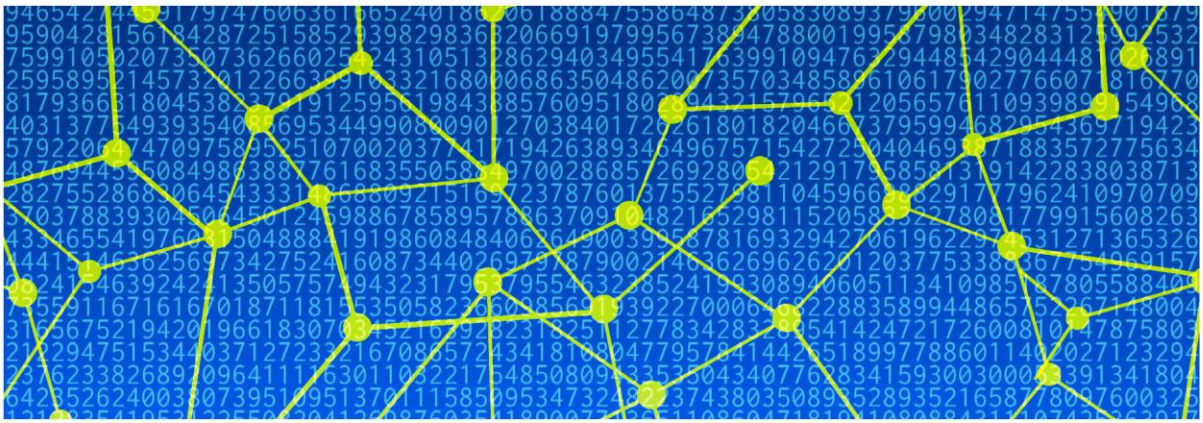

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 7/2018 des EDSB

zu dem Vorschlag für eine Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und anderer Dokumenten

10. August 2018

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und speziell mit einem konstruktiven und proaktiven Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzauswirkungen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern. Dies steht im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung". Der EDSB setzt sich zwar für eine Erhöhung der Sicherheit von Personalausweisen und Aufenthaltsdokumenten ein, die insgesamt zu einer sichereren Union beiträgt, doch sollte seiner Ansicht nach der Vorschlag in bestimmten Kernaspekten verbessert werden, damit den Grundsätzen des Datenschutzes Genüge getan wird.

Zusammenfassung

In der vorliegenden Stellungnahme wird die Haltung des EDSB zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und ihren Familienangehörigen in Ausübung ihres Rechts auf Freizügigkeit ausgestellt werden, dargelegt.

In diesem Zusammenhang stellt der EDSB fest, dass sich die Kommission eindeutig dafür entschieden hat, den die Freizügigkeit betreffenden Aspekten des Vorschlags Vorrang einzuräumen und das sicherheitsbezogene Ziel als sekundär zu behandeln. Der EDSB merkt an, dass sich dies auf die Prüfung der Notwendigkeit und Verhältnismäßigkeit der Elemente des Vorschlags auswirken könnte.

Der EDSB unterstützt die Europäische Kommission in ihrer Zielsetzung, die für Personalausweise und Aufenthaltsdokumente geltenden Sicherheitsstandards zu verbessern und damit zur Sicherheit der Union insgesamt beizutragen. Gleichzeitig ist der EDSB der Auffassung, dass der Vorschlag die Notwendigkeit der Verarbeitung von zwei Arten biometrischer Daten (Gesichtsbild und Fingerabdrücke) in diesem Zusammenhang nicht ausreichend begründet, zumal der angegebene Zweck auch mit einem weniger in die Privatsphäre eindringenden Vorgehen erreicht werden könnte.

Gemäß dem EU-Rechtsrahmen sowie dem modernisierten Übereinkommen Nr. 108 gelten biometrische Daten als sensible Daten und unterliegen sie besonderem Schutz. Der EDSB unterstreicht, dass sowohl Gesichtsbilder als auch Fingerabdrücke, die nach dem Vorschlag verarbeitet würden, eindeutig in die Kategorie sensibler Daten fallen würden.

Des Weiteren ist der EDSB der Ansicht, dass der Vorschlag weitreichende Auswirkungen auf bis zu 370 Millionen EU-Bürger hätte, da er möglicherweise bei 85 % der EU-Bevölkerung die obligatorische Abnahme von Fingerabdrücken verlangen würde. Dieser breit angelegte Anwendungsbereich sowie die höchst sensiblen Daten, die verarbeitet werden (Gesichtsbilder in Kombination mit Fingerabdrücken), verlangen eine gründliche Prüfung auf der Grundlage einer strengen Prüfung der Notwendigkeit.

Der EDSB räumt darüber hinaus ein, dass in Anbetracht der Unterschiede zwischen Personalausweisen und Reisepässen die Einführung auch für Personalausweise von Sicherheitsmerkmalen, die für Reisepässe möglicherweise als angemessen gelten, nicht automatisch geschehen darf, sondern der Überlegung und einer gründlichen Analyse bedarf.

Der EDSB unterstreicht ferner, dass Artikel 35 Absatz 10 der Datenschutz-Grundverordnung (im Folgenden *„DSGVO“*)[1] auf die hier zu prüfende Verarbeitung Anwendung finden würde. In diesem Zusammenhang weist der EDSB darauf hin, dass die Folgenabschätzung zum Vorschlag anscheinend die von der Kommission gewählte Option nicht unterstützt, nämlich die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise (und Aufenthaltsdokumente). Folglich kann nicht davon ausgegangen werden, dass die Folgenabschätzung zum Vorschlag für den Zweck der Einhaltung von

Artikel 35 Absatz 10 DSGVO genügt. Der EDSB empfiehlt daher, vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.

Der Vorschlag sollte ferner explizit Garantien mit Blick auf Mitgliedstaaten vorsehen, die im Rahmen der Umsetzung des Vorschlags nationale Fingerabdruckdatenbanken aufbauen. Dem Vorschlag sollte eine Bestimmung hinzugefügt werden, die ausdrücklich besagt, dass in diesem Zusammenhang verarbeitete biometrische Daten nach ihrer Speicherung auf dem Chip unverzüglich zu löschen sind und nicht für andere als die im Vorschlag explizit erwähnten Zwecke weiterverarbeitet werden dürfen.

Nach dem Verständnis des EDSB könnte die Verwendung biometrischer Daten als legitime Maßnahme zur Betrugsbekämpfung gelten, doch begründet der Vorschlag nicht die Notwendigkeit der Speicherung von zwei Arten biometrischer Daten für seine Zwecke. Eine erwägenswerte Option wäre die Beschränkung der verwendeten biometrischen Daten auf eine Art (z. B. nur Gesichtsbilder).

Der EDSB weist darüber hinaus darauf hin, dass nach seinem Verständnis die Speicherung von Fingerabdrücken die Interoperabilität verbessert, dass sie aber gleichzeitig die Menge verarbeiteter biometrischer Daten und das Risiko der Identitätserschleichung bei einer Verletzung des Schutzes personenbezogener Daten erhöht. Der EDSB empfiehlt daher, die im Dokument auf dem Chip gespeicherten Fingerabdruckdaten auf Minuzien oder Muster zu beschränken, also auf eine Untermenge der aus dem Fingerabdruckbild extrahierten Merkmale.

Schließlich empfiehlt der EDSB in Anbetracht der vorstehend geschilderten breit gefächerten und potenziellen Auswirkungen des Vorschlags, die Altersgrenze für die Abnahme von Fingerabdrücken bei Kindern im Einklang mit anderen Instrumenten des EU-Rechts auf 14 Jahre festzulegen.

INHALTSVERZEICHNIS

1. EINLEITUNG UND HINTERGRUND 6

2. ZIELE UND HINTERGRUND DES VORSCHLAGS 7

3. VERHÄLTNISMÄSSIGKEIT UND NOTWENDIGKEIT DER VERARBEITUNG BIOMETRISCHER DATEN 9

3.1. BIOMETRISCHE DATEN SIND SENSIBLE DATEN 9

3.2. BREIT ANGELEGTER ANWENDUNGSBEREICH UND WEITREICHENDE AUSWIRKUNGEN DES VORSCHLAGS 9

3.3. RECHTFERTIGUNG DES VORSCHLAGS: NATIONALE PERSONALAUSWEISE VS. REISEPÄSSE UND DIE AUSWIRKUNGEN DER FREIZÜGIGKEIT 10

3.4. BEDARF AN EINER DATENSCHUTZ-FOLGENABSCHÄTZUNG 12

4. VERARBEITUNG BIOMETRISCHER DATEN: ERFORDERLICHE GARANTIEN 14

4.1. ZWECKBINDUNG 14

4.2. DATENMINIMIERUNG 16

4.3 BEFREIUNGEN VON DER ABNAHME VON FINGERABDRÜCKEN 18

7. SCHLUSSFOLGERUNGEN 19

Endnoten 21

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die 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)[2],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[3], insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d,

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[4] —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Am 17. April 2018 veröffentlichte die Europäische Kommission (im Folgenden *„Kommission“*) den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und ihren Familienangehörigen in Ausübung ihres Rechts auf Freizügigkeit ausgestellt werden[5], mit dem die Sicherheitsmerkmale der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente ihrer Familienangehörigen aus Drittstaaten verbessert werden sollen (im Folgenden *„Vorschlag“*).

2. Dieser Vorschlag ist Teil des Aktionsplans vom Dezember 2016 *„für ein wirksameres europäisches Vorgehen gegen Reisedokumentenbetrug“* (im Folgenden *„Aktionsplan vom Dezember 2016“*)[6], in dem die Kommission vor dem Hintergrund der jüngsten terroristischen Anschläge in Europa Maßnahmen im Bereich der Dokumentensicherheit einschließlich Personalausweisen und Aufenthaltsdokumenten auflistete.

3. Personalausweise spielen eine wichtige Rolle bei der sicheren Identifizierung einer Person für administrative und kommerzielle Zwecke, wie es die Kommission in ihrer Mitteilung vom 14. September 2016*„Mehr Sicherheit in einer von Mobilität geprägten Welt: Besserer Informationsaustausch bei der Terrorismusbekämpfung und ein stärkerer Schutz der Außengrenzen“*[7] unterstrichen hat. Der Bedarf an einer verbesserten Sicherheit dieser Dokumente wurde auch in dem Bericht über die Unionsbürgerschaft 2017 hervorgehoben.

4. Es gehört zu den Aufgaben des EDSB, die Dienststellen der Kommission bei der Abfassung neuer Legislativvorschläge, die Auswirkungen auf den Datenschutz haben, zu beraten.

5. Der EDSB begrüßt die Tatsache, dass er von der Europäischen Kommission bereits informell zum Entwurf des Vorschlags konsultiert worden war und Gelegenheit hatte, sich zu Datenschutzaspekten zu äußern.

2. ZIELE UND HINTERGRUND DES VORSCHLAGS

6. Der EDSB hält fest, dass der Vorschlag den Themen **Sicherheit und Bekämpfung von Terrorismus und organisierter Kriminalität** großes Gewicht beimisst. Gleich am Anfang der Begründung heißt es: *„Die Gewährleistung der Sicherheit von Reise- und Identitätsdokumenten ist von maßgeblicher Bedeutung für die Bekämpfung von Terrorismus und organisierter Kriminalität“*. Des Weiteren wird dort unterstrichen: *„Eine höhere Dokumentensicherheit trägt maßgeblich zur Erhöhung der Sicherheit innerhalb der EU und an deren Grenzen sowie zur Verwirklichung einer wirksamen und echten Sicherheitsunion bei.“*.[8] Das Hauptziel der Verordnung besteht darin, *„die Sicherheitsnormen für Personalausweise, die die Mitgliedstaaten ihren Staatsangehörigen ausstellen, und für Aufenthaltsdokumente, die die Mitgliedstaaten Unionsbürgern und deren Familienangehörigen in Ausübung ihres Rechts auf Freizügigkeit ausstellen, zu verschärfen“*.[9]

7. In der Folgenabschätzung zum Vorschlag werden noch weitere Ziele des Vorschlags erwähnt, darunter *„die Verringerung des Dokumentenbetrugs, die Verbesserung der Akzeptanz und Authentifizierung der Personalausweise und Aufenthaltsdokumente und die Verbesserung der auf ihnen beruhenden Identifizierung von Personen“.* Als weitere werden genannt *„die Sensibilisierung von Bürgern, nationalen Behörden und privatem Sektor bezüglich der ausgestellten Dokumente und des mit ihnen verknüpften Rechts auf Freizügigkeit“.* Schließlich heißt es dort: *„Vereinfachung des Alltags für EU-Bürger, Abbau von Bürokratie und geringere Kosten sowohl für die Bürger als auch für private und öffentliche Einrichtungen durch den Abbau von Verwaltungshemmnissen ... im Zusammenhang mit der Verwendung von Personalausweisen und Aufenthaltsdokumenten“.*[10]

8. Der EDSB hält fest, dass die Rechtsgrundlage für den Vorschlag Artikel 21 Absatz 2 AEUV ist. Diese Bestimmung besagt: *„Erscheint zur Erreichung dieses Ziels [Freizügigkeit] ein Tätigwerden der Union erforderlich (...), so können das Europäische Parlament und der Rat gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften erlassen, mit denen die Ausübung“* des Rechts auf Freizügigkeit *„erleichtert wird“*. **Der EDSB stellt fest, dass sich die Kommission eindeutig dafür entschieden hat, den die Freizügigkeit betreffenden Aspekten des Vorschlags Vorrang einzuräumen und das sicherheitsbezogene Ziel als sekundär zu behandeln. Der EDSB stellt fest, dass sich dies auf die Prüfung der Notwendigkeit und Verhältnismäßigkeit der Elemente des Vorschlags auswirken könnte** (siehe weiter unten).

9. Derzeit sind in der Richtlinie über Rechte der Unionsbürger (EU) 2004/38[11] **das Format und die Mindestnormen für Personalausweise nicht geregelt und werden auch keine spezifischen Normen** für **Aufenthaltsdokumente** formuliert, die für Unionsbürger und deren Familienangehörige aus Drittstaaten ausgestellt werden. Folglich **verlangt** die Richtlinie (EU) 2004/38 **nicht,** dass den Bürgern der Union ausgestellte Personalausweise oder Familienangehörigen von Unionsbürgern aus Drittstaaten ausgestellte Aufenthaltsdokumente **biometrische Daten** wie ein Gesichtsbild des Ausweisinhabers und/oder Fingerabdrücke in interoperablen Formaten **enthalten**.

10. Ziel des Vorschlags ist eine Verbesserung der Sicherheit der Personalausweise von Unionsbürgern und von Aufenthaltskarten für deren Familienangehörige aus Drittstaaten, und zwar durch die **obligatorische Aufnahme biometrischer Daten (zwei Fingerabdrücke und ein Gesichtsbild) in Personalausweise**, die von Mitgliedstaaten für ihre Bürger ausgestellt werden, und **in Aufenthaltskarten für Familienangehörige**, die nicht die Staatsangehörigkeit eines Mitgliedstaats besitzen. Hierzu sieht der Vorschlag vor, dass die von den Mitgliedstaaten ausgestellten Personalausweise im ID-1-Format hergestellt werden und den im ICAO-Dokument 9303 (siebte Auflage, 2015) festgelegten Mindestsicherheitsnormen entsprechen müssen. Gemäß dem ICAO-Dokument 9303 (siebte Auflage, 2015) (im Folgenden *„ICAO-Dokument"*) werden die biometrischen Daten im Hinblick auf eine Verwendung mit Gesichts-, Fingerabdruck- oder Iris-Erkennungssystemen gespeichert.[12]

11. Bezüglich der **Aufenthaltskarten für Familienangehörige**, die nicht die Staatsangehörigkeit eines Mitgliedstaats besitzen, besagt Artikel 7 Absatz 1 des Vorschlags Folgendes: *„Bei der Ausstellung von Aufenthaltskarten für Familienangehörige von Unionsbürgern, die nicht die Staatsangehörigkeit eines Mitgliedstaats besitzen, legen die Mitgliedstaaten dieselbe Gestaltung zugrunde, wie sie mit der Verordnung (EG) Nr. 1030/2002 des Rates zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige festgelegt wurde."* Heute sieht Artikel 5 der Verordnung (EG) Nr. 1030/2002[13] zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige vor, dass die Verordnung (EG) Nr. 1030/2002 unter anderem nicht gilt für *„Drittstaatenangehörige, die Familienangehörige von Unionsbürgern sind, die ihr Recht auf Freizügigkeit ausüben (...)*". Das bedeutet im Ergebnis, dass derzeit Artikel 4a der Verordnung (EG) Nr. 1030/2002, dem zufolge in dem Aufenthaltstitel für Drittstaatenangehörige ein Gesichtsbild und zwei Fingerabdrücke als biometrische Merkmale zu speichern sind, nicht für Drittstaatenangehörige gilt, die Familienangehörige von Unionsbürgern sind.

12. **Der EDSB unterstützt die Europäische Kommission in ihrer Zielsetzung, die für Personalausweise und Aufenthaltsdokumente geltenden Sicherheitsstandards zu verbessern und damit zur Sicherheit der Union insgesamt beizutragen.** Gleichzeitig **ist der EDSB der** nachstehend näher erläuterten **Auffassung, dass der Vorschlag die Notwendigkeit der Verarbeitung von zwei Arten biometrischer Daten (Gesichtsbild und Fingerabdrücke) in diesem Zusammenhang nicht ausreichend begründet, zumal der angegebene Zweck auch mit einem weniger in die Privatsphäre eindringenden Vorgehen erreicht werden könnte.**

3. VERHÄLTNISMÄSSIGKEIT UND NOTWENDIGKEIT DER VERARBEITUNG BIOMETRISCHER DATEN

3.1. Biometrische Daten sind sensible Daten

13. Der EDSB unterstreicht, dass **die Verarbeitung biometrischer Daten eine Einschränkung der Grundrechte auf Privatsphäre und auf Schutz personenbezogener Daten** darstellt und wie jeder Eingriff in ein Grundrecht **die Kriterien von Artikel 52 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „*Charta*") erfüllen muss.**[14] Jede Einschränkung muss nicht nur gesetzlich vorgesehen sein, sondern muss auch den Wesensgehalt des Rechts achten und darf unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie erforderlich ist und den von der Union anerkannten Zielsetzungen und den Erfordernissen des Schutzes der Rechte und Freiheiten tatsächlich entspricht.

14. Fingerabdrücke sind personenbezogene Daten, da sie objektiv einmalige Informationen über natürliche Personen enthalten, die eine genaue Identifizierung dieser Personen erlauben.[15] Im EU-Rechtsrahmen **sind biometrische Daten definiert als** mit speziellen technischen Verfahren gewonnene **personenbezogene Daten** zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die **die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.**[16] **Im EU-Rechtsrahmen**[17] **sowie in dem modernisierten Übereinkommen Nr. 108**[18] **gelten biometrische Daten als eine besondere Kategorie personenbezogener Daten**[19] **und genießen sie besonderen Schutz**: Ihre Verarbeitung ist grundsätzlich verboten, und es gibt eine geringe Anzahl von Voraussetzungen, unter denen ihre Verarbeitung rechtmäßig ist. Dies gilt insbesondere für zum Zweck der Identifizierung einer Person verarbeitete biometrische Daten. **Der EDSB unterstreicht, dass sowohl Gesichtsbilder als auch Fingerabdrücke, die nach dem Vorschlag verarbeitet würden, eindeutig in die Kategorie sensibler Daten fallen würden.**

15. Daher muss nach Auffassung des EDSB unbedingt sichergestellt werden, dass die Verarbeitung biometrischer Daten gemäß dem Vorschlag **auf das Maß beschränkt wird, das für das Erreichen seiner angegebenen Ziele zwingend erforderlich ist.** Aufgrund des besonders sensiblen Charakters biometrischer Daten wird es darüber hinaus erforderlich sein, **geeignete Garantien** vorzusehen (siehe weiter unten).

3.2. Breit angelegter Anwendungsbereich und weitreichende Auswirkungen des Vorschlags

16. Der EDSB erinnert daran, dass, wie in seinem „Necessity Toolkit"[20] dargelegt, die **Notwendigkeit ein wesentlicher Grundsatz bei der Prüfung einer Einschränkung von Grundrechten** wie dem Recht auf Schutz personenbezogener Daten **ist**. Nach der Rechtsprechung muss die Einschränkung des Grundrechts auf Schutz personenbezogener Daten wegen der Rolle, die die Verarbeitung personenbezogener Daten für eine ganze Reihe von Grundrechten mit sich bringt, zwingend erforderlich sein. **Die Notwendigkeit**

ist anhand objektiver Beweise zu begründen und ist der erste Schritt bei der Beurteilung der Verhältnismäßigkeit der Einschränkung. Die Notwendigkeit spielt auch bei der Beurteilung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten eine wesentliche Rolle. Die Verarbeitungsvorgänge, die Kategorien verarbeiteter Daten und die Dauer der Datenspeicherung sind für den Zweck der Verarbeitung erforderlich.

17. Der Vorschlag verpflichtet die Mitgliedstaaten nicht, Personalausweise oder Aufenthaltsdokumente einzuführen, wenn diese nach nationalem Recht nicht vorgesehen sind; ebenso wenig berührt er die Zuständigkeit der Mitgliedstaaten für die Ausstellung anderer Aufenthaltsdokumente nach nationalem Recht, die nicht in den Anwendungsbereich des Unionsrechts fallen.[21] Somit **betreffen die neuen Vorschriften in dem Vorschlag nur die Mitgliedstaaten, die bereits Personalausweise oder Aufenthaltsdokumente ausstellen**, seien diese nun obligatorisch oder nicht.

18. In diesem Zusammenhang sei darauf hingewiesen, dass Dänemark und das Vereinigte Königreich gar keine Personalausweise ausstellen. Von den 26 Mitgliedstaaten, die Personalausweise ausstellen, ist der Besitz eines solchen Ausweises nur in 15 Mitgliedstaaten vorgeschrieben.[22] Derzeit enthalten von 13 Mitgliedstaaten ausgestellte Personalausweise gar keine biometrischen Daten.[23] Kurz gesagt: **Bis zu 370 der 440 Millionen Bürger in 26 Mitgliedstaaten wären von dem Vorschlag betroffen; das entspricht fast 85 % der 440 Millionen EU-Bürger.**[24] Die 370 Millionen Bürger entsprechen der *„Gesamtanzahl potenzieller Inhaber von Personalausweisen in 26 Mitgliedstaaten"*[25], und 175 Millionen von ihnen müssten der neuen Verpflichtung nachkommen, sich Fingerabdrücke für Personalausweise abnehmen zu lassen[26] (16 Mitgliedstaaten). Die verbleibenden 195 Millionen EU-Bürger, die bereits nach bestehendem nationalem Recht zum Besitz eines Personalausweises verpflichtet sind, wären von den neuen Anforderungen ebenfalls betroffen, denn nach einer Einführung auf EU-Ebene könnten die Mitgliedstaaten Anforderungen bezüglich Fingerabdrücken in Personalausweisen nicht allein mit nationalen Maßnahmen aufheben[27].

19. Folglich **ist der EDSB der Ansicht, dass der Vorschlag weitreichende Auswirkungen auf bis zu 370 Millionen EU-Bürger hätte, da er bei 85 % der EU-Bevölkerung möglicherweise die obligatorische Abnahme von Fingerabdrücken verlangen würde. Dieser breit angelegte Anwendungsbereich sowie die höchst sensiblen Daten, die verarbeitet werden (Gesichtsbilder in Kombination mit Fingerabdrücken), verlangen eine gründliche Prüfung auf der Grundlage einer strengen Prüfung der Notwendigkeit.**

3.3. Rechtfertigung des Vorschlags: nationale Personalausweise vs. Reisepässe und die Auswirkungen der Freizügigkeit

20. Der EDSB stellt fest, dass der Vorschlag wiederholt versucht, die von EU-Mitgliedstaaten ihren Bürgern ausgestellten nationalen Personalausweise als **rechtlich und von der Funktion her Reisepässen gleichwertig** darzustellen. In der Begründung des Vorschlags heißt es[28]: Aufgrund der Aufnahme zweier biometrischer Identifikatoren wird *„das Sicherheitsniveau der Personalausweise von EU-Bürgern und der Familienangehörigen aus Drittstaaten ausgestellten Aufenthaltskarten an die Normen angepasst, die für EU-*

Bürgern ausgestellte Reisepässe bzw. Aufenthaltstitel, die nicht Familienangehörige von EU-Bürgern sind, gelten".

21. Der Vorschlag verwendet die Begriffe „Personalausweise" und „Reisepässe" praktisch austauschbar im Zusammenhang mit der Ausübung des Rechts auf Freizügigkeit durch EU-Bürger (und ihre Familienangehörigen) und führt Anforderungen ein, die den für Reisepässe geltenden gleichwertig sind. Gemäß der Verordnung (EG) Nr. 2252/2004 des Rates sind derzeit die von den Mitgliedstaaten ausgestellten **Pässe und Reisedokumente mit einem Speichermedium mit einem hohen Sicherheitsstandard versehen, das ein Gesichtsbild und zwei** bei flach aufgelegten Fingern abgenommene **Fingerabdrücke** in interoperablen Formaten **enthält.** Folglich sieht der Vorschlag die obligatorische Aufnahme eines Gesichtsbilds und zweier Fingerabdrücke als biometrische Identifikatoren in von den Mitgliedstaaten für Familienangehörige von Unionsbürgern ausgestellte Aufenthaltskarten vor.

22. In diesem Zusammenhang **unterstützt der EDSB das Ziel der Kommission, die Freizügigkeit zu erleichtern. Dessen ungeachtet weist der EDSB darauf hin, dass die beiden Arten von Dokumenten – Personalausweise und Reisepässe – sowohl aus rechtlicher Sicht als auch im Hinblick auf ihre Verwendung in der Praxis höchst unterschiedlich sind.** Auch wenn sie als Reisedokumente im Kontext der Freizügigkeit verwendet werden, können nationale Personalausweise, anders als Pässe, nur für Reisen in EU-Mitgliedstaaten und diejenigen Drittländer verwendet werden, die EU-Bürgern die Einreise mit ihrem nationalen Personalausweis gestatten. Vor diesem Hintergrund fragt sich der EDSB, welchen Mehrwert die Aufnahme biometrischer Daten in die Personalausweise bringt, da diese bei Reisen zwischen den EU-Mitgliedstaaten nicht routinemäßig kontrolliert werden.

23. Noch viel wichtiger ist, dass **Personalausweise für eine Vielfalt von Zwecken genutzt werden, die über die Ausübung des Rechts auf Freizügigkeit** in Verbindung mit der Unionsbürgerschaft weit **hinausgehen**, nämlich für die Interaktion mit Verwaltungen im Heimatland eines Bürgers und für die Interaktion mit einer Vielzahl von Akteuren aus dem gesamten privaten Sektor (Banken, Fluggesellschaften usw.). Des Weiteren, so die Folgenabschätzung zum Vorschlag, leben rund 15 Millionen EU-Bürger in einem anderen EU-Mitgliedstaat und arbeiten 11 Millionen in einem anderen Mitgliedstaat.[29] Hieraus schließt der EDSB, dass für die überwiegende Mehrheit der EU-Bürger die Hauptfunktionen von Personalausweisen nicht unmittelbar mit der Freizügigkeit zu tun haben. Man kann auch bei Weitem nicht davon ausgehen, dass alle potenziell von den Anforderungen des Vorschlags, ihre Fingerabdrücke in nationale Personalausweise aufnehmen zu lassen, betroffenen EU-Bürger ihr Recht auf Freizügigkeit tatsächlich wahrnehmen. Ganz im Gegenteil: Mobile EU-Bürger machen eine kleine Minderheit dieser potenziell von dem Vorschlag Betroffenen aus. Und selbst diejenigen, die ihr Recht auf Freizügigkeit tatsächlich ausüben, können dies häufig mit einem Pass und nicht mit einem Personalausweis tun und tun es auch. **Die** von der Kommission vorgetragene **Rechtfertigung des Vorschlags ist daher nicht gänzlich überzeugend.**

24. Der Vorschlag spricht auch von der Notwendigkeit, Dokumentenbetrug zu bekämpfen, insbesondere die Fälschung von Dokumenten und die Vorspiegelung falscher Tatsachen

in Bezug auf die an das Aufenthaltsrecht geknüpften Bedingungen. Nicht klar wird, inwiefern verbesserte Sicherheitsmerkmale einschließlich biometrischer Daten bei der Lösung des Problems *„Vorspiegelung falscher Tatsachen“* helfen könnten. Jedenfalls hat die Europäische Agentur für die Grenz- und Küstenwache (FRONTEX), wie in der Folgenabschätzung zum Vorschlag erwähnt wird, **in den Jahren 2013-2017** Statistiken über gefälschte Personalausweise und Aufenthaltsdokumente erhoben und **lediglich 38 870 gefälschte Personalausweise ermittelt.**[30]

25. Außerdem **ging**, wie es in Anhang 6 der Folgenabschätzung zum Vorschlag heißt, die Zahl der Personen, die aus Drittländern mit gefälschten Personalausweisen und Aufenthaltsdokumenten ankommen, **im Jahr 2015 um 11 % (8 373) zurück**.[31] Diese Tendenz bestätigt auch die FRONTEX Risikoanalyse 2017[32], der zufolge die Zahl der Personen mit gefälschten Dokumenten **2016 weiter auf 7 044 zurückging**. Der Trend bei **Personalausweisen** verläuft ähnlich wie bei gefälschten Dokumenten insgesamt, wobei im Jahr **2016 weniger Fälle aufgedeckt wurden**.[33]

26. Nach Ansicht des EDSB rechtfertigen **diese relativ niedrige Zahl[34]** gefälschter Personalausweise und Aufenthaltsdokumente und die Tatsache, dass **die Zahl der Personen** aus Drittländern, die gefälschte Personalausweise und Aufenthaltsdokumente verwenden, **allmählich sinkt,** an sich noch nicht die in dem Vorschlag vorgelegten weitreichenden Lösungen.

27. **Der EDSB ist** folglich **der Auffassung, dass in Anbetracht der Unterschiede zwischen Personalausweisen und Reisepässen die Einführung auch für Personalausweise von Sicherheitsmerkmalen, die für Reisepässe als möglicherweise angemessen gelten, nicht automatisch geschehen darf, sondern der Überlegung und einer gründlichen Analyse bedarf.**

3.4. Bedarf an einer Datenschutz-Folgenabschätzung

28. Der EDSB hält ferner fest, dass gemäß Artikel 35 Absatz 1 der Datenschutz-Grundverordnung (im Folgenden *„DSGVO“*)[35] eine Datenschutz-Folgenabschätzung (im Folgenden *„DSFA“*) durchzuführen ist, bevor eine Verarbeitung erfolgt, die *„voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat“*. Nach Auffassung des EDSB gilt diese Anforderung in vollem Umfang auch im Kontext des Vorschlags. Die **DSFA sollte alle Verarbeitungsvorgänge abdecken, die für beide Kategorien biometrischer Daten vorgesehen sind, also für Gesichtsbilder und für Fingerabdrücke.** Die DSFA sollte sich insbesondere mit einer Beurteilung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie mit den Maßnahmen beschäftigen, mit denen gegen diese Risiken vorgegangen werden soll, wie Garantien und Sicherheitsvorkehrungen.

29. Der EDSB weist in diesem Zusammenhang darauf hin, dass **Artikel 35 Absatz 10 DSGVO auf die hier zu prüfende Verarbeitung anzuwenden wäre** (die ihre Rechtsgrundlage im Unionsrecht, nämlich dem Vorschlag, hätte). **Sofern** also **die DSFA nicht im Zusammenhang mit der Annahme des Vorschlags durchgeführt wird, sind die Mitgliedstaaten verpflichtet, sie zu einem späteren Zeitpunkt durchzuführen.** In

diesem Zusammenhang **weist der EDSB darauf hin, dass die Folgenabschätzung zum Vorschlag anscheinend die von der Kommission gewählte Option nicht unterstützt**, nämlich die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise (und Aufenthaltsdokumente).

30. Bei der Betrachtung der verschiedenen ID-Optionen heißt es in der Folgenabschätzung: ***„Bei den Optionen ID 2 und ID 3 müssen sich Bürger bei der Beantragung eines Personalausweises ihre Fingerabdrücke abnehmen lassen.*** *Diese Verpflichtung stellt einen Eingriff in die Grundrechte auf Privatsphäre und Datenschutz dar. In der Rechtssache Schwarz*[36] *befand der EuGH zwar, dass der Eingriff im Hinblick auf Reisepässe gemessen an dem Ziel, die Sicherheit aufrechtzuerhalten, verhältnismäßig ist,* ***doch könnte im Kontext von Personalausweisen die Schwelle für das Bestehen des Notwendigkeitstests höher liegen, weil Personalausweise in einigen Mitgliedstaaten , in denen derzeit noch keine Fingerabdrücke abgenommen werden, verpflichtend sind“***[37]***.***

31. Nach einem Vergleich der Optionen kommt die Folgenabschätzung zu dem Schluss, Option ID 1 sei am besten geeignet, die Ziele einer Verbesserung der Sicherheit an den Grenzen und innerhalb der Mitgliedstaaten sowie die Freizügigkeit zu verbessern. Bemerkenswert ist, dass die von der Folgenabschätzung bevorzugte Option ID 1 einen *„****verpflichtenden RFID-Chip einschließlich biometrischer Daten (Gesichtsbild obligatorisch, Fingerabdrücke fakultativ)****“* beinhalten würde.[38] Mit anderen Worten: Die von der Folgenabschätzung zum Vorschlag vorgezogene Option würde die Abnahme von Fingerabdrücken **als Option** betrachten, **nicht als verpflichtende Anforderung**.

32. Überraschenderweise entschied sich die Kommission ungeachtet des Ergebnisses der Folgenabschätzung zum Vorschlag dafür, die obligatorische Aufnahme von Fingerabdrücken in Personalausweise in den Vorschlag aufzunehmen. In der Begründung des Vorschlags wird Folgendes hierzu ausgeführt: ***„Um die Wirksamkeit im Hinblick auf die Sicherheit weiter zu erhöhen, wurde die bevorzugte Option für Personalausweise durch obligatorische Fingerabdrücke ergänzt.*** *Aufgrund der Aufnahme zweier biometrischer Identifikatoren (Gesichtsbild, Fingerabdrücke) wird eine bessere Identifizierung von Personen möglich sein und das Sicherheitsniveau der Personalausweise von EU-Bürgern und der Familienangehörigen aus Drittstaaten ausgestellten Aufenthaltskarten an die Normen angepasst, die für EU-Bürgern ausgestellte Reisepässe bzw. Aufenthaltstitel, die nicht Familienangehörige von EU-Bürgern sind, gelten.“*[39]

33. **Folglich kann nicht davon ausgegangen werden, dass die Folgenabschätzung zum Vorschlag für den Zweck der Einhaltung von Artikel 35 Absatz 10 DSGVO genügt. Der EDSB empfiehlt** daher, **vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.**

4. VERARBEITUNG BIOMETRISCHER DATEN: ERFORDERLICHE GARANTIEN

34. Artikel 3 Absatz 3 des Vorschlags verlangt, dass in der EU ausgestellte Personalausweise **mit einem einen hohen Sicherheitsstandard erfüllenden Speichermedium zu versehen sind, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen Formaten enthält**.

4.1. Zweckbindung

35. Nach dem Grundsatz der Zweckbindung[40] dürfen personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. In diesem Zusammenhang **begrüßt der EDSB, dass Artikel 10 des Vorschlags ausführlich die Zwecke aufführt, für die die personenbezogenen Daten verarbeitet werden sollen.**

36. Gemäß Artikel 10 Absatz 3 des Vorschlags ist ferner die Verarbeitung von in Personalausweisen und Aufenthaltsdokumenten gespeicherten biometrischen Daten zu zwei Zwecken gestattet, nämlich

> *„um*
> *a) den Personalausweis oder das Aufenthaltsdokument auf seine Echtheit zu überprüfen,*
> *b) die Identität des Inhabers anhand direkt verfügbarer abgleichbarer Merkmale zu überprüfen, wenn die Vorlage des Personalausweises oder Aufenthaltsdokuments gesetzlich vorgeschrieben ist“.*

37. Vorab stellt der EDSB fest, dass **die Übereinstimmung zwischen auf dem Chip des Dokuments gespeicherten biometrischen Daten** und **von dem Dokumentinhaber bereitgestellten biometrischen Daten** lediglich **ein Beweis dafür** ist**, dass das Dokument dem Dokumentinhaber gehört.** Die Übereinstimmung an sich ist kein Identitätsnachweis, es sei denn, das Dokument hat sich auch als echt erwiesen.

38. Die Echtheit des Dokuments könnte nachgewiesen werden durch eine **Übereinstimmung zwischen auf dem Chip gespeicherten biometrischen Daten** und einer **Kopie der bei der Erfassung erhobenen biometrischen Daten**. Der Aufbau nationaler Fingerabdruckdatenbanken, der in dem Vorschlag keineswegs ins Auge gefasst wird, sollte allerdings vermieden werden. Somit wäre die einzige Option, die auf dem Chip gespeicherten Daten mit den im Dokument abgedruckten Daten abzugleichen. Die Integrität der auf dem Chip gespeicherten Daten beruht auf dem digitalen Zertifikat, das ebenfalls auf dem Chip gespeichert ist. Digitale Zertifikate haben ein Ablaufdatum und können von der ausstellenden Behörde widerrufen werden. Jedes Überprüfungssystem bräuchte also einen Internetanschluss oder eine alternative Methode, um seine Liste mit widerrufenen Zertifikaten aktualisieren zu können.

39. Es sei eingestanden, dass die Verwendung biometrischer Daten die Wahrscheinlichkeit erfolgreicher Dokumentenfälschungen verringert, weshalb sie als legitime Maßnahme im Kampf gegen Betrug gelten könnte. Allerdings ist die praktische Umsetzung eines Authentifizierungsverfahrens auf der Grundlage der in den Personalausweisen gespeicherten biometrischen Daten ein komplexes und langfristiges Vorhaben. Ein solches Vorhaben wird in dem Vorschlag jedoch nicht erwähnt, und ohne es kann mit der Speicherung biometrischer Daten der beabsichtigte Zweck nicht erreicht werden.

40. Im Aktionsplan vom Dezember 2016 heißt es außerdem: ***„Damit die Behörden die elektronischen Komponenten der e-Reisepässe und e-Aufenthaltstitel abgleichen können, muss ihnen der Mitgliedstaat, der das Dokument ausgestellt hat, die entsprechenden Zertifikate zur Verfügung stellen“***[41], sodass sie Zugriff auf die Fingerabdrücke nehmen können, die in dem Chip gespeichert sind. Der systematische elektronische Abgleich der Chipdaten würde zur Aufdeckung der gebräuchlichsten Formen des Dokumentenbetrugs führen, wie Manipulationen am Foto des Inhabers. **Leider geben nicht alle Mitgliedstaaten ihre Zertifikate weiter.** Der Aktionsplan vom Dezember 2016 enthält eine Maßnahme, der zufolge die Kommission *„im dritten Quartal 2017 für eine regelmäßig aktualisierte Liste der Zertifikate sorgt, die für die elektronische Authentifizierung von Reisedokumenten benötigt werden“.*[42] In der Folgenabschätzung zum Vorschlag heißt es jedoch, dass sich *„die Schlüssel für den Zugriff auf die Daten im Zeitverlauf ändern und nicht immer unverzüglich den einschlägigen nationalen Behörden mitgeteilt werden“.*[43]

41. **Der EDSB weist ferner darauf hin, dass in der Folgenabschätzung zum Vorschlag ausdrücklich anerkannt wird, dass es schwierig ist, die Notwendigkeit und Verhältnismäßigkeit einer im Vorschlag vorgesehenen Einschränkung des Grundrechts auf Schutz personenbezogener Daten zu rechtfertigen**, insbesondere was die Aufnahme von Fingerabdrücken in von den Mitgliedstaaten ihren Staatsangehörigen ausgestellte Personalausweise angeht. Er unterstreicht, dass bezüglich der Aufnahme von Fingerabdrücken der Rechtsprechung des Europäischen Gerichtshofs Rechnung zu tragen ist. In diesem Zusammenhang befand der Gerichtshof in der Rechtssache *Schwarz*[44], dass die Erfassung und die Speicherung von Fingerabdrücken in Reisepässen zwar einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen, die Aufnahme von Fingerabdrücken in Pässe jedoch in Anbetracht des allgemeinen Ziels der Verhinderung der *„illegalen Einreise in das Unionsgebiet“* rechtmäßig ist.[45] In der Folgenabschätzung heißt es hingegen: ***„In Anbetracht der Tatsache, dass Personalausweise sehr viel mehr Zwecken dienen als dem Grenzübertritt, sowie der Tatsache, dass es in den Mitgliedstaaten unterschiedliche Traditionen bei der Verwendung von Personalausweisen gibt, liegt es nicht auf der Hand, dass die gleiche Schlussfolgerung gezogen werden kann.“***[46]

42. Der EDSB unterstreicht außerdem, dass die Verarbeitung personenbezogener Daten auf den legitimen Zweck beschränkt werden muss, für den die personenbezogenen Daten ursprünglich bei der betroffenen Person erhoben wurden. So **sollte** der Vorschlag insbesondere **explizit Garantien mit Blick auf Mitgliedstaaten vorsehen**, die im Rahmen der Umsetzung des Vorschlags **nationale Fingerabdruckdatenbanken aufbauen**. Dem Vorschlag sollte eine Bestimmung hinzugefügt werden, die ausdrücklich

besagt, dass **in diesem Zusammenhang verarbeitete biometrische Daten nach ihrer Speicherung auf dem Chip unverzüglich zu löschen sind** und nicht für andere als die im Vorschlag explizit erwähnten Zwecke weiterverarbeitet werden dürfen.

4.2. Datenminimierung

43. Der EDSB weist nachdrücklich darauf hin, dass **Datenminimierung einer der Kerngrundsätze des EU-Datenschutzrechts ist**. Gemäß diesem Prinzip müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[47]

44. Zwar bieten biometrische Techniken an sich Vorteile gegenüber herkömmlichen Techniken zur Identifizierung von Personen, doch besteht hier ein großes Problem bei der Gewährleistung von Sicherheit und Integrität der biometrischen Daten. Werden beispielsweise biometrische Daten einer Person (z. B. ihr Fingerabdruckbild) gestohlen (z. B. illegal abgerufen und kopiert), ist es nicht möglich, sie zu ersetzen, anders als bei einer gestohlenen oder verlorenen Kreditkarte, einem Personalausweis auf Papier oder einem Passwort. Ein auf biometrischen Daten beruhendes Überprüfungssystem funktioniert nur reibungslos, wenn das überprüfende IT-System garantieren kann, dass die biometrischen Daten zum Zeitpunkt der Erfassung von der legitimen Person stammten.

45. Vor diesem Hintergrund lassen sich Systeme zur Erkennung von Fingerabdrücken in drei Klassen unterteilen:[48]
    - Systeme, die **Bilder** von Fingerabdrücken speichern und vergleichen;
    - Systeme, die **Minuzien** speichern und vergleichen, also eine Untermenge der aus Fingerabdruckbildern extrahierten Merkmale,
    - Systeme, die **Muster** speichern und vergleichen, die aus Fingerabdruckbildern extrahierten wurden.

46. Das ICAO-Dokument[49] verlangt die Speicherung der Bilder der Fingerabdrücke, damit die Interoperabilität der verschiedenen Arten von Technologien zur Fingerabdruckerkennung gewährleistet ist. Es gibt Normen, dank derer Fingerabdruckerkennungssysteme verschiedener Anbieter innerhalb ihrer Klasse interoperabel sind, doch besteht über die Klassengrenzen hinweg keine Interoperabilität zwischen den Systemen.

47. Die Speicherung von Fingerabdruckbildern erlaubt die Berechnung von Teilmengen ihrer Merkmale, während das Gegenteil nicht möglich ist. Sobald das Bild des Fingerabdrucks auf dem Chip des Dokuments gespeichert ist, können Mitgliedstaaten, die sich für irgendeine Klasse von Technologien für die Fingerabdruckerkennung entschieden haben, biometrische Daten verwenden. Wenn jedoch Minuzien auf dem Chip gespeichert sind, kann ein Mitgliedstaat, der eine bildbasierte Technologie zur Fingerabdruckerkennung einsetzt, keine biometrischen Daten verwenden, weil aus Minuzien keine Fingerabdruckbilder gewonnen werden können. Gleichzeitig kann im Fall eines Verstoßes gegen die Sicherheitsvorschriften das auf einem verlorenen oder gestohlenen

Identitätsdokument gespeicherte Fingerabdruckbild von Kriminellen abgerufen und zur Herstellung eines gefälschten Satzes Fingerabdrücke benutzt werden, mit dessen Hilfe die Identität des Ausweisinhabers verschleiert werden kann.

48. **Der EDSB sieht durchaus, dass die Speicherung von Fingerabdruckbildern die Interoperabilität verbessert**, dass sie aber gleichzeitig **die Menge verarbeiteter biometrischer Daten und das Risiko der Identitätserschleichung bei einer Verletzung des Schutzes personenbezogener Daten erhöht. Der EDSB empfiehlt** daher, **die im Dokument auf dem Chip gespeicherten Fingerabdruckdaten auf Minuzien oder Muster zu beschränken, also auf eine Untermenge der aus dem Fingerabdruckbild extrahierten Merkmale.**

49. **Des Weiteren ist der EDSB der Auffassung, dass die im Vorschlag vorgesehene Verarbeitung zweier verschiedener Arten biometrischer Daten (Gesichtsbild obligatorisch, Fingerabdrücke fakultativ) mit Blick auf die angegebenen Ziele nicht gerechtfertigt ist.** Die in Artikel 10 Absatz 3 des Vorschlags genannten Ziele lassen sich sehr wohl nur mit einer Art biometrischer Daten erreichen. Der Vorschlag erläutert nicht, ob zur Feststellung der Identität des Inhabers beide Arten biometrischer Daten abgeglichen werden sollten oder nicht.

50. Doppelabgleiche biometrischer Daten bergen eigene Risiken aufgrund des Anteils falsch negativer Ergebnisse (ein Fehlerergebnis bei einer Überprüfung, die eigentlich positiv hätte enden sollen) der betreffenden Technologie (Fingerabdruck oder Gesichtsbild). Werden Fingerabdrücke und Gesichtsbilder überprüft, könnte es zu Situationen kommen, in denen der Abgleich des Gesichtsbildes erfolgreich ist, der Abgleich des Fingerabdrucks hingegen nicht, und umgekehrt. Auch wenn der Prozentsatz falsch negativer Ergebnisse bei einer bestimmten Technologie zur Erkennung biometrischer Merkmale niedrig ist, könnte doch bei einer Anwendung wie im vorliegenden Fall auf eine sehr große Population eine beträchtliche Anzahl von Personen davon betroffen sein. Schließlich ist es denkbar, dass nicht beide Arten biometrischer Daten verwendet werden; in diesem Fall sollte nur die Art gespeichert werden, die auch verwendet wird.

51. Artikel 3 Absatz 1 des Vorschlags befasst sich mit den im ICAO-Dokument festgelegten Mindestsicherheitsnormen. Einzelheiten der verlangten, empfohlenen und optionalen Sicherheitsvorkehrungen sind in Teil 11 (Sicherheitsmechanismen) des ICAO-Dokuments niedergelegt. Gemäß seinem Abschnitt 3.1 wird für den Chip als einzige Maßnahme die *Passive Authentifizierung* gefordert. In dem ICAO-Dokument heißt es, dass diese Maßnahme eine genaue Kopie oder Substitution eines Personalausweises und auch Skimming[50] nicht verhindert. Gemäß seinem Abschnitt 3.1 wird für das Überprüfungssystem als einzige Maßnahme die *Grundlegende Zugangskontrolle* gefordert. In dem ICAO-Dokument heißt es, dass diese Maßnahme eine genaue Kopie oder Substitution eines Personalausweises nicht verhindert, auch wenn sie auch ein Kopieren des herkömmlichen Dokuments erfordert und komplexer ist. Nach Auffassung des EDSB sollte der Vorschlag, wenn biometrische Daten von 85 % der EU-Bevölkerung auf Personalausweisen gespeichert werden sollen, die Mindestanforderungen zur Vermeidung dieser Risiken erhöhen.

52. Nach diesem Vorschlag könnte jeder Mensch mit Zugriff auf einen Personalausweis und ein Lesegerät, das die in dem ICAO-Dokument festgelegten Normen erfüllt, auf die biometrischen Daten einer Person zugreifen, indem er einfach Zugang zu dem Dokument hat, selbst wenn die biometrischen Daten nicht zur Überprüfung der Identität des Inhabers durch den Dritten verwendet werden.

53. Folglich steht die im Vorschlag vorgesehene obligatorische Aufnahme von Fingerabdrücken in die Personalausweise von EU-Bürgern **nicht im Einklang mit dem Grundsatz der Datenminimierung,** dem zufolge ein für die Verarbeitung Verantwortlicher die Verarbeitung personenbezogener Daten auf das Maß beschränken sollte, das für einen bestimmten Zweck erheblich und notwendig ist.

54. Dessen ungeachtet **weist der EDSB darauf hin, dass Sicherheitsdrucktechniken** wie die Verwendung von Hologrammen oder Wasserzeichen **keine Verarbeitung personenbezogener Daten bedeuten, aber die Möglichkeit geben, Fälschungen zu verhindern und die Echtheit eines Personalausweises oder eines Aufenthaltsdokuments zu überprüfen.**

4.3 Befreiungen von der Abnahme von Fingerabdrücken

55. Artikel 3 Absatz 5 Buchstabe a des Vorschlags besagt, dass Kinder unter zwölf Jahren und Personen, bei denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist, von der Abgabe von Fingerabdrücken befreit sind. **Der EDSB begrüßt die Einführung von Ausnahmen von der Abnahme von Fingerabdrücken auf der Grundlage des Alters der Person oder der physischen Unmöglichkeit, bei der Person Fingerabdrücke abzunehmen.** Diese Befreiungen sind Teil der Ausweichverfahren, die implementiert werden sollten.

56. Gleichzeitig weist der EDSB auf die Notwendigkeit hin, im Einklang mit Artikel 24 der Charta das **Kindeswohl** bei allen Maßnahmen zu bedenken, die Behörden und private Akteure im Hinblick auf Kinder ergreifen. Ganz ähnlich heißt es in Erwägungsgrund 38 der DSGVO: *„Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.“*

57. In diesem Zusammenhang betont der EDSB, dass bei großen Populationen die Altersgrenze für die Abnahme von Fingerabdrücken bei Kindern derzeit bei 14 Jahren festgelegt ist.[51] In Anbetracht der vorstehend geschilderten **breit gefächerten und potenziellen Auswirkungen des Vorschlags** empfiehlt der EDSB, **die Altersgrenze für die Abnahme von Fingerabdrücken bei Kindern im Einklang mit anderen Instrumenten des EU-Rechts auf 14 Jahre festzulegen.**

58. Wir halten außerdem fest, dass der Vorschlag das Ziel verfolgt, **die Abnahme von Fingerabdrücken auch bei Kindern zu verlangen, die im Besitz von Aufenthaltsdokumenten sind**, weil sie aus Drittstaaten kommende Familienangehörige von EU-Bürgern sind. Anknüpfend an seine vorstehenden Bemerkungen **empfiehlt der EDSB, die Altersgrenze im Vorschlag bei 14 Jahren festzusetzen.**

7. SCHLUSSFOLGERUNGEN

Der EDSB stellt fest, dass sich die Kommission eindeutig dafür entschieden hat, den die Freizügigkeit betreffenden Aspekten des Vorschlags Vorrang einzuräumen und das sicherheitsbezogene Ziel als sekundär zu behandeln. Der EDSB merkt an, dass sich dies auf die Prüfung der Notwendigkeit und Verhältnismäßigkeit der Elemente des Vorschlags auswirken könnte.

Der EDSB unterstützt die Europäische Kommission in ihrer Zielsetzung, die für Personalausweise und Aufenthaltsdokumente geltenden Sicherheitsstandards zu verbessern und damit zur Sicherheit der Union insgesamt beizutragen. Gleichzeitig ist der EDSB der Auffassung, dass der Vorschlag die Notwendigkeit der Verarbeitung von zwei Arten biometrischer Daten (Gesichtsbild und Fingerabdrücke) in diesem Zusammenhang nicht ausreichend begründet, zumal der angegebene Zweck auch mit einem weniger in die Privatsphäre eindringenden Vorgehen erreicht werden könnte.

Gemäß dem EU-Rechtsrahmen sowie dem modernisierten Übereinkommen Nr. 108 gelten biometrische Daten als sensible Daten und unterliegen sie besonderem Schutz. Der EDSB unterstreicht, dass sowohl Gesichtsbilder als auch Fingerabdrücke, die nach dem Vorschlag verarbeitet würden, eindeutig in die Kategorie sensibler Daten fallen würden.

Des Weiteren ist der EDSB der Ansicht, dass der Vorschlag weitreichende Auswirkungen auf bis zu 370 Millionen EU-Bürger hätte, da er bei 85 % der EU-Bevölkerung die obligatorische Abnahme von Fingerabdrücken verlangen würde. Dieser breit angelegte Anwendungsbereich sowie die höchst sensiblen Daten, die verarbeitet werden (Gesichtsbilder in Kombination mit Fingerabdrücken), verlangen eine gründliche Prüfung auf der Grundlage einer strengen Prüfung der Notwendigkeit.

Der EDSB räumt darüber hinaus ein, dass in Anbetracht der Unterschiede zwischen Personalausweisen und Reisepässen die Einführung auch für Personalausweise von Sicherheitsmerkmalen, die für Reisepässe als möglicherweise angemessen gelten, nicht automatisch geschehen darf, sondern der Überlegung und einer gründlichen Analyse bedarf.

Der EDSB unterstreicht ferner, dass Artikel 35 Absatz 10 DSGVO auf die hier zu prüfende Verarbeitung Anwendung finden würde. In diesem Zusammenhang weist der EDSB darauf hin, dass die Folgenabschätzung zum Vorschlag anscheinend die von der Kommission gewählte Option nicht unterstützt, nämlich die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise (und Aufenthaltsdokumente). Folglich kann nicht davon ausgegangen werden, dass die Folgenabschätzung zum Vorschlag für den Zweck der Einhaltung von Artikel 35 Absatz 10 DSGVO genügt. Der EDSB empfiehlt daher, vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.

Der Vorschlag sollte ferner explizit Garantien mit Blick auf Mitgliedstaaten vorsehen, die im Rahmen der Umsetzung des Vorschlags nationale Fingerabdruckdatenbanken aufbauen. Dem Vorschlag sollte eine Bestimmung hinzugefügt werden, die ausdrücklich besagt, dass in diesem Zusammenhang verarbeitete biometrische Daten nach ihrer Speicherung auf dem Chip unverzüglich zu löschen sind und nicht für andere als die im Vorschlag explizit erwähnten Zwecke weiterverarbeitet werden dürfen.

Nach dem Verständnis des EDSB könnte die Verwendung biometrischer Daten als legitime Maßnahme zur Betrugsbekämpfung gelten, doch begründet der Vorschlag nicht die Notwendigkeit der Speicherung von zwei Arten biometrischer Daten für seine Zwecke. Eine erwägenswerte Option wäre die Beschränkung der verwendeten biometrischen Daten auf eine Art (z. B. nur Gesichtsbilder).

Der EDSB weist darüber hinaus darauf hin, dass nach seinem Verständnis die Speicherung von Fingerabdrücken die Interoperabilität verbessert, dass sie aber gleichzeitig die Menge verarbeiteter biometrischer Daten und das Risiko der Identitätserschleichung bei einer Verletzung des Schutzes personenbezogener Daten erhöht. Der EDSB empfiehlt daher, die im Dokument auf dem Chip gespeicherten Fingerabdruckdaten auf Minuzien oder Muster zu beschränken, also auf eine Untermenge der aus dem Fingerabdruckbild extrahierten Merkmale.

Schließlich empfiehlt der EDSB in Anbetracht der vorstehend geschilderten breit gefächerten und potenziellen Auswirkungen des Vorschlags, die Altersgrenze für die Abnahme von Fingerabdrücken bei Kindern im Einklang mit anderen Instrumenten des EU-Rechts auf 14 Jahre festzulegen.

Brüssel,

Giovanni BUTTARELLI

Endnoten

[1] 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).
[2] ABl. L 119 vom 4.5.2016, S. 1.
[3] ABl. L 8 vom 12.1.2001, S. 1.
[4] ABl. L 119 vom 4.5.2016, S. 89.
[5] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates vom 17. April 2018 *zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und ihren Familienangehörigen in Ausübung ihres Rechts auf Freizügigkeit ausgestellt werden*, COM(2018) 212 final, 2018/0104 (COD).
[6] Mitteilung der Kommission an das Europäische Parlament und den Rat vom 8. Dezember 2016: *Aktionsplan für ein wirksameres europäisches Vorgehen gegen Reisedokumentenbetrug*, COM(2016) 790 final.
[7] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat *Mehr Sicherheit in einer von Mobilität geprägten Welt: Besserer Informationsaustausch bei der Terrorismusbekämpfung und ein stärkerer Schutz der Außengrenzen*, COM(2016) 602 final.
[8] Siehe Begründung des Vorschlags, S. 2.
[9] Artikel 1 des Vorschlags.
[10] Folgenabschätzung zum Vorschlag, SWD(2018) 110 final, S. 21.
[11] Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über das Recht der Unionsbürger und ihrer Familienangehörigen, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten, zur Änderung der Verordnung (EWG) Nr. 1612/68 und zur Aufhebung der Richtlinien 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG und 93/96/EWG (ABl. L 158 vom 30.4.2004, S. 77).
[12] ICAO-Dokument 9303 (siebte Auflage, 2015), Teil 9, Kapitel 3.1.
[13] Verordnung (EG) Nr. 1030/2002 des Rates vom 13. Juni 2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige (ABl. L 157 vom 15.6.2002, S. 1).
[14] In Artikel 2 des Vertrags über die Europäische Union („*EUV*“) heißt es: *„Die Werte, auf die sich die Union gründet, sind die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören“*. Ferner werden in Artikel 6 Absatz 1 EUV die Rechte, Freiheiten und Grundsätze anerkannt, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind, die den Verträgen rechtlich gleichrangig ist, und Artikel 6 Absatz 3 EUV besagt: *„Die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts.“*
[15] EGMR, Urteil vom 13. Mai 2008, *Rechtssache S. und Marper / Vereinigtes Königreich*, Rn. 68 und 84, ECHR 2008.
[16] Artikel 4 Absatz 14 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).
[17] Siehe Artikel 9 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), und Artikel 10 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates* (ABl. L 119, 4.5.2016, S. 89).
[18] Artikel 6 des modernisierten Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, angenommen am 17./18. Mai 2018
[19] In der Datenschutz-Grundverordnung werden sensible personenbezogene Daten als *„besondere Kategorien personenbezogener Daten“* bezeichnet (siehe Artikel 9 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).

[20] Toolkit des EDSB: *Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken*, 11. April 2017.
[21] Erwägungsgrund 6 des Vorschlags.
[22] Anhang 5 der Folgenabschätzung zum Vorschlag, S. 104f. Siehe ferner Abschnitt 2.3 des CSES-Berichts, der weitere Informationen zu den Arten von Personalausweisen und Aufenthaltsdokumenten enthält, die von nationalen Behörden ausgestellt werden.
[23] Folgenabschätzung zum Vorschlag, S. 12.
[24] Folgenabschätzung zum Vorschlag, S. 9, und Anhang 8 der Folgenabschätzung zum Vorschlag, S. 123.
[25] Anhang 8 der Folgenabschätzung zum Vorschlag, S. 123.
[26] Von dieser neuen Verpflichtung wären 16 Mitgliedstaaten betroffen: Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Luxemburg, Malta, Niederlande, Österreich, Polen, Rumänien, Schweden, Slowakei, Slowenien und die Tschechische Republik. Siehe: Anhang 8 der Folgenabschätzung zum Vorschlag, S. 123.
[27] http://www.statewatch.org/analyses/no-331-biometrics-for-identity-cards.pdf
[28] S. 7 des Vorschlags.
[29] Folgenabschätzung zum Vorschlag, S. 4; auch wenn es aus dem Bericht nicht klar hervorgeht, kann angenommen werden, dass es zwischen diesen beiden Zahlen eine erhebliche Überschneidung gibt.
[30] Folgenabschätzung zum Vorschlag, S. 12.
[31] Anhang 6 der Folgenabschätzung zum Vorschlag, S. 109, FRONTEX. 2016. Jährliche Risikoanalyse. S. 14.
[32] FRONTEX Risikoanalyse, S. 22.
[33] Anhang 6 der Folgenabschätzung zum Vorschlag, S. 109.
[34] In diesem Zusammenhang sei unterstrichen, dass selbst die Kommission in der erwähnten Folgenabschätzung einräumt, dass *„die Zahl der entdeckten Dokumente nicht besonders hoch zu sein scheint“*. Siehe: Folgenabschätzung zum Vorschlag, S. 12.
[35] 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).
[36] EuGH, Urteil vom 17. Oktober 2013, Rechtssache C-291/12, *Schwarz / Stadt Bochum.*
[37] Folgenabschätzung zum Vorschlag, S. 51.
[38] Folgenabschätzung zum Vorschlag, S. 27.
[39] Begründung des Vorschlags, S. 6.
[40] Verankert in Artikel 5 Absatz 1 Buchstabe b DSGVO.
[41] Aktionsplan vom Dezember 2016, S. 12.
[42] Aktionsplan vom Dezember 2016, S. 13.
[43] Folgenabschätzung zum Vorschlag, S. 14.
[44] EuGH, Urteil vom 17. Oktober 2013, Rechtssache C-291/12, *Schwarz / Stadt Bochum.*
[45] EuGH, Urteil vom 17. Oktober 2013, Rechtssache C-291/12, *Schwarz / Stadt Bochum,* Rn. 37.
[46] Folgenabschätzung zum Vorschlag, S. 60.
[47] Artikel 5 Absatz 1 Buchstabe c DSGVO.
[48] Abgeschnittene und verkleinerte Fingermuster, gefolgt von der zellulären Darstellung des Fingermusterbilds zur Generierung der Daten für den Fingermusteraustausch.
[49] Teil 9, Kapitel 4.2.
[50] Als Skimming bezeichnet man eine Art des Angriffs, bei dem ein Gerät in der Nähe des Personalausweises eingesetzt wird, das die Daten aus dem Dokument bei dessen Verwendung abgreift.
[51] Siehe beispielsweise: Artikel 14 der Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 *über die Einrichtung von „Eurodac“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts* (ABl. L 180 vom 29.6.2013, S. 1).