Formulierungshilfe

für einen Änderungsantrag

zu dem Gesetzentwurf der Bundesregierung

– BT-Drucksache 20/XXXX –

Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG)

Der Bundestag wolle beschließen,

den Gesetzentwurf auf BT-Drucksache **20/8093** mit folgender Maßgabe, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:
   a) Nummer 1 wird wie folgt geändert:
      aa) § 1 Absatz 1 wird wie folgt geändert:
         aaa) In Nummer 1 wird das Wort „sowie“ durch das Wort „einschließlich“ ersetzt.
         bbb) In Nummer 2 wird das Wort „sowie“ durch die Wörter „und einschließlich“ ersetzt.
      bb) § 1a wird wie folgt geändert:
         aaa) Absatz 1 wird wie folgt gefasst:

> (1) „ Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Davon abweichend sollen Verwaltungsleistungen, die der Ausführung von Bundesgesetzen dienen und ausschließlich Nutzer im Sinne des § 2 Absatz 4 Nummer 2 betreffen, spätestens mit Ablauf des fünften auf die Verkündung des Gesetzes vom … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] folgenden Kalenderjahres ausschließlich elektronisch angeboten werden. Von dem ausschließlich elektronischen Angebot einer Verwaltungsleistung nach Satz 2 kann bei berechtigtem Interesse des Nutzers abgewichen werden. Erfolgt ein ausschließlich elektronisches Angebot bereits vor Ablauf des Zeitraums nach Satz 2, so ist darüber an geeigneter Stelle mit angemessenem Vorlauf elektronisch zu informieren.“

         bbb) Nach Absatz 1 wird folgender Absatz 2 eingefügt:

> „(2) Nach Ablauf des vierten auf die Verkündung des Gesetzes vom … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] folgenden Kalenderjahres haben Nutzer einen Anspruch auf einen elektronischen

Zugang zu den Verwaltungsleistungen des Bundes. Schadensersatzansprüche und Entschädigungsansprüche sind ausgeschlossen.“

ccc) Die bisherigen Absätze 2 und 3 werden die Absätze 3 und 4.

b) Nummer 2 Buchstabe c wird wie folgt gefasst:

‚c) Die Absätze 4 und 5 werden wie folgt gefasst:

„(4) „Nutzer“ im Sinne dieses Gesetzes sind

1. natürliche Personen,
2. Unternehmen im Sinne des § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes und
3. Behörden.

(5) Ein „Nutzerkonto“ ist eine zentrale IT-Komponente zur einmaligen oder dauerhaften Identifizierung und Authentifizierung der Nutzer zu Zwecken der Inanspruchnahme von Verwaltungsleistungen der öffentlichen Verwaltung sowie zur vorgangsbezogenen sicheren Kommunikation über ein Postfach im Sinne des Absatzes 7. Ein Nutzerkonto wird als Bürger- oder Organisationskonto bereitgestellt. Das „Bürgerkonto“ ist ein Nutzerkonto, das natürlichen Personen zur Verfügung steht. Das „Organisationskonto“ ist ein Nutzerkonto, das Unternehmen im Sinne des § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes sowie Behörden zur Verfügung steht.“‘

c) Nummer 3 wird wie folgt geändert:

aa) Die Angabe „§§ 3, 3a und 3b“ wird durch die Angabe „§§ 3 und 3a“ ersetzt.

bb) § 3b wird gestrichen.

d) Nummer 4 Buchstabe c wird wie folgt gefasst:

‚c) Folgender Absatz 3 wird angefügt:

„(3) Bei der Bereitstellung der IT-Komponenten im Sinne des Absatzes 1 sollen offene Standards und offene Schnittstellen verwendet werden und soll Open-Source-Software vorrangig vor solcher Software eingesetzt werden, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.“‘

e) Nummer 6 wird wie folgt gefasst:

‚6. § 6 wird wie folgt gefasst:

„§ 6

Standards; Verordnungsermächtigungen

(1) Für die informationstechnischen Systeme, die für den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern genutzt werden, legt das Bundesministerium des Innern und für Heimat im

Benehmen mit dem IT-Planungsrat bis zum Ablauf des zweiten auf die Verkündung des Gesetzes … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] folgenden Kalenderjahres durch Rechtsverordnung ohne Zustimmung des Bundesrates die erforderlichen

1. Architekturvorgaben,
2. Qualitätsanforderungen und
3. Interoperabilitätsstandards einschließlich der Prozessmodelle, Datenformate, Transportprotokolle, Schnittstellenbeschreibungen zur Anbindung von Onlineverfahren und Fachverfahren sowie die für die Anbindung von Basisdiensten erforderlichen Schnittstellen

fest.

(2) Für die Abwicklung von Verwaltungsverfahren, die der Durchführung unmittelbar geltender Rechtsakte der Europäischen Union, für die dem Bund die Gesetzgebungskompetenz zusteht, oder der Ausführung von Bundesgesetzen dienen, legt das für den jeweiligen Rechtsakt oder das jeweilige Bundesgesetz zuständige Bundesministerium im Einvernehmen mit dem Bundesministerium des Innern und für Heimat durch Rechtsverordnung ohne Zustimmung des Bundesrates die Vorgaben im Sinne des Absatzes 1 fest. Das Bundesministerium des Innern und für Heimat setzt sich mit dem IT-Planungsrat hierzu ins Benehmen.

(3) Die Einhaltung der durch die Rechtsverordnung nach den Absätzen 1 und 2 festgelegten Vorgaben ist für alle Stellen verbindlich, deren Verwaltungsleistungen über den Portalverbund angeboten werden. Von den durch die Rechtsverordnung nach den Absätzen 1 und 2 getroffenen Regelungen kann durch Landesrecht nicht abgewichen werden. § 4 Absatz 2 gilt entsprechend.

(4) Das Bundesministerium des Innern und für Heimat oder die von ihm beauftragte Stelle veröffentlicht in strukturierter Form elektronisch an zentraler Stelle die im Anwendungsbereich des Onlinezugangsgesetzes von Bund und Ländern angewendeten Standards. Zu Schnittstellen von IT-Komponenten sollen Spezifikationen und Dokumentationen in der jeweils aktuellen Fassung veröffentlicht werden. Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung mit Zustimmung des Bundesrates die Aufgabe nach Satz 1

1. mit dessen Einvernehmen einem Land oder
2. einer anderen öffentlich-rechtlich getragenen Einrichtung

übertragen.“‘

f) In Nummer 7 wird dem § 7 Absatz 1 folgender Satz angefügt:

„Nutzer sollen in die Entwicklung neuer elektronischer Angebote einbezogen werden.“

g) Nummer 8 wird wie folgt gefasst:

‚8. § 8 wird wie folgt gefasst:

„§ 8

Rechtsgrundlagen der Datenverarbeitung in Nutzerkonten und zu Identifizierungszwecken

(1) Zur Feststellung der Identität des Nutzers eines Bürgerkontos dürfen, soweit dies erforderlich ist, folgende Daten verarbeitet werden:

1. Daten nach § 18 Absatz 3 des Personalausweisgesetzes,
2. die eindeutige Kennung sowie die spezifischen Daten, die von notifizierten elektronischen Identifizierungsmitteln nach der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73), die zuletzt durch die Richtlinie (EU) 2022/2555 (Abl. L 333 vom 27.12.2022, S. 80) geändert worden ist, übermittelt werden,
3. die eindeutige Kennung, die von sonstigen anerkannten elektronischen Identifizierungsmitteln übermittelt wird, und
4. die Postfachreferenz des Nutzerkontos.

Bei späterer Nutzung des Nutzerkontos mit dem elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes sind grundsätzlich das dienste- und kartenspezifische Kennzeichen und die Anschrift zu übermitteln, bei elektronischen Identifizierungsmitteln nach Satz 1 Nummer 2 und 3 nur die jeweilige eindeutige Kennung.

(2) Zur Feststellung der Identität des Nutzers eines Organisationskontos und zur Feststellung der Vertretungs- oder Handlungsbefugnis einer für die Organisation handelnden natürlichen oder juristischen Person dürfen, soweit dies erforderlich ist, folgende Daten verarbeitet werden:

1. Unternehmensbasisdaten nach § 3 des Unternehmensbasisdatenregistergesetzes,
2. Daten nach § 139b Absatz 4a und § 139c Absatz 6a der Abgabenordnung,
3. die eindeutige Kennung sowie spezifische Daten, die von notifizierten elektronischen Identifizierungsmitteln nach der Verordnung (EU) Nr. 910/2014 übermittelt werden,
4. die eindeutige Kennung, die von sonstigen anerkannten elektronischen Identifizierungsmitteln übermittelt wird,
5. die Postfachreferenzen des Nutzerkontos,
6. Daten zur Vertretungs- oder Handlungsbefugnis sowie Daten nach Absatz 1 der für eine Organisation handelnden natürlichen Personen und
7. Daten der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter.

Ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so können deren Daten nach diesem Absatz verwendet werden.

(3) Zur Feststellung der Identität eines Nutzers darf die Finanzbehörde, die im Auftrag der obersten Finanzbehörden des Bundes und der Länder das sichere Verfahren nach § 87a Absatz 6 der Abgabenordnung betreibt,

1. die in § 139b Absatz 4a und § 139c Absatz 6a der Abgabenordnung aufgeführten Daten des Bundeszentralamts für Steuern sowie entsprechende, für das Besteuerungsverfahren gespeicherte Daten der Finanzämter bei diesen Finanzbehörden im automatisierten Verfahren auf Veranlassung des Nutzers abrufen und
2. die abgerufenen Daten auf Veranlassung des Nutzers an dessen Nutzerkonto übermitteln.

(4) Daten im Sinne der Absätze 1 und 2 dürfen auf Veranlassung des Nutzers auch zwischen den Nutzerkonten im Portalverbund ausgetauscht werden.

(5) Zur Kommunikation mit dem Nutzer dürfen zusätzlich folgende Daten verarbeitet werden:

1. Anrede,
2. weitere Anschriften,
3. De-Mail-Adresse oder vergleichbare Adresse eines Zustelldienstes eines Mitgliedstaats der Europäischen Union oder eines anderen Vertragsstaats des Abkommens über den Europäischen Wirtschaftsraum nach der Verordnung (EU) Nr. 910/2014,
4. E-Mail-Adresse,
5. Telefon- oder Mobilfunknummer,
6. Telefaxnummer und
7. Kommunikationsinhaltsdaten.

(6) Auf Veranlassung des Nutzers dürfen elektronische Dokumente zu Verwaltungsvorgängen und Status- und Verfahrensinformationen an das Nutzerkonto übermittelt und für Zwecke des Nutzerkontos verarbeitet werden, soweit dies erforderlich ist.

(7) Auf Veranlassung des Nutzers ist eine dauerhafte Speicherung der Daten nach den Absätzen 1, 2, 5 und 6 zulässig. Im Falle der dauerhaften Speicherung muss der Nutzer jederzeit die Möglichkeit haben, das Nutzerkonto und alle gespeicherten Daten selbständig zu löschen. Das Bürgerkonto wird bei zweijähriger Inaktivität des Nutzers automatisch gelöscht. Der Nutzer wird zwei Monate vorher automatisch elektronisch über die anstehende Löschung benachrichtigt. Die elektronische Identifizierung kann jeweils mittels einer einmaligen Abfrage der Identitätsdaten erfolgen.

(8) Die für den jeweiligen Zweck erforderlichen Daten nach den Absätzen 1, 2, 5 und 6 sowie nach § 9 Absatz 1 dürfen

auf Veranlassung des Nutzers an die für die Verwaltungsleistung zuständige Behörde, ein Verwaltungsportal oder einen Onlinedienst übermittelt werden und durch diese verarbeitet werden, soweit dies für die Zwecke der Unterstützung bei der Inanspruchnahme elektronischer Verwaltungsleistungen oder deren Abwicklung erforderlich ist. Die Verantwortung für die Zulässigkeit der Übermittlung trägt der Dritte, an den die Daten übermittelt werden. Soweit gesetzlich nichts anderes bestimmt ist, darf der Dritte die Daten nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden.

(9) Soweit nach den Absätzen 5 bis 8 Daten verarbeitet werden dürfen, gilt dies auch für besondere Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

(10) Für die Verarbeitung personenbezogener Daten im Nutzerkonto nach den Absätzen 1 bis 9 ist die für das Nutzerkonto jeweils zuständige Stelle nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2, S. 2; L 74 vom 4.3.2021, S. 35) ausschließlich verantwortlich. Teilen sich mehrere Stellen die Zuständigkeit für ein Nutzerkonto, sind diese nach Artikel 26 der Verordnung (EU) 2016/679 gemeinsam verantwortlich.“‘

h) Nummer 9 wird wie folgt geändert:

aa) Die Überschrift des § 8a wird wie folgt gefasst:

„§ 8a

Rechtsgrundlagen der Datenverarbeitung in einem länderübergreifenden Onlinedienst“.

bb) In § 8a Absatz 1 Satz 1 und Satz 2, Absatz 2 Satz 1, Absatz 3 Satz 3 und Absatz 4 Satz 1 wird jeweils vor dem Wort „Onlinedienst“ das Wort „länderübergreifenden“ eingefügt.

i) Nummer 12 wird wie folgt geändert:

aa) Nach Buchstabe b werden die folgenden Buchstaben c und d eingefügt:

‚c) In Absatz 1 Satz 2 werden vor dem Wort „diejenigen“ die Wörter „bis zum Vorliegen der technischen und rechtlichen Voraussetzungen für eine Erfassung weiterer Datenübermittlungen zunächst“ eingefügt.

d) Absatz 2 Satz 1 wird wie folgt gefasst:

„Im Datenschutzcockpit werden nach Maßgabe von Absatz 4 Satz 3 ausschließlich Protokolldaten nach § 9 des Identifikationsnummerngesetzes einschließlich der dazu durch die Registermodernisierungsbehörde und die Register

übermittelten Inhaltsdaten sowie die Bestandsdaten der Register angezeigt.“‘

bb) Die bisherigen Buchstaben c und d werden die Buchstaben e und f.

j) Nummer 13 wird wie folgt gefasst:

‚13. § 11 wird wie folgt gefasst:

„§ 11

Monitoring und Evaluierung

Das Bundesministerium des Innern und für Heimat führt beginnend mit dem … [einsetzen: Datum des Inkrafttretens nach Artikel 9 dieses Gesetzes] fortlaufend ein Monitoring zu der Umsetzung der Vorschriften dieses Gesetzes durch. Das Bundesministerium des Innern und für Heimat beauftragt eine fachunabhängige wissenschaftliche Einrichtung, dieses Gesetz alle drei Jahre, erstmals nach Ablauf von drei Jahren nach dem… [einsetzen: Datum des Inkrafttretens nach Artikel 9 dieses Gesetzes], zu evaluieren. Die Evaluationsberichte werden elektronisch veröffentlicht.“‘

k) Nummer 14 wird wie folgt gefasst:

‚14. Folgender § 12 wird angefügt:

„§ 12

Übergangsregelungen zu § 3; Verordnungsermächtigungen

(1) Bis zum … [einsetzen: Tag und Monat des Inkrafttretens nach Artikel 9 dieses Gesetzes sowie Jahr des dritten auf das Inkrafttreten dieses Gesetzes folgenden Jahres] kann die Identifizierung und Authentifizierung der Nutzer im Sinne des § 2 Absatz 4 Nummer 1 für elektronische Verwaltungsleistungen im Portalverbund auch über die bisherigen Nutzerkonten der Länder oder eines Fachportals erfolgen.

(2) Bis zum 30. Juni 2026 kann der elektronische Identitätsnachweis im Bürgerkonto außerdem für elektronische Verwaltungsleistungen, für die höchstens das Vertrauensniveau „substantiell“ erforderlich ist, durch ein sicheres Verfahren nach § 87a Absatz 6 der Abgabenordnung oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mindestens mit dem Sicherheitsniveau „substantiell“ im Sinne des Artikels 8 Absatz 2 Buchstabe b der Verordnung (EU) Nr. 910/2014 anerkannt worden ist, erfolgen. Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, eine von Satz 1 abweichende längere Frist festzulegen. Bis zum 30. Juni 2026 werden die nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung bis einschließlich 31. Dezember 2019 eingesetzten sicheren Verfahren bundesweit zum Nachweis der

Identität auf dem Vertrauensniveau „substantiell“ anerkannt. Das Bundesministerium des Innern und für Heimat und das Bundesministerium der Finanzen werden ermächtigt, durch gemeinsame Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, eine von Satz 3 abweichende längere Frist festzulegen.

(3) Abweichend von § 3 Absatz 3 ist bis zum Ablauf der Frist nach § 3 Absatz 4 Nummer 2 Buchstabe a von der Verwendung des einheitlichen Organisationskontos abzusehen, wenn für die Inanspruchnahme einer elektronischen Verwaltungsleistung und die sonstige elektronische Kommunikation ausnahmsweise ein höheres Vertrauensniveau erforderlich ist.

(4) Öffentliche Stellen sind von der Verpflichtung nach § 3 Absatz 3 bis einschließlich 31. Dezember 2031 ausgenommen in Bezug auf elektronische Verwaltungsleistungen, die der Durchführung der Verordnung (EU) 2021/1060 des Europäischen Parlaments und des Rates vom 24. Juni 2021 mit gemeinsamen Bestimmungen für den Europäischen Fonds für regionale Entwicklung, den Europäischen Sozialfonds Plus, den Kohäsionsfonds, den Fonds für einen gerechten Übergang und den Europäischen Meeres-, Fischerei- und Aquakulturfonds sowie mit Haushaltsvorschriften für diese Fonds und für den Asyl-, Migrations- und Integrationsfonds, den Fonds für die innere Sicherheit und das Instrument für finanzielle Hilfe im Bereich Grenzverwaltung und Visumpolitik (ABl. L 231 vom 30.6.2021, S. 159), die zuletzt durch die Verordnung (EU) 2023/435 des Europäischen Parlaments und des Rates vom 27. Februar 2023 zur Änderung der Verordnung (EU) 2021/241 in Bezug auf REPowerEU-Kapitel in den Aufbau- und Resilienzplänen und zur Änderung der Verordnungen (EU) Nr. 1303/2013, (EU) 2021/1060 und (EU) 2021/1755 sowie der Richtlinie 2003/87/EG (ABl. L 63 vom 28.2.2023, S. 1) geändert worden ist, sowie der Verordnung (EU) 2021/2115 des Europäischen Parlaments und des Rates vom 2. Dezember 2021 mit Vorschriften für die Unterstützung der von den Mitgliedstaaten im Rahmen der gemeinsamen Agrarpolitik zu erstellenden und durch den Europäischen Garantiefonds für die Landwirtschaft (EGFL) und den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) zu finanzierenden Strategiepläne (GAP-Strategiepläne) und zur Aufhebung der Verordnung (EU) Nr. 1305/2013 sowie der Verordnung (EU) Nr. 1307/2013 (ABl. L 435 vom 6.12.2021, S. 1), die zuletzt durch die Delegierte Verordnung (EU) 2022/648 der Kommission vom 15. Februar 2022 (ABl. L 119 vom 21.4.2021, S. 1) geändert worden ist, und der Verordnung (EU) 2021/2116 des Europäischen Parlaments und des Rates vom 2. Dezember 2021 über die Finanzierung, Verwaltung und Überwachung der Gemeinsamen Agrarpolitik und zur Aufhebung der Verordnung (EU) Nr. 1306/2013 (ABl. L 435 vom 6.12.2021, S. 187), die zuletzt durch die Delegierte Verordnung (EU) 2022/1408 der Kommission (ABl. L 216 vom 19.8.2021, S. 1) geändert worden ist, dienen.

(5) Das Bundesministerium des Innern und für Heimat und das Bundesministerium der Finanzen werden ermächtigt, durch gemeinsame Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die Fristen nach § 3 Absatz 4 Nummer 2 Buchstabe a und b zu verlängern.

(6) Wird der Nachweis der Identität nach § 3 Absatz 4 Nummer 1 erbracht, so kann die spätere Authentisierung des Nutzers auch durch Authentisierungsmittel nach § 10 Absatz 3a des Personalausweisgesetzes erfolgen.“ ‘

2. Artikel 2 wird wie folgt geändert:

a) Nummer 3 wird wie folgt geändert:

aa) Nach Buchstabe a wird folgender Buchstabe b eingefügt:

„b) Absatz 2 wird aufgehoben.“

bb) Der bisherige Buchstabe b wird Buchstabe c und wird wie folgt gefasst:

‚c) Absatz 3 wird Absatz 2 und wird wie folgt gefasst:

„(2) Jede Behörde des Bundes ist verpflichtet, in Verwaltungsverfahren, in denen sie die Identität einer Person auf Grund einer Rechtsvorschrift festzustellen hat oder aus anderen Gründen eine Identifizierung für notwendig erachtet, einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anzubieten. Mit der Anbindung an das Bürgerkonto nach § 3 Absatz 1 des Onlinezugangsgesetzes wird diese Verpflichtung erfüllt.“‘

b) In Nummer 4 wird dem § 2a Absatz 1 folgender Satz angefügt:

„Auf der Grundlage einer Verwaltungsvereinbarung mit dem Bundesministerium des Innern und für Heimat können Länder diesen Siegeldienst zur Unterstützung der elektronischen Verwaltungstätigkeit ihrer Behörden mitnutzen.“

c) Nummer 6 wird wie folgt gefasst:

‚6. § 4 Absatz 1 wird wie folgt gefasst:

„(1) Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren oder sonstige Forderungen an, muss die Behörde die Einzahlung dieser Gebühren oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an verschiedenen im elektronischen Geschäftsverkehr üblichen, möglichst barrierefreien und hinreichend sicheren Zahlungsverfahren ermöglichen.“‘

d) Nummer 8 wird wie folgt geändert:

aa) Dem § 5 Absatz 3 werden die folgenden Sätze angefügt:

„Die Datenübermittlungen zwischen öffentlichen Stellen nach diesem Absatz sind durch die jeweiligen Stellen in einer Weise zu protokollieren, die eine Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Die Pflicht nach Satz 3 gilt ab dem Tag, der dem Tag folgt, an dem das Bundesministerium des Innern und für Heimat im Bundesanzeiger bekannt gibt, dass die technischen und rechtlichen Voraussetzungen für eine Anzeige der

Datenübermittlungen nach diesem Absatz im Datenschutzcockpit nach § 10 des Onlinezugangsgesetzes vorliegen. § 9 Absatz 2 und 3 des Identifikationsnummerngesetzes gilt ab diesem Zeitpunkt entsprechend.“

bb) In § 6 Absatz 3 werden die Wörter „durch Rechtsverordnung mit Zustimmung des Bundesrates nach Anhörung der kommunalen Spitzenverbände“ durch die Wörter „nach Anhörung der kommunalen Spitzenverbände durch Rechtsverordnung mit Zustimmung des Bundesrates“ ersetzt.

e) In Nummer 10 werden in § 9a Absatz 3 Nummer 6 die Wörter „mindestens einem“ durch das Wort „verschiedenen“ und die Wörter „und hinreichenden“ durch die Wörter „, möglichst barrierefreien und hinreichend sicheren“ ersetzt.

f) Nummer 13 wird wie folgt gefasst:

‚13. § 16 wird durch die folgenden §§ 16 und 16a ersetzt:

„§ 16

Nutzerfreundlichkeit und Barrierefreiheit

Die Behörden des Bundes gestalten die elektronische Kommunikation und die elektronischen Dokumente nutzerfreundlich und barrierefrei. Für die barrierefreie Gestaltung gilt die Barrierefreie-Informationstechnik-Verordnung entsprechend.

§ 16a

Open Source

Die Behörden des Bundes sollen offene Standards nutzen und bei neu anzuschaffender Software Open-Source-Software vorrangig vor solcher Software beschaffen, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt.“‘

3. In Artikel 3 Nummer 1 werden in § 3 Absatz 2 nach dem Wort „ermächtigt,“ die Wörter „nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik und“ eingefügt.

4. Artikel 7 Nummer 2 wird wie folgt gefasst:

‚2. In § 1 werden die Wörter „juristischen Personen, Vereinigungen, denen ein Recht zustehen kann, natürlichen Personen, die gewerblich oder beruflich tätig sind,“ durch die Wörter „Unternehmen im Sinne des § 3 Absatz 2 des Unternehmensbasisdatenregistergesetzes“ und die Wörter „bereit zu stellen“ durch das Wort „bereitzustellen“ ersetzt.‘

5. Nach Artikel 8 werden die folgenden Artikel 8a bis 8g eingefügt:

‚Artikel 8a

Änderung der Abgabenordnung

Die Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 24 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411) geändert worden ist, wird wie folgt geändert:

1. § 139b wird wie folgt geändert:

   a) Absatz 3 Nummer 7 wird wie folgt gefasst:

      „7. amtlicher Gemeindeschlüssel,“.

   b) Absatz 4a wird wie folgt gefasst:

      „(4a) Die in Absatz 3 Nummer 3 bis 8 und 10 aufgeführten Daten werden bei einer natürlichen Person, die ein Nutzerkonto im Sinne des § 2 Absatz 5 des Onlinezugangsgesetzes nutzt, auch zum Nachweis der Identität als Nutzer dieses Nutzerkontos gespeichert; diese Daten dürfen auf Veranlassung des Nutzers eines Nutzerkontos elektronisch an das Nutzerkonto übermittelt werden.“

   c) Absatz 6 Satz 1 Nummer 5 wird wie folgt gefasst:

      „5. amtlicher Gemeindeschlüssel,“.

2. § 139c wird wie folgt geändert:

   a) In Absatz 3 Nummer 9, Absatz 4 Nummer 10 und Absatz 5 Nummer 11 werden jeweils nach dem Wort „Registergericht“ die Wörter „einschließlich Altgericht“ eingefügt.

   b) Absatz 6a wird wie folgt gefasst:

      „(6a) Die in Absatz 3 Nummer 1, 3, 5, 7, 8 und 9, in Absatz 4 Nummer 1, 3, 5, 7, 8 und 10 sowie in Absatz 5 Nummer 1, 4, 6, 8, 9 und 11 aufgeführten Daten werden bei einem Unternehmen im Sinne des Unternehmensbasisdatenregistergesetzes, das ein Nutzerkonto im Sinne des § 2 Absatz 5 des Onlinezugangsgesetzes nutzt, auch zum Nachweis der Identität als Nutzer dieses Nutzerkontos gespeichert; diese Daten dürfen auf Veranlassung des Nutzers eines Nutzerkontos elektronisch an das Nutzerkonto übermittelt werden.“

Artikel 8b

Änderung des Einführungsgesetzes zur Abgabenordnung

Artikel 97 § 5a des Einführungsgesetzes zur Abgabenordnung vom 14. Dezember 1976 (BGBl. I S. 3341; 1977 I S. 667), das zuletzt durch Artikel 26 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411) geändert worden ist, wird wie folgt geändert:

1. Die Überschrift wird wie folgt gefasst:

„Artikel 97 § 5a

Identifikationsnummer und Wirtschafts-Identifikationsnummer“.

2. Der Wortlaut wird Absatz 1.

3. Folgender Absatz 2 wird angefügt:

„(2) § 139b Absatz 3, 4a und 6 sowie § 139c Absatz 3, 4, 5 und 6a der Abgabenordnung in der Fassung des Artikels 8a Nummer 1 des Gesetzes vom … [einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes] sind ab dem Tag anzuwenden, der dem Tag folgt, an dem das Bundesministerium der Finanzen im Bundesgesetzblatt bekannt gibt, dass die technischen Voraussetzungen für die Verarbeitung des amtlichen Gemeindeschlüssels und des Altgerichts jeweils vorliegen.“

Artikel 8c

Änderung der Zivilprozessordnung

Die Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 411) geändert worden ist, wird wie folgt geändert:

1. § 371a Absatz 3 wird wie folgt gefasst:

„(3) Auf elektronische Dokumente, die von einer Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind (öffentliche elektronische Dokumente), finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Ist das Dokument von der Behörde mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel oder von der mit öffentlichem Glauben versehenen Person mit einer qualifizierten elektronischen Signatur versehen, so gilt § 437 entsprechend. Das Gleiche gilt, wenn das Dokument im Auftrag der Behörde oder der mit öffentlichem Glauben versehenen Person durch einen akkreditierten Diensteanbieter mit seiner qualifizierten elektronischen Signatur gemäß § 5 Absatz 5 des De-Mail-Gesetzes versehen ist und die Absenderbestätigung die Behörde oder die mit öffentlichem Glauben versehene Person als Nutzer des De-Mail-Kontos ausweist.“

2. § 371b wird wie folgt gefasst:

„§ 371b

Beweiskraft gescannter öffentlicher Urkunden

Wird eine öffentliche Urkunde nach dem Stand der Technik von einer Behörde oder von einer mit öffentlichem Glauben versehenen Person in ein elektronisches Dokument übertragen und liegt die Bestätigung vor, dass das elektronische Dokument mit der Urschrift bildlich und inhaltlich übereinstimmt, finden auf das elektronische

Dokument die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Sind das Dokument und die Bestätigung von der Behörde mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel oder von der mit öffentlichem Glauben versehenen Person mit einer qualifizierten elektronischen Signatur versehen, so gilt § 437 entsprechend.“

Artikel 8d

Änderung des Bundesberggesetzes

In § 16 Absatz 1 Satz 1 des Bundesberggesetzes vom 13. August 1980 (BGBl. I S. 1310), das zuletzt durch Artikel 4 des Gesetzes vom 22. März 2023 (BGBl. 2023 I Nr. 88) geändert worden ist, werden die Wörter „; die elektronische Form ist ausgeschlossen“ gestrichen.

Artikel 8e

Änderung des Zehnten Buches Sozialgesetzbuch

Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 7a des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 408) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Nach der Angabe zu § 67e wird folgende Angabe eingefügt:

      „§ 67f Erhebung und Übermittlung von Sozialdaten zur Nachweiserbringung“.

   b) Nach der Angabe zu § 77 wird folgende Angabe eingefügt:

      „§ 77a Grenzüberschreitende Nachweisabrufe“.

2. Nach § 67a Absatz 2 Satz 1 wird folgender Satz eingefügt:

   „Als Erhebung nach Satz 1 gilt auch die Entscheidung der betroffenen Person nach § 67f Absatz 1 Satz 1 Nummer 1 in Verbindung mit Absatz 4 Satz 2 oder ein ausdrückliches Ersuchen im Anwendungsbereich des § 77a.“

3. Nach § 67e wird folgender § 67f eingefügt:

„§ 67f

Erhebung und Übermittlung von Sozialdaten zur Nachweiserbringung

(1) Wird ein Verwaltungsverfahren elektronisch durchgeführt, ist die Erhebung von Sozialdaten zulässig, wenn nach Wahl der betroffenen Person

1. die nachweisanfordernde Stelle den jeweiligen Nachweis automatisiert bei der nachweisliefernden Stelle abruft, sofern der

jeweils erforderliche Nachweis elektronisch vorliegt und ohne zeitlichen Verzug automatisiert abgerufen werden kann, oder

2. die betroffene Person den jeweiligen Nachweis elektronisch einreicht.

Nachweise sind Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. Nachweisanfordernde Stelle kann die für die Entscheidung zuständige Behörde oder eine andere öffentliche Stelle sein, die dafür zuständig ist, Nachweise einzuholen und an die für die Entscheidung zuständige Behörde weiterzuleiten. Nachweisliefernde Stelle ist diejenige öffentliche Stelle, die dafür zuständig ist, den Nachweis auszustellen.

(2) Hat sich die betroffene Person für den automatisierten Nachweisabruf entschieden, darf die nachweisanfordernde Stelle den Nachweis der betroffenen Person bei der nachweisliefernden Stelle abrufen und die nachweisliefernde Stelle den Nachweis an die nachweisanfordernde Stelle übermitteln, wenn

1. dies zur Erfüllung der Aufgabe der nachweisanfordernden Stelle erforderlich ist und

2. die nachweisanfordernde Stelle den Nachweis auch aufgrund anderer Rechtsvorschriften bei der betroffenen Person erheben dürfte.

Die in Absatz 1 Satz 3 Alternative 2 genannte andere öffentliche Stelle darf den Nachweis an die für die Entscheidung zuständige Stelle übermitteln. Die Datenübermittlungen zwischen öffentlichen Stellen nach diesem Absatz sind durch die jeweiligen Stellen in einer Weise zu protokollieren, die eine Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Die Pflicht nach Satz 3 gilt ab dem Tag, der dem Tag folgt, an dem das Bundesministerium des Innern und für Heimat im Bundesanzeiger bekannt gibt, dass die technischen und rechtlichen Voraussetzungen für eine Anzeige der Datenübermittlungen nach diesem Absatz im Datenschutzcockpit nach § 10 des Onlinezugangsgesetzes vorliegen. § 9 Absatz 2 und 3 des Identifikationsnummerngesetzes gilt ab diesem Zeitpunkt entsprechend.

(3) Soll der Nachweis aus einem Register, welches in der Anlage zum Identifikationsnummerngesetz aufgeführt ist, abgerufen werden, darf die nachweisanfordernde Stelle die Identifikationsnummer nach § 1 des Identifikationsnummerngesetzes zur Zuordnung der Datensätze der betroffenen Person und zum Abruf des Nachweises an die nachweisliefernde Stelle übermitteln. Das Nachweisabrufersuchen darf zusätzlich weitere Daten im Sinne von § 4 Absatz 2 und 3 des Identifikationsnummerngesetzes, in der Regel das Geburtsdatum, zur Validierung der Zuordnung enthalten. Zu diesem Zweck darf die nachweisliefernde Stelle diese Daten verarbeiten.

(4) Bevor die für die Entscheidung zuständige Behörde den abgerufenen Nachweis verwenden darf, hat die betroffene Person im Fall des Absatzes 1 Satz 1 Nummer 1 die Möglichkeit, den Nachweis vorab einzusehen. Die betroffene Person kann entscheiden, ob der Nachweis für das Verwaltungsverfahren verwendet werden soll.

(5) Die Verantwortung für die Zulässigkeit der Nachweiserhebung und des Nachweisabrufs nach Absatz 1 Satz 1 Nummer 1 trägt die nachweisanfordernde Stelle.“

4. Nach § 77 wird folgender § 77a eingefügt:

„§ 77a

Grenzüberschreitende Nachweisabrufe

(1) Die zuständige Behörde darf bei einer Behörde eines anderen Mitgliedsstaats der Europäischen Union einen Nachweis nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1) automatisiert abrufen, wenn dies zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(2) Die automatisierte Übermittlung eines Nachweises nach Artikel 14 Absatz 2 der Verordnung (EU) 2018/1724 an eine Behörde eines anderen Mitgliedsstaats der Europäischen Union ist zulässig, wenn diese Behörde zuständig ist und die Übermittlung zur Erfüllung ihrer Aufgaben für eines der Verfahren nach Artikel 14 Absatz 1 der Verordnung (EU) 2018/1724 erforderlich ist.

(3) Bei der Verarbeitung nach den Absätzen 1 und 2 können intermediäre Plattformen zum Einsatz kommen.“

Artikel 8f

Änderung des Personalausweisgesetzes

Nach § 10 des Personalausweisgesetzes vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 2 des Gesetzes vom 8. Oktober 2023 (BGBl. 2023 I Nr. 271) geändert worden ist, wird folgender Absatz 3a eingefügt:

„(3a) Das Bundesministerium des Innern und für Heimat soll nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik für Fälle, in denen der Nachweis der Identität durch einen elektronischen Identitätsnachweis nach § 18 dieses Gesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erbracht wurde, für die spätere Authentisierung des Inhabers des elektronischen Identitätsnachweises auch andere Authentisierungsmittel befristet zulassen. Das Bundesministerium des Innern und für Heimat gibt die Zulassung und die Dauer der Befristung im Bundesanzeiger bekannt.“

Artikel 8g

Änderung des Identifikationsnummerngesetzes

§ 6 Absatz 3 des Identifikationsnummerngesetzes vom 28. März 2021 (BGBl. I S. 591; 2023 I Nr. 230), das durch Artikel 15 des Gesetzes vom 28.

Juni 2021 (BGBl. I S. 2250; 2023 I Nr. 230) geändert worden ist, wird wie folgt geändert:

1. Nach Nummer 1 wird folgende Nummer 2 eingefügt:

   „2. Sofern ein Datenabrufersuchen nach Nummer 1 nicht veranlasst werden kann, weil Wohnort und Postleitzahl nicht vorliegen, kann ein Datenabrufersuchen durchgeführt werden, wenn das Datenabrufersuchen mindestens den Familiennamen, den Vornamen und das Geburtsdatum enthält.“

2. Die bisherige Nummer 2 wird Nummer 3.‘

6. Artikel 9 wird wie folgt gefasst:

„Artikel 9

Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft.

(2) In Artikel 1 Nummer 14 tritt § 12 Absatz 2 Satz 3 mit Wirkung vom 1. Juli 2023 in Kraft.“

Begründung

Zu Nummer 1 (Änderung Artikel 1)

Zu Buchstabe a (Artikel 1 Nummer 1)

Zu Doppelbuchstabe aa (§ 1 Onlinezugangsgesetz)

Die Änderungen dienen der Klarstellung, dass es sich bei der mittelbaren Staatsverwaltung nicht um eine eigenständige Verwaltungsebene handelt.

Zu Doppelbuchstabe bb (§ 1a Onlinezugangsgesetz)

Zu Dreifachbuchstabe aaa (§ 1a Absatz 1 Onlinezugangsgesetz)

Die Streichung der Wörter „auf dem Gebiet des Rechts der Wirtschaft“ dient der Klarstellung, dass Unternehmensleistungen auch der Ausführung von Bundesgesetzen dienen können, die auf anderen Kompetenztiteln als Artikel 74 Absatz 1 Nummer 11 Grundgesetz beruhen.

Die Streichung der Wörter „und 3“ stellt eine Folgeänderung zu Nummer 1 Buchstabe b Doppelbuchstabe aa dar.

Die Neufassung des Satzes 3 dient der Klarstellung, dass die jeweils zuständige Behörde in begründeten Einzelfällen nur von der Pflicht, die jeweilige Verwaltungsleistung „ausschließlich elektronisch“ anzubieten, entbunden wird, nicht aber von der grundsätzlichen Verpflichtung, die jeweilige Verwaltungsleistung überhaupt elektronisch anzubieten.

Zu Dreifachbuchstabe bbb (§ 1a Absatz 2 Onlinezugangsgesetz)

Nach Ablauf des vierten auf die Verkündung des Gesetzes folgenden Jahres wird Nutzern ein subjektives öffentliches Recht auf ein Angebot von elektronischen Verwaltungsleistungen des Bundes eingeräumt.

Der einklagbare Anspruch besteht analog zu der behördlichen Verpflichtung nach Absatz 1 Satz 1, ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Der Anspruch ist somit auf den elektronischen Zugang des Nutzers zu der jeweiligen Verwaltungsleistung beschränkt und vermittelt kein Recht auf eine vollständig elektronische Abwicklung weiterer, insbesondere behördeninterner, Verfahrensschritte.

Es besteht kein Anspruch auf den elektronischen Zugang zu einer Verwaltungsleistung, soweit deren elektronisches Angebot aufgrund rechtlicher oder tatsächlicher Unmöglichkeit ausgeschlossen ist. Insoweit besteht bereits keine behördliche Verpflichtung zum elektronischen Angebot der Verwaltungsleistung (BT-Drs. 18/11135, S. 91, zu § 1 Absatz 1). Rechtliche Unmöglichkeit liegt vor, wenn eine Leistung auf Grund rechtlicher Vorgaben nicht elektronisch erbracht werden kann, etwa weil für ihre Abwicklung ein persönliches Erscheinen eines oder mehrerer Beteiligter zwingend vorgeschrieben ist. Ein Fall der tatsächlichen Unmöglichkeit liegt etwa vor, wenn die Abwicklung einer Verwaltungsleistung eine physische Handlung erfordert, die digital nicht abgebildet werden kann.

Der Anspruch soll darüber hinaus nicht im Hinblick auf solche Verwaltungsleistungen bestehen, deren elektronisches Angebot wirtschaftlich unzumutbar ist. Wirtschaftliche Unzumutbarkeit liegt vor, wenn eine Verwaltungsleistung nur von einer geringen Anzahl an Nutzern in Anspruch genommen wird (insbesondere weniger als 1.000 Fälle pro Jahr) und das elektronische Angebot dieser Leistung einen im Vergleich zu den Nutzungszahlen unverhältnismäßig hohen finanziellen Aufwand erfordern würde (zu beurteilen anhand einer Wirtschaftlichkeitsbetrachtung). Die Vorschrift vermittelt zudem lediglich einen Anspruch auf die elektronische Bereitstellung einer Verwaltungsleistung an sich. Ein Recht auf die jederzeitige elektronische Verfügbarkeit der Leistung geht damit, insbesondere mit Blick auf mögliche lediglich temporäre Einschränkungen aufgrund zeitlich begrenzter technischer Ausfälle oder Wartungsarbeiten, nicht einher.

Satz 2 stellt klar, dass der Anspruch auf ein elektronisches Angebot der Verwaltungsleistungen des Bundes nicht mit Schadensersatz- oder Staatshaftungsansprüchen des Nutzers gegenüber dem Bund einhergeht.

Zu Dreifachbuchstabe ccc

Folgeänderung zu Dreifachbuchstabe bbb.

Zu Buchstabe b (§ 2 Onlinezugangsgesetz)

Zu § 2 Absatz 4:

Der Verweis auf § 3 Absatz 1 des Unternehmensbasisdatenregistergesetzes (UBRegG) trägt der Systematik des OZG Rechnung, die primär zwischen Nutzern und Verwaltungsleistungen im wirtschaftlichen und im privaten Bereich unterscheidet, und schafft zudem Klarheit hinsichtlich der systematischen Einordnung natürlicher Personen, die wirtschaftlich tätig sind. Die bisherigen Nutzergruppen der juristischen Personen und Vereinigungen, soweit ihnen ein Recht zusteht, sind auch in der neuen Formulierung enthalten.

Zu § 2 Absatz 5:

Die Kommunikation über das Postfach soll hohen Sicherheitsstandards genügen. Bei einer Weiterentwicklung des Nutzerkontopostfachs soll daher nach Zurverfügungstellung entsprechender Haushaltsmittel auf eine Ende-zu-Ende-Verschlüsselung umgestiegen werden. Entsprechende technische Anpassungen sind auch bei allen mit dem Nutzerkontopostfach kommunizierenden Diensten im Portalverbund erforderlich. Zu Buchstabe c (§ 3b Onlinezugangsgesetz)

Der bisherige § 3b wird gestrichen und dessen Regelungsgehalt als neuer Absatz 4 in § 6 aufgenommen.

Zu Buchstabe d (§ 4 Onlinezugangsgesetz)

Die Streichung der Einschränkung „dort, wo es technisch möglich und wirtschaftlich ist“ dient der Klarstellung, dass die Verwendung von Open-Source-Software den Regelfall darstellen und eine Abweichung nur in begründeten Ausnahmefällen möglich sein soll. Wird eine genutzte Software weiterentwickelt, so ist der weiterentwickelte Quellcode unter eine geeignete offene Software- und Open-Source-Lizenz zu stellen und zu veröffentlichen, soweit der Veröffentlichung keine zwingenden sicherheitsrelevanten Gründe entgegenstehen und dies lizenzrechtlich zulässig ist. Die Software soll auch als Referenzimplementierung veröffentlicht werden. Neben Open-Source-Software sollen zudem offene Standards und offene Schnittstellen verwendet werden.

Zu Buchstabe e (§ 6 Onlinezugangsgesetz)

Die Erfahrungen der bisherigen OZG-Umsetzung belegen die große Bedeutung einer modularen IT-Architektur. Verbindliche Standards und einheitliche Schnittstellen sind unverzichtbare Voraussetzung für das Funktionieren der für den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern erforderlichen IT-Infrastruktur.

Die Änderung der Vorschrift dient der Klarstellung, dass sich die Verordnungsermächtigung auf sämtliche Standards und Schnittstellen erstreckt, die für das Funktionieren der OZG-Rahmenarchitektur, die Interoperabilität der hierfür erforderlichen IT-Komponenten sowie die Abwicklung von Verwaltungsverfahren, für die der Bund die Regelungskompetenz besitzt, relevant sind.

Zu § 6 Absatz 1:

Absatz 1 regelt die Vorgabe dieser Standards im Rahmen des übergreifenden informationstechnischen Zugangs zu den Verwaltungsleistungen von Bund und Ländern, für den der Bund gemäß Artikel 91c Absatz 5 GG die ausschließliche Gesetzgebungskompetenz besitzt. Die Vorschrift enthält nunmehr auch eine Frist, innerhalb derer der Bund diese Standards durch Rechtsverordnung vorzugeben hat. Diese Fristsetzung ist erforderlich, um den Standardisierungsprozess als Grundlage für eine schnelle und nachhaltige Verwaltungsdigitalisierung spürbar zu beschleunigen. Die Rechtsverordnung soll auf Grundlage eines dynamischen Verweises Standards in der jeweils aktuellen Version vorgeben, so dass bei Änderung oder Ergänzung des jeweiligen Standards keine Änderung dieser Rechtsverordnung erforderlich ist. Es sollen offene Standards vorgegeben werden.

Im Rahmen eines Konsultationsprozesses wird derzeit eine Rahmenarchitektur für die künftige OZG-Umsetzung von Bund und Ländern erarbeitet. Die sich daraus ergebenden Architekturvorgaben sollen in eine Rechtsverordnung aufgenommen werden.

Im Rahmen der Festlegung der Qualitätsanforderungen soll künftig auch der Servicestandard, der programmübergreifende Qualitätsprinzipien für die Digitalisierung von Verwaltungsleistungen definiert, für verbindlich erklärt werden. Zu diesen Qualitätsanforderungen zählen insbesondere auch Vorgaben zu einer nutzerfreundlichen Ausgestaltung digitaler Verwaltungsangebote sowie das Reifegradmodell, das vor dem Hintergrund der vorgesehenen Ende-zu-Ende-Digitalisierung entsprechend erweitert werden soll. Durch die Vorgabe verbindlicher Standards soll zudem ein einheitliches Barrierefreiheitsniveau von Verwaltungsleistungen im Sinne des OZG gewährleistet werden.

Die Vorschrift erstreckt sich darüber hinaus auf alle relevanten Interoperabilitätsstandards einschließlich der Prozessmodelle, Datenformate, Transportprotokolle und Schnittstellenbeschreibungen zur Anbindung von Onlinediensten, Fachverfahren und Basisdiensten.

Zu § 6 Absatz 2:

Vorgaben zu Schnittstellen für die Anbindung von Fachverfahren an den Portalverbund waren bisher in Absatz 2 geregelt. Da diese nunmehr bereits über Absatz 1 vorgegeben werden können, regelt Absatz 2 nur noch die Vorgabe von Standards für die Abwicklung von Verwaltungsverfahren, die der Ausführung von Bundesgesetzen oder der Durchführung von Rechtsakten der Europäischen Union, für die dem Bund die Gesetzgebungskompetenz zusteht, dienen.

Zu § 6 Absatz 3:

Der bisherige Absatz 3 wird gestrichen, da dessen Regelungsgehalt nunmehr ebenfalls in Absatz 1 enthalten ist.

Der bisherige Absatz 4 wird Absatz 3. Bei den geringfügigen Änderungen handelt es sich lediglich um Folgeanpassungen zu den Änderungen in den Absätzen 1 und 2.

Zu § 6 Absatz 4:

Die im Regierungsentwurf derzeit als § 3b OZG vorgesehene Regelung ist nunmehr auf Grund des bestehenden Sachzusammenhangs als neuer Absatz 4 in § 6 OZG enthalten und wird um einen neuen Satz 3 ergänzt, der die Übertragung der Veröffentlichung von Standards und Schnittstellen auf andere Stellen regelt.

Zu Buchstabe f (§ 7 Onlinezugangsgesetz)

Durch die Einbeziehung von Nutzerinnen und Nutzern bei der Planung und Entwicklung neuer elektronischer Angebote sollen die Anforderungen aller Nutzergruppen von Beginn an berücksichtigt werden, um ein größtmögliches Maß an Nutzerfreundlichkeit und Barrierefreiheit zu gewährleisten. Die Erfahrungen aus der Einbeziehung von Nutzenden nach § 7 OZG sollen auch in die kontinuierliche Weiterentwicklung des Servicestandards zu Qualitätsanforderungen für eine nutzerfreundliche Ausgestaltung, der künftig durch Rechtsverordnung nach § 6 OZG für verbindlich erklärt werden soll, einfließen.

Hierbei sollen insbesondere auch die Belange von Menschen mit unterschiedlichen Beeinträchtigungen berücksichtigt werden. Die Gestaltung neuer elektronischer Angebote hat daher nach Maßgabe des Behindertengleichstellungsgesetzes und der Barrierefreie Informationstechnik-Verordnung zu erfolgen. Elektronische Verwaltungsleistungen sollen insbesondere auch im Rahmen von Nutzertests auf ihre Barrierefreiheit hin überprüft werden.

Bei dem Angebot elektronischer Verwaltungsleistungen sind auch die Belange nicht-deutschsprachiger Nutzerinnen und Nutzer sowie regionaler Minderheiten angemessen zu berücksichtigen.

Zu Buchstabe g (§ 8 Onlinezugangsgesetz)

Um die Nachvollziehbarkeit und die Gesetzessystematik zu verbessern, wird § 8 insgesamt neu geordnet.

Zu § 8 Absatz 1:

In den neuen Absätzen 1 und 2 werden die Identifizierungsdaten des Bürgerkontos und des Organisationskonto jeweils in getrennten Absätzen dargestellt. Statt einzelne Identifizierungsdaten aufzuzählen wird außerdem, soweit wie möglich, auf einschlägige Regelungen zu den jeweiligen Datenquellen verwiesen. Auf diese Weise werden die Vorschriften harmonisiert und Unstimmigkeiten und Redundanzen vermieden. Die vorangestellte Einschränkung „soweit dies erforderlich ist“ stellt klar, dass nicht bei jeder Nutzeridentifizierung der vollständige Datensatz benötigt wird. Die Stelle, die eine Identifizierung jeweils anfordert, prüft die Erforderlichkeit im Hinblick auf die von ihr angebotene Leistung.

Absatz 1 Satz 1 Nummer 1 verweist für die Identifizierung im Rahmen des Bürgerkontos auf den maßgeblichen § 18 Absatz 3 des Personalausweisgesetzes (PAuswG), der alle Daten benennt, die bei Nutzung der eID-Funktion des Personalausweises übermittelt werden können. Die bisherige Aufzählung einzelner Daten in den Buchstaben a bis j ist damit obsolet. Dies gilt insbesondere auch für die Abkürzung „D“ für Bundesrepublik Deutschland, die Dokumentenart sowie das dienste- und kartenspezifische Kennzeichen, welche zum Datensatz der eID gehören. Durch die Verweisung auf § 18 Absatz 3 PAuswG wird der sogenannte Gemeindeschlüssel einbezogen, der für die Adressierung der zuständigen Meldebehörde über einen Verzeichnisdienst benötigt wird.

§ 12 des eID-Karte-Gesetzes und § 78 Absatz 5 des Aufenthaltsgesetzes (AufenthG) verweisen ebenfalls bereits auf § 18 Absatz 3 PAuswG, sodass insgesamt ein Gleichlauf der Vorschriften hergestellt wird.

Zu § 8 Absatz 2:

Die Datenquelle für Identifizierungsdaten im Rahmen des Organisationskonto sind die Register des Bundeszentralamts für Steuern (BZSt) sowie der Finanzämter. Zukünftig wird außerdem das im Aufbau befindliche Unternehmensbasisdatenregister zur Verfügung stehen. Absatz 2 referenziert daher neben § 139b Absatz 4a und § 139c Absatz 6a der Abgabenordnung (AO) auch auf § 3 UBRegG, der die Stammdaten, Identifikationsnummern und Metadaten von Unternehmen beschreibt. Auch wenn die in den Registern angelegten Daten bezüglich juristischer Personen und wirtschaftlich tätiger natürlicher Personen nur zum Teil personenbezogen sind, wird durch die Verweisung sichergestellt, dass die technische Ausgestaltung der Datenübermittlung an das Organisationskonto transparent erfolgt.

Der Verweis auf § 139b Absatz 4a AO ist notwendig, um alle relevanten Nutzergruppen im Rahmen des Organisationskontos abbilden zu können. § 139c AO erfasst nur solche Nutzer, die eine Wirtschafts-Identifikationsnummer erhalten. Es gibt Fallkonstellationen, in denen wirtschaftlich handelnden Personen (z.B. Freiberuflern, Gründern und vereinzelt auch Einzelunternehmern) eine solche Wirtschafts-Identifikationsnummer nicht zugewiesen wird. Entsprechend kann ihnen nach § 139c AO auch kein Datenkranz zugeordnet werden, sodass zur Identifizierung auf die in § 139b AO gelisteten Daten zurückgegriffen werden muss.

Durch die Verweisung auf § 139c Absatz 6a AO werden zugleich Verarbeitungsgrundlagen für die Identifizierung natürlicher Personen geschaffen, die wirtschaftlich tätig sind. In der bisherigen Fassung des OZG fehlte hier insbesondere das Datum „Firma oder Name des Unternehmens“.

In Absatz 2 Nummer 6 wurden die Identitätsdaten nach Absatz 1 sowie die Berechtigungsdaten der für eine Organisation handelnden natürlichen Person aufgenommen. Damit können sich neben gesetzlichen Vertretern und Mitgliedern eines Vertretungsorgans nun auch andere Vertreter und sonstige für eine Organisation handelnde Personen bei Nutzung des Organisationskontos identifizieren und dabei ihre Handlungsberechtigung anzeigen. Notwendig ist dies zum einen im Hinblick auf das Berechtigungsmanagement innerhalb des Organisationskontos. Zum anderen gibt es einzelne Unternehmensleistungen, die nur von bestimmten Personen beantragt werden dürfen (z.B. Geschäftsführer, Architekten). In diesem Fall besteht daher auch fachrechtlich die Notwendigkeit, eine für eine Organisation handelnde natürliche Person eindeutig identifizieren zu können.

Zu § 8 Absatz 3:

Infolge der Aufteilung des bisherigen Absatzes 1 wird der bisherige Absatz 2 zu Absatz 3.

§ 8 trifft alle notwendigen Festlegungen, um die Datenverarbeitung zum Zwecke der Identifizierung und Authentisierung zu erlauben. Das gilt insbesondere auch hinsichtlich natürlicher Personen, die sich authentifizieren, um für eine Organisation zu handeln. Gleichwohl sah die Rechtsgrundlage bisher vor, dass ergänzend dazu eine Einwilligung des Nutzers vorliegen muss (Mischtatbestand). Hier soll zukünftig mehr Klarheit geschaffen werden, indem der Begriff „mit Einwilligung“ durch die Formulierung „auf Veranlassung“ ersetzt wird. Das Gesetz und die dort verankerte Zweckbindung erlauben die Datenverarbeitung. Die bisherige Einwilligung ist kein zusätzlicher datenschutzrechtlicher Erlaubnistatbestand, sondern regelt die notwendige Steuerung durch den Nutzer.

Die Datenverarbeitung darf nur nach entsprechender freiwilliger Willensäußerung des Nutzers in Form eines aktiven Handelns erfolgen. Die jeweiligen Verarbeitungszwecke sowie Inhalt und Umfang der Datenverarbeitung sind dem Nutzer vorab transparent zu machen. Die Bereitstellung hinreichender Nutzerinformationen zur Veranlassung von Datenverarbeitungen ist dienstespezifisch zu prüfen und umzusetzen. Im Rahmen der BundID wird dies beispielsweise bei der Nutzerführung durch entsprechende Hinweise und Erklärungen gewährleistet werden.

Zu § 8 Absatz 4:

Infolge der Aufteilung des bisherigen Absatzes 1 wird der bisherige Absatz 1 Satz 3 zu einem eigenen Absatz 4. Die Vorschrift wird begrifflich an Absatz 5 angepasst. Der Begriff „mit Einwilligung“ wird in Angleichung an Absatz 3 außerdem durch die Formulierung „auf Veranlassung“ ersetzt.

Zu § 8 Absatz 5:

Der bisherige Absatz 3 wird zu Absatz 5. Der Verarbeitungstatbestand wird außerdem im Hinblick auf Funktionalitätserweiterungen des Nutzerkontos hin zu einer vorgangsbezogenen bidirektionalen Kommunikationskomponente erweitert.

Zu § 8 Absatz 6:

Der bisherige Absatz 4 wird zu Absatz 6.

Zu § 8 Absatz 7:

Der bisherige Absatz 5 wird zur Verbesserung der Gesetzessystematik aufgeteilt. Die einzelnen Regelungen finden sich nun nach Regelungszwecken geordnet in Absatz 7 und Absatz 8. Absatz 7 regelt die Speicherung personenbezogener Daten in Nutzerkonten. Hinsichtlich der Datenhaltung im Nutzerkonto gelten die Vorgaben des Anhangs 4 Nummer 2.8 der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) unabhängig von dem in Teil 3 der BSI-KritisV festgelegten Schwellenwert entsprechend.

Die Ergänzung einer 2-jährigen Löschfrist bei Inaktivität eines Bürgerkontos in Satz 3 verschafft sowohl den verantwortlichen Stellen als auch den betroffenen Nutzern Rechtsklarheit. Durch die automatische Hinweisfunktion gemäß Satz 4 werden ungewollte Datenverluste vermieden. Der Begriff „mit Einwilligung“ wird in Angleichung an Absatz 3 außerdem durch die Formulierung „auf Veranlassung“ ersetzt.

Zu § 8 Absatz 8:

Satz 1 ermöglicht die zur vollständig elektronischen Verfahrensabwicklung erforderliche Übermittlung und Weiterverarbeitung von Daten. Dazu zählen u.a. Kommunikationsdaten und Kommunikationsinhaltsdaten. Die Übermittlung der Daten an die für die Verwaltungsleistung zuständige Behörde, ein Verwaltungsportal oder einen Onlinedienst und die Verwendung der Daten durch diese kann beispielsweise erforderlich sein, um den Nutzer für die Inanspruchnahme von Servicefunktionalitäten eines Verwaltungsportals zu identifizieren oder einen „Single-Sign-On“, d. h. die einmalige Identifizierung an einem Portal zur Inanspruchnahme mehrerer Verwaltungsleistungen, zu ermöglichen, solange diese sich in derselben Domäne befinden. Daten können außerdem an einen Onlinedienst nach § 2 Absatz 8 OZG übermittelt werden, der diese dann gebündelt mit dem Antrag an die für eine Verwaltungsleistung zuständige Behörde übermittelt. Klarstellend werden nun auch die für die Abwicklung der elektronischen Bekanntgabe nach § 9 Absatz 1 OZG erforderlichen Daten aufgenommen.

Satz 2 stellt klar, dass die Verantwortung für den Datenabruf bei der abrufenden Stelle liegt, etwa bei der Fachbehörde. Der für das Nutzerkonto verantwortlichen Stelle ist es nicht möglich, zu prüfen, ob bzw. welche Daten für die jeweilige Leistung tatsächlich erforderlich sind.

Satz 3 trägt dem Zweckbindungsgrundsatz Rechnung und bestimmt, dass die Vorschrift keine Erlaubnis für zweckändernde Verarbeitungen beinhaltet. Dies ist auch deshalb geboten, weil zum Beispiel Kommunikationsinhaltsdaten eine Vielzahl (auch sensibler) Daten beinhalten können. Mit dem Zusatz "soweit gesetzlich nichts anderes bestimmt ist" wird insbesondere bereits bestehenden Rechtsvorschriften im Fachrecht Rechnung getragen, wenn dort eine zweckändernde Verarbeitung zugelassen wird.

Der Begriff „mit Einwilligung“ wird in Angleichung an Absatz 3 außerdem durch die Formulierung „auf Veranlassung“ ersetzt.

Zu § 8 Absatz 9:

Der neu gefasste Absatz 9 stellt klar, dass Datenverarbeitungen nach den Absätzen 1 bis 8 auch dann zulässig sind, wenn bei der elektronischen Abwicklung einer Verwaltungsleistung besondere Kategorien personenbezogener Daten anfallen. Die Regelung ist geboten, da die Nutzerkonten für alle Verwaltungsleistungen des Portalverbunds einsetzbar sein sollen. Dazu können bspw. auch Gesundheitsleistungen zählen.

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach Artikel 9 Absatz 2 Buchstabe g Verordnung (EU) 2017/679 zulässig, denn es besteht ein erhebliches öffentliches Interesse an der Ermöglichung einer vollständig digitalen Inanspruchnahme von Verwaltungsleistungen für Bürgerinnen und Bürgern sowie Unternehmen und an der Schaffung eines übergreifenden informationstechnischen Zugangs zu digitalen Verwaltungsleistungen, s. verfassungsrechtlicher Handlungsauftrag in Artikel 91c Absatz 5 GG. Mit der Bereitstellung von Nutzerkonten wird das Ziel verfolgt, diesen übergreifenden Zugang zu eröffnen und eine vollständig elektronische Abwicklung von Verwaltungsleistungen zu unterstützen. Bürgerinnen und Bürgern sowie Unternehmen wird ermöglicht, sich einheitlich für die im Portalverbund angebotenen elektronischen Verwaltungsleistungen zu identifizieren sowie übergreifend im Rahmen des jeweiligen Vorgangs mit der zuständigen Fachbehörde zu kommunizieren und insbesondere Bescheide elektronisch zu erhalten.

Die jeweils datenschutzrechtlich verantwortliche Stelle hat für die Verarbeitung insbesondere sensibler Daten gemäß Artikel 9 Absatz 1 Verordnung (EU) 2017/679 besondere technisch-organisatorische Maßnahmen zu treffen. Eine Orientierung an § 22 Absatz 2 Bundesdatenschutzgesetz (BDSG) bietet sich an.

Zu § 8 Absatz 10:

Gemäß Artikel 4 Nummer 7 Halbsatz 2 der Verordnung (EU) 2017/679 kann die datenschutzrechtliche Verantwortlichkeit auf Grundlage mitgliedstaatlichen Rechts bestimmt werden. Voraussetzung hierfür ist, dass Zwecke und Mittel der Datenverarbeitung durch das mitgliedstaatliche Recht ausreichend konkret vorgegeben sind. Die Zwecke und Mittel der Datenverarbeitung im Zusammenhang mit der Kontonutzung werden in § 8 Absatz 1 bis 9 ausführlich beschrieben. Vor dem Hintergrund, dass sowohl das Organisationskonto als auch das Bürgerkonto zukünftig zentrale, bundesweit angeschlossene Dienste sein werden, ist die gesetzgeberische Klarstellung der datenschutzrechtlichen Verantwortlichkeit aus Gründen der Transparenz und Rechtsklarheit geboten. Sie erleichtert die Zusammenarbeit von Bund und Ländern: Unsicherheiten bezüglich einer gemeinsamen Verantwortlichkeit der für die Konten zuständigen und der die Konten anbindenden Stellen gemäß Artikel 26 der Verordnung (EU) 2017/679, oder einer Auftragsdatenverarbeitung wird begegnet, indem stattdessen eine konzentrierte, alleinige datenschutzrechtliche Verantwortlichkeit der für das Nutzerkonto zuständigen Stelle festgelegt wird. Satz 2 stellt klar, dass die konzentrierte Verantwortlichkeit auch von mehreren für die Konten zuständigen Stellen gemeinsam getragen werden kann.

Ausdrücklich keine Festlegung soll mit der Regelung bezüglich der Verantwortlichkeit der an die Konten angebundenen Fachverfahren, Onlinedienste oder Verwaltungsportale getroffen werden, diese bleibt dadurch unberührt.

Zu Buchstabe h (§ 8a Onlinezugangsgesetz)

Die Formulierung „länderübergreifender Onlinedienst“ dient der Klarstellung, dass die Vorschrift lediglich auf solche Onlinedienste Anwendung findet, die länderübergreifend entwickelt und betrieben werden, nicht jedoch auf landesspezifische Lösungen.

Zu Buchstabe i (§ 10 Onlinezugangsgesetz)

Zu Doppelbuchstabe aa

Zu § 10 Absatz 1:

Das Datenschutzcockpit soll es den Bürgerinnen und Bürgern ermöglichen, jederzeit nachzuvollziehen, welches Register personenbezogene Daten an welche öffentliche Stelle übermittelt hat und welche Bestandsdaten bei den Registern hinterlegt sind. Die Realisierung dieses Anspruchs sollte aufgrund der noch ausstehenden Vernetzung der Behörden Schritt für Schritt mit der Einführung der Identifikationsnummer erfolgen.

Für diesen Transparenzanspruch ist ein IT-Architekturmodell zugrunde gelegt worden, welches auf zusätzliche Speicherung von personenbezogenen Daten verzichtet und verhindert, dass an einer Stelle alle Daten der Bürgerinnen und Bürger gespeichert und von Unberechtigten abgerufen werden können (sog. Quellenmodell).

Der Abruf der Daten zur Anzeige im Datenschutzcockpit erfolgt in jeder Sitzung nach Anforderung durch den Nutzer erneut, d.h. beim Datenschutzcockpit werden keine Daten dauerhaft vorgehalten. Um eine hohe Datenqualität sicherzustellen und zu verhindern, dass Daten von anderen Personen aufgrund von Verwechslungen bei der Zuordnung angezeigt werden, dient die Identifikationsnummer als Zuordnungsmerkmal für die Anfrage des Datenschutzcockpits und Rückmeldung der registerführenden Stellen. Aus diesem Grund ist der Anwendungsbereich des Datenschutzcockpits derzeit auf Protokoll- und Inhaltsdaten nach § 9 des Identifikationsnummerngesetzes (IDNrG) und Bestandsdaten der Register beschränkt. Sobald eine technische Erweiterung möglich ist, sollen, nachdem die rechtlichen Voraussetzungen dafür geschaffen wurden, jegliche Datenübermittlungen zwischen öffentlichen Stellen angezeigt werden, die ohne Verwendung der Identifikationsnummer erfolgten. Durch die Ergänzung, dass „bis zum Vorliegen der technischen und rechtlichen Voraussetzungen für eine Erfassung weiterer Datenübermittlungen zunächst“ diejenigen Datenübermittlungen erfasst sind, bei denen eine Identifikationsnummer nach § 5 IDNrG zum Einsatz kommt, wird sichergestellt, dass die technische Entwicklung des Datenschutzcockpits eine Erweiterungsmöglichkeit im Sinne des Entschließungsantrags der Fraktionen SPD, BÜNDNIS 90/Die Grünen und FDP vom 19. Juni 2023 (Ausschussdrucksache 20(4)258) schafft, die Schritt für Schritt umgesetzt werden soll. Die Erweiterungsmöglichkeiten sehen insbesondere vor, dass im Rahmen des Nachweisabrufs und der Nachweiserbringung nach § 5 des E-Government-Gesetzes (EGovG) auch solche Datenübermittlungen im Datenschutzcockpit für die Bürgerinnen und Bürger angezeigt werden, bei denen andere Identifier als die Identifikationsnummer nach dem Identifikationsnummerngesetz als Zuordnungsmerkmal genutzt werden. Dies setzt auch die Schaffung entsprechender Protokollierungsregelungen solcher Datenübermittlungen voraus, wie sie für die Datenübermittlungen unter Nutzung der Identifikationsnummer in § 9 IDNrG bereits vorgesehen sind. Dies gilt entsprechend für die sozialdatenschutzrechtliche Regelung in § 67f des Zehnten Buches Sozialgesetzbuch (SGB X).

Zu § 10 Absatz 2:

§ 10 Absatz 2 Satz 1 OZG bezieht sich derzeit auf die Protokolldaten gemäß § 9 IDNrG, sowie auf die zugehörigen Inhalts- und Bestandsdaten der Register. Adressat der Anzeigepflicht waren bisher nur die Register (vgl. § 2 Nr. 3 IDNrG).

Damit der gesamte Weg der Datenübermittlungen unter Nutzung der Identifikationsnummer vollständig und verständlich für die Bürgerinnen und Bürger im Datenschutzcockpit angezeigt werden kann, sollen zusätzlich die Datenübermittlungen der Registermodernisierungsbehörde im Datenschutzcockpit zur Anzeige gebracht werden.

Die Registermodernisierungsbehörde protokolliert die Datenübermittlungen zwischen der Registermodernisierungsbehörde und dem Bundeszentralamt für Steuern sowie alle Datenabrufe von öffentlichen Stellen bei der Registermodernisierungsbehörde, vgl. § 9 Absatz 1 Satz 2 IDNrG. Dabei ruft die Registermodernisierungsbehörde auf Anforderung berechtigter öffentlicher Stellen (§ 6 Absatz 1 und 2 IDNrG) die Identifikationsnummer und ggf. weitere Daten zur Person (§ 4 Absatz 2 und 3 IDNrG) beim Bundeszentralamt für Steuern ab und übermittelt diese an die abrufende Stelle. Diese Datenübermittlungen werden bisher jedoch nicht im Datenschutzcockpit angezeigt. Um die Anfragen bei der Registermodernisierungsbehörde und die sich daran anschließenden Datenübermittlungen vollständig abzubilden, soll auch die Registermodernisierungsbehörde an das Datenschutzcockpit angeschlossen werden.

Bei der Registermodernisierungsbehörde liegen jedoch keine Bestandsdaten vor, die angezeigt werden könnten. Aus diesem Grund können nur die Bestandsdaten der Register im Datenschutzcockpit zur Anzeige gebracht werden.

Zu Doppelbuchstabe bb

Folgeänderung zu Doppelbuchstabe aa.

Zu Buchstabe j (§ 11 Onlinezugangsgesetz)

§ 11 OZG stellte eine Übergangsregelung zum Einsatz des Datenschutzcockpits bis zum Inkrafttreten des § 10 OZG dar. Mit dem Inkrafttreten des § 10 OZG am 31. August 2023 (vgl. Bekanntmachung des Bundesministeriums des Innern und für Heimat vom 24. August 2023, BGBl. 2023 I Nr. 230 vom 31. August 2023) ist der bisherige § 11 OZG gegenstandslos geworden und wird durch eine Regelung zu Monitoring und Evaluierung ersetzt.

Die gesetzliche Verankerung des Monitorings für die Umsetzung der Vorschriften dieses Gesetzes unterstreicht die Bedeutung, die ein laufendes und qualitatives Monitoring für die weitere OZG-Umsetzung hat. Das Bundesministerium des Innern und für Heimat wird sein regelmäßiges Monitoring zur Umsetzung der Vorschriften dieses Gesetzes verstärken und im Bund und bei den Ländern, einschließlich der Kommunen, insbesondere folgende Kriterien in seinem Monitoring abfragen: Nutzerfreundlichkeit, Barrierefreiheit, Reifegrad, Umsetzungsstand einer „Einer für Alle“-Leistung (EfA-Leistung), Überblick über den Anteil der "digitalen" Verwaltungsvorgänge im Verhältnis zu den "nichtdigitalen" Bestandsprozessen, Nutzungs- und Abbruchquoten, Zufriedenheitswerte, Verbreitungsgrade, Nutzung von Standards und Open-Source-Produkten, Angabe der Lizenz und Benennung der Fachverfahrenshersteller. Aus dem Monitoring soll sich in geeigneter Darstellung ergeben, welche Länder und Kommunen die jeweiligen OZG-Leistungen nicht digital anbieten.

Das Bundesministerium des Innern und für Heimat stellt die durch das Monitoring gewonnenen Daten über das „Dashboard Digitale Verwaltung“ der allgemeinen Öffentlichkeit auf Basis einer offenen Schnittstelle bereit.

Die Evaluierung des Gesetzes erfolgt durch eine vom Bundesministerium des Innern und für Heimat zu beauftragende fachunabhängige wissenschaftliche

Einrichtung. Die Evaluierung nutzt unter anderem die frei und öffentlich zugänglichen Daten des Monitorings und wird möglichst zeitgleich mit dem Inkrafttreten des Gesetzes als fortlaufende wissenschaftliche Begleitung beauftragt.

Zu Buchstaben k (§ 12 Onlinezugangsgesetz)

Als Folgeänderung zu der Aufhebung des § 11 OZG wird der bisherige § 13 OZG-E zu § 12 OZG-E.

Zu § 12 Absatz 1:

Absatz 1 bleibt unverändert.

Zu § 12 Absatz 2:

Durch den neu eingefügten § 12 Absatz 2 Satz 2 wird das Bundesministerium des Innern und für Heimat ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, eine von § 12 Absatz 2 Satz 1 abweichende längere Frist für die Möglichkeit des Einsatzes von ELSTER-Softwarezertifikaten als Identifizierungsmittel im Bürgerkonto festzulegen. Angesichts des hohen Verbreitungsgrades von ELSTER-Softwarezertifikaten und der vergleichsweise noch weniger verbreiteten Nutzung der eID-Funktion des Personalausweises wird so der Überlegung Rechnung getragen, dass auch nach Ablauf der Frist nach § 12 Absatz 2 Satz 1 ein Bedürfnis für eine Verlängerung des Einsatzes von ELSTER-Softwarezertifikaten als Beschleuniger für den Nutzungsgrad digitaler Verwaltungsleistungen bestehen könnte.

Zu § 12 Absatz 3:

Durch die Änderung von einer Ermessensvorschrift in eine gebundene Vorschrift wird klargestellt, dass eine öffentliche Stelle bis zum Ablauf der Frist nach § 3 Absatz 4 Nummer 2 Buchstabe a OZG-E von der Verwendung des einheitlichen Organisationskontos abzusehen hat, wenn für die Inanspruchnahme einer elektronischen Verwaltungsleistung und die sonstige elektronische Kommunikation ein höheres Vertrauensniveau als „substantiell“ erforderlich ist und ein Identifizierungsmittel auf einem höheren Vertrauensniveau im Organisationkonto noch nicht zur Verfügung steht.

Zu § 12 Absatz 4:

Im Rahmen von EU-Agrarförderprogrammen auf Grundlage der hier abschließend aufgezählten EU-Verordnungen werden digitale Förderanträge im Rahmen der LEADER-Förderung gestellt. Über ein etabliertes elektronisches Antragsverfahren erfolgt die Authentifizierung der Antragstellenden über Software-Zertifikate. Die Berücksichtigung der Fonds ELER und EGFL im Rahmen der Übergangsregelung gemäß § 12 Absatz 4 stellt sicher, dass die Nutzung bereits digitalisierter, bis zum Ablauf der EU-Förderperiode 2027 befristeter Lösungen für Fachverfahren noch möglich ist und eine hinreichende Umbaufrist bis 2031 gewährt wird.

Zu § 12 Absatz 5:

Das Bundesministerium des Innern und für Heimat und das Bundesministerium der Finanzen werden ermächtigt, durch gemeinsame Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, die Fristen für den Einsatz von ELSTER-Softwarezertifikaten und anderer Identifizierungsmittel, die nach der eIDAS-Verordnung auf dem Vertrauensniveau „substantiell“ anerkannt sind, im Organisationskonto zu verlängern, falls nach Ablauf der Frist nach § 3 Absatz 4 Nummer 2 Buchstabe a und b für Unternehmen kein Identifizierungsmittel auf dem Vertrauensniveau „hoch“ zur Verfügung steht.

Zu § 12 Absatz 6:

§ 10 Absatz 3a des Personalausweisgesetzes (PAuswG) sieht vor, dass das Bundesministerium des Innern und für Heimat nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik für Fälle, in denen der Nachweis der Identität durch einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erbracht wurde, für die spätere Authentisierung des Inhabers des elektronischen Identitätsnachweises bis zur Einführung und ausreichenden Verbreitung der EU-Wallet auch andere Authentisierungsmittel befristet zulassen soll (vgl. Artikel 8f).

Um auch im Rahmen der Inanspruchnahme elektronischer Verwaltungsleistungen eine niederschwellige Authentisierung zu ermöglichen, kann die Authentisierung über das Bürgerkonto durch befristet zugelassene Authentisierungsmittel nach § 10 Absatz 3a PAuswG erfolgen, sofern die (Erst-)Identifizierung durch einen elektronischen Identitätsnachweis nach § 3 Absatz 4 Nummer 1 OZG erfolgt ist und die Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik ergibt, dass das Authentisierungsmittel ein für die elektronische Abwicklung von Verwaltungsleistungen geeignetes Vertrauensniveau erfüllt.

Zu Nummer 2 (Änderung Artikel 2)

Zu Buchstabe a (§ 2 E-Government-Gesetz)

Zu Doppelbuchstabe aa

Die Verpflichtung von Bundesbehörden zur Eröffnung eines elektronischen Zugangs durch eine De-Mail-Adresse hat sich angesichts der geringen Nutzung von De-Mail als unwirtschaftlich erwiesen und soll zukünftig nicht mehr bestehen.

Zu Doppelbuchstabe bb

Folgeänderung zu Nummer 2 Buchstabe a Doppelbuchstabe aa.

Zu Buchstabe b (§ 2a E-Government-Gesetz)

Die Länder sollen die Möglichkeit erhalten, den zentralen Siegeldienst des Bundes, insbesondere im Rahmen des Zusammenwirkens von Bund und Ländern nach Artikel 91c Absatz 1 GG bei der Umsetzung des OZG, auf der Grundlage einer entsprechenden Verwaltungsvereinbarung, welche auch die konkrete Ausgestaltung und die Bedingungen (insbesondere auch die Kostentragung) für eine Nachnutzung durch die Länder regelt, mitzunutzen. Eine über die Nutzung für elektronische Verwaltungstätigkeiten im Rahmen der OZG-Umsetzung hinausgehende Nutzung wird nicht verwehrt.

Zu Buchstabe c (§ 4 E-Government-Gesetz)

Zur Gewährleistung einer möglichst nutzerfreundlichen Abwicklung von Zahlungsverfahren im Rahmen elektronisch durchgeführter Verwaltungsverfahren ist die jeweilige Behörde zum Angebot verschiedener im elektronischen Geschäftsverkehr üblicher Zahlungsverfahren verpflichtet. Dabei haben Verwaltungsleistungen auch kreditkartenunabhängige Zahlungsverfahren anzubieten. Da eine vollständig barrierefreie Ausgestaltung sämtlicher gängiger Zahlungsverfahren privater Anbieter nicht sichergestellt werden kann, gängige Zahlungsverfahren aber auch nicht ausgeschlossen werden sollen, werden die Behörden zum Angebot „möglichst barrierefreier“ Zahlungsverfahren verpflichtet.

Zu Buchstabe d

Zu Doppelbuchstabe aa (§ 5 E-Government-Gesetz)

Die Einfügung steht im Zusammenhang mit der in § 10 Absatz 1 Satz 2 OZG erfolgten Ergänzung, wonach im Datenschutzcockpit bei Vorliegen der rechtlichen und technischen Voraussetzungen zukünftig auch Datenübermittlungen ohne Nutzung der Identifikationsnummer nach dem IDNrGangezeigt werden sollen. Derzeit ist der Anwendungsbereich des Datenschutzcockpits auf die Nutzung einer Identifikationsnummer nach dem IDNrG beschränkt.

Sobald eine technische Erweiterung möglich ist, sollen, nachdem die rechtlichen Voraussetzungen dafür geschaffen wurden, jegliche Datenübermittlungen zwischen öffentlichen Stellen im Datenschutzcockpit angezeigt werden, die ohne Verwendung der Identifikationsnummer erfolgen. Diese Ergänzung trägt der Erweiterungsmöglichkeit im Sinne des Entschließungsantrags der Fraktionen SPD, BÜNDNIS 90/Die Grünen und FDP vom 19. Juni 2023 (Ausschussdrucksache 20(4)258) Rechnung, die Schritt für Schritt umgesetzt werden soll. Die Erweiterungsmöglichkeiten sehen insbesondere vor, dass im Rahmen des Nachweisabrufs und der Nachweiserbringung nach § 5 EGovG auch solche Datenübermittlungen im Datenschutzcockpit für die Bürgerinnen und Bürger angezeigt werden, bei denen andere Identifier als die Identifikationsnummer nach dem IDNrG als Zuordnungsmerkmal genutzt werden. Die Einfügung schafft entsprechende Protokollierungsregelungen für solche Datenübermittlungen, wie sie für die Datenübermittlungen unter Nutzung der Identifikationsnummer in § 9 IDNrG bereits vorgesehen sind.

Sobald die technischen und rechtlichen Voraussetzungen für eine Anzeige der Datenübermittlungen im Datenschutzcockpit vorliegen und das Bundesministerium des Innern und für Heimat dies im Bundesanzeiger bekannt gibt, besteht bei Datenübermittlungen zwischen öffentlichen Stellen eine Protokollierungspflicht durch die jeweiligen Stellen in einer Weise, die die Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt.

Die Regelung legt die Art und Weise der Protokollierung fest. Die Maßgabe, dass die Protokolle die Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützen, soll es ermöglichen, aus den Protokolldaten vereinfacht Hinweise auf die ggf. missbräuchliche Durchführung von Datenabrufen abzulesen oder Protokolldaten automatisiert auszulesen. Damit kann beispielsweise ein Fall gehäufter Abrufe von Registern nach bestimmten, mit der Aufgabenerfüllung der jeweiligen Behörde nicht in Zusammenhang stehenden Ereignissen erkannt werden. Dies dient der datenschutzrechtlichen Kontrolle der Datenabrufe und des Zugriffsmanagements. Der Umfang der Protokolldaten ergibt sich aus Artikel 15 Absatz 1 und Artikel 5 Absatz 2 der DSGVO.

Zu Doppelbuchstabe bb (§ 6 E-Government-Gesetz)

Die Änderung dient der Klarstellung, dass die Anhörung der kommunalen Spitzenverbände vor der Beteiligung des Bundesrates zu erfolgen hat.

Zu Buchstabe e (§ 9a E-Government-Gesetz)

Durch die Änderung soll eine zu § 4 Absatz 1 EGovG gleichlautende Formulierung hergestellt werden.

Zu Buchstabe f (§§ 16 und 16a E-Government-Gesetz)

Nach § 16 wird ein neuer § 16a eingefügt. Zur Steigerung der digitalen Souveränität sollen die Behörden des Bundes offene Standards nutzen und vorrangig Software mit offenem Quellcode einsetzen. Wird eine genutzte Software weiterentwickelt, so ist der weiterentwickelte Quellcode unter eine

geeignete Software- und Open-Source-Lizenz zu stellen und zu veröffentlichen, soweit der Veröffentlichung keine zwingenden sicherheitsrelevanten Gründe entgegenstehen und dies lizenzrechtlich zulässig ist. Die Software soll auch als Referenzimplementierung veröffentlicht werden.

Zu Nummer 3 (Änderung des IT-Netz-Gesetzes)

Die Änderung dient der Klarstellung, dass vor der Festlegung anderer Netze nach § 3 Absatz 1 IT-Netz-Gesetzes eine Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik zu erfolgen hat.

Zu Nummer 4 (Änderung der Verordnung nach § 3 Absatz 2 Satz 2 des Onlinezugangsgesetzes)

Folgeänderung zu Nummer 1 Buchstabe b.

Zu Nummer 5

Zu Artikel 8a Nummer 1 (§ 139b Abgabenordnung)

Für die Adressierung der zuständigen Meldebehörde über einen Verzeichnisdienst ist die Verwendung des sogenannten amtlichen Gemeindeschlüssels (AGS – DSMeld-Blatt 1201) erforderlich. § 18 Absatz 3 Nummer 6a PAuswG regelt eine entsprechende Übermittlungsbefugnis für den AGS aus dem Personalausweis. In 139c Absatz 3 bis 5 der Abgabenordnung (AO) ist der amtliche Gemeindeschlüssel bereits als Datum verankert. Eine korrespondierende Norm in § 139b AO gab es bisher nicht, deshalb werden Absatz 3 Nummer 7 und Absatz 6 Satz 1 Nummer 5 entsprechend neugefasst.

Die nach § 139b AO gespeicherten Daten dürfen nur auf Veranlassung des Nutzers eines Nutzerkontos elektronisch an das Nutzerkonto übermittelt werden.

Zu Artikel 8a Nummer 2 (§ 139c Abgabenordnung)

Zu Buchstabe a

Die Speicherung des Altgerichts ist notwendig, um in einigen Fallkonstellationen eindeutig Handelsregisterauszüge zu Unternehmen zuordnen zu können. Den Angaben des Ministeriums der Justiz des Landes Nordrhein-Westfalens zufolge wird für ca. 12 Prozent der Eintragungen im Handelsregister der Parameter „Altgericht“ notwendig sein, um den Rechtsträger eindeutig zu identifizieren. Es existieren Rechtsträger, die sich bei gleicher Kombination von Registergericht/Registerart/Registernummer nur durch das Altgericht eindeutig zuordnen lassen.

Zu Buchstabe b

Der Speicherungs- und Übermittlungsbefugnisse zum Zwecke der Identifizierung per OZG-Nutzerkonto werden u. a. durch Verweis auf § 139c Absatz 3 AO ergänzt. Dies ist notwendig, um auch die unternehmensbezogenen Daten von natürlichen Personen, die wirtschaftlich tätig sind, an ein Organisationskonto im Sinne des OZG zu übermitteln und damit das Konto für sie nutzbar machen zu können. Die nach § 139c AO gespeicherten Daten dürfen allerdings nur auf Veranlassung des Nutzers eines Nutzerkontos elektronisch an das Nutzerkonto übermittelt werden.

Zu Artikel 8b (Änderung des Einführungsgesetzes zur Abgabenordnung)

In Artikel 97 § 5a des Einführungsgesetzes zur Abgabenordnung wird in einem neuen Absatz 2 bestimmt, dass die Neuregelungen in § 139b Absatz 3, 4a und 6 sowie § 139c Absatz 3 bis 6a AO (vgl. Artikel 8a) erst ab dem Tag anzuwenden sind, an dem das Bundesministerium der Finanzen im Bundesgesetzblatt bekannt

gibt, dass die technischen Voraussetzungen für die Verarbeitung des amtlichen Gemeindeschlüssels und des Altgerichts jeweils vorliegen.

Zu Artikel 8c (Änderung der Zivilprozessordnung)

Durch die Änderungen soll für elektronische Dokumente von Behörden oder von ihnen in ein elektronisches Dokument übertragene öffentliche Urkunden die Echtheitsvermutung des § 437 ZPO auch dann gelten, wenn das elektronische Dokument mit einem qualifizierten elektronischen Siegel (vgl. Artikel 35 ff. der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [eIDAS-VO]) der Behörde versehen ist. Die Änderung knüpft an die vorgesehenen Regelungen zur schriftformersetzenden Verwendung von qualifizierten elektronischen Siegeln in Verwaltungsentscheidungen an.

Die Streichung des Zusatzes „öffentliche“ Behörde ist lediglich redaktioneller Natur. Eine Rechtsänderung ist damit nicht verbunden.

Zu Artikel 8d (Änderung des Bundesberggesetzes)

Nach den Vorgaben des OZG sind auch die bergrechtlichen Genehmigungsverfahren zu digitalisieren. Die jetzige Fassung des § 16 des Bundesberggesetzes steht dem jedoch entgegen, weil in dieser Formvorschrift die elektronische Form für Bergbauberechtigungen ausdrücklich ausgeschlossen wird. Um die digitale Verfahrensführung auch hier zu ermöglichen, wird diese Einschränkung aufgehoben.

Zu Artikel 8e (Änderung des Zehnten Buches Sozialgesetzbuch)

Zu Artikel 8e Nummer 1 (Änderung der Inhaltsübersicht)

Es handelt sich um Folgeänderungen in der Inhaltsübersicht aufgrund der Einfügungen von § 67f des Zehnten Buches Sozialgesetzbuch (SGB X) und § 77a SGB X.

Zu Artikel 8e Nummer 2 (§ 67a Zehntes Buch Sozialgesetzbuch)

Es wird klargestellt, dass die Wahlentscheidung der betroffenen Person nach § 67f Absatz 1 Satz 1 Nummer 1 in Verbindung mit Absatz 4 Satz 2 SGB X eine unmittelbare Erhebung von Sozialdaten bei der betroffenen Person darstellt. Gleiches gilt für den Anwendungsbereich des § 77a SGB X in Verbindung mit Artikel 14 der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1; Single Digital Gateway-Verordnung, SDG-VO), nach dem eine Nachweiserbringung auf ausdrückliches Ersuchen der betroffenen Person zu erfolgen hat.

Zu Artikel 8e Nummer 3 (§ 67f Zehntes Buch Sozialgesetzbuch)

Die Regelung schafft die sozialdatenschutzrechtliche Grundlage für die effiziente und zielgerichtete Umsetzung des Once-Only-Prinzips entsprechend des neuen § 5 EGovG. Nach dem Grundsatz der einmaligen Datenerfassung (Once-Only-Prinzip) sollen Bürgerinnen und Bürger sowie Unternehmen die für Verwaltungsleistungen erforderlichen Nachweise nur noch einmal übermitteln müssen; im Gegenzug sollen Behörden die vorhandenen Daten auf Veranlassung der betroffenen Person einfach und sicher austauschen können. Die Entscheidung der Bürgerin oder des Bürgers, den Nachweisabruf zu veranlassen, ist ein voluntatives Element, das ihre oder seine Mitwirkung absichert.

Die Generalklausel in § 5 EGovG stellt dabei aber keine sozialdatenschutzrechtliche Verarbeitungsgrundlage dar, da der Sozialdatenschutz im Sozialgesetzbuch (in Verbindung mit der Datenschutzgrundverordnung – DSGVO) abschließend geregelt ist (vgl. § 35 Absatz 2 Satz 1 des Ersten Buches Sozialgesetzbuch (SGB I)) und auch das EGovG für den Sozialdatenschutz keine Anwendung findet (vgl. § 1 Absatz 4 EGovG). Erforderlich ist daher eine eigenständige datenschutzrechtliche Regelung im Bereich des Sozialdatenschutzes für die Sozialverwaltung, damit auch Sozialdaten nach dem Once-Only-Prinzip verarbeitet werden dürfen.

Die Neuregelung legt fest, dass die betroffene Person im Sinne eines sonstigen voluntativen Elements bei elektronischen Verwaltungsverfahren die Wahl hat zwischen zwei Möglichkeiten: Sie kann den Nachweis entweder selbst digital einreichen oder einen behördenseitigen, elektronischen Nachweisabruf veranlassen. Sozialdaten, die der Verwaltung damit bereits vorliegen, können somit nach Wahl der betroffenen Person automatisiert abgerufen werden („die Daten sollen laufen, nicht die Bürgerin oder der Bürger"). Die Möglichkeit, den Nachweis selbst digital einzureichen, bleibt daher bestehen.

Die Neuregelungen des § 67f SGB X und auch des § 77a SGB X sind in Form sozialdatenschutzrechtlicher Generalklauseln selbst Rechtsgrundlage im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO. Parallel dazu regelt auch die Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates (SDG-Verordnung) in Artikel 14 Absatz 4, dass die Nutzung des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen (EU-Once-Only-Technical-System, EU-OOTS) grundsätzlich nicht verbindlich und nur auf ausdrückliches Ersuchen des Nutzers gestattet ist. Dieses ausdrückliche Ersuchen stellt nach Auffassung der Europäischen Kommission keine Einwilligung im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a DSGVO dar (vgl. Europäische Kommission, Arbeitsdokument, Datenschutzfolgenabschätzung zur Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates, SWD(2022) 211 final, S. 5f.).

Die Begriffe der nachweisanfordernden und der nachweisliefernden Stelle wurden im Gleichlauf mit § 5 EGovG in Anlehnung an den Wortlaut in Artikel 1 Nummer 2 und 3 der Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates gewählt (dort „Nachweise anfordernde Behörde“ und „Nachweislieferant“). Verfolgt wird damit das Ziel einer möglichst einheitlichen Bezeichnung der datenaustauschenden Akteure auf europäischer und nationaler Ebene.

Zu § 67f Absatz 1:

Absatz 1 Satz 1 Nummer 1 dient der Umsetzung des Once-Only-Prinzips. Nachweise, die der Verwaltung bereits vorliegen, können direkt bei der ausstellenden Behörde abgerufen werden. Inhaltlich korrespondiert die Regelung mit § 5 Absatz 1 und 2 EGovG.

Nach Absatz 1 Satz 1 erhält die betroffene Person bei elektronischer Durchführung eines Verwaltungsverfahrens hinsichtlich der Art der

Nachweiserbringung grundsätzlich die Wahlmöglichkeit zwischen zwei verschiedenen Wegen. Sie hat die Wahl zwischen einem behördenseitigen, automatisierten Nachweisabruf (Nummer 1) oder der Möglichkeit, den Nachweis selbst elektronisch zu erbringen (Nummer 2). Diese Möglichkeit verbleibt daher weiterhin.

Die Wahlmöglichkeit nach Absatz 1 Satz 1 Nummer 1 gegenüber der nachweisanfordernden Stelle besteht nur, wenn der jeweilige Nachweis bereits elektronisch vorliegt und ohne zeitlichen Verzug, d.h. innerhalb kürzester Zeit, automatisiert abgerufen werden kann. Gemeint ist ein fachlich synchrones Abrufverfahren. Sobald also eine menschliche Interaktion notwendig ist und es sich daher um ein asynchrones Abrufverfahren handelt, kann die Behörde zwar eine Abrufmöglichkeit eröffnen, muss dies aber nicht. Für welche Nachweise ein Once-Only-Nachweisabruf möglich ist, steht im Vorfeld fest und ist technisch hinterlegt. Dasselbe gilt für die für das jeweilige Verfahren erforderlichen Nachweise und Stellen, welche im konkreten Fall nachweisanfordernde und nachweisliefernde Stelle sind. Die Norm berücksichtigt zudem die Möglichkeit, dass für ein Verwaltungsverfahren mehrere Nachweise erforderlich sein können. Insofern kann die Wahlmöglichkeit für den „jeweiligen“ Nachweis ausgeübt werden, sofern die Voraussetzungen für den Once-Only-Nachweisabruf vorliegen.

Der Wortlaut der Norm stellt mangels Einschränkung darüber hinaus klar, dass sowohl antragsgebundene als auch antragslose Verwaltungsverfahren nach dem Sozialgesetzbuch erfasst sind.

Der Anwendungsbereich der Norm ist insofern verengt, als sie sich nur auf die elektronische Durchführung von Verwaltungsverfahren erstreckt. Die Kommunikation zwischen einer Behörde und einer Bürgerin oder einem Bürger per E-Mail fällt in diesem Kontext nicht unter den Begriff der elektronischen Durchführung eines Verwaltungsverfahrens. Gemeint ist die Nutzung eines Onlinedienstes, welcher beispielsweise über ein Verwaltungsportal auffindbar ist. Dazu zählt auch ein hybrides Verfahren, bei dem nicht nur Nachweise im Sinne der Norm erforderlich sind, sondern auch andere Beweismittel, welche nicht elektronisch erbracht werden können. Dies ist zum Beispiel der Fall, wenn gemäß § 21 Absatz 1 Nummer 4 SGB X etwas in Augenschein genommen werden muss. Nach dem Untersuchungsgrundsatz (§ 20 SGB X) hat die für die Entscheidung zuständige Behörde aber auch weiterhin die Möglichkeit, einen Nachweis im Original zu verlangen, sofern beispielsweise im Einzelfall Zweifel an der Authentizität eines Dokuments bestehen. Die in den §§ 20 und 21 SGB X genannten Möglichkeiten zur Sachverhaltsermittlung bleiben weiterhin bestehen. Insofern ist ein hybrides Verfahren mit elektronischen Nachweisen und analoger Beweisführung denkbar.

In Absatz 1 Satz 2 bis 4 werden die zentralen, normbestimmenden Begriffe „Nachweis“, „nachweisanfordernde“ und „nachweisliefernde Stelle“ entsprechend § 5 Absatz 2 EGovG definiert.

Nachweise sind nach Absatz 1 Satz 2 Unterlagen und Daten jeder Art unabhängig vom verwendeten Medium, die zur Ermittlung des Sachverhalts geeignet sind. In Anlehnung an die Definition in Artikel 3 Nummer 5 der Verordnung (EU) 2018/1724 vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1) wird der Nachweisbegriff weit gefasst. Der weite Nachweisbegriff wird aber bezüglich des automatisierten Abrufs insofern eingeschränkt, als nur solche Nachweise erfasst sind, die elektronisch vorliegen und ohne zeitlichen Verzug automatisiert abgerufen werden können. Durch das

Begriffspaar „Unterlagen und Daten“ wird dem Verständnis des Datenbegriffs in der Informatik Rechnung getragen, der dort enger aufgefasst wird als im allgemeinen Sprachgebrauch. Das Begriffspaar „Unterlagen und Daten“ wird im SGB X in Anlehnung an Artikel 3 Nummer 5 der Verordnung (EU) 2018/172) und § 5 EGovG Absatz 2 EGovG verwendet und erfasst Sozialdaten (§ 67a Absatz 2 Satz 1 SGB X) sowie den Sozialdaten gleichgestellte Betriebs- und Geschäftsgeheimnisse (§ 35 Absatz 4 SGB I, § 67 Absatz 2 Satz 2 SGB X).

Die Begriffe der nachweisanfordernden Stelle und der nachweisliefernden Stelle wurden in Anlehnung an den Wortlaut in Artikel 1 Nummer 2 und 3 der Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates ausgewählt (dort „Nachweise anfordernde Behörde“ und „Nachweislieferant“). Verfolgt wird damit das Ziel einer möglichst einheitlichen Bezeichnung der datenaustauschenden Akteure auf europäischer sowie nationaler Ebene. Die Sätze entsprechen § 5 Absatz 2 EGovG.

Gemäß Absatz 1 Satz 3 kann die nachweisanfordernde Stelle entweder die öffentliche Stelle selbst sein, die entscheidet, oder aber eine andere öffentliche Stelle, die dafür zuständig ist, den Nachweis einzuholen und anschließend an die zuständige Behörde weiterzuleiten. Solche anderen öffentlichen Stellen können beispielsweise Stellen sein, die für eine Portallösung oder einen „Einer für Alle“-Onlinedienst (EfA-Onlinedienst) zuständig sind. In Satz 4 wird klargestellt, dass die nachweisliefernde Stelle diejenige Stelle ist, die für die Ausstellung des Nachweises zuständig ist. Damit wird der Umstand berücksichtigt, dass mehrere Behörden über einen Nachweis verfügen können, aber nur eine Stelle für die Aktualität des Nachweises verantwortlich ist und insofern beispielsweise das „führende“ Register für den jeweiligen Nachweis betreibt. Welche konkrete Stelle das jeweils ist, muss vorab technisch hinterlegt sein.

Zu § 67f Absatz 2:

Absatz 2 enthält gemäß dem sogenannten Doppeltürmodell des Bundesverfassungsgerichts und im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e und Absatz 3 DSGVO die datenschutzrechtlichen Rechtsgrundlagen für den Abruf der Nachweise. Es soll ein vollständiger digitaler Nachweis ermöglicht werden. In Satz 1 ist die Datenabrufbefugnis der nachweisanfordernden Stelle und die Übermittlungsbefugnis der nachweisliefernden Stelle geregelt. In Satz 1 werden weitere Voraussetzungen für den Nachweisabruf festgelegt. Zum einen wird der datenschutzrechtliche Zweckbindungsgrundsatz gestützt, indem der Nachweisabruf für die Erfüllung der Aufgabe erforderlich sein muss. Durch ein hypothetisches Direkterhebungselement als zusätzliches Tatbestandsmerkmal wird zum anderen sichergestellt, dass die Behörde den Nachweis hypothetisch bei der betroffenen Person erheben darf. Satz 2 deckt einen weiteren möglichen Datenfluss ab, wenn die nachweisanfordernde Stelle nicht selbst die für die Entscheidung zuständige Behörde ist. In diesem Fall darf die nachweisanfordernde Stelle (zum Beispiel ein Portal) den Nachweis einholen und anschließend an die für die Entscheidung zuständige Stelle übermitteln.

Die Sätze 3 bis 5 entsprechen der Ergänzung in § 5 Absatz 3 Satz 3 bis 5 EGovG und stehen im Zusammenhang mit der in § 10 Absatz 1 Satz 2 OZG erfolgten Ergänzung, wonach im Datenschutzcockpit bei Vorliegen der rechtlichen und technischen Voraussetzungen zukünftig auch Datenübermittlungen ohne Nutzung der Identifikationsnummer nach dem IDNrG angezeigt werden sollen. Derzeit ist

der Anwendungsbereich des Datenschutzcockpits auf die Nutzung einer Identifikationsnummer nach dem IDNrG beschränkt. Auf die Begründung zu § 5 Absatz 3 EGvoG wird verwiesen.

Zu § 67f Absatz 3:

Absatz 3 gilt nur für solche Nachweise, die aus einem der in der Anlage zum IDNrG aufgeführten Register abgerufen werden sollen. Im Sinne der Ziele des Registermodernisierungsgesetzes, insbesondere der Einführung eines registerübergreifenden Identitätsmanagements zum Zwecke der Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz, ermöglicht die Regelung in Absatz 3 die Übermittlung der Identifikationsnummer gemäß § 139b AO und der weiteren Daten nach § 4 Absatz 2 und 3 IDNrG an die nachweisliefernde Stelle zum Zwecke der Zuordnung der Datensätze, der Validierung dieser Zuordnung zur betroffenen Person und zum Zwecke des Nachweisabrufs.

Im Sinne des datenschutzrechtlichen Grundsatzes der Datenminimierung nach Artikel 5 Buchstabe c DSGVO sollen nur diejenigen Daten im Sinne von § 4 Absatz 2 und 3 IDNrG übermittelt werden, die für Zweckerreichung erforderlich sind. Die nachweisliefernde Stelle kann anhand dieser Daten den zu der betroffenen Person gehörigen Nachweis ermitteln und an die nachweisanfordernde Stelle weitergeben. Damit bei der nachweisanfordernden Stelle der Nachweis wiederum richtig zugeordnet werden und eine Überprüfung dazu stattfinden kann, ob es sich um den angefragten Nachweis handelt, können hierzu die Identifikationsnummer und die weiteren Daten nach § 4 Absatz 2 und 3 IDNrG in der Antwortnachricht der nachweisliefernden Stelle an die nachweisanfordernde Stelle enthalten sein. Absatz 3 regelt daher die Verarbeitung im Sinne des § 6 Absatz 2 IDNrG.

Zu § 67f Absatz 4:

Absatz 4 regelt die sogenannte Vorschaufunktion und entspricht inhaltlich § 5 Absatz 5 EGovG. Die Vorschaufunktion ermöglicht der betroffenen Person, die automatisiert abgerufenen Nachweise vor deren Verwendung einzusehen und zu entscheiden, ob sie mit dem Verwaltungsverfahren unter Verwendung des angezeigten Nachweises fortfahren möchte. Die betroffene Person kann auf die Vorschau verzichten. Dies muss sie nicht aktiv tun. Eine technische Umsetzung, nach der die betroffene Person die Vorschau aktiv anstoßen muss, ist zulässig. Die Vorschaufunktion veranschaulicht der betroffenen Person, welche Daten konkret abgerufen wurden sowie welche Daten für das Verwaltungsverfahren verwendet werden sollen, und steigert dadurch die Transparenz des digitalen Verwaltungsverfahrens. Auch der europäische Once-Only-Nachweisabruf sieht – vorbehaltlich mitgliedstaatlicher oder unionsrechtlicher Ausnahmeregelungen im Sinne von Artikel 14 Absatz 5 der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (ABl. L 295 vom 21.11.2018, S. 1) (SDG-VO) – eine Vorschau vor. Mittels Vorschaufunktion kann die betroffene Person bei unrichtigen oder veralteten Daten die Verwendung des Nachweises unterbinden und dadurch selbst dazu beitragen, dass Verwaltungsentscheidungen effizient und auf Grundlage von aktuellen, richtigen Daten getroffen werden.

Entscheidet sich die betroffene Person nach Einsicht der Daten in der Vorschau gegen die Verwendung dieser Daten, bleiben ihr die Möglichkeiten, den Nachweis selbst elektronisch einzureichen, einen Antrag unvollständig einzureichen oder das elektronische Verwaltungsverfahren abzubrechen und den analogen Weg zu beschreiten.

Die Vorschaufunktion dient der Verwirklichung des Transparenzgebots im Sinne von Artikel 5 Absatz 1 Buchstabe a DSGVO und dem Recht auf informationelle Selbstbestimmung (Artikel 1 Absatz 1 in Verbindung mit Artikel 2 Absatz 1 GG). Die Vorschaufunktion bietet eine Einsichts- und Kontrollmöglichkeit der betroffenen Person im Vorfeld und das unabhängig von der Verwendung der Identifikationsnummer. Die Vorschaufunktion greift also auch bei solchen Datenübermittlungen, bei denen die betroffene Person auch weiterhin anhand der Basisdaten identifiziert werden kann.

Zu § 67f Absatz 5:

Abweichend von § 67d SGB X weist Absatz 5 die Verantwortung für den Nachweisabruf einseitig der nachweisanfordernden Stelle zu und trifft eine gesetzliche Bestimmung dazu, wer Verantwortlicher im Falle eines Once-Only-Nachweisabrufs ist. Auf diese Art werden die datenschutzrechtlichen Pflichten klar und eindeutig sowie im Einklang mit der Interessenlage der nachweisanfordernden Stelle zugewiesen.

Eine solche Regelung ist gemäß Artikel 4 Nummer 7 DSGVO zulässig, sofern wie hier Zwecke und Mittel der Verarbeitung gesetzlich vorgegeben sind. Die Regelung entspricht § 5 Absatz 1 Satz 3 EGovG.

Zu Artikel 8e Nummer 4 (§ 77a Zehntes Buch Sozialgesetzbuch)

Die Regelung entspricht § 5a EGovG und dient der Umsetzung von Artikel 14 SDG-VO. Nach Artikel 14 SDG-VO errichten die Kommission und die Mitgliedsstaaten gemeinsam ein technisches System für den automatisierten Austausch von Nachweisen zwischen zuständigen Behörden in verschiedenen Mitgliedsstaaten (EU-OOTS) zur Umsetzung des Grundsatzes der einmaligen Erfassung (Once-Only-Prinzip). Nach dem europäischen Once-Only-Prinzip sollen in der Verwaltung bereits vorliegende Nachweise im Rahmen weiterer Verwaltungsprozesse nicht erneut bei Bürgerinnen und Bürgern oder Unternehmen erhoben, sondern zwischen öffentlichen Stellen ausgetauscht werden. Dies entspricht bezogen auf Behörden innerhalb Deutschlands dem Regelungsgegenstand des § 67f SGB X und des § 5 EGovG.

Die Generalklausel in § 5a EGovG stellt keine sozialdatenschutzrechtliche Verarbeitungsgrundlage dar, da der Sozialdatenschutz im SGB (in Verbindung mit der DSGVO) abschließend geregelt ist (vgl. § 35 Absatz 2 Satz 1 SGB I) und auch das EGovG für den Sozialdatenschutz keine Anwendung findet (vgl. § 1 Absatz 4 EGovG). Erforderlich ist daher eine separate datenschutzrechtliche Regelung im Bereich des Sozialdatenschutzes, das heißt für die Sozialverwaltung.

Die Vorschrift dient damit als sozialdatenschutzrechtliche Verarbeitungsgrundlage der Umsetzung des und der Anbindung an das EU-OOTS im Sinne von Artikel 14 SDG-VO. § 77 SGB X bleibt unberührt.

Die sozialdatenschutzrechtliche Ermächtigung der Stellen, die Nachweise auszutauschen, ist zudem nicht Gegenstand von Artikel 14 SDG-VO (vgl. Europäischer Datenschutzbeauftragter (EDSB), Stellungnahme 8/2017, Stellungnahme des EDSB zu dem Vorschlag für eine Verordnung über die Einrichtung eines zentralen digitalen Zugangstors und den Grundsatz der „einmaligen Erfassung“, S. 15; Europäische Kommission, Arbeitsdokument, Datenschutzfolgenabschätzung zur Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates, SWD(2022) 211 final, S. 3f). Diese muss

auf Ebene der Union oder im Recht der Mitgliedsstaaten geschaffen werden. In diesem Sinne enthält § 77a SGB X entsprechend § 5a EGovG die erforderliche sozialdatenschutzrechtliche Rechtsgrundlage für den Nachweisaustausch über das EU-OOTS. Als Verordnung gilt Artikel 14 SDG-VO unmittelbar, weshalb darauf verzichtet wurde, auf relevante Systemspezifika des EU-OOTS explizit Bezug zu nehmen. So sollen Nachweise über das EU-OOTS grundsätzlich nur auf ausdrückliches Ersuchen des Nutzers hin ausgetauscht werden und dem Nutzer grundsätzlich die Möglichkeit einer Vorschau des abgerufenen Nachweises ermöglicht werden (vgl. Artikel 14 Absatz 3 Buchstaben a und f SDG-VO). Die Absätze 4 und 5 räumen den Mitgliedsstaaten und dem Unionsgesetzgeber selbst einen diesbezüglichen Regelungsspielraum ein. Von diesen Öffnungsklauseln wird mit den Regelungen des § 5a EGovG und § 77a SGB X kein Gebrauch gemacht.

Die Durchführungsverordnung (Durchführungsverordnung (EU) 2022/1463 der Kommission vom 5. August 2022 zur Festlegung technischer und operativer Spezifikationen des technischen Systems für den grenzüberschreitenden automatisierten Austausch von Nachweisen und zur Anwendung des Grundsatzes der einmaligen Erfassung gemäß der Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates) enthält daneben weitere technische und operative Spezifikationen. Insbesondere weist sie in Artikel 34 die datenschutzrechtliche Verantwortung für die Vollständigkeit und Rechtmäßigkeit des Nachweisabrufs der nachweisanfordernden Stelle („evidence requester“) zu.

§ 77a SGB X gilt wie § 5a EGovG dabei nur für solche Nachweise im Sinne von Artikel 14 Absatz 2 SDG-VO, die für Verfahren nach Artikel 14 Absatz 1 SDG-VO relevant sind. Die relevanten Verfahren nach Artikel 14 Absatz 1 SDG-VO ergeben sich einerseits aus Anhang II der SDG-VO sowie aus den Richtlinien 2005/36/EG, 2006/123/EG, 2014/24/EU und 2014/25/EU. Eine Legaldefinition für den Nachweisbegriff hat der Unionsgesetzgeber in Artikel 3 Nummer 5 SDG-VO aufgenommen. Danach sind Nachweise „alle Unterlagen oder Daten, einschließlich Text- oder Ton-, Bild- oder audiovisuellen Aufzeichnungen, unabhängig vom verwendeten Medium, die von einer zuständigen Behörde verlangt werden, um Sachverhalte oder die Einhaltung der in Artikel 2 Absatz 2 Buchstabe b SDG-VO genannten Verfahrensvorschriften nachzuweisen“. Artikel 14 Absatz 2 SDG-VO verengt seinen Anwendungsbereich wiederum auf solche Nachweise, die bereits innerstaatlich in einem elektronischen Format ausgestellt und automatisiert ausgetauscht werden. Insofern stellt der Unionsgesetzgeber in Artikel 14 Absatz 2 SDG-VO keine Digitalisierungspflicht für Nachweise auf, sondern stellt auf die individuellen Verhältnisse in den Mitgliedsstaaten ab.

Zu § 77a Absatz 1:

Absatz 1 enthält die sozialdatenschutzrechtliche Rechtsgrundlage für Nachweisabrufe deutscher Behörden bei Behörden eines anderen Mitgliedsstaats der Europäischen Union.

Zu § 77a Absatz 2:

Absatz 2 regelt die sozialdatenschutzrechtliche Rechtsgrundlage für Nachweisübermittlungen deutscher Behörden an Behörden eines anderen Mitgliedsstaats der Europäischen Union.

Zu § 77a Absatz 3:

Nach Absatz 3 können bei der Verarbeitung nach den Absätzen 1 und 2 intermediäre Plattformen zum Einsatz kommen. Diese Möglichkeit folgt unmittelbar aus der Durchführungsverordnung (EU) 2022/1463 (vgl. insbesondere Artikel 2 Buchstabe b und die Legaldefinition in Artikel 1

Absatz 6). Intermediäre Plattformen können sowohl auf der Seite des Mitgliedsstaats zum Einsatz kommen, der einen Nachweis aus einem anderen Mitgliedsstaat über das EU-OOTS abrufen möchte, als auch auf der Seite des nachweisliefernden Staates. Es obliegt der Verwaltungsorganisation der Mitgliedsstaaten, über das „Ob“ und „Wie“ des Einsatzes intermediärer Plattformen zu entscheiden. Die Durchführungsverordnung (EU) 2022/1463 lässt insbesondere offen, ob intermediäre Plattformen im eigenen Namen, das heißt in Ausübung einer eigenen Verantwortlichkeit, oder im Namen anderer Behörden, das heißt im Auftrag oder nur als technischer Dienst tätig werden sollen. Im nationalen Kontext muss dies erst noch entschieden werden. Mit Blick auf die vorwiegend dezentrale Registerstruktur in Deutschland wird eine Anbindung über intermediäre Plattformen beabsichtigt.

Anders als § 5a Absatz 3 EGovG beschränkt sich Absatz 3 nicht auf personenbezogene Daten. Dies trägt dem Umstand Rechnung, dass im Zweifel auch Betriebs- und Geschäftsgeheimnisse, die den Sozialdaten gleichgestellt sind (§ 35 Absatz 4 SGB I), aber nicht zwingend personenbezogenen Daten sind, ebenfalls erfasst werden sollen.

Zu Artikel 8f (Änderung des Personalausweisgesetzes)

Die europäischen Entscheidungen zur Entwicklung der europäischen Digital Identity Wallet sehen vor, dass (Erst-)Identifizierungen gegenüber der künftigen Wallet auf dem Vertrauensniveau „hoch“ durchzuführen sind. Auf welchem Vertrauensniveau und durch welche Authentisierungsmittel die spätere Authentisierung des Nutzers erfolgen soll, wird im Zuge der genauen Ausgestaltung der EU-Wallet geklärt und ist derzeit nicht absehbar.

Um eine flächendeckende und nutzerfreundliche Verwendung des elektronischen Identitätsnachweises voranzutreiben, sollen bis zur Etablierung der EU-Wallet vorübergehend niederschwellige Authentisierungsmöglichkeiten zugelassen werden, sofern die (Erst-)Identifizierung durch einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgt ist.

Die Möglichkeit einer niederschwelligen Authentisierung wird derzeit in verschiedenen Bereichen für den sektorspezifischen Einsatz geprüft. So sollen etwa im Gesundheitsbereich auf der Grundlage von § 291 Absatz 8 des Fünften Buches Sozialgesetzbuch (SGB V) entsprechende niederschwellige Authentisierungsmittel in Anwendungen der Krankenkassen zum Einsatz kommen.

Auch außerhalb des Gesundheitsbereichs soll Nutzern eines elektronischen Identitätsnachweises eine mit Authentisierungsmitteln nach § 291 Absatz 8 SGB V vergleichbare Möglichkeit der niederschwelligen Authentisierung eröffnet werden. Das Bundesministerium des Innern und für Heimat soll nach Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik entsprechende Authentisierungsmittel zeitlich befristet zulassen. Der Zeitraum der Befristung soll sich an dem für eine Etablierung der EU-Wallet zu erwartenden Zeitrahmen orientieren.

Zu Artikel 8g (Änderung des Identifikationsnummerngesetzes)

Zu Nummer 1

Die Ergänzung ist notwendig, um das Datenabrufersuchen auch bei Registern nach der Anlage des IDNrG durchführen zu können, in denen der vollständige Datenkranz nach der bisherigen Fassung nicht vorliegt. Hierzu gehören etwa die Personenstandsregister, in denen keine Informationen zu Wohnort und

Postleitzahl einer Person erfasst werden. Dabei soll Nummer 2 eine Ausnahme zu Nummer 1 darstellen, da eine möglichst hohe Trefferquote nur erzielt werden kann, wenn auch Wohnort und Postleitzahl als Suchkriterium angegeben werden. Hierbei handelt es sich nur um einen Mindestdatensatz für das Datenabrufersuchen. Es steht den Registern weiterhin offen, beim Datenabrufersuchen die Daten zu übermitteln, die vom Datenkranz des § 4 Absatz 2 erfasst sind.

Die Ergänzung in § 6 IDNrG ist notwendig, um den automatisierten Datenabruf unter Verwendung einer Identifikationsnummer nach § 5 EGovG zu ermöglichen.

Zu Nummer 2

Folgeänderung zu Artikel 8g Nummer 1.

Zu Nummer 6 (Änderung Inkrafttreten)

Der Gesetzentwurf regelt wichtige Voraussetzungen für eine schnelle und effiziente Digitalisierung der Verwaltung. Um eine möglichst zeitnahe Umsetzung der Regelungen zu gewährleisten und Regelungslücken – insbesondere auch im Bereich des Datenschutzrechts (§ 8a OZG) – zu schließen, soll das Gesetz am Tag nach der Verkündung in Kraft treten.

Um Regelungslücken im Hinblick auf die Anerkennung von ELSTER-Softwarezertifikaten auf dem Sicherheitsniveau „substantiell“ zu vermeiden, sieht Absatz 2 ein rückwirkendes Inkrafttreten der Verlängerung der Übergangsvorschrift nach § 12 Absatz 2 Satz 3 OZG vor.

Erfüllungsaufwand

Aus dieser Formulierungshilfe ergibt sich für die Verwaltung ein zusätzlicher Erfüllungsaufwand. Das Statistische Bundesamt soll daher gebeten werden, den Erfüllungsaufwand nachzuberechnen.