Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 E

Bonn, den 17.05.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat
am 17.05.2021

zum **Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät** – BT-Drs. 19/28169

unter Berücksichtigung der mit **Anträgen der Fraktionen der CDU/CSU und der SPD** –

A-Drs. **19(4)825** und **19(4)826** vom 30.04.2021 – vorgeschlagenen Änderungen

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Allgemeines

Mit dem Entwurf des Gesetzes zur Einführung eines elektronischen Identitätsnachweises sollen durch Änderungen im Personalausweisgesetz (PAuswG), im eID-Karte-Gesetz (eIDKG) und im Aufenthaltsgesetz rechtliche Grundlagen für einen elektronischen Identitätsnachweis mit einem mobilen Endgerät geschaffen werden. Diese zusätzliche Nachweis-Funktion soll neben der hochsicheren eID-Funktion des Personalausweises, der eID-Karte bzw. des elektronischen Aufenthaltstitels ermöglicht werden.

Dem Gesetzentwurf ist bisher nicht zu entnehmen, ob der elektronische Identitätsnachweis mittels eines mobilen Endgeräts die gleichen Sicherheitsanforderungen wie die bisherigen elektronischen Identitätsnachweise mittels Personalausweis, eID-Karte oder elektronischen Aufenthaltstitel erfüllt bzw. erfüllen soll. Insbesondere fehlen Informationen, welches Sicherheitsniveau gemäß der eIDAS-Verordnung durch den elektronischen Identitätsnachweis mit einem mobilen Endgerät erreicht werden soll. Hier sollte der Gefahr, dass das Sicherheitsniveau zugunsten der erwünschten Nutzerfreundlichkeit abgeschwächt wird, vorgebeugt werden. Unbeantwortet bleibt auch die Frage, ob für denjenigen, dem gegenüber die elektronische Identifikation erfolgt, die Wahl des Mittels (eID-Karte oder mobiles Endgerät) erkennbar sein muss, etwa weil auf Seiten des Empfängers besondere Voraussetzungen für den Fall der Nutzung des elektronischen Identitätsnachweises mittels mobilem Endgerät vorliegen müssen. Hierzu sollten zumindest in der Gesetzesbegründung Ausführungen gemacht werden.

Die mit A-Drs. 19(4)826 vom 30.04.2021 zum Ausdruck gebrachte Unterstützung dieses Anliegens begrüße ich daher.

Ebenfalls auf Antrag der Fraktionen der CDU/CSU und der SPD (A-Drs. 19(4)825) soll der Gesetzentwurf u. a. eine Erweiterung dahingehend erfahren, dass sowohl im Passgesetz (PassG) als auch im PAuswG eine Regelungsbefugnis zugunsten der Länder eingeräumt wird, ein zentrales Register zur vereinfachten Durchführung eines automatisierten Abrufs des Lichtbilds und der Unterschrift in den Fällen des § 22a Absatz 2 PassG bzw. § 25 Absatz 2 PAuswG einzurichten. Dieses Vorhaben stößt auf nachstehend erläuterte grundsätzliche datenschutzrechtliche Bedenken.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

2. Zu einzelnen Änderungsbefehlen

a) Zu **Artikel 1 – Änderung des Passgesetzes** (§ 27a – neu PassG-E)

Die hier durch einen neu einzufügenden § 27a PassG-E eingeräumte Befugnis, auf Länderebene zentrale Passregisterdatenbestände zum Zweck des automatisierten Abrufs des Lichtbilds und der Unterschrift einrichten zu können, wird hauptsächlich damit begründet, dass es für viele Kommunen bereits eine große Herausforderung bedeuten würde, allein die technischen Voraussetzungen für den automatisierten Abruf sicherzustellen, und dass eine zentrale Datenhaltung neben einer Erleichterung der Umsetzung der Abrufe auch die Möglichkeit der Einbindung spezialisierter Einrichtungen zur Gewährleistung eines hohen Maßes an Datensicherheit biete.

Diesen Erwägungen steht allerdings gegenüber, dass der in den Pass- und Personalausweisbehörden für einen automatisierten Abruf vorhandene Datenbestand auf Landesebene zusätzlich noch einmal gespiegelt und dauerhaft für die gesetzlich vorgesehenen Abrufzwecke vorgehalten würde. Da jeder neu und auf Dauer geschaffene Bestand an personenbezogenen Daten das Risiko einer zweckfremden Verwendung oder eines Missbrauchs potenziell deutlich erhöht, ist seine Einrichtung vor allem an den datenschutzrechtlichen Grundsätzen der Datenminimierung und Erforderlichkeit zu messen. Schon in dieser Hinsicht bedarf es unabweisbarer Gründe, um einen solchen zusätzlichen Datenbestand zu legitimieren.

Die Anforderungen an diesen Prüfungsmaßstab steigen noch, wenn – wie hier hinsichtlich des biometrischen Lichtbilds – eine Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO erfolgt. An dieser Stelle sehe ich auch einen entscheidenden Unterschied zu den bereits etablierten zentralen (Spiegel-)Melderegistern der Länder zum Zweck eines automatisierten Abrufs bestimmter Meldedaten nach § 39 Abs. 3 Bundesmeldegesetz – denn hierbei handelt es sich nicht um eine Verarbeitung besonders sensibler Daten im Sinne des Art. 9 DSGVO.

Im Lichte dessen kann die Begründung des Änderungsantrags daher nicht überzeugen. Insbesondere ist ein erhebliches öffentliches Interesse an der Errichtung eines solchen Registers auf der Grundlage eines nationalen Gesetzes, wie es Art. 9 Abs. 2 lit. g) DSGVO verlangt, wenn die Betroffenen nicht ausdrücklich in diese Datenverarbeitung eingewilligt haben, nicht herauslesbar.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Dieser strenge Maßstab kommt nach meiner Auffassung bereits dann zum Tragen, wenn mit dem nationalen Gesetz zunächst lediglich eine entsprechende Ermächtigung im Wege einer Öffnungsklausel für den darauf tätig werdenden Landesgesetzgeber geschaffen wird. Denn die Festlegung, es bestehe ein erhebliches öffentliches Interesse an der Errichtung zentraler Abrufregister für Lichtbild und Unterschrift auf Landesebene, trifft der (Bundes-)Gesetzgeber bereits an dieser Stelle der Aufnahme der Öffnungsklausel, vor allem, wenn er sich die von Länderseite dazu vorgebrachten Argumente zu eigen macht.

Wie in der Begründung zum Änderungsantrag ausgeführt, müssen die technischen Voraussetzungen eines bundesweiten automatisierten Abrufs im Wege einheitlicher Kommunikationsstandards ohnehin noch geschaffen werden. Eine Einbindung sämtlicher Pass- und Personalausweisbehörden in diesen Prozess ist technisch sicherlich möglich, wenn auch aufwändiger. Das grundsätzlich nachvollziehbare Motiv einer Verfahrenserleichterung reicht für die Bejahung eines „erheblichen“ öffentlichen Interesses jedenfalls nicht aus – hierzu bedarf es vielmehr eines qualifizierten Interesses mit ausreichend Gewicht, wie beispielsweise im Fall humanitärer Notlagen infolge von Naturkatastrophen oder zur Überwachung von Epidemien und deren Ausbreitung (siehe ErwGr. 46 DSGVO).

Aus den genannten Gründen kann ich der vorgeschlagenen Änderung bzw. Ergänzung des PassG durch die Aufnahme eines § 27a nicht zustimmen.

Mit den gleichen Erwägungen bitte ich, den inhaltlich deckungsgleichen Regelungsvorschlag eines neu einzufügenden **§ 34a PAuswG-E** (**Änderungsbefehl Nr. 19** des o. g. Änderungsantrags **A-Drs. 19(4)825**) ebenfalls nicht zu berücksichtigen.

b) Zu **Artikel 2 – neu – Änderungsbefehl Nr. 8** (§ 10a – neu PAuswG-E)

Mit dem neu einzufügenden § 10a PAuswG-E soll die Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät generell regelt werden.

aa) Gültigkeitsdauer der Anwendung (§ 10a Absatz 2 PAuswG-E)

§ 10a Absatz 2 PAuswG-E befasst sich mit der Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät. Sie soll maximal fünf Jahre betragen. Durch Rechtsverordnung soll aber eine kürze Gültigkeitsdauer festgelegt werden können. Laut

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Gesetzesbegründung soll zunächst sogar eine kürzere Geltungsdauer von zwei Jahren in der Personalausweisverordnung (PAuswV) normiert werden, da gerade zu Beginn damit zu rechnen sei, dass sich der Stand der Technik in einem entsprechenden Zeitintervall verändern werde. Eine entsprechende Änderung der PAuswV fehlt allerdings im Gesetzentwurf.

Generell halte ich eine Gültigkeitsdauer von fünf Jahren für einen elektronischen Identitätsnachweises mit einem mobilen Endgerät für deutlich zu lang. Für die vorgesehene Funktion sind besondere sicherheitstechnische Anforderungen an das mobile Endgerät zu stellen. Um Missbrauch zu vermeiden, ist darauf zu achten, dass das jeweilige Endgerät aus Gründen der Datensicherheit immer auf dem aktuellsten Stand ist, also alle vom Hersteller bereitgestellten Sicherheitspatches installiert wurden. In der Regel stellen die Hersteller von mobilen Endgeräten längstens fünf Jahre lang Sicherheitspatches zur Verfügung. Danach dürften die mobilen Endgeräte die Sicherheitsanforderungen für einen elektronischen Identitätsnachweis nicht mehr erfüllen. Es ist somit davon auszugehen, dass ein elektronischer Identitätsnachweis auch auf einem mobilen Endgerät eingerichtet werden kann, das ab dem Zeitpunkt der Einrichtung keine fünf Jahre lang mehr durch den Hersteller mit Sicherheitspatches versorgt wird und somit Sicherheitslücken aufweist, die negative Auswirkungen auf die Zuverlässigkeit der Identifizierung und Anerkennung als sicheres Identifizierungsverfahren haben könnten. Die gesetzlich festgelegte Gültigkeitsdauer muss diesem Umstand Rechnung tragen und grundsätzlich auf einen kürzeren Zeitraum begrenzt werden. Zudem ist zu berücksichtigen, dass sich der Stand der Technik im Bereich der mobilen Endgeräte erfahrungsgemäß in immer kürzeren Abständen weiterentwickelt und nicht erst nach Ablauf von fünf Jahren überholt sein dürfte.
Zwar soll durch die im Gesetzentwurf angeführte, aber im Rahmen dieses Rechtsetzungsvorhabens von der Bundesregierung nicht vorgelegte, Rechtsverordnung die Festlegung einer kürzeren Gültigkeitsdauer für den elektronischen Identitätsnachweis mit einem mobilen Endgerät ermöglicht werden. Da die zeitliche Bemessung der Gültigkeit jedoch einen unmittelbaren Einfluss auf die Zuverlässigkeit einer Identifizierung hat, handelt es sich hierbei um eine wesentliche Regelung, die im PAuswG selbst festgelegt werden sollte. Demgemäß halte ich es für erforderlich, die Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät gesetzlich generell auf zwei Jahre zu begrenzen. Entsprechend müsste § 10a Absatz 2 Satz 1 PAuswG-E wie folgt gefasst werden:

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 18 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt höchstens zwei Jahre.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Der mit der Verkürzung der Gültigkeitsdauer verbundene Mehraufwand für eine häufigere Wiedereinrichtung des elektronischen Identitätsnachweises durch die Nutzenden steht dabei, gerade mit Blick auf das damit verbundene Mehr an Sicherheit, der Schaffung eines nutzerfreundlichen elektronischen Identitätsnachweises und seiner Akzeptanz sicherlich nicht im Wege.

bb) Ergänzende Regelung für Fälle einer Sperrung der Nachweisfunktion

§ 10a Absatz 4 PAuswG-E regelt den Fall, dass die auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten unrichtig werden. An dieser Stelle fehlt eine Regelung, die die Änderung von Daten auf dem Personalausweis oder auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises durch die Personalausweisbehörde mit einer Änderung der Daten im Speicher- und Verarbeitungsmedium des mobilen Endgeräts koppelt. Zwar dürfte der Ausweisinhaber einen elektronischen Identitätsnachweis mittels mobilem Endgerät nicht durchführen, wenn die Daten unrichtig sind. Jedoch kann nicht ausgeschlossen werden, dass sich der Ausweisinhaber an diese Vorgabe nicht hält.
Zudem fehlt im Gesetzentwurf eine § 10 Absatz 5 PAuswG-E entsprechende Regelung für die Sperrung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät, z. B. für den Fall, dass das mobile Endgerät abhandenkommt.

Daher halte ich es für angezeigt, § 10a PAuswG-E um einen Absatz 6 wie folgt zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat zur Aktualisierung der Sperrliste unverzüglich die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Ausweisinhabers,*
3. *der Ungültigkeit eines Ausweises nach § 28 Absatz 1 oder Absatz 2 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.bfdi.bund.de

c) Zu **Artikel 3 – neu – Änderungsbefehl Nr. 5** (§ 8a – neu eIDKG-E)

Das zu § 10a – neu PAuswG-E Ausgeführte trifft auch auf den Regelungsinhalt des § 8a – neu eID-Karte-Gesetz zu. Zur Vermeidung von Wiederholungen verweise ich insoweit auf meine Ausführungen zu Gliederungspunkt 2. b) aa) oben und rege an, § 8a Absatz 2 Satz 1 eIDKG-E wie folgt zu ändern:

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 12 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt höchstens 2 Jahre.

Darüber hinaus wäre – entsprechend meinen Ausführungen oben zu Gliederungspunkt 2. b) bb) – § 8a eIDKG-E ebenfalls um einen neuen Absatz 6 wie folgt zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Karteninhabers,*
3. *der Ungültigkeit einer eID-Karte nach § 21 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

Auf meine Stellungnahme vom 22.03.2021 gegenüber dem Ausschuss für Inneres und Heimat zu diesem Gesetzgebungsvorhaben nehme ich ergänzend Bezug.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn FAX +49 (0)228-997799-5550 INTERNET www.bfdi.bund.de