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 -

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)229

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

DATUM Bonn, 02.06.2023
GESCHÄFTSZ. 21-206-6/001#0001

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

BETREFF **Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens**

Sehr geehrter Herr Prof. Dr. Castellucci,

anliegend übersende ich meine Stellungnahme zu dem Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens mit der Bitte um Berücksichtigung.

Mit freundlichen Grüßen

[redacted]

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 02.06.2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens

(BT-Drs. 20/6519)

unter Berücksichtigung der

Stellungnahme des Bundesrats

(BR-Drs. 144/23(B))

und der

Gegenäußerung der Bundesregierung

(BT-Drs. 20/7076)

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

1. Allgemeines

Mit dem Gesetzentwurf sollen die Verarbeitungsbefugnisse der sowohl sichtbar auf Pässen und Personalausweisen aufgedruckten, aber auch der auf dem jeweiligen Chip gespeicherten Daten erweitert werden. Bisher bestehende Beschränkungen, etwa dass in dem Chip gespeicherte Daten nur zum Zweck der Prüfung der Echtheit des Dokuments oder der Identität des Inhabers verwendet werden dürfen, sollen gelockert werden. Zugleich soll die Möglichkeit eröffnet werden, dass jegliche öffentlichen Stellen für Identifizierungszwecke auf die im Chip gespeicherten Daten, darunter das biometrische Lichtbild, zugreifen, wenn es gesetzlich oder auf Grund eines Gesetzes vorgesehen ist. Die Verarbeitung biometrischer Daten stellt jedoch einen schwerwiegenden Eingriff in die Rechte der betroffenen Personen dar. Die Rechtfertigung unterliegt deshalb entsprechend hohen Anforderungen. Auf Grundlage des nationalen Rechts ist eine Verarbeitung nur aus Gründen *erheblicher öffentlicher Interessen* zulässig (Art. 9 Abs. 2 lit. g DS-GVO). Der Gesetzgeber darf deshalb nur solchen Stellen Zugriff auf die in dem Chip von Pässen und Personalausweisen zu hoheitlichen Zwecken verarbeiteten Daten gewähren, die Aufgaben in erheblichem öffentlichen Interesse wahrnehmen und einen solchen Zugriff zur Erfüllung dieser Aufgaben zwingend benötigen.

2. § 16a Abs. 2, § 16b Abs. 2 PassG-E sowie § 16 Abs. 2, § 17 Abs. 2 PAuswG-E

Mit den Vorschriften soll ermöglicht werden, dass Polizeivollzugsbehörden und die Zollverwaltung, sowie Pass-, Personalausweis- und Meldebehörden (bei Personalausweisen auch Steuerfahndungsstellen der Länder) Daten, die sie im Rahmen einer Identitätsprüfung aus dem Chip ausgelesen haben, medienbruchfrei in anderen Datenverarbeitungssystemen weiterverarbeitet können, sofern sie dazu durch ein Gesetz oder aufgrund eines Gesetzes berechtigt sind. Nach der Gesetzesbegründung soll dadurch das bislang erforderliche händische Übertragen in andere Systeme entfallen, falls die Daten für Folgemaßnahmen benötigt werden. Nach dem Änderungsvorschlag des Bundesrats soll dies auch für die im Chip gespeicherten biometrischen Daten gelten.

Zwar ist das Ziel – Vermeidung von Medienbrüchen – nachvollziehbar, wenn die im Rahmen einer Identitätsfeststellung erhobenen Daten für andere Zwecke weiterverarbeitet werden müssen. Meines Erachtens genügen die Vorschriften in der vorgeschlagenen Form aber nicht den Anforderungen der DSGVO und des BDSG an die Zweckbindung (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO, § 47 Nr. 2 BDSG) und das Gebot der Datenminimierung bei der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DSGVO, § 47 Nr. 3 BDSG). Denn die Normen enthalten keine Beschränkungen für die Weiterverarbeitung der Daten,

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

insbesondere hinsichtlich Zweck und Dauer der Verarbeitung. Schon in einer solchen Öffnungsklausel ist aber mindestens festzulegen, dass Daten nur dann elektronisch weiterverarbeitet werden dürfen, wenn

- eine ausdrückliche gesetzliche Rechtsgrundlage im Fachrecht besteht, die die Weiterverarbeitung gestattet,
- sich die weitere Maßnahme zeitlich unmittelbar an die Identitätsfeststellung anschließt (andernfalls sind die Daten unverzüglich zu löschen),
- die elektronische Weiterverarbeitung der ausgelesenen Daten auf diejenigen Daten beschränkt wird, die für den Zweck, für den die Daten weiterverarbeitet werden, zwingend erforderlich sind,
- die Daten nur für den Zweck und die Dauer der Durchführung der Folgemaßnahme verarbeitet werden dürfen und
- der Betroffene unverzüglich über die weitere Verarbeitung seiner Daten, die der Identitätsprüfung nachfolgt, aufgeklärt wird.

Es muss ausgeschlossen werden, dass Schattendatenbanken entstehen, in denen Daten aus Identitätsfeststellungen ohne klare Zweckbindung für möglicherweise erst in der Zukunft erforderliche weitere Datenverarbeitungen gespeichert werden.

Kritisch sehe ich außerdem den Vorschlag des Bundesrats, dass auch biometrische Daten gespeichert werden dürfen (Streichung der Ausnahme biometrischer Daten in § 16a Abs. 2 PassG-E/§ 16 Abs. 2 PAuswG-E). Richtigerweise merkt der Bundesrat zwar an, dass eine automatisierte Speicherung nach dem jeweiligen Absatz 2 zusätzlich einer spezialgesetzlichen Rechtsgrundlage bedarf. Die Verarbeitung biometrischer Daten stellt einen schwerwiegenden Grundrechtseingriff dar, an dessen Rechtfertigung daher besonders hohe Anforderungen zu stellen sind (Art. 9 Abs. 2 DSGVO). Dies auch vor dem Hintergrund des § 48 BDSG, nach dem "die Verarbeitung besonderer Kategorien personenbezogener Daten nur zulässig [ist], wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist". Eine Speicherung biometrischer Daten muss aber wegen damit verbundenen Grundrechtseingriffs generell ausgeschlossen bleiben. Meines Erachtens kann die in der Stellungnahme des Bundesrats zur Begründung genannte, ohnehin nur in Einzelfällen notwendige Erstellung von Wahllichtbildvorlagen eine allgemeine zweckändernde Speicherbefugnis biometrischer Daten (die im übrigen auch Fingerabdrücke umfassen würde) nicht rechtfertigen. Ich teile daher

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

die Auffassung der Bundesregierung in ihrer Gegenäußerung, dass die Begründung nicht geeignet ist, die Verhältnismäßigkeit des Eingriffs darzulegen (BT-Drs. 20/7076, zu Nummer 1, S. 8).

3. § 16a Abs. 3 PassG-E, § 20 Abs. 4a PAuswG-E, § 78 Absatz 7 Satz 3 AufenthG-E

Mit der beabsichtigten Neuregelung in § 16a Abs. 3 PassG-E, § 20 Abs. 4a PAuswG-E und § 78 Abs. 7 Satz 3 AufenthG-E soll ermöglicht werden, dass öffentliche Stellen zur Prüfung der Identität des Dokumenteninhabers Daten einschließlich des Lichtbilds aus dem Chip bzw. dem elektronischen Speicher- und Verarbeitungsmedium auslesen, wenn durch Gesetz oder auf Grund eines Gesetzes hierzu ermächtigt wird und der Pass- oder Personalausweisinhaber zustimmt.

Nach bisheriger Rechtslage dürfen nur solche öffentlichen Stellen Daten aus dem Chip des Passes bzw. des Personalausweises auslesen, die dies zwingend für ihre Aufgabenerfüllung benötigen: Polizeivollzugsbehörden, die Zollverwaltung sowie Pass-, Personalausweis- und Meldebehörden (bei Personalausweisen auch Steuerfahndungsstellen der Länder). Eine Notwendigkeit für die nun vorgeschlagene gesetzliche Öffnungsklausel für alle öffentlichen Stellen ist nicht erkennbar, da der Personalausweis bereits jetzt im Rechtsverkehr die zuverlässige Identifizierung einer Person ermöglicht. Der Abgleich des ausgelesenen biometrischen Lichtbilds mit dem Videobild lässt unter anderem wegen technischer Manipulierbarkeit auch von Echtzeit-Videoaufnahmen („deep fakes“) keine zuverlässige Identifikation einer Person zu. Eine sichere Identifikation wäre stattdessen durch Eingabe der PIN des Ausweisdokuments durch den Videokonferenzteilnehmer möglich, da diese nur dem Ausweisinhaber bekannt ist. Auf den Lichtbildabgleich kann (bzw. sollte mangels Erforderlichkeit) dann verzichtet werden.

Darüber hinaus begründet eine solche Öffnungsklausel die Gefahr, dass nunmehr vielfach öffentliche Stellen Zugriff auf die im Chip gespeicherten Daten einschließlich biometrischer Daten erhalten, die diese sensiblen Daten gerade nicht wie bislang zur Erfüllung (besonders gewichtiger) Aufgaben insbesondere der Gewährleistung der öffentlichen Sicherheit benötigen.

Zudem darf nach dem Gesetzentwurf ein Teil der ausgelesenen Daten (z.B. Seriennummer, Abkürzungen für Geschlecht und Staatsangehörigkeit) nicht verwendet werden, sondern ist unverzüglich nach dem Auslesen zu löschen. Eine technische Lösung, welche das Auslesen lediglich der erforderlichen Daten ermöglicht, wäre aus Datenschutzsicht vorzugswür-

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

dig. Im Übrigen kommt es in solchen und ähnlichen Fällen der Identitätsfeststellung besonders darauf an, dass ausreichende technische und organisatorische Anforderungen an die Verfahren zur sicheren Übermittlung des Lichtbilds gestellt und eingehalten werden.

4. § 16b Abs. 1 PassG-E, § 17 Abs. 1 PAuswG-E

Abzulehnen ist auch der in der Stellungnahme des Bundesrats zu dem Gesetzentwurf vorgeschlagene Formulierung, dass die sichtbar aufgedruckten Daten durch „sichere“ Verfahren oder „automatisiert“ verarbeitet werden dürfen (anstelle von „nicht automatisiert“, BR-Drs. 144/23(B), Nr. 1 zu § 16b Abs. 1 PassG-E, § 17 Abs. 1 PAuswG-E). Denn diese Formulierung würde jegliche Art des Scannens, Fotografierens und vergleichbare Verarbeitungsformen gestatten. Das automatisierte Auslesen muss auch in diesen Fällen auf die maschinenlesbare Zone beschränkt sein. Es ist schon die Notwendigkeit einer solchen Ermächtigung nicht ersichtlich, da bereits die Berechtigung zum Auslesen des Chips sowie der maschinenlesbaren Zone eine hinreichende Befugnis zur automatisierten Verarbeitung der personenbezogenen Daten des Dokumenteninhabers enthalten. In den vermutlich äußerst seltenen Ausnamefällen, dass beides nicht möglich ist, können die sichtbar aufgedruckten Daten nach wie vor abgelesen und in andere Verarbeitungssysteme eingegeben werden. Solche absoluten Einzelfälle rechtfertigen eine generelle Befugnisnorm zum automatisierten Auslesen der sichtbar aufgedruckten Daten meines Erachtens nicht. Die im Gesetzentwurf vorgesehenen Regelungen des § 16a Abs. 2 PassG-E, § 17 PAuswG-E decken die notwendigen Befugnisse ab. Ich schließe mich insoweit der Gegenäußerung der Bundesregierung an (BT-Drs. 20/7076, zu Nummer 1, S. 8).

5. § 19 Abs. 4a PassG-E, § 8 Abs. 1a PAuswG-E, § 7 Abs. 1a eID-Karte-Gesetz-E

Bisher war für Pass- und Personalausweisangelegenheiten sowie die eID-Karte einer Person immer (nur) eine Behörde zuständig: die Gemeindebehörde am Wohnsitz der Person. Künftig soll aber immer die Behörde das Pass-, Personalausweis- und eID-Karte-Register führen, die den Pass, Personalausweis oder die eID-Karte ausgestellt hat, während für die Pass-, Personalausweis- und eID-Karte-Angelegenheiten im Übrigen die Behörde am Wohnsitz zuständig sein wird. Das wird nach einem Umzug und damit in einer sehr großen Zahl an Fällen zu einem Auseinanderfallen von registerführender und örtlich zuständiger Behörde führen.

Da einerseits die Registerdaten aktuell gehalten werden müssen und nunmehr zwei Behörden die im Register gespeicherten Daten zur Erfüllung ihrer Aufgaben jedenfalls teilweise benötigen, sieht der Gesetzentwurf beiderseits automatisierte Mitteilungs- und Datenabrufbefugnisse (§ 6a Abs. 3 Nr. 6, § 22 Abs. 1a PassG-E, § 24 Abs. 1a, § 34 Satz 1 Nr. 12

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

PAuswG-E; § 19a, § 25 Satz 1 Nr. 12 eID-Karte-Gesetz-E) sowie eine Speicherbefugnis der örtlich zuständigen Behörde (§ 21 Abs. 6 PassG-E, § 23 Abs. 6 PAuswG-E, § 19 Abs. 5 eID-Karte-Gesetz-E) vor.

Einen sachlichen Grund für eine solche Doppelzuständigkeit vermag ich nicht zu erkennen. Meines Erachtens sollte der Ansatz überdacht werden. Er führt zu einer Vervielfachung von Datenverarbeitungsvorgängen, zu unnötigem bürokratischem Aufwand und eröffnet Fehlerquellen. Welche Datenquelle bei Widersprüchen letztlich „führend“ ist, bleibt offen. Diese Probleme bestehen auch dann, wenn künftig nur noch die registerführende Behörde die führende Datenquelle verwaltet, da es gleichwohl zu Verarbeitungsvorgängen bei der örtlich zuständigen Behörde kommen muss.

Wird dennoch an der Regelung festgehalten, muss durch technische Maßnahmen sichergestellt werden, dass Abrufe bei der registerführenden Behörde nur durch die laut Pass- oder Personalausweisregister örtlich zuständige Pass- oder Personalausweisbehörde möglich sind. Dabei sind automatisierte Datenabrufe jedenfalls biometrischer Daten auszuschließen, da diese letztlich einen Abruf von Pass- und Personalausweisdaten ermöglichen würde ohne weitere Prüfung, ob die hierfür notwendigen Voraussetzungen tatsächlich vorliegen.

6. Abruf von Lichtbildern im automatisierten Verfahren, zentrale Pass- und Personalausweisregister der Länder

Die Einführung eines nahezu voraussetzungslosen Lichtbildabrufs im automatisierten Verfahren durch die Sicherheitsbehörden nach § 22a Abs. 2 S. 5 PassG bzw. § 25 Abs. 2 S. 4 PAuswG durch das Gesetz zur Förderung des elektronischen Identitätsnachweises vom 07.07.2017 (BGBl I S. 2310) hatte ich bereits in meiner damaligen Stellungnahme kritisiert und aus datenschutzrechtlicher Sicht abgelehnt.[1] Meine dahingehenden Bedenken halte ich im Hinblick auf die vorgesehenen Neuregelungen in § 22a Abs. 3 PassG-E und § 35 Abs. 3 PAuswG zum automatisierten Abruf von Lichtbildern aufrecht. Durch die in § 22a Abs. 3 PassG-E bzw. § 25 Abs. 3 PAuswG-E vorgesehene, spiegelbildliche Verpflichtung der Pass- und Personalausweisbehörden zur Sicherstellung einer solchen Abrufmöglichkeit wird diese Rechtslage weiter verfestigt.

Kritisch bewertet hatte ich seinerzeit auch die Ermächtigung zur Einrichtung zentraler Pass- und Personalausweisregisterdatenbestände in den Ländern nach §§ 27a PassG und § 34a PAuswG durch das Gesetz zur Einführung eines elektronischen Identitätsnachweises

[1] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2017/StgN_elektronischer_Identit%C3%A4tsnachweis.pdf?__blob=publicationFile&v=5

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

mit einem mobilen Endgerät vom 05.07.2021 (BGBl I S. 2281). Die damals geäußerten erheblichen datenschutzrechtlichen Bedenken bestehen fort.[2]

[2] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/StgN_elektr-Identit%C3%A4tsnachweis-mobil.pdf?__blob=publicationFile&v=2

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