentation vorliegen.

### 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 sowie über einen maschinenlesbaren Raum verfügen.

2.2.2. Zu den optisch prüfbaren Sicherheitsmerkmalen zählen jeweils unter anderem (je nach Dokument):

2.2.2.1. beugungsoptisch wirksame Merkmale:

2.2.2.1.1. Hologramme

2.2.2.1.2. Identigram

2.2.2.1.3. kinematische Strukturen

2.2.2.2. Personalisierungstechnik:

2.2.2.2.1. Laserkippbilder

2.2.2.2.2. Ausfüllschrift

2.2.2.3. Material:

2.2.2.3.1. Fenster (z. B. personalisiert)

2.2.2.3.2. Sicherheitsfaden (personalisiert)

2.2.2.3.3. optisch variable Farbe

2.2.2.4. Sicherheitsdruck:

2.2.2.4.1. Mikroschrift

2.2.2.4.2. Guillochenstruktur

**2.3. Anforderungen an den Identifizierungsvorgang**

2.3.1. Die Identifizierung, die durch das mit der Identifikation beauftragte Personal durchgeführt wird, muss mittels einer Videoübertragung mit sprachlicher oder unmittelbarer textlicher Kontaktaufnahme (z.B. Chat) in Echtzeit und ohne Unterbrechung stattfinden.

2.3.2. Bei der Zuteilung eines Identifizierungsvorgangs an die im konkreten Fall mit der Identifikation beauftragte Person müssen Mechanismen eingesetzt werden, die einer vorhersehbaren Zuteilung von Identifizierungsvorgängen und damit der dadurch bestehenden Möglichkeit einer Manipulation entgegenwirken.

2.3.3. 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.

2.3.4. Der Anlass für die Identifikation ist durch die zu identifizierende Person zu bestätigen, auch damit für diese klar ersichtlich ist, wofür sie sich identifiziert.

2.3.5. Die Echtheit des Identitätsdokuments ist im Rahmen einer Gültigkeits- und Plausibilitätsprüfung unter Einbeziehung der in *Ziffer 2.2.2.* genannten Sicherheitsmerkmale zuverlässig zu prüfen, ebenso wie die Zugehörigkeit zu der zu identifizierenden Person. Es sind geeignete Maßnahmen zu ergreifen, um eine Manipulation des Videobildes, des Identitätsdokuments und der zu identifizierenden Person zu erkennen. Hierzu können sowohl organisatorische als auch technische Maßnahmen gehören, die durch Interaktion mit dem verwendeten Ausweisdokument oder der zu identifizierenden Person gemäß Anweisung der die Identifikation durchführenden Person, eine Manipulation erkennbar machen. Eine regelmäßig aktualisierte Ausweisdatenbank kann zu Referenzzwecken genutzt werden. Ferner können Maßnahmen getroffen werden, um eine Veränderung des Videostreams zu erkennen.

2.3.6. Überdies ist die Übereinstimmung der, vorher gemäß § 172 Absatz 2 Satz 1 TKG, erhobenen Daten mit den im Identitätsdokument enthaltenen Daten in geeigneter Weise zu 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.

**2.4. Anforderungen an die Dokumentation**

2.4.1. 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.

2.4.2. Zu den wesentlichen Punkten der Dokumentation gehören:

2.4.2.1. Wann wurde der Identifizierungsvorgang durchgeführt?

2.4.2.2. Wer ist die durchführende Person?

2.4.2.3. Wer ist die zu identifizierende Person?

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

**2.5. Räumliche Anforderungen**

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

**2.6. Technische Anforderungen**

2.6.1. 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.

2.6.2. 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).

2.6.3. 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. Abbruch des Identifizierungsvorgangs

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

2.7.2. 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.

## 3. Anlassbezogene automatisierte Video-Identifikation

### 3.1. Anforderungen an geeignete Identitätsdokumente

3.1.1. Für dieses Verfahren zugelassene Identitätsdokumente müssen über ausreichend fälschungssichere und mittels verfügbarer Technik im Verfahren prüfbare Sicherheitsmerkmale sowie über einen maschinenlesbaren Raum verfügen.

3.1.2. Zu den optisch prüfbaren Sicherheitsmerkmalen zählen jeweils unter anderem (je nach Dokument):

- 3.1.2.1. beugungsoptisch wirksame Merkmale:
  - 3.1.2.1.1. Hologramme
  - 3.1.2.1.2. Identigram
  - 3.1.2.1.3. kinematische Strukturen
- 3.1.2.2. Personalisierungstechnik:
  - 3.1.2.2.1. Laserkippbilder
  - 3.1.2.2.2. Ausfüllschrift
- 3.1.2.3. Material:
  - 3.1.2.3.1. Fenster (z.B. personalisiert)
  - 3.1.2.3.2. Sicherheitsfaden (personalisiert)
  - 3.1.2.3.3. optisch variable Farbe
- 3.1.2.4. Sicherheitsdruck:
  - 3.1.2.4.1. Mikroschrift
  - 3.1.2.4.2. Guillochenstruktur

### 3.2. Anforderungen an den Identifizierungsvorgang

3.2.1. Ein Identifizierungsvorgang, der durch ein IT-System durchgeführt wird, hat aus einem automatisierten Ablauf von einzelnen sukzessiven Identifizierungsschritten zu bestehen. Diese müssen zeitlich zusammenhängend erfolgen und zwecks Lebenderkennung eine unmittelbare Interaktion zwischen der zu identifizierenden Person und dem IT-System umfassen.

3.2.2. Die wesentlichen Schritte des Identifizierungsvorgangs sind in ihrem zeitlichen Ablauf zur Ermöglichung einer nachträglichen Stichprobenüberprüfung in geeigneter Weise zu dokumentieren. Hierzu können sowohl die Aufnahme von Videosequenzen mit Ton,

Bilddaten der zu identifizierenden Person und des Identitätsdokuments, als auch die Erfassung der visuellen und maschinenlesbaren Zone des Identitätsdokuments gehören.

3.2.3. Während des gesamten Identifizierungsvorgangs muss eine ausreichende Bild- und ggf. Tonqualität gegeben sein, um eine zweifelsfreie Identifizierung anhand aller in dieser Verfügung geforderten Prüfungen uneingeschränkt zu ermöglichen.

3.2.4. Die Echtheit des Identitätsdokuments ist im Rahmen einer Gültigkeits- und Plausibilitätsprüfung unter Einbeziehung der in *Ziffer 3.1.2.* genannten Sicherheitsmerkmale zuverlässig zu prüfen, ebenso wie die Zugehörigkeit zu der zu identifizierenden Person. Es sind geeignete technische Maßnahmen zu ergreifen, um eine Manipulation des Identitätsdokuments und der zu identifizierenden Person sowie ihrer Aufnahmen zu erkennen. Eine regelmäßig aktualisierte Ausweisdatenbank kann zu Referenzzwecken genutzt werden.

3.2.5. Überdies ist die Übereinstimmung der vorher gemäß § 172 Absatz 2 Satz 1 TKG erhobenen Daten mit den im Identitätsdokument enthaltenen Daten in geeigneter Weise zu 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.

3.2.6. Im Rahmen des Identifizierungsprozesses muss die Interaktion mit der zu identifizierenden Person mindestens im Hinblick auf deren Ablauf variationsreich in Bezug auf Reihenfolge und / oder Art der gestellten Fragen / Anweisungen sein.

3.2.7. Die technische Überprüfung der erhobenen Nachweisdaten (*vgl. Ziffer 3.2.2*) muss im unmittelbaren zeitlichen Anschluss an die automatisierte Durchführung der sukzessiven Identifizierungsschritte in einer vertrauenswürdigen, kontrollierten Umgebung erfolgen, *vgl. Ziffer 3.5.1.*

### 3.3. Anforderungen an die Dokumentation

3.3.1. Die wesentlichen Punkte des Identifizierungsvorgangs sind in geeigneter Weise zu dokumentieren, um eine spätere Nachvollziehbarkeit der Umstände der Identifikation gewährleisten zu können.

3.3.2. Zu den wesentlichen Punkten der Dokumentation gehören:

3.3.2.1. Wann wurde der Identifizierungsvorgang durchgeführt?

3.3.2.2. Wer ist die zu identifizierende Person?

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

3.3.2.4. Mit welchem IT-System (inkl. Versionskennung) wurde der Identifizierungsvorgang durchgeführt?

### 3.4. Anforderungen an Transparenz und Einwilligung

3.4.1. Die zu identifizierende Person hat der durch automatisierte Entscheidungsfindungssysteme erfolgende Verarbeitung Ihrer Daten ausdrücklich zuzustimmen. Die Einwilligung ist in geeigneter Weise zu dokumentieren.

3.4.2. Ferner hat die zu identifizierende Person zu Beginn der automatisierten Identifikation ihre ausdrückliche Einwilligung zur Aufzeichnung der Identifizierungsschritte mit dem Ziel der Ermöglichung von Stichprobenüberprüfungen im Rahmen eines kontinuierlichen Qualitätsmanagements entsprechend der Vorgaben nach *Ziffer 3.8.1. und 3.8.2.* zu erklären. Die Einwilligung ist in geeigneter Weise zu dokumentieren.

3.4.3. Eine Nutzung der Nachweisdaten (*vgl. Ziffer 3.2.2.*) zum Zwecke der Verbesserung des IT-Systems sowie zu vergleichbaren Zwecke sind nicht Gegenstand dieser Verfügung. Jedoch schließt sie diese Nutzung nicht aus, sofern die erforderlichen datenschutzrechtlichen Voraussetzungen vorliegen.

3.4.4. Vorab sind der zu identifizierenden Person aussagekräftige Informationen zu vermitteln über die beim Einsatz automatisierter Entscheidungsfindungssysteme involvierte Technologie und Logik sowie die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung. Selbiges gilt für den Umfang der Einwilligung (z. B. worauf bezieht sich die Einwilligung im Einzelnen, welche Art der Datenverarbeitung ist vorgesehen, durch wen und wie lange werden die Daten gespeichert, was geschieht mit

den Daten bei Abbruch der Identifizierung bzw. nach Abschluss der Stichprobenüberprüfung).

### 3.5. Räumliche Anforderungen

3.5.1. Die zur automatisierten Identifikation nach diesem Verfahren genutzten IT-Systeme müssen sich permanent in abgetrennten und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.

### 3.6. Technische Anforderungen

3.6.1. Das zur automatisierten Identifikation genutzte IT-System muss eine ausreichende Performanz (Korrektheit) gewährleisten, die durch angemessene Robustheits- sowie Penetrationstests überprüft wurde.

3.6.2. Die automatisierte Interaktion und Kommunikation sowie der Upload der erhobenen Nachweisdaten (*vgl. Ziffer 3.2.2.*) und ihre Speicherung sind in Bezug auf Integrität und Vertraulichkeit ausreichend abzusichern. Aus diesem Grund sind nur Ende-zu-Ende verschlüsselte Verfahren 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.

3.6.3. 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).

3.6.4. 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.

### 3.7. Abbruch des Identifizierungsvorgangs

3.7.1. Ist die visuelle Überprüfung, etwa aufgrund von schlechten Lichtverhältnissen oder einer schlechten Bildqualität/-übertragung und / oder ist eine Interaktion bzw. Kommunikation mit der zu identifizierenden Person nicht möglich, ist der Identifizierungsprozess abzubrechen.

3.7.2. 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.

### 3.8. Anforderungen an ein kontinuierliches Qualitätsmanagement

3.8.1. 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 (*vgl. Ziffer 3.2.2.*) die Ergebnisse der automatisierten Prüfungen in *Ziffer 3.2.4. und 3.2.5.* überprüft.

3.8.2. Die Stichprobenüberprüfung hat innerhalb von 7 Tagen nach Beendigung des Identifizierungsvorgangs stattzufinden. Die erhobenen Nachweisdaten (*vgl. Ziffer 3.2.2.*) 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.

3.8.3. Für die Qualifikation des mit der Stichprobenüberprüfung beauftragten Personals gilt *Ziffer 2.1.1.* entsprechend.

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

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

## 4. Abgleich bei anlassunabhängiger Vorabidentifikation

### 4.1. Anforderungen an den Datenabgleich und den vorherigen Identifizierungsvorgang

4.1.1. 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 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 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 erfüllen. Die in den *Ziffern A.II.1.2.2 und A.II.2.4.2.* aufgestellten Dokumentationspflichten können hierbei durch andere geeignete Informationen zu den Umständen der Identifikation ersetzt werden.

4.1.2. Statt eines Datenabgleichs der vorgehaltenen Daten mit den erhobenen Daten ist auch ein Datenabruf zulässig, vgl. Art. 6 Absatz 1 lit. c DSGVO in Verbindung mit § 172 Absatz 1 Satz 1 sowie Absatz 2 Satz 1 TKG.

4.1.3. Der Dritte hat durch geeignete technische und / oder organisatorische Maßnahmen sicherzustellen, dass die vorgehaltenen Daten in ihrer Integrität geschützt sind und hierbei einer angemessenen Aktualitätsprüfung unterliegen. Dies kann beispielsweise durch Vorsehen einer Neu-Identifikation bei Ablauf des Gültigkeitsdatums des genutzten Identitätsdokuments oder einer Aktualisierungspflicht in den Nutzungsbedingungen oder durch eine regelmäßige Aktualisierungsabfrage erfolgen.

### 4.2. Technische Anforderungen

4.2.1. Bei Übermittlungen für Zwecke des Datenabgleichs oder -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.

### 4.3. Anforderungen an die Einwilligung

4.3.1. Bei Alternative a) ist sicherzustellen, dass die Übermittlung der vorgehaltenen Daten durch den Dritten an den Diensteanbieter nur erfolgt, soweit die zu identifizierende Person nach einem vorgesehenen Verfahren verbunden mit einer Authentifizierung der zu identifizierenden Person (etwa durch Eingabe einer PIN) zugestimmt hat. Eine Initiierung

der Übermittlung zwischen dem Dritten und dem Diensteanbieter unmittelbar durch die zu identifizierende Person kann ebenso möglich sein.

4.3.2. 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. Diese ist in geeigneter Weise zu dokumentieren.

### III. Zeitliche Geltung

1. Diese Festlegung gilt **rückwirkend ab dem 1. Dezember 2021**. Sie ersetzt ab diesem Zeitpunkt die Festlegung in Verfügung Nr. 132/2020 im Amtsblatt der Bundesnetzagentur 24/2020, S. 1888 ff. (Stand: 16.12.2020). Diese Allgemeinverfügung gilt abweichend von § 210 Satz 3 TKG entsprechend § 41 Absatz 4 Satz 4 Verwaltungsverfahrensgesetz (VwVfG) am Tag nach ihrer Bekanntmachung im Amtsblatt der Bundesnetzagentur als bekannt gegeben.
2. Gemäß § 230 Absatz 9 TKG kann die Bundesnetzagentur festlegen, dass für eine von ihr zu bestimmende Übergangszeit von nicht mehr als zwölf Monaten auf das Erfordernis eines vorherigen Konformitätsnachweises verzichtet werden kann. Die Bundesnetzagentur macht hiermit von dieser Ermächtigung Gebrauch: Es wird festgelegt, dass das vorherige Nachweiserfordernis in § 172 Absatz 2 Satz 4 TKG erst mit Wirkung **ab dem 1. Dezember 2022** gilt.

## B. Begründung

### I. Rechtsgrundlage, Konformitätsbewertung, Übergangsregelung

Im Bundesgesetzblatt Nr. 35 vom 28. Juni 2021 wurde mit dem Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) die Neufassung der Regelung über Daten für Auskunftsersuchen der Sicherheitsbehörden in § 172 (bislang § 111) des Telekommunikationsgesetzes (TKG) verkündet. Sie tritt am 1. Dezember 2021 in Kraft.

In § 172 Absatz 2 Satz 3 TKG wird der Bundesnetzagentur die Aufgabe zugewiesen, 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.

Hiermit wird nach Anhörung der betroffenen Kreise gemäß § 172 Absatz 2 Satz 3 TKG festgelegt, welche Anforderungen an solche anderen geeigneten Verfahren zu stellen sind. Die Feststellung der Übereinstimmung eines konkreten Verfahrens mit der Festlegung der Bundesnetzagentur wird gemäß § 172 Absatz 2 Satz 4 TKG zukünftig durch Konformitätsbewertungsstellen getroffen.

Die Bundesnetzagentur erteilt keine rechtsverbindlichen Auskünfte zur Konformität von konkreten Identifizierungsverfahren mit den Vorgaben im oben aufgeführten Katalog. Die Feststellung der Übereinstimmung eines konkreten Verfahrens mit der Festlegung der Bundesnetzagentur wird gemäß § 172 Absatz 2 Satz 4 TKG zukünftig durch Konformitätsbewertungsstellen getroffen.

Entsprechend der gesetzgeberischen Vorgabe in § 172 Absatz 2 Satz 4 TKG haben Anbieter von im Voraus bezahlten Mobilfunkdiensten (Diensteanbieter) 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.

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. Sobald nähere Informationen zur Konformitätsüberprüfung verfügbar sind, werden diese auf der Internetseite der Bundesnetzagentur bzw. als Mitteilung im Amtsblatt veröffentlicht.

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

Grundsätzlich gilt, dass die Diensteanbieter die Anforderungen im oben aufgeführten Katalog 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.

## II. Regelungsumfang dieser Verfügung

§ 172 TKG sieht zunächst in Absatz 1 Satz 1 eine Erhebung und Speicherung von enumerativ aufgelisteten Daten für die Auskunftsverfahren nach den §§ 173 und 174 TKG vor. Aus Sinn und Zweck der Vorschrift ergibt sich, dass es sich bei den erhobenen Daten um vollständige und zutreffende Daten handeln soll. In Absatz 2 sieht der Gesetzgeber in diesem Sinne eine noch weitergehende Überprüfungspflicht für diejenigen Daten vor, die von Anbietern von im Voraus bezahlten Mobilfunkdiensten erhoben wurden. Dieser Überprüfung von Daten geht damit immer denknotwendig eine Erhebung derjenigen Daten voraus, die zu überprüfen sind.

Als Regelfall sieht § 172 Absatz 2 Satz 1 TKG die Überprüfung der Anschlussinhaberdaten anhand einer Vorlage von Identitätsdokumenten vor, worunter eine Vor-Ort Prüfung unter Anwesenden zu verstehen ist. Lediglich für juristische Personen und Personengesellschaften kann der Vorlagebegriff weiter verstanden werden, da in § 172 Absatz 2 Satz 1 Nr. 7 TKG ergänzend die Einsichtnahme in die relevanten Dokumente / Register zugelassen wird.

Diese Verfügung legt Anforderungen an andere geeignete Verfahren für die Überprüfung der Anschlussinhaberdaten fest, sofern es sich beim Anschlussinhaber um eine natürliche Person handelt. Im obenstehenden Katalog wird der Anschlussinhaber mit dem neutraleren Begriff der „zu identifizierenden Person“ referenziert.

Wie bereits dargelegt, handelt es sich bei der Überprüfungspflicht um eine Verpflichtung, die in engem Zusammenhang zu dem in § 172 Absatz 1 Satz 1 TKG geregelten Vorgang der Datenerhebung steht. Daher werden in dieser Verfügung Anforderungen an die Tätigkeit der Datenerhebung als den der Datenüberprüfung 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.

Die in dieser Verfügung festgelegten aufsichtsrechtlichen Anforderungen gelten unbeschadet der parallel zu beachtenden gesetzlichen, insbesondere datenschutzrechtlichen Anforderungen.

## III. Inhaltliche Neugestaltung im Vergleich zur Vorversion

Mit dieser Verfügung wird die Festlegung der Bundesnetzagentur im Vergleich zur Vorversion (Verfügung Nr. 132/2020) zum Teil umfangreich neugestaltet.

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 und bisherige Verfahrensdarstellungen strukturell neu geordnet.

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.

Die Regelung zur 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 den Verfügungstext aufgenommen, vgl. *Ziffer A.II.1.1.3.*

Die Ausgestaltung des klassischen Video-Identifizierungsverfahrens wurde 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). Darüber hinaus begrüßt die Bundesnetzagentur, wenn die gemäß § 172 TKG verpflichteten Unternehmen ihr Identifizierungsangebot auf größtmögliche Barrierefreiheit ausrichten, soweit dies mit regulatorischen Vorgaben vereinbar ist.

Nähere Hinweise zur Eignung bestimmter Sicherheitsmaßnahmen beabsichtigt die Bundesnetzagentur in einer diese Verfügung erläuternden Handreichung zu veröffentlichen. Hierbei wird auch auf regulatorische Vorgaben aus anderen Rechtsbereichen Bezug genommen werden.

Ein Verfahren zur Video-Identifikation mit automatisierten Entscheidungsfindungssystemen unter Nutzung von Neuentwicklungen im Bereich Künstlicher Intelligenz wurde erstmalig als anderes geeignetes Verfahren im Sinne des § 172 Absatz 2 Satz 3 TKG aufgenommen. Hierbei wurde einem kontinuierlichen Qualitätsmanagement mit Stichprobenüberprüfungen durch entsprechend geschultes

Personal ebenso ein hoher Stellenwert eingeräumt, wie spezifischen datenschutzrechtlichen Belangen, die mit einem solchen Verfahren einhergehen.

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

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.

Im Lichte der Neuregelung in § 7 Absatz 2 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) wurde auf die Regelung des Identifikationsverfahrens mit einem elektronischen Identitätsnachweis verzichtet. Der Regelungsbedarf besteht insofern nicht mehr, da bereits der Gesetzgeber eine Gleichstellung der Nutzung entsprechender Verfahren nach § 18 des Personalausweisgesetzes, § 12 des eID-Karte-Gesetzes oder § 78 Absatz 5 des Aufenthaltsgesetzes gegenüber der Vorlage eines amtlichen Ausweises geregelt hat.

Nähere Informationen und Erläuterungen zu dieser Verfügung können der Handreichung entnommen werden, die in engem zeitlichen Zusammenhang zur Verfügung veröffentlicht wird.

## IV. Berücksichtigung von Stellungnahmen im Rahmen des Anhörungsverfahrens

In Amtsblattmitteilung Nr. 271/2021 vom 13.10.2021 wurde eine Entwurfsfassung der neugestalteten Verfügung veröffentlicht und eine erneute Anhörung eingeleitet. Zum einen wurde unter Beteiligung von knapp 30 Teilnehmern aus Industrie und Verwaltung eine Online-Anhörung am 28.10.2021 durchgeführt. Darüber hinaus bestand die Möglichkeit zur ergänzenden Eingabe von schriftlichen Stellungnahmen bis zum 10.11.2021.

Die mündlichen und schriftlich eingegangenen Stellungnahmen wurden zum Anlass genommen die Verfügung punktuell noch einmal zu überarbeiten, insbesondere mit Blick auf die nachfolgend dargestellten Punkte:

Verfahrensübergreifend wurde die Ausgestaltung der Dokumentationspflichten überarbeitet und aus datenschutzrechtlichen Gründen wurde eine klarstellende Bezugnahme auf die Rechtsgrundlage für Datenerhebungstätigkeiten im Rahmen der Identifizierungsvorgänge ergänzt.

Zum Verfahren in *Ziffer A.II.1.* wurde auf Anregung der beteiligten Verbände (Bitkom/VATM) eine Erläuterung in *Ziffer 1.1.3.* aufgenommen. Diese hat klarstellenden Charakter und steht im Einklang mit der Rechtsauffassung des Verwaltungsgerichts Köln in Klageverfahren gegen die Verfügung (VG Köln, Urteile vom 13.11.2020 - Az. 9 K 573/18, 9 K 574/18 und 9 K 1378/18).

Im Verfahren in *Ziffer A.II.2.* wurden ebenfalls auf Anregung der beteiligten Verbände (Bitkom/VATM) die Anforderungen an die Schulung des bei der Video-Identifikation eingesetzten Personals dahingehend konkretisiert, dass für die Durchführung der Schulungen eine Beauftragung externer Stellen nicht verpflichtend, sondern lediglich zulässig ist. Die Nennung der in diesem Kontext aufgeführten Stellen erfolgt beispielsweise und bestimmt damit den Kreis externer Anbieter nicht abschließend.

Die umfassendste Neugestaltung im Zuge dieses Anhörungsverfahrens hat das Automatisierte Video-Identifikations-Verfahren gemäß *Ziffer A.II.3.* erfahren. Bereits im Rahmen der Online-Anhörung waren aus dem Teilnehmerkreis konstruktive Vorschläge geäußert worden, um sprachlich der technischen Praxis derartiger Verfahren besser gerecht zu werden. Die Bundesnetzagentur hat die Vorschläge,

welche auch im Rahmen schriftlicher Stellungnahmen vorgetragen wurden, wohlwollend geprüft und insbesondere die Anforderungen an den Identifizierungsvorgang in *Ziffer A.II.3.2*. hieran orientiert umgestaltet.

Darüber hinaus wurden unter Berücksichtigung von Eingaben seitens des BSI und des BfDI einzelne technische Sicherheitsanforderungen ergänzt (vgl. *Ziffer A.II.3.6.)* und die datenschutzrechtlichen Rahmenbedingungen für die Aufbewahrung der Nachweisdaten für Stichprobenüberprüfungen (insb. Löschfristen) ausdrücklich geregelt (vgl. *Ziffer A.II.3.8.2*). Zu den Sicherheitsanforderungen werden konkretisierende Hinweise darüber hinaus in die bereits erwähnte Handreichung Eingang finden.

Schließlich wurde in *Ziffer A.II.3.4.3.* klargestellt, dass die Nutzung von Nachweisdaten für andere Zwecke als für den ursprünglichen Identifizierungsvorgang und die Stichprobenüberprüfung hinaus nicht Gegenstand dieser Verfügung ist. Sofern eine solche Nutzung beabsichtigt ist, regelt sich die Zulässigkeit nach den allgemeinen datenschutzrechtlichen Vorgaben.

Das Verfahren in *Ziffer A.II.4.* wurde um eine Sicherheitsanforderung gegenüber Dritten ergänzt, die die in Bezug genommene anlassunabhängige Vorabidentifikation durchgeführt haben: In *Ziffer 4.1.3.* wird verlangt, dass der Dritte geeignete Maßnahmen zum Schutz der Datenintegrität vorsieht, neben den bereits im Entwurfstext vorgesehenen Aktualisierungsmaßnahmen.

Im Gegenzug wurden – auf Anregung einzelner Wirtschaftsbeteiligter (yes IDP GmbH) sowie der Verbände (Bitkom/VATM) – die Anforderungen an die Dokumentationspflichten für diese Vorabidentifikation flexibler ausgestaltet, um die Nutzung von Synergieeffekten mit anderen Regelungsbereichen zu erleichtern.

Nicht entsprochen werden konnte einer Forderung aus Wirtschaftskreisen betreffend die Regelungen zur zeitlichen Geltung in *Ziffer A.III.2.* und die dazugehörigen Begründungserwägungen in *Ziffer B.I.,* die auf eine übergangsweise Anerkennung von Konformitätsnachweisen aus dem Bereich der Vertrauensdienste ausgerichtet war. Der Anforderungskatalog nach dieser Verfügung ist eigenständig und weicht in Zielsetzung und Ausgestaltung von den Anforderungen im Bereich der Vertrauensdienste ab. Eine auch nur zeitweise Anerkennung eines anderen Anforderungskatalogs lässt sich daher nicht rechtfertigen. Das Interesse der Wirtschaftsbeteiligten zur Nutzung von Synergieeffekten mit anderen Regelungsbereichen wird jedoch im Rahmen der Ausgestaltung von Konformitätsverfahren seitens der Bundesnetzagentur Berücksichtigung finden.