Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)303 H

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Stellvertretender Vorsitzender
des Ausschusses für Inneres und Heimat
des Deutschen Bundestages
Herrn Prof. Dr. Lars Castellucci

- Nur per E-Mail -

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat21@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 06.10.2023
GESCHÄFTSZ. 21-501-2/008#0140-OZGÄndG

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Stellungahme zum Entwurf eines OZG-Änderungsgesetzes**
ANLAGEN Stellungnahme

Sehr geehrter Herr Prof. Dr. Castellucci,

anliegend übersende ich meine Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung mit der Bitte um Berücksichtigung.

Mit freundlichen Grüßen

Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 06.10.2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung
des Ausschusses für Inneres und Heimat des Deutschen Bundestages
am 09.10.2023

zum Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung – OZG-Änderungsgesetz (BT-Drs. 20/8093)

unter Berücksichtigung
der Stellungnahme des Bundesrates
und der Gegenäußerung der Bundesregierung

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. **Definition „länderübergreifender Onlinedienst“**
   Zu Artikel 1 Nummer 2 Buchstabe d (§ 2 Absatz 8 Satz 1, 2 und 3 OZG-E); Nr. 10 der Stellungnahme des Bundesrates

Eine Definition, wann ein Onlinedienst ein "länderübergreifender" Dienst ist, fehlt derzeit. Eine Begriffsbestimmung erscheint mit Blick auf die vom Bundesrat dargestellten Konstellationen (Stellungnahme d. Bundesrates, Nr. 10) jedenfalls im Begründungstext empfehlenswert, wenn § 8a OZG-E als Regelung über die Verarbeitung personenbezogener Daten ausschließlich auf länderübergreifende Onlinedienste anwendbar sein soll mit der Folge, dass die Norm als Rechtsgrundlage für lediglich auf Landesebene angebotene Onlinedienste ausscheidet und daher auf landesrechtliche Rechtsgrundlagen abzustellen ist.

2. **Einführung eines zentralen Bürgerkontos**
   Zu Artikel 1 Nr. 3 (§ 3 Abs. 1 OZG-E)

Unter Fortfall landeseigener Bürgerkonten soll nur noch ein zentrales, vom Bund bereitgestelltes Bürgerkonto angeboten werden, womit Identifizierung und Authentifizierung für die Inanspruchnahme von Verwaltungsleistungen bundesweit zentralisiert würden. Hierdurch würde die Inanspruchnahme von Verwaltungsleistungen aller Bürgerinnen und Bürger über sämtliche Verwaltungsträger hinweg verfolg- und auswertbar und ein Einblick in die Nutzung von OZG-Leistungen der gesamten Bevölkerung ermöglicht.

Um möglichen Begehrlichkeiten einer solchen zentralen Datenschnittstelle und Gefahren für die Grundrechte des Einzelnen entgegenzuwirken, sollte das Konzept dezentraler Bürgerkonten beibehalten werden. Zu hohen Anforderungen an Interoperabilität und damit der Überforderung der kommunalen Ebene wird durch die Entwicklung länderstandardisierter IT-Komponenten durch Verwaltungsvereinbarung des Bundes und der Länder begegnet (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten – FINK).

3. **ELSTER-Softwarezertifikate als Identifizierungsmittel im Bürgerkonto**
   Zu Artikel 1 Nummer 3, 14 (§ 3 Abs. 4 Nr. 1, § 13 Abs. 2 OZG-E); Nr. 16 der Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Nach dem Gesetzentwurf sollen ELSTER-Softwarezertifikate als Identifizierungsmittel im Bürgerkonto für Verwaltungsleistungen, die nur ein Vertrauensniveau „substantiell“ erfordern, jedenfalls bis 30.06.2026 genutzt werden können. Diese Frist soll durch das Bundesministerium des Innern und für Heimat und das Bundesministerium der Finanzen im Wege der Rechtsverordnung unbeschränkt verlängert werden können.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

ELSTER-Zertifikate sind aber nicht als Identifizierungsmittel für das Sicherheitsniveau substantiell nach Art. 8 Abs. 2 lit. b Verordnung (EU) 910/2014 (eIDAS-Verordnung) notifiziert. Eine gesetzlich angeordnete Anerkennung als Identifizierungsmittel mit dem Sicherheitsniveau substantiell im OZG ist daher abzulehnen, soweit ELSTER die entsprechenden Anforderungen an ein Identifizierungsmittel mit diesem Sicherheitsniveau faktisch nicht erfüllt. Nicht mehr vertretbar erscheint insbesondere die Verordnungsermächtigung in § 13 Abs. 2 Satz 3 OZG-E, wonach die Frist unbegrenzt verlängert werden kann. Die Notwendigkeit einer Fristverlängerung erschließt sich auch deshalb nicht, weil Bürger/-innen unter anderem mit der eID-Funktion des Personalausweises bereits jetzt flächendeckend über ein sicheres Identifizierungsmittel verfügen. § 13 Abs. 2 OZG-E sollte wie folgt geändert werden:

„(2) Bis zum 30. Juni 2026 kann der elektronische Identitätsnachweis im Bürgerkonto außerdem für bestehende 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. ~~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 2 abweichende Frist festzulegen.~~“

4. ELSTER-Softwarezertifikate als Identifizierungsmittel im Organisationskonto

Zu Artikel 1 Nummer 3, 14 (§ 3 Abs. 4 Nr. 2, § 13 Abs. 3 OZG-E); Nr. 34 der Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Nach dem Gesetzentwurf sollen ELSTER-Softwarezertifikate als Identifizierungsmittel im Organisationskonto für eine Übergangsfrist von fünf Jahren zugelassen werden (§ 3 Abs. 4 Nr. 2 OZG-E). Die Frist soll nach dem Gesetzentwurf in der Fassung, wie sie in der Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrats vorgeschlagen wird, durch Rechtsverordnung des Bundesministeriums des Innern und für Heimat und das Bundesministerium der Finanzen unbeschränkt verlängert werden können (§ 13 Abs. 5 OZG-E). Behörden sollen von der zwingenden Nutzung des Unternehmskontos absehen können, wenn im Einzelfall ein höheres Vertrauensniveau erforderlich ist (§ 13 Abs. 3 OZG-E).

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Wie dargestellt erfüllt das ELSTER-Verfahren jedoch nicht die Mindestanforderungen an ein geeignetes, sicheres Identifizierungsmittel. Eine Verordnungsermächtigung, wonach die Fünfjahresfrist unbegrenzt verlängert werden kann, ist erst recht nicht zu rechtfertigen. Stattdessen sollten die Anstrengungen, ein geeignetes, sicheres Identifizierungsmittel zu entwickeln, intensiviert werden. Da im Organisationskonto teils sensible personenbezogene Daten verarbeitet werden, beispielsweise Gesundheitsdaten wie Angaben zu Schwerbehinderung oder Schwangerschaft von Beschäftigten, sollten Behörden zudem *verpflichtet* werden, von der Nutzung des Unternehmenskontos abzusehen, wenn ein höheres Sicherheitsniveau erforderlich ist. In solchen Fällen ist für eine abweichende Ermessensentscheidung der Behörde kein Raum. Vielmehr würde eine solche Entscheidung gegen Art. 32 DSGVO verstoßen, indem Unternehmen zur Nutzung des Organisationskontos gezwungen werden, obwohl eine hinreichend sichere Identifizierung der Nutzer nicht möglich ist.

§ 13 Abs. 3 OZG-E sollte wie folgt gefasst werden:

*„(3) Abweichend von § 3 Absatz 3 ~~kann~~ **hat** eine öffentliche Stelle bis zum Ablauf der Frist nach § 3 Absatz 4 Nummer 2 Buchstabe a von der Verwendung des einheitlichen Organisationskontos ab**zu**sehen, wenn für die Inanspruchnahme einer elektronischen Verwaltungsleistung und die sonstige elektronische Kommunikation ausnahmsweise ein höheres Vertrauensniveau erforderlich ist.“*

Die vom Bundesrat vorgeschlagene Ergänzung der Norm um § 13 Abs. 5 OZG-E ist abzulehnen.

Nach Ablauf der Übergangsfrist sind zudem die vom Bundesamt für Sicherheit in der Informationstechnik in der technische Richtlinie *TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government: Vertrauensniveaus und Mechanismen“* festgelegten Vorgaben zu erfüllen. Dies sollte in den Begründungstext aufgenommen werden.

5. Sicherheitsvorgaben für Nutzerkonto und bidirektionales Postfach
Zu Art. 1 Nr. 2 lit. c, d (§ 2 Abs. 5, 7 OZG-E)

Mit den De-Mail-Diensten existieren bereits funktional vollwertige elektronische Kommunikationsdienste mit Vorgaben für eine sichere, datenschutzgerechte Ausgestaltung und den Betrieb dieser Dienste. Vergleichbare Anforderungen an das Postfach des Nutzerkontos wie auch an das Nutzerkonto selbst fehlen im OZG. Ein solches Postfach bedarf aber nicht nur wegen der Übertragung teils sensibler personenbezogener Daten hinreichender Vorgaben zu Datenschutz und Datensicherheit. Es muss ein mit einem De-Mail-Konto und damit der Technischen Richtlinie BSI TR-01201 vergleichbares Sicherheitsniveau bieten, das an den Stand der Technik angepasst wurde (vertrauenswürdige IT-Basisinfrastruktur, sicherer Betrieb eines Postfach- und Versanddienstes, vertrauenswürdiges Account-Management,

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

sichere Dokumentenablage, Identitätsbestätigungsdienst, Erfüllung allgemeiner Anforderungen an die Informationssicherheit). Zusätzlich sollte eine Ende-zu-Ende-Verschlüsselung gesetzlich vorgeschrieben werden. Eine Ergänzung entsprechender gesetzlicher Vorgaben wird empfohlen.

6. Freiwillige Nutzung des Postfachs
Zu Art. 1 Nr. 2 lit. d) (§ 2 Abs. 7 OZG-E)

Dass die Nutzung des Bürgerkontos auch weiterhin freiwillig sein soll, ist zu begrüßen (§ 3 Abs. 1 Satz 2 OZG-E). Für die Nutzung des Postfachs fehlt eine vergleichbare Vorgabe, so dass Bürger/-innen gezwungen werden können, die Korrespondenz im elektronischen Verfahren über das Postfach des Nutzerkontos abzuwickeln und dort eingehende Behördenmitteilungen gegen sich gelten zu lassen. In § 2 Abs. 7 OZG-E sollte daher der in der derzeit geltenden Fassung des OZG enthaltene Satz wieder aufgenommen werden:

„Die Nutzung des Postfachs ist für die Nutzer freiwillig.“

Soll die Nutzung des Postfachs entgegen der hier empfohlenen Regelung verpflichtend sein, bedarf es einer entsprechend eindeutigen gesetzlichen Regelung.

7. Ersetzung des Begriffs „Einwilligung“ durch „auf Veranlassung“

Der in der DSGVO legaldefinierte Begriff der Einwilligung soll an verschiedenen Stellen durch das Tatbestandsmerkmal „*auf Veranlassung*“ des Nutzers bzw. der Nutzerin ersetzt werden. Zwar ist die Begründung, dass eine begriffliche Anpassung angezeigt ist, weil es sich hier nicht um eine datenschutzrechtliche Einwilligung in Form eines Erlaubnistatbestands handele, zutreffend.

Die sprachliche Anpassung darf jedoch nicht zu einer inhaltlichen Absenkung der freien Entscheidungsrechte der Bürgerinnen und Bürger führen, beispielsweise indem Betroffene faktisch zur Nutzung bestimmter Dienste oder Funktionen gezwungen werden. Es sollte daher zumindest in der Begründung klargestellt werden, dass das Tatbestandsmerkmal „auf Veranlassung“ des Nutzers bzw. der Nutzerin dahin auszulegen ist, dass die Person auf der Grundlage umfassender Informationen und in Kenntnis der daraus folgenden Datenverarbeitungsvorgänge frei darüber entscheiden können muss, ob sie von dem betreffenden Angebot Gebrauch macht oder eine Leistung oder Funktion nutzt.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

„Die Datenverarbeitung darf nur nach entsprechender freiwilliger Willensäußerung des Nutzers in Form eines aktiven Handelns (z. B. Ankreuzen eines Feldes oder Anklicken einer Schaltfläche mit Zustimmungserklärung) erfolgen. Die jeweiligen Verarbeitungszwecke sowie Inhalt und Umfang der Datenverarbeitung sind dem Nutzer vorab transparent zu machen."

8. Zu Art. 1 Nr. 10 (§ 8a OZG-E)

Die geplanten Änderungen in § 8a Abs. 1 und Abs. 2 OZG-E sind zu begrüßen. Nach § 8a Abs. 3 Satz 3 OZG-E ist eine längere als 30 Tage andauernde Aufbewahrung von zwischengespeicherten Daten des Nutzers durch den Onlinedienst nur noch ausnahmsweise zulässig. Diese Regelung ist aus Gründen der Datenminimierung und der klaren Zweckbestimmung aber nicht ausreichend. Ich schlage daher folgende Neuformulierung vor.

„(3) […] vorab zu informieren. ~~Davon unabhängig sind längerfristige Speicherungen von Daten im Onlinedienst ausnahmsweise zulässig, wenn dies für die Erfüllung der durch den Antragsassistenten erfassten Zwecke erforderlich ist.~~ *Eine Zwischenspeicherung von Daten im Onlinedienst ist ausschließlich für die Erfüllung eigener Zwecke zulässig. Eine längerfristige Speicherung ist nur dann ausnahmsweise zulässig, wenn dies zwingend erforderlich ist."*

9. Zu Art. 1 Nr. 13 (§ 10 OZG-E)Datenschutzcockpit

Das Datenschutzcockpit droht auf halber Strecke stehen zu bleiben und wird sein umfassendes Transparenzversprechen in Bezug auf die digitalisierte Verwaltung in seiner jetzigen Form nicht einlösen können. Die Bestandsdatenauskunft ist nicht nur bei den Registern selbst relevant, sondern bei allen öffentlichen Stellen, die auf Grundlage dieses Gesetzes in Zukunft die IDNr. für OZG-Leistungen verarbeiten werden. Insofern ist § 10 Abs. 2 OZG anzupassen.

In der Entwurfsfassung des § 10 OZG-E besteht ein Dissens zwischen Absatz 1 und Absatz 2 der Norm. Der Gesetzgeber hat bei der Formulierung des § 10 Abs. 2 OZG-E im Rahmen des Gesetzes zur Regelung des Erscheinungsbilds von Beamtinnen und Beamten sowie zur Änderung weiterer dienstrechtlicher Vorschriften nicht auf ausreichende Konsistenz zu § 10 Abs. 1 OZG-E geachtet. Mit dem genannten Gesetz bezweckte der Gesetzgeber eine begrüßenswerte Erweiterung des Transparenzanspruchs des Datenschutzcockpits. In seiner aktuellen Ausgestaltung ist jedoch unklar, an wen sich welche Aspekte des gesetzlichen Transparenzauftrags richten (Register bzw. Nicht-Register; beides öffentliche Stellen im Sinne des § 10 Abs. 1 OZG). Insbesondere vor dem Hintergrund der Regelungen des Art. 2 Änderungsbefehl Nr. 8 (§ 5 EGovG-E) sowie des Entschließungsantrags 20(4)258 vom 19.06.2023 erscheint eine Klarstellung notwendig, dass auch nicht-registerführende Stellen von der Bestandsdatenauskunft gemäß § 10 Abs. 2 OZG-E erfasst sind. Ich schlage daher folgende Formulierung vor:

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

„(2) Im Datenschutzcockpit werden nach Maßgabe von Absatz 4 Satz 3 ausschließlich Protokolldaten nach § 9 des Identifikationsnummerngesetzes einschließlich der dazu übermittelten Inhaltsdaten sowie die Bestandsdaten der ~~Register~~ ***öffentlichen Stellen im Sinne des Absatzes 1*** *angezeigt. […]“*

10. Zu Art. 2 Nr. 8 (§ 5 EGovG-E) Once-Only-Klausel

Auch die Regelungen der Once-Only-Generalklausel werden dem Transparenzanspruch des Datenschutzcockpits und des Entschließungsantrags 20(4)258 vom 19.06.2023 nicht gerecht. Obwohl § 9 IDNrG als auch § 10 Abs. 1 OZG bereits jetzt aufgrund klarer gesetzgeberischer Vorstellungen auf die Transparenzmachung durch alle öffentlichen Stellen ausgerichtet sind, fehlt eine entsprechende Verpflichtung dieser Stellen zum Anschluss an das Datenschutzcockpit. Die aktuelle Regelung des § 2 Nr. 3 IDNrG verpflichtet nur die Register selbst sich an das Datenschutzcockpit anzubinden. Die Generalklausel muss also um eine Anschlusspflicht für alle öffentliche Stellen, die in Zukunft die IDNr. verarbeiten werden, ergänzt werden. Die Transparenz hat der IDNr. zu folgen.

Die Regelung des § 5 EGovG-E bedarf insofern einer grundsätzlichen Ergänzung. Mit der Once-Only-Regelung soll der Verwaltung in elektronischen, antragsbasierten Verfahren erlaubt werden, hierfür notwendige Nachweise (z. B. Geburtsurkunde im Elterngeldverfahren) von einem Register direkt abzurufen, so dass der Verwaltung bereits vorliegende Nachweise vom Bürger nicht mehrfach in verschiedenen Verfahren eingereicht werden müssen. Der Gesetzgeber hat Maßnahmen zu implementieren, die die Transparenz der Datenverarbeitung, Kontrolle durch den Betroffenen und die Schaffung struktureller Hemmnisse vor zweckändernden Datenverarbeitungen sicherstellen. Dies ist mit Blick auf die Bedeutsamkeit dieser Regelung für die Zukunft der Verwaltungsdigitalisierung besonders wichtig.

Dabei wiegt das Fehlen der Verpflichtung der nicht-registerführenden Stellen zum Anschluss an das Datenschutzcockpit besonders schwer. Dies ist ein deutlicher Bruch zu den Zielsetzungen des Identifikationsnummerngesetzes (IDNrG), die vor allem mit Blick auf die Regelung des § 10 Abs. 1 OZG alle Übermittlungen über das Datenschutzcockpit transparent und nachvollziehbar machen wollte. Die ohnehin kritische Bewertung der Verfassungsmäßigkeit des IDNrG verschärft sich hierdurch nochmals gravierend. Ich schlage daher folgende Ergänzung durch einen neuen Absatz vor:

„Öffentliche Stellen, die Nachweise im Sinne des Abs. 2 abrufen oder erbringen, haben natürlichen Personen die Übermittlung und den Bestand ihrer Daten digital über eine zentrale

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Stelle transparent zu machen (Datenschutzcockpit) soweit hierfür die Identifikationsnummer nach § 1 des Identifikationsnummerngesetzes Verwendung findet.“

Ein weniger gravierendes, aber dennoch bestehendes Problem ist die Regelung zur datenschutzrechtlichen Verantwortlichkeit in § 5 Abs. 1 Satz 3 EGovG-E (siehe auch die Begründung auf S. 64 f des Entwurfs). Bei der Regelung ist unklar, was eigentlich der Regelungszweck sein soll. Der gesetzliche Auftrag des Onlinedienstes ist der Abruf von Nachweisen bei einer anderen öffentlichen Stelle. Der gesetzliche Auftrag des Registers ist es, die Anfrage des Onlinedienstes zu prüfen, freizugeben und die entsprechenden Nachweise zu übermitteln. An diesen gesetzlichen Aufträgen orientiert sich auch die datenschutzrechtliche Verantwortlichkeit im Sinne des Art. 4 Nr. 7 DS-GVO. Beide entscheiden innerhalb ihres gesetzlichen Auftrags über die Zwecke und Mittel der Verarbeitung. Es ist also auch ohne weitere Regelung klar, dass das Register im Rahmen seiner Verantwortlichkeit nicht die materielle Richtigkeit der Anfrage durch den Onlinedienst zu prüfen hat. Bestenfalls ist die geplante Regelung insofern deklaratorisch. **Sie sollte daher vollständig gestrichen werden.**

11. Datenverarbeitung im Verwaltungsportal des Bundes

Zu Art. 2 Nr. 11 Buchst. c und d (§ 9b Abs. 3 und 4 EGovG-E)

Die Befugnisse zur Verarbeitung personenbezogener Daten von Bürgerinnen und Bürgern im Verwaltungsportal des Bundes soll mit der vorgeschlagenen Änderung nicht mehr nur auf die Speicherung und Bereitstellung von Antragsdaten an die zuständige Fachbehörde beschränkt sein.

Die für die Erbringung einer Verwaltungsleistung erfolgende Speicherung von Verfahrensdaten wird aber weiterhin primär im jeweiligen Fachverfahren bzw. bei der zuständigen Fachbehörde erfolgen. Das Verwaltungsportal dient insoweit nur als Datendrehscheibe. Damit es nicht zu einer unzulässigen, weil nicht erforderlichen doppelte Datenhaltung einerseits zentral im Verwaltungsportal des Bundes, andererseits im Fachverfahren bei der zuständigen Fachbehörde kommt, sind Verfahrensdaten im Verwaltungsportal zu löschen, sobald sie erfolgreich an die Fachbehörde übermittelt worden sind, es sei denn der Nutzer wünscht eine längere Speicherung. Dabei ist zu berücksichtigen, dass im Verwaltungsportal teils besondere Kategorien personenbezogener Daten – und damit sensible Informationen – auf einer zentralen Plattform verarbeitet werden. Um den mit einer solchen zentralen Datenspeicherung verbundenen Eingriff auf das zwingend notwendige Maß zu begrenzen, bedarf es hinreichender gesetzlicher Vorgaben zur Speicherdauer.

Ich schlage daher in Anlehnung an die bestehende Regelung folgende Änderungen an § 9b EGovG-E vor:

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

„(1) Die für die Zwecke nach § 9a Absatz 3 erforderlichen personenbezogenen Daten dürfen im Verwaltungsportal des Bundes ~~verarbeitet~~ ***erhoben und an die zuständige Behörde übermittelt*** *werden.* ***Hierzu dürfen die Daten im Verwaltungsportal gespeichert werden, soweit dies erforderlich ist, um der zuständigen Behörde den Antrag über einen sicheren Übermittlungsweg zum Abruf bereitzustellen. Sobald die zuständige Behörde den Antrag aus dem Verwaltungsportal des Bundes abgerufen hat, sind die Antragsdaten unverzüglich aus dem Verwaltungsportal des Bundes zu löschen. Ruft die zuständige Behörde den Antrag nicht innerhalb von 12 Monaten nach der Antragstellung ab, so sind die Stamm- und Verfahrensdaten vorbehaltlich einer Speicherung nach Absatz 2 zu löschen. Nimmt der Antragsteller den Antrag zurück, sind die Antragsdaten unverzüglich aus dem Verwaltungsportal des Bundes zu löschen.*** *Dies gilt auch für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 […].“*

Absatz 3 Satz 3 sollte wie folgt gefasst werden:

„Nach der Übermittlung des Online-Formulars an die zuständige Behörde zwischengespeicherte Verfahrensdaten sind zu löschen, wenn diese für die Zwecke nach Absatz 2 nicht mehr erforderlich sind oder der Nutzer diese erkennbar nicht mehr weiterverwenden möchte, ***spätestens jedoch nach Ablauf von 2 Jahren nach der erstmaligen Speicherung****. Der Nutzer ist vorab über eine automatische Löschung der Verfahrensdaten zu informieren.“*

12. Änderung des IT-Netz-Gesetzes

Zu Artikel 3 Nr. 1 (§ 3 IT-NetzG-E)

In § 3 Abs. 1 IT-NetzG soll für den Anwendungsbereich des OZG eine Möglichkeit geschaffen werden, neben dem Verbindungsnetz auch „andere Netze des Bundes“ für den Datenaustausch zwischen Bund und Ländern nutzen zu können. Die Öffnungsklausel ist in Bezug auf das Sicherheitsniveau (und damit auch in Bezug auf Sicherheit der zwischen Bund und Ländern ausgetauschten personenbezogenen Daten) zu unbestimmt. Andere Regelungen, etwa Vorgaben im Bereich der Registermodernisierung, verweisen wiederum auf das IT-NetzG, um das notwendige Sicherheitsniveau für den Austausch festzulegen.

Ich schlage daher vor, § 3 Abs. 1 und 2 IT-NetzG-E wie folgt zu konkretisieren, um ein dem Verbindungsnetz vergleichbares Sicherheitsniveau festzuschreiben:

„(1) Der Datenaustausch zwischen dem Bund und den Ländern erfolgt über das Verbindungsnetz. Im Anwendungsbereich des Onlinezugangsgesetzes kann der Datenaustausch auch

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

über andere Netze des Bundes ***erfolgen****, die ~~einen dem beabsichtigten Datenaustausch entsprechenden IT-Sicherheitsstandard aufweisen, erfolgen~~* ***die Anforderungen gemäß § 4 Absatz 1 erfüllen****, erfolgen.*

In § 3 Abs. 2 IT-NetzG-E wird das Bundesministerium des Innern und für Heimat ermächtigt, zusätzlich nutzbare Netze und deren IT-Sicherheitsstandards per Rechtsverordnung festzulegen. Auch dies muss anhand nachvollziehbarer Kriterien und technischer Bewertungen erfolgen. Ich empfehle daher eine vorherige Beteiligung des BSI. Absatz 2 sollte um folgenden Satz ergänzt werden:

„Die Einhaltung der Anforderungen nach Absatz 1 ist vom Bundesamt für Sicherheit in der Informationstechnik festzustellen.“

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de