

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/21789 –**

Pflicht zur Speicherung von Fingerabdrücken in neuen Personalausweisen

Vorbemerkung der Fragesteller

Bis zu 370 Millionen Bürgerinnen und Bürger der Europäischen Union müssen in den nächsten Jahren zwangsweise ihre Fingerabdrücke in Personalausweisen speichern lassen.

Gemäß Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates werden Personalausweise künftig „mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält.“ Die Bundesregierung beabsichtigt die Umsetzung dieser Verordnung mit einem Gesetzentwurf zur „Stärkung der Sicherheit im Pass- Ausweis- und ausländerrechtlichen Dokumentenwesen“ (<https://portal2.dbtg.de/SharedDocs/gesetzgebungsv erfahren/DE/,DanaInfo=www.bmi.bund.de,SSL+gesetz-zur-staerkung-der-sicherheit-im-pass-und-ausweiswesen.html#>, hier: § 5 Absatz 9 des Personalausweisgesetzes, demzufolge die Abdrücke der Zeigefinger gespeichert werden müssen). Diese Pflicht tritt dem Entwurf zufolge zum 2. August 2021 in Kraft. Alte Ausweise behalten ihre Gültigkeit.

Bisher werden in Personalausweisen, anders als bei Reisepässen, Fingerabdrücke nur auf Wunsch der Antragstellerinnen und Antragsteller, also freiwillig, gespeichert.

Die EU-Verordnung begründet die zwangsweise Einführung der Fingerabdruckspeicherung damit, es gebe „immer mehr gefälschte Personalausweise“, zudem sei die Erhöhung der Fälschungssicherheit ein Beitrag im Kampf gegen Kriminalität und Terrorismus.

Die Neuregelung stellt nach vielfacher Auffassung einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar – und zwar, wie der Europäische Datenschutzbeauftragte erklärt, von bis zu 370 Millionen EU-Bürgerinnen und Bürgern (https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de.pdf).

Die Abgeordnete Cornelia Ernst (GUE/NGL-Fraktion) warnte in der Aussprache des Europäischen Parlaments, Fingerabdrücke könnten „gehackt und nachgebildet werden, wie der Chaos-Computer-Club schon 2008 nachgewiesen hat“ (https://www.europarl.europa.eu/doceo/document/CRE-8-2019-04-03-ITM-016_DE.html). Aus Sicht der Fragestellerinnen und Fragesteller muss

auch der Umstand beachtet werden, dass Fingerabdrücke heutzutage häufig gleichsam wie Schlüssel oder Passwörter verwendet werden (für Telefone, Computer, Fahrzeuge, selbst Gebäude), und somit die Pflicht zur Abgabe von Fingerabdrücken mit der Pflicht zur Herausgabe von Schlüsseln bzw. Passwörtern verglichen werden kann. Anders als bei gestohlenen Passwörtern ist ein Austausch von Fingerabdrücken jedoch nicht möglich. Somit ist aus Sicht der Fragestellerinnen und Fragesteller fraglich, ob die Neuregelung nicht vielmehr ein Einfallstor für neue kriminelle Praktiken darstellt. Die Sicherheit des Speichermediums über zehn Jahre (die maximale Gültigkeitsdauer des Ausweises) gewährleisten zu wollen, ist aus ihrer Sicht nicht möglich.

Auch der Europäische Datenschutzbeauftragte (EDSB) weist auf die Gefahr hin, dass „das auf einem verlorenen oder gestohlenen Identitätsdokument gespeicherte Fingerabdruckbild von Kriminellen abgerufen und zur Herstellung eines gefälschten Satzes Fingerabdrücke benutzt werden (könne), mit dessen Hilfe die Identität des Ausweisinhabers verschleiert werden kann“ (https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de.pdf).

Er verweist zudem auf die Unterschiede zwischen Personalausweisen und Reisepässen. Reisepässe werden regelmäßig für Reisen außerhalb der EU benötigt, während Personalausweise ganz überwiegend bei Binnenreisen (sowie privatwirtschaftlichen Vorgängen, Behördenbesuchen usw.) eingesetzt werden. Vor diesem Hintergrund fragt der EDSB, „welchen Mehrwert die Aufnahme biometrischer Daten in die Personalausweise bringt, da diese bei Reisen zwischen den EU-Mitgliedstaaten nicht routinemäßig kontrolliert werden.“

Dazu kommt, dass einige Mitgliedstaaten keine Personalausweise ausgeben bzw. keine Personalausweispflicht kennen. Nur in 15 Mitgliedstaaten seien Personalausweise vorgeschrieben. In Anbetracht dieser Unterschiede könnten Sicherheitsmerkmale, „die für Reisepässe möglicherweise als angemessen gelten, nicht automatisch“ auch auf Personalausweise ausgedehnt werden.

Bemerkenswert aus Sicht der Fragestellerinnen und Fragesteller ist der Umstand, dass die Folgenabschätzung der Kommission zur Frage der Fingerabdrücke nicht ihre obligatorische, sondern lediglich ihre fakultative Speicherung empfohlen hat: „Given the key objective to improve the security of ID cards as travel documents, a mandatory RFID chip including biometrics (facial image mandatory, fingerprints optional) is proposed“ (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0110&from=EN>). Dennoch hat sich die Kommission dafür entschieden, die obligatorische Aufnahme von Fingerabdrücken vorzusehen. Die hierzu abgegebene Begründung, die Sicherheit weiter zu erhöhen, widerspricht allerdings den Feststellungen der Folgenabschätzung.

Außerdem hielt die Folgenabschätzung fest, angesichts der unterschiedlichen Funktionen und Anwendungsbereiche von Reisepässen und Personalausweisen sei es nicht selbstverständlich, dass hinsichtlich der Aufnahme von Fingerabdrücken die gleiche Schlussfolgerung gezogen werden könne.

Der EDSB hält die zwangsweise Speicherung von Fingerabdrücken für „nicht ausreichend begründet“. Der angegebene Zweck könne auch mit einem weniger in die Privatsphäre eindringenden Verfahren erreicht werden. Zudem genüge die Folgenabschätzung nicht den Vorgaben von Artikel 35 Absatz 10 der Datenschutz-Grundverordnung (DSGVO).

Zur Frage, wie groß das Problem gefälschter Personalausweise tatsächlich ist, verweist der EDSB auf Angaben von Frontex, denen zufolge in den Jahren 2013 bis 2017 lediglich 38 870 gefälschte Personalausweise ermittelt wurden. Seit Jahren gehe außerdem die Zahl der Personen, die mit gefälschten Personalausweisen bzw. Aufenthaltsdokumenten einreisen, zurück. Diese niedrigen Zahlen rechtfertigen nach Auffassung des EDSB nicht die obligatorische Fingerabdruckspeicherung. Der Vorschlag der EU entspreche auch nicht dem Grundsatz der Datenminimierung.

Nach Kenntnis der Fragestellerinnen und Fragesteller datiert die letzte Regelung, die deutsche Staatsbürgerinnen und Staatsbürger zur Abgabe von Finger-

abdrücken in Inlandsausweisen zwang, vom 22. Juli 1938, als die Nazibehörden Fingerabdrücke auf sog. Kennkarten verlangten.

Aus Sorge um den Schutz ihrer Daten und ihr Grundrecht auf informationelle Selbstbestimmung rät der Verein Digitalcourage dazu, noch vor dem Stichtag am 2. August 2021 einen neuen Personalausweis zu beantragen (<https://digitalcourage.de/blog/2020/keine-fingerabdruecke-personalausweis-persoohnefinge#epabstimmung>).

1. Wie positioniert sich die Bundesregierung zu der Auffassung des Europäischen Datenschutzbeauftragten, die Folgenabschätzung genüge nicht den Anforderungen der DSGVO (bitte begründen), und welche Konsequenzen zieht sie daraus?

Wann wird nach ihrer Kenntnis eine den Anforderungen des Artikel 35 DSGVO genügende Datenschutzfolgenabschätzung durchgeführt?

Das mit dem im April 2018 von der Europäischen Kommission (EU Kommission) vorgelegten 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 (COM(2018) 212 final) verfolgte Ziel, die Sicherheitsmerkmale von vorgenannten Dokumenten zu stärken und damit insgesamt zur Erhöhung der Sicherheit in der Europäischen Union (EU) beizutragen, wurde vom Europäischen Datenschutzbeauftragten in seiner Stellungnahme vom 10. August 2018 (Ratsdokument 11629/18 vom 17. August 2018) nach Auffassung der Bundesregierung grundsätzlich begrüßt.

Wie dieses Ziel konkret erreicht werden sollte, war Gegenstand der Beratungen zum Verordnungsentwurf. Sowohl der Europäische Datenschutzbeauftragte als auch der Rat als Organ, in dem die Mitgliedstaaten vertreten sind, und das Europäische Parlament hatten im Rahmen des Rechtsetzungsverfahrens zum Verordnungsentwurf diversen Diskussions- und Anmerkungsbedarf geltend gemacht – auch zu datenschutzrechtlichen Fragestellungen. Die Verhandlungen führten im Ergebnis zu der geltenden Fassung der Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben. Nicht zuletzt auch detailliertere datenschutzrechtliche Ausgleichsmaßnahmen wie beispielsweise die Pflicht zur Löschung der biometrischen Daten am Tag der Abholung des Dokuments und spätestens nach 90 Tagen wurden in den Verordnungstext aufgenommen (vergleiche Artikel 10 Absatz 3 der Verordnung (EU) 2019/1157).

In Deutschland bleibt die bisherige Regelung bestehen, wonach die Fingerabdrücke in der Behörde spätestens nach Aushändigung des Dokuments gelöscht werden (vergleiche § 26 Absatz 2 des Personalausweisgesetzes). Der Ausweis hersteller löscht die personenbezogenen Daten nach Abschluss der Produktion (vergleiche § 26 Absatz 3 Satz 2 des Personalausweisgesetzes).

Im Übrigen bleiben nach Artikel 11 Absatz 1 der Verordnung (EU) 2019/1157 die Vorgaben der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) zu beachten. Darüber hinaus enthält Artikel 11 der Verordnung (EU) 2019/1157 besondere Vorgaben zum Schutz der betreffenden biometrischen Daten, einschließlich einer engen Zweckbindung zur Verwendung dieser Daten in Absatz 6.

2. Gibt es bereits konkrete Überlegungen, auf welchen Rechtsgrundlagen die Übermittlung personenbezogener Daten durch Fotografen im Sinne von Artikel 13, Nummer 1 erfolgen soll?

Lichtbilder können von Fotografinnen und Fotografen zur Ausweisbehörde bereits aktuell auf gesichertem elektronischen Weg zur Behörde übermittelt werden (§ 7 Absatz 1 Nummer 1 der Personalausweisverordnung). Dazu hat das Bundesamt für Sicherheit in der Informationstechnik Verfahren und Sicherheitsvorgaben in Form der Technischen Richtlinie 03146 (Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente / TR E-Bild hD) veröffentlicht. Die Übermittlung erfolgt dabei über De-Mail. Neben dem eigentlichen Lichtbild werden dabei nur die Initialen des Antragstellers (zwei Stellen), der Geburtstag des Antragstellers (zwei Stellen) und der Geburtsmonat des Antragstellers (zwei Stellen) als Teil des Dateinamens übermittelt. Weitere personenbezogene Daten des Antragstellers werden nicht übermittelt.

Die Bundesregierung prüft gemäß § 12 Absatz 2 des Personalausweisgesetzes regelmäßig, ob und inwieweit neue technische Systeme, Verfahren und Sicherheitsvorgaben eingeführt werden sollen, damit die eingesetzten Verfahren dem gegenwärtigen Stand der Technik entsprechen. Zur etwaigen Umsetzung des in der Fragestellung erwähnten Artikel 13 Nummer 1 des Entwurfs eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (Bundratsdrucksache 435/20) werden konkrete Überlegungen erst nach Beschlussfassung des Gesetzgebers erfolgen.

3. Welche Regelungen gelten gegenwärtig hinsichtlich
 - a) der Verfahren und technischen Anforderungen zur Aufnahme, elektronischen Erfassung, Echtheitsbewertung und Qualitätssicherung der Fingerabdrücke, die Reihenfolge der zu speichernden Fingerabdrücke bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdruckes oder Verletzungen der Fingerkuppe sowie

Für die Erfassung und Qualitätssicherung der Antragsdaten ist die Technische Richtlinie TR-03104 zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für hoheitliche Dokumente (TR PDÜ hD) des Bundesamtes für Sicherheit in der Informationstechnik maßgeblich.

- b) der Form und den Einzelheiten für das Verfahren der Übermittlung sämtlicher Ausweis-antragsdaten von den Personalausweisbehörden an Ausweishersteller?

Die Kommunikation zwischen den Pass-/ Personalausweisbehörden und dem Hersteller Bundesdruckerei GmbH richtet sich nach der Technischen Richtlinie TR-03123 XML-Datenaustauschformat für hoheitliche Dokumente (TR-XhD).

4. Wie hat sich die Bundesregierung im Prozess der Entstehung der genannten Verordnung positioniert, insbesondere zur Frage, ob
 - a) überhaupt eine rechtlich verbindliche Regelung nötig ist, und
 - b) ob die optionale oder obligatorische Speicherung von Fingerabdrücken nötig sei(bitte jeweils begründen)?

Die Fragen 4a und 4b werden aufgrund des Sachzusammenhanges gemeinsam beantwortet.

Die Bundesregierung hat die in dem Verordnungsentwurf vorgesehene verpflichtende Abgabe von Fingerabdrücken intensiv geprüft und hierzu im Rahmen der Verhandlungen bis zuletzt einen Prüfvorbehalt eingelegt. Im Ergebnis hat die Bundesregierung den im Rahmen der Verhandlungen erzielten Kompromiss akzeptiert, einerseits an der von der Kommission vorgeschlagenen verpflichtenden Speicherung von Fingerabdrücken festzuhalten, andererseits aber ausdrücklich vorzuschreiben, dass die biometrischen Daten auf Grundlage der Verordnung grundsätzlich nur dezentral in dem jeweiligen Identitätsdokument gespeichert werden dürfen, wohingegen die Speicherung außerhalb des Dokuments nach der Verordnung auf die Phase der Produktion des Identitätsdokuments bezogen und dementsprechend mit einer Höchstfrist und einer Löschungsregelung versehen wurde.

Neben den bereits in der Antwort zu Frage 1 erläuterten datenschutzrechtlichen Sicherungen enthält die Verordnung (EU) 2019/1157 in der finalen Kompromissfassung überdies in Erwägungsgrund 21 die ausdrückliche Klarstellung, dass sie keine rechtliche Grundlage für eine zentrale Speicherung biometrischer Daten auf nationaler Ebene oder auf der Ebene der Union darstellt. Überdies wird in Erwägungsgrund 19 klargestellt, dass die Mitgliedstaaten als allgemeine Praxis zur Überprüfung der Identität des Inhabers in der Regel vorrangig das Gesichtsbild überprüfen und nur darüber hinaus, falls zur zweifelsfreien Bestätigung der Identität des Inhabers notwendig, auch die Fingerabdrücke überprüfen sollten.

5. Welche Konsequenzen zieht die Bundesregierung aus der Entscheidung der Kommission, sich entgegen der Folgenabschätzung für eine obligatorische Speicherung der Fingerabdrücke auszusprechen, und wie hat sie sich diesbezüglich selbst verhalten (bitte begründen)?

Die Verordnung (EU) 2019/1157 wurde vom EU-Gesetzgeber, bestehend aus dem Rat als Organ, in dem die Mitgliedstaaten vertreten sind, und dem Europäischen Parlament verabschiedet. Die Detailinformationen in der Folgenabschätzung der Kommission wurden neben anderen Informationen in der Beratung des Verordnungsentwurfs berücksichtigt.

Im Übrigen wird auf die Antworten der Bundesregierung zu den Fragen 1, 4a und 4b verwiesen.

6. Inwiefern ist aus Sicht der Bundesregierung die Pflicht zur Abgabe von Fingerabdrücken in Personalausweisen ein verhältnismäßiger Eingriff in die Grundrechte der betroffenen Unionsbürgerinnen und Unionsbürger?

Die Speicherung des Fingerabdruckes in Identitätsdokumenten dient dem Zweck, bei Zweifeln an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person die Identität dennoch unmittelbar feststellen zu können. Die derzeit in Zweifelsfällen noch teilweise notwendigen und zeitaufwändigen Nachfragen bei anderen Behörden können damit künftig entfallen.

Zudem wird der betroffenen Person eine direkte Wiederinanspruchnahme ihrer vollen Freizügigkeit ermöglicht. Der Fingerabdruck soll bei alldem stets nur subsidiär genutzt werden. In dieser Hinsicht wird auch auf die Antwort zu Frage 4 verwiesen.

Der staatliche Schutz der Identität der Bürgerinnen und Bürger umfasst auch, den Identitätsmissbrauch mit staatlichen Ausweisdokumenten wirksam einzudämmen. Ein milderer Mittel, das Unionsbürgerinnen und Unionsbürger glei-

chermaßen schnell und sicher identifiziert und ihnen zugleich die zügige Wiederinanspruchnahme ihrer vollen Freizügigkeit ermöglicht, steht im Ausweiswesen nicht zur Verfügung. Für Reisepässe hat der europäische Gesetzgeber bereits im Jahr 2004 eine vergleichbare Regelung getroffen. Die Verordnung (EU) 2019/1157 weitet dies nunmehr auch auf Personalausweise aus, welche innerhalb der EU und zu ausgewählten Nachbarstaaten ebenfalls als Reisedokument dienen.

7. Inwiefern hat sich die Bundesregierung mit dem Missbrauchspotential, das nach Auffassung der Fragestellerinnen und Fragesteller der Pflicht zur Speicherung der Fingerabdrücke innewohnt, auseinandergesetzt, auch mit der Gefahr, dass Kriminelle u. U. durch die unbefugte Nutzung der Fingerabdrücke Zugang zu gesicherten Gegenständen oder Gebäuden haben (sofern die Eigentümer ihre Fingerabdruck als Schlüssel verwenden)?

Der im Chip des Personalausweises (oder Reisepasses) gespeicherte Fingerabdruck ist nur mit einem hoheitlichen Berechtigungszertifikat auslesbar, welche nur an explizit berechnigte Stellen ausgegeben werden. Die Fingerabdruckdaten sind durch kryptographische Maßnahmen (Extended Access Control) entsprechend den Vorgaben in der Technischen Richtlinie TR-03110 „Advanced Security Mechanisms for Machine Readable Travel Documents“ gegen unberechtigten Zugriff geschützt. Die Einhaltung dieser Vorgaben ist aufgrund der EU Vorgaben für europäische Reisepässe und elektronische Aufenthaltstitel (sowie ab 2. August 2021) für den Personalausweis) verpflichtend. Dies sind die gleichen Sicherungsmechanismen wie beim schon lange etablierten elektronischen Reisepass und elektronischen Aufenthaltstitel. Eine Speicherung von Fingerabdrücken in Datenbanken findet nicht statt. In dieser Hinsicht wird auch auf die Antwort zu Frage 4 verwiesen.

8. Wie beurteilt die Bundesregierung die auch vom Europäischen Datenschutzbeauftragten gesehene Gefahr, dass Kriminelle die Fingerabdrücke auslesen, nutzen oder manipulieren können, und für wie sicher hält sie die hiergegen eingebauten Sicherungsmaßnahmen?

Die Sicherheit der Speichermedien wird nach international anerkannten Verfahren (Common Criteria) als resistent gegen Angriffe mit „hohem Angriffspotential“ zertifiziert.

- a) Wie will sie bzw. ihrer Kenntnis nach die EU sicherstellen, dass Speichermedien und darin gespeicherte Fingerabdrücke, die zum Zeitpunkt der Ausstellung eines Ausweises noch als sicher eingeschätzt werden, bis zum Ablauf der Gültigkeitsdauer (bis zu zehn Jahre lang) weiterhin sicher sind?

Die fortwährende Angriffsresistenz wird durch das Bundesamt für Sicherheit in der Informationstechnik durch die fortlaufende Beobachtung der genutzten Chiptypen über den Lebenszyklus der Chips geprüft. Die diesbezüglichen Erkenntnisse werden anlassbezogen auf EU-Ebene und in internationalen Arbeitsgruppen (u. a. der ICAO) ausgetauscht, um die Aktualität der Common Criteria immer wieder neu zu bewerten und eine etwaige Erforderlichkeit der Überarbeitung zu prüfen.

Um größtmögliche Fälschungssicherheit zu erreichen, werden die physikalischen und elektronischen Sicherheitsmerkmale kontinuierlich geprüft und nach Möglichkeit verbessert. Fälle eines missbräuchlichen Auslesens der Fingerab-

drücke (Reisepass, Aufenthaltstitel und Personalausweise mit optional gespeicherten Fingerabdrücken) sind nicht bekannt.

- b) Inwiefern beabsichtigt die Bundesregierung, den Inhabern von Personalausweisen im Fall, dass das Speichermedium sich als nicht ausreichend sicher vor unbefugtem Zugriff erweist, einen kostenlosen Umtausch des Ausweises anzubieten?

Bereits aktuell wird die elektronische und physikalische Funktionalität des Personalausweises während der zehnjährigen Gültigkeitsdauer bei regelgerechtem Gebrauch durch die mit dem Hersteller Bundesdruckerei GmbH vertraglich vereinbarte Möglichkeit gewährleistet, bei begründeten Reklamationen von der Personalausweisbehörde gebührenfrei einen neuen Personalausweis ausgestellt zu erhalten.

9. Welche Behörden oder sonstige Stellen sollen Zugriff auf die Fingerabdruckdaten im Personalausweis erhalten (bitte nach Möglichkeit nach deutschen sowie Behörden im Ausland unterscheiden)?

Nur inländische Behörden, die zur Identitätsfeststellung berechtigt sind, dürfen die im Chip gespeicherten Daten nur zum Zwecke der Überprüfung der Echtheit des Ausweises oder der Identität der Ausweisinhaberin/des Ausweisinhabers nach Maßgabe des Personalausweisgesetzes auslesen und verwenden (vergleiche § 2 Absatz 2, § 17 des Personalausweisgesetzes). Dazu gehören neben den Personalausweis-, Pass- und Meldebehörden die Polizeivollzugsbehörden, die Zollverwaltung und die Steuerfahndungsstellen der Länder.

Die Berechtigungszertifikate zum Auslesen der Fingerabdrücke werden nur zwischen den EU-Mitgliedstaaten – einschließlich der Staaten, welche bei der Umsetzung des Schengen-Besitzstands assoziiert sind – ausgetauscht. Bisher haben die folgenden Staaten bereits die Berechtigungszertifikate mit Deutschland ausgetauscht: Belgien, Frankreich, Italien, Litauen, Luxemburg, Polen, Portugal, Rumänien, Schweden, Schweiz, Tschechische Republik. Mit Staaten außerhalb der EU wird das Berechtigungszertifikat zum Auslesen der Fingerabdrücke nur mit Staaten mit Schengen-Assoziation geteilt.

Die Liste der zum Zugriff auf biometrische Daten berechtigten Behörden in den Mitgliedstaaten wird durch die EU-Kommission gemäß Artikel 11 Absatz 7 Satz 2 der Verordnung (EU) 2019/1157 veröffentlicht.

10. Wie genau wird sichergestellt, dass die zugriffsberechtigten, auslesenden Behörden oder sonstigen Stellen keine Datenbanken mit ausgelesenen Fingerabdrücken aufbauen, und kann dies nach Auffassung der Bundesregierung in Hinblick auf autoritäre Staaten sowie die Vielzahl privatrechtlicher Anlässe, in denen Personalausweise verwendet werden, überhaupt sichergestellt werden (bitte ggf. ausführen)?

Die EU Mitgliedstaaten erheben und verwenden personenbezogene Daten, zu denen auch biometrische Identifikatoren wie das Lichtbild und Fingerabdrücke gehören, gemäß den Vorgaben der Datenschutz-Grundverordnung. Artikel 11 Absatz 6 der Verordnung 2019/1157 beschränkt die Verwendung der auf dem elektronischen Speichermedium enthaltenen biometrischen Daten auf Prüfung der Echtheit des Dokuments und Zwecke der Identitätskontrolle; der Aufbau von nationalen Datenbanken, in denen aus Reisedokumenten ausgelesene Fingerabdrücke von Unionsbürgerinnen und Unionsbürgern gesammelt werden, ist davon nicht umfasst.

Die Erhebung und Verarbeitung personenbezogener Daten aus Anlass von grenzpolizeilichen Kontrollen erfolgt nach einheitlichen europäischen und nationalen Vorgaben, vor allem der Verordnung (EU) 2016/399 (Schengener Grenzkodex) und dem Bundespolizeigesetz. Sämtliche in Deutschland (technisch) angebotenen Stellen wurden auf die Verpflichtung zum rechtskonformen Gebrauch der Fingerabdruckdaten gemäß § 16a des Passgesetzes und § 17 des Personalausweisgesetzes hingewiesen.

Andere Staaten außerhalb der EU (oder Staaten mit Schengen-Assoziierung), wozu auch autoritäre Staaten gehören können, sowie private Stellen erhalten keinen Zugriff auf die im Chip gespeicherten Fingerabdrücke (vergleiche Antwort zu Frage 9).

11. Inwiefern soll bei der (Zwischen-)Speicherung, Übermittlung oder Verarbeitung der Fingerabdrücke mit externen Dienstleistern zusammengearbeitet werden (bitte ggf. angeben, um wen es sich handeln soll, in welcher Form die Zusammenarbeit erfolgt, inwiefern die Dienstleister unmittelbar Zugriff auf die Fingerabdruckdateien haben, welche Kriterien der Auswahl der Dienstleister zugrunde liegen und inwiefern die Datensicherheit gewährleistet werden soll)?

Die Erhebung und Verarbeitung von Fingerabdrücken zur Speicherung im Personalausweis erfolgt ausschließlich durch Behördenpersonal und nicht durch externe Dienstleister.

12. Wie viele Fälle sind der Bundesregierung bekannt, in denen die Echtheitsprüfung von Personalausweisen an fehlenden biometrischen Daten, insbesondere Fingerabdrücken, gescheitert ist (bitte auf den Zeitraum der letzten drei Jahre beziehen)?

Die Echtheitsüberprüfung von Personalausweisen erfolgt anhand hochwertiger und in der Regel auch maschinell prüfbarer Sicherheitsmerkmale, die im Weißlicht (Tageslicht), in Infrarot- und in ultraviolettem Licht in diversen Ausprägungen dargestellt werden. Die wesentlichsten Sicherheitsmerkmale des Personalausweises (als auch des Reisepasses) hat das Bundesministerium des Innern, für Bau und Heimat in einem Flyer veröffentlicht. Biometrische Identifikatoren werden zur Echtheitsüberprüfung der Dokumente nicht benötigt.

13. Welche Zahlen liegen der Bundesregierung zur Häufigkeit gefälschter Ausweisdokumente sowie zur Erkennungsquote gefälschter Ausweisdokumente im Zeitraum der vergangenen zehn Jahre vor (bitte nach Deutschland und EU differenzieren)?

Fälschungen nationaler Identitätskarten und Missbrauch echter Dokumente durch unbefugte Personen im Zeitraum von 2010 bis 2019 werden in Deutschland am häufigsten mit Bezug zu nationalen Identitätskarten der Länder Italien, Rumänien, Griechenland, Bulgarien und Frankreich festgestellt (Anzahlen: Italien: 3395, Rumänien: 2925, Griechenland: 2184, Bulgarien: 1343, Frankreich: 1022). Die Auswertungen insgesamt zeigen, dass die Zahl der in Deutschland festgestellten gefälschten Identitätskarten pro Jahr in den letzten Jahren kontinuierlich gestiegen ist.

Die mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Behörden konnten festgestellte gefälschte Grenzübertrittsdokumente – einschließlich des Missbrauchs echter Dokumente – wie folgt registrieren

(Quelle: Polizeiliche Eingangsstatistik der Bundespolizei). Daten zu einer sog. „Erkennungsquote“ liegen hier nicht vor.

	ge- und verfälschte Grenzübertrittsdokumente (einschl. Reisepässe, ID-Karten, Aufenthaltstitel, Visa)		ge- und verfälschte Reisepässe		ge- und verfälschte ID-Karten	
	Europäische Dokumente	davon deutsche Dokumente	Europäische Dokumente	davon deutsche Dokumente	Europäische Dokumente	davon deutsche Dokumente
2010	2.442	475	992	35	847	83
2011	2.732	317	980	33	1.148	83
2012	2.930	368	938	81	1.256	58
2013	2.964	317	844	89	1.170	48
2014	3.134	207	532	33	1.190	47
2015	3.776	225	578	36	1.221	38
2016	2.904	323	552	36	1.170	58
2017	2.961	423	553	82	1.374	45
2018	2.946	409	603	63	1.786	59
2019	5.414	524	900	64	3.919	71

Quelle: PES

Indem die Ausweisdokumente aufgrund verbesserter Sicherheitsmerkmale zunehmend schwerer zu (ver-)fälschen sind, wird vermehrt der Missbrauch echter Dokumente durch ähnlich aussehende Personen („look-alike fraud“) festgestellt. Die Bundespolizei verzeichnet in ihrem Zuständigkeitsbereich eine Steigerung der Anzahl von Strafanzeigen wegen Ausweismissbrauchs (Missbrauch echter Identitätsdokumente durch ähnlich aussehende Personen) wie folgt:

Jahr	2014	2015	2016	2017	2018	01-11/ 2019
Gesamt	434	455	598	708	727	950

Die vorstehenden Zahlen betreffen die Feststellungen im gesamten Zuständigkeitsbereich der Bundespolizei und damit auch die sog. „Inlandsfeststellungen“.

Gerade in solchen Fällen des Missbrauchs echter Dokumente durch ähnlich aussehende Personen steht mit dem Fingerabdruck eine weitere, von der augenscheinlichen (und ggfs. auch biometrischen) Ähnlichkeit der Gesichter unabhängige Komponente zur Identifizierung zur Verfügung.

14. In welchen konkreten Fällen von als terroristisch eingestuften Straftaten hat das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Ausweisdokumenten nach Kenntnis der Bundesregierung dazu geführt, dass die Taten nicht verhindert bzw. nicht aufgeklärt und die Täter nicht ermittelt werden konnten?

Es sind keine konkreten Fälle von als terroristisch eingestuft Straftaten bekannt, in denen das Nichtvorhandensein gespeicherter Fingerabdrücke auf Personalausweisen sowie anderen Ausweisdokumenten mutmaßlich dazu geführt hätten, dass die Taten nicht verhindert bzw. nicht aufgeklärt und die Täter ermittelt werden konnten.

15. Welche Angaben (Statistiken, Studien, Einschätzungen) über die Rolle von digital gespeicherten Fingerabdrücken auf Ausweisdokumenten zur Aufklärung von Kriminalität liegen der Bundesregierung vor, und was sind deren wesentliche Inhalte?

Die in Personalausweisen und Reisepässen gespeicherten Fingerabdrücke dienen der schnellen Identitätsfeststellung, wenn Zweifel an der Übereinstimmung der sich ausweisenden mit der auf dem Lichtbild des Dokuments abgebildeten Person bleiben. Auf die Antwort zu Frage 6 wird verwiesen.

Für ein besseres Erkennen von Straftaten des Ausweismissbrauchs (Missbrauch der Identitäten anderer Personen) spielen in Ausweisdokumente gespeicherte Fingerabdrücke eine wesentliche Rolle. Das Erkennen eines Ausweismissbrauchs durch eine Person, die dem Lichtbild im Ausweis ähnlich sieht, erfordert derzeit teilweise zeitaufwändige Nachfragen bei anderen Behörden. Mit Hilfe des Fingerabdrucks im Ausweisdokument kann das Erkennen von Ausweismissbrauch beschleunigt werden. Zu den statistischen Angaben des Ausweismissbrauchs vergleiche Antwort zu Frage 13.

16. In wie vielen Personalausweisen sind nach Kenntnis der Bundesregierung derzeit (freiwillig) Fingerabdrücke der Inhaberinnen und Inhaber gespeichert?
17. Wie viele Bürgerinnen und Bürger haben bei der Personalausweisbeantragung im vergangenen Jahr freiwillig ihre Fingerabdrücke speichern lassen, und wie viele nicht (falls konkrete Zahlen nicht vorliegen, bitte möglichst die Quote angeben, wie oft Fingerabdrücke gespeichert bzw. nicht gespeichert werden, wenn möglich auch eine ungefähre Einschätzung)?

Die Fragen 16 und 17 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Aus den monatlichen statistischen Erhebungen des Ausweisherstellers Bundesdruckerei GmbH im Jahr 2019 geht hervor, dass zwischen 38,5 Prozent und 43,7 Prozent der Anträge auf Ausstellung eines Personalausweises freiwillig erhobene Fingerabdruckdaten enthalten. Zu den Daten aus den vorherigen Jahren siehe nachfolgende Tabelle:

Jahr	Produzierte Stückzahl	Anteil mit Fingerabdrücken
2013	6.115.299	1.948.148 (entspricht ca. 31,86 %)
2014	7.230.798	2.234.906 (entspricht ca. 30,91 %)
2015	7.881.954	2.311.336 (entspricht ca. 29,32 %)
2016	6.519.363	2.184.760 (entspricht ca. 33,51 %)
2017	6.935.118	2.533.088 (entspricht ca. 36,53 %)
2018	7.607.861	2.831.878 (entspricht ca. 37,22 %)

18. Wie viele Bundesbürgerinnen und Bundesbürger sind nach Kenntnis der Bundesregierung personalausweispflichtig und somit in den nächsten zehn Jahren voraussichtlich von der Pflicht zur Speicherung der Fingerabdrücke im Personalausweis betroffen?

Konkrete Zahlen der personalausweispflichtigen Personen (ab Vollendung des 16. Lebensjahres) liegen der Bundesregierung nicht vor, da für den Vollzug von Ausweisangelegenheiten grundsätzlich die von den Ländern bestimmten Behörden zuständig sind (§ 7 des Personalausweisgesetzes). In der Regel liegen die Informationen lediglich in den örtlichen Personalausweisregistern vor.

Auf Bundesebene ist lediglich bekannt, dass der Ausweishersteller Bundesdruckerei GmbH jährlich zwischen sieben und 8,5 Millionen Personalausweise produziert (einschließlich Ersatzausweise für verlorene Dokumente und Neuausstellungen z. B. wegen Namensänderung, ohne Differenzierung nach sechsjähriger oder zehnjähriger Gültigkeitsdauer und ohne Aufschlüsselung, ob die antragstellenden Personen personalausweispflichtig sind).

19. Beabsichtigt die Bundesregierung, den Eingriff in die Grundrechte mehrerer Millionen Bundesbürgerinnen und Bundesbürger durch andere Maßnahmen im Sinne einer Überwachungsgesamtrechnung zu kompensieren (falls ja, bitte ausführen, falls nein, bitte begründen)?

Die Speicherung der Fingerabdrücke im Chip des Personalausweises dient der Möglichkeit einer schnellen Identifikation vor Ort, wenn Zweifel nach Abgleich des Lichtbilds bleiben (vergleiche § 9 Absatz 3 Satz 5 des Personalausweisgesetzes). Eine sonstige Speicherung des Fingerabdrucks, welcher im Rahmen der Personalausweisbeantragung erhoben wurde, findet in Deutschland nicht statt. Eine Überwachung der Ausweisinhaberin oder des Ausweisinhabers ist – unabhängig von der Speicherung von Fingerabdrücken im Ausweisdokument – allein auf Basis des Personalausweisdokuments nicht möglich.

20. Welche Sicherungen gegen (ungewollte) physische Einwirkungen sollen dem Datenträger eingebaut werden?

Inwieweit ist die Auslesbarkeit der Fingerabdruckdaten gefährdet, wenn der Ausweis Mikrowellen ausgesetzt wird oder in Waschmaschinen gerät?

Die Resistenz gegen Angriffe auf die Vertraulichkeit der gespeicherten Daten durch äußere Einflüsse (u. a. Mikrowellen) wird im Rahmen der Zertifizierung geprüft (vergleiche Antwort zu Frage 8). Störungen der Funktionsfähigkeit des elektronischen Speicher- und Verarbeitungsmediums berühren nicht die Gültigkeit des Personalausweises (§ 28 Absatz 3 des Personalausweisgesetzes).

Eine gezielte Zerstörung des elektronischen Speicher- und Verarbeitungsmediums ist eine Veränderung des Ausweises, welche zur Ungültigkeit führt (§ 28 Absatz 1 Nummer 1 des Personalausweisgesetzes). Durch die versehentliche oder absichtliche Zerstörung des Chips wird die Vertraulichkeit der gespeicherten Fingerabdrücke jedoch nicht beeinträchtigt, sie stehen anschließend weder berechtigten noch unberechtigten Stellen zur Verfügung.

21. Welche Regelungen sind vorgesehen für den Fall, dass das Speichermedium auf einem Personalausweis während dessen Gültigkeitsdauer schadhaft bzw. beschädigt ist?

Soll auch ein Personalausweis, dessen Speichermedium infolge jedweder Einwirkungen beschädigt wurde, weiterhin seine Gültigkeit behalten, oder sollen die Inhaberinnen und Inhaber verpflichtet werden, einen neuen Ausweis zu beantragen?

Bezüglich der Funktionsunfähigkeit des elektronischen Speicher- und Verarbeitungsmediums wird auf die Antwort zu Frage 20 verwiesen. Zur Gewährleistung der elektronischen Funktionalität des Ausweises bei regelgerechtem Gebrauch wird auf die Antwort zu Frage 8 verwiesen.

22. Welche Verfahrensweise ist vorgesehen, wenn Bürgerinnen und Bürger die Abgabe der Fingerabdrücke verweigern?

Vergleichbar der Rechtslage bei Reisepässen wird die Ausstellung eines Personalausweises nach Maßgabe des Entwurfs eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (Bundratsdrucksache 435/20) ab dem 2. August 2021 abzulehnen sein, wenn sich die antragstellende Person weigert, ihre Fingerabdrücke erfassen zu lassen, obwohl dies nach den Umständen des Einzelfalls möglich erscheint und die antragstellende Person keine ärztliche Bescheinigung vorlegt, aus denen sich Gründe ergeben, die einer Fingerabdruckerfassung entgegenstehen (vergleiche Nummer 4.4.0 der Passverwaltungsvorschrift).

23. Gehen die Fragestellerinnen und Fragesteller recht in der Annahme, dass bei einem Personalausweis-antrag, der bis zum 30. Juli 2021 gestellt wird, noch keine Pflicht zur Abgabe von Fingerabdrücken besteht, auch wenn das Ausgabedatum nach dem 1. August 2021 liegt (bitte ggf. korrigieren)?

Bei Anträgen auf Ausstellung von Personalausweisen, welche am 2. August 2021 oder danach gestellt werden, würde die Fingerabdruckerfassung nach Artikel 11 i. V. m. Artikel 16 Absatz 3 des Entwurfs eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen (Bundratsdrucksache 435/20) verpflichtend. Wird ein Personalausweis zuvor beantragt, steht es der antragstellenden Person entsprechend der geltenden Rechtslage (§ 5 Absatz 9 Satz 1 des Personalausweisgesetzes) frei, der Aufnahme von Fingerabdrücken zuzustimmen oder nicht.

24. Warum enthält der in Bezug genommene Gesetzentwurf keine Aussage zu den durch die obligatorische Aufnahme von zwei Fingerabdrücken entstehende Mehrkosten für die Verwaltung und die Bürgerinnen und Bürger?

Von welchen Mehrkosten geht die Bundesregierung ggf. aus?

Im Entwurf eines Gesetzes zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen ist der Aufwand für die Behörden dargestellt (Bundratsdrucksache 435/20, S. 19 bis 21): Die Behörden werden durch den künftig entbehrlichen Aufklärungsaufwand um den gleichen Erfüllungsaufwand entlastet, der benötigt wird, um die Fingerabdrücke zu erfassen. Im Ergebnis ist daher nicht mit zusätzlichem Erfüllungsaufwand zu rechnen.

25. In welchen der EU-Staaten, in denen es Personalausweise bereits heute gibt, gibt es nach Kenntnis der Bundesregierung bislang die fakultative Aufnahme oder die obligatorische Aufnahme von Fingerabdrücken in Personalausweise oder vergleichbare Identitätsdokumente?

Die EU Mitgliedstaaten stellen auf Basis der Verordnung (EG) 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, geändert durch Verordnung (EG) 444/2009 des Europäischen Parlaments und des Rates vom 28. Mai 2009, reguläre Reisepässe mit Chip aus, welche das Lichtbild und zwei Fingerabdrücke enthalten. Deutschland hat den elektronischen Reisepass zum 1. November 2005 und die Speicherung von Fingerabdrücken in Pässe zum 1. November 2007 eingeführt.

Die Aufnahme von Fingerabdrücken in Personalausweise ist in Deutschland bislang optional.

Einer Erhebung der EU-Kommission zufolge [vergleiche Anhang 5 der Folgenabschätzung; KOM-Dokument SWD(2018) 110 final vom 17. April 2018] können in nationale Identitätskarten der folgenden EU Mitgliedstaaten Fingerabdrücke gespeichert werden: Bulgarien, Ungarn, Italien, Lettland, Litauen, Portugal, Spanien und Zypern.

