

28.04.23**Empfehlungen
der Ausschüsse**

In - Fz - R

zu **Punkt ...** der 1033. Sitzung des Bundesrates am 12. Mai 2023

**Entwurf eines Gesetzes zur Modernisierung des Pass-, des
Ausweis- und des ausländerrechtlichen Dokumentenwesens****A**Der federführende **Ausschuss für Innere Angelegenheiten**

empfiehlt dem Bundesrat, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

bei An-
nahme
entfallen
Ziffern 2
und 3

1. Zu Artikel 1 Nummer 9 (§ 16a Absatz 1 Satz 2, Absatz 2 Satz 1, § 16b Absatz 1 PassG),
Artikel 2 Nummer 7 (§ 16 Absatz 1 Satz 2, Absatz 2 Satz 1, § 17 Absatz 1 PAuswG)

- a) Artikel 1 Nummer 9 ist wie folgt zu ändern:
 - aa) § 16a ist wie folgt zu ändern:
 - aaa) Absatz 1 Satz 2 ist wie folgt zu fassen:

„Echtheits- und Identitätskontrollen sind nur über gesicherte Kommunikationswege zulässig.“
 - bbb) In Absatz 2 Satz 1 sind die Wörter “mit Ausnahme der biometrischen Daten“ zu streichen.
 - bb) In § 16b Absatz 1 sind die Wörter „nicht automatisierte“ durch das Wort „sichere“ zu ersetzen.

b) Artikel 2 Nummer 7 ist wie folgt zu ändern:

aa) § 16 ist wie folgt zu ändern:

aaa) Absatz 1 Satz 2 ist wie folgt zu fassen:

„Echtheits- und Identitätskontrollen sind nur über gesicherte Kommunikationswege zulässig.“

bbb) In Absatz 2 Satz 1 sind die Wörter „mit Ausnahme der biometrischen Daten“ zu streichen.

bb) In § 17 Absatz 1 sind die Wörter „nicht automatisierte Verfahren erheben und verwenden“ durch die Wörter „sichere Verfahren verarbeiten“ zu ersetzen.

Begründung:

Die Vorschriften des Pass- und Personalausweisgesetzes werden an die Bedürfnisse der ausleseberechtigten Behörden angepasst. Insbesondere soll es der Polizei ermöglicht werden, bereits im Rahmen einer Identitätsfeststellung erhobene Daten aus Pässen und Personalausweisen weiter zu verwenden, ohne sie erneut zu erheben und händisch übertragen zu müssen.

Um entsprechenden Nutzen zu entfalten, wurde die neu eingefügte Vorgabe, dass Echtheits- und Identitätskontrollen über öffentliche Kommunikationswege unzulässig sind, durch eine Zulässigkeit bei Vorliegen sicherer Kommunikationswege ersetzt (vgl. hierzu auch § 3 PassDEÜV). Diese Formulierung eröffnet die Möglichkeit des Einsatzes dienstlicher Smartphones, die unmittelbar auf geschützte polizeiliche Datensysteme zugreifen.

Die von der automatisierten Speicherung in einem Datenverarbeitungssystem in § 16a Absatz 2 PassG-E und § 16 Absatz 2 PAuswG-E ausgenommenen biometrischen Daten können aus Ermittlungsansätzen ebenfalls erforderlich sein, wenn z. B. lediglich der Ausweis, nicht aber die Person selbst greifbar ist. Die automatisierte Speicherung dieser Daten ist ohnehin nur zulässig, wenn die berechtigten Behörden dazu durch ein Gesetz oder aufgrund eines Gesetzes berechtigt sind.

Schließlich dürfen die sichtbar in Reisepässen oder Personalausweisen aufgedruckten Daten nur dann von den berechtigten Behörden verarbeitet werden, wenn die hierfür verwendeten Verfahren sicher sind. Die Vorgabe von „nicht automatisierten Verfahren“ lässt im Hinblick auf die Digitalisierung der Verwaltung nur eine sehr eingeschränkte Weiterverarbeitung zu, welche dem Änderungszweck der Regelung nicht nahekommt. Ein von der Praxis gefordertes App-basiertes Auslesen kann damit nicht sichergestellt werden, weshalb eine Änderung erforderlich ist, um den gewünschten Nutzen zu erzielen.

Nachdem die Daten in jedem Fall erhoben und verarbeitet werden dürfen, stellt sich die Frage, weshalb hinsichtlich der Möglichkeiten und Wege der „Entnahme“ der Daten aus dem Identitätsdokument solch hohe Hürden normiert werden. Zwar handelt es sich streng genommen um eine Zweckänderung, die aber durch die erforderliche fachrechtliche Rechtsgrundlage ihre Zulässigkeit entfaltet.

bei An-
nahme
entfällt
Ziffer 3

2. Hilfsempfehlung zu Ziffer 1

Zu Artikel 1 Nummer 9 (§ 16a Absatz 1 Satz 1 Nummer 01 – neu –,
Nummer 3, Satz 2, Absatz 2 Satz 1, §16b PassG),
Artikel 2 Nummer 7 (§ 16 Absatz 1 Satz 1 Nummer 01 – neu –, Nummer 3,
Satz 2, Absatz 2 Satz 1, §17 PAuswG)

a) Artikel 1 Nummer 9 ist wie folgt zu ändern:

aa) § 16a ist wie folgt zu ändern:

aaa) Absatz 1 ist wie folgt zu ändern:

aaaa) Satz 1 ist wie folgt zu ändern:

aaaaa) Der Nummer 1 ist folgende Nummer voranzustellen:

„01. die auf dem Pass sichtbar aufgedruckten Daten automatisiert zu erheben,“

bbbbb) In Nummer 3 ist das Wort „biometrischen“ durch das Wort „erhobenen“ zu ersetzen.

bbbb) In Satz 2 ist das Wort „öffentliche“ durch das Wort „ungesicherte“ zu ersetzen.

bbb) In Absatz 2 Satz 1 sind die Wörter „mit Ausnahme der biometrischen Daten“ durch die Wörter „sowie die sichtbar aufgedruckten Daten des Passes“ zu ersetzen und nach dem Wort „sofern“ die Wörter „und soweit“ einzufügen.

bb) § 16b ist wie folgt zu fassen:

„§ 16b

Nicht automatisierte Verarbeitung der sichtbaren Daten des Passes

Können die Daten des Passes nach § 16a nicht automatisiert verarbeitet

werden, dürfen die in § 16a Absatz 1 Satz 1 genannten Behörden die auf dem Pass sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren verarbeiten, sofern und soweit sie dazu durch ein Gesetz oder aufgrund eines Gesetzes berechtigt sind.“

b) Artikel 2 Nummer 7 ist wie folgt zu ändern:

aa) § 16 ist wie folgt zu ändern:

aaa) Absatz 1 ist wie folgt zu ändern:

aaaa) Satz 1 ist wie folgt zu ändern:

aaaaa) Der Nummer 1 ist folgende Nummer voranzustellen:

„01. die auf dem Pass sichtbar aufgedruckten Daten automatisiert zu erheben,“

bbbbb) In Nummer 3 ist das Wort „biometrischen“ durch das Wort „erhobenen“ zu ersetzen.

bbbb) In Satz 2 ist das Wort „öffentliche“ durch das Wort „ungesicherte“ zu ersetzen.

bbb) In Absatz 2 Satz 1 sind die Wörter „mit Ausnahme der biometrischen Daten“ durch die Wörter „sowie die sichtbar aufgedruckten Daten des Personalausweises“ zu ersetzen und nach dem Wort „sofern“ die Wörter „und soweit“ einzufügen.

bb) § 17 ist wie folgt zu fassen:

„§ 17

Nicht automatisierte Verarbeitung der sichtbaren Daten des Personalausweises

Können die Daten des Personalausweises nach § 16 nicht automatisiert verarbeitet werden, dürfen die in § 16 Absatz 1 Satz 1 genannten Behörden die auf dem Personalausweis sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren erheben und verwenden, sofern und soweit sie dazu durch ein Gesetz oder aufgrund eines Gesetzes berechtigt sind.“

Begründung:Zu Buchstabe a Doppelbuchstabe aa und
Buchstabe b Doppelbuchstabe aa:

Das Erheben der auf dem Pass sichtbar aufgedruckten Daten ist essentieller Bestandteil einer validen Dokumentenprüfung und soll daher in § 16a Absatz 1 Satz 1 Nummer 01 PassG-E und in § 16 Absatz 1 Nummer 01 PAuswG-E ergänzt werden. Für eine sachgerechte Echtheitsprüfung des Dokuments bedarf es einer inhaltlichen Schlüssigkeitsprüfung unter Einbeziehung der Informationen aus der maschinenlesbaren Zone, dem Chip (diese beiden Elemente erzeugen im Zusammenspiel einen Zugriffs- bzw. Berechtigungsschlüssel für die zweite, biometrische Informationsebene) sowie den aufgedruckten Daten in Verbindung mit dem Layout des Ausweisdokumentes. Eine tragfähige Echtheitsüberprüfung des Reisepasses benötigt daher die Daten der maschinenlesbaren Zeile, des Chips sowie der aufgedruckten Daten (innere Logikprüfung).

Gemäß der Einzelbegründung sollen ungesicherte Kommunikationswege nicht genutzt werden (S. 38 der BR-Drucksache 144/23). In § 16a Absatz 1 Satz 2 PassG-E sowie in § 16 Absatz 1 Satz 2 PAuswG-E soll daher das Wort „öffentliche“ durch das Wort „ungesicherte“ ersetzt werden, um die Nutzung von gesicherten Übertragungswegen im öffentlichen Netz nicht auszuschließen (z. B. VPN-Tunnel).

§ 16a Absatz 2 Satz 1 PassG-E sowie § 16 Absatz 1 Satz 2 PAuswG-E werden um die „sichtbar aufgedruckten Daten“ ergänzt. Auch diese Daten sollen im Rahmen der Vorgangsbearbeitung verarbeitet werden können. Der Einschub „und soweit“ soll unterstreichen, dass der Umfang der Daten, die in ein Datenverarbeitungssystem übernommen werden können, seine Grenze im Fachrecht findet (Identitätsfeststellung, erkennungsdienstliche Behandlung etc.).

In § 16a Absatz 2 Satz 1 PassG-E sowie § 16 Absatz 1 Satz 2 PAuswG-E werden zudem der Ausschluss der Verarbeitung der biometrischen Daten in einem Datenverarbeitungssystem gestrichen. Da beispielsweise im Rahmen erkennungsdienstlicher Maßnahmen für die Anfertigung von Wahllichtbildvorlagen ein Lichtbild erhoben werden dürfte, könnte – soweit die fachrechtlichen Voraussetzungen im Einzelfall vorliegen – dieses auch direkt aus dem Dokument erhoben werden; eine Notwendigkeit zu einer weiteren freiheitsbeschränkenden Maßnahme (erkennungsdienstliche Maßnahme) könnte dadurch in Einzelfällen im Interesse des Betroffenen entfallen.

Zu Buchstabe a Doppelbuchstabe bb und
Buchstabe b Doppelbuchstabe bb:

Bedingt durch die Ergänzungen in § 16a Absatz 1 Nummer 01 und in Absatz 2 PassG-E und § 16 Absatz 1 Nummer 01 und in Absatz 2 PAuswG-E können § 16b PassG-E und § 17 PAuswG-E kürzer gefasst werden, da die Übernahme der sichtbar aufgedruckten Daten in ein Datenverarbeitungssystem nunmehr dort vorgesehen ist. Es bedarf daher lediglich der hier vorgeschlagenen Regelung für den Fall, dass eine automatisierte Übernahme der Daten nicht möglich ist. Zudem wird klargestellt, dass zur Identitätsfeststellung berechnete Behörden Daten aus dem Pass auf herkömmliche Art und Weise erheben dürfen, so-

fern sie durch spezialgesetzliche Regelungen hierzu ermächtigt sind.

Die Überschriften werden zur Klarstellung konkretisiert, da die Normen auf nicht automatisierte Verarbeitungen beschränkt und die automatisierte Verarbeitung der sichtbaren Daten des Passes in § 16a PassG-E sowie § 16 PAuswG-E vorgesehen sind.

3. Hilfs-Hilfsempfehlung zu Ziffer 1 bzw. Hilfsempfehlung zu Ziffer 2

Zu Artikel 1 Nummer 9 (§ 16a Absatz 1 Satz 2, § 16b Absatz 1 Satz 1, Satz 2, 3 – neu – PassG),

Artikel 2 Nummer 7 (§ 16 Absatz 1 Satz 2, § 17 Absatz 1 Satz 1, Satz 2, 3 – neu –, Absatz 2 Satz 1 PAuswG)

a) Artikel 1 Nummer 9 ist wie folgt zu ändern:

aa) In § 16a Absatz 1 Satz 2 ist das Wort „öffentliche“ durch das Wort „ungesicherte“ zu ersetzen.

bb) § 16b Absatz 1 ist wie folgt zu ändern:

aaa) Nach dem Wort „Verfahren“ sind die Wörter „erheben und diese“ einzufügen.

bbb) Folgende Sätze sind anzufügen:

„Sie dürfen unter den Voraussetzungen des Satzes 1 die sichtbar auf dem Pass aufgedruckten Daten mit Ausnahme des Lichtbildes durch optoelektronische Verfahren erheben und diese verarbeiten. Für das automatisierte Auslesen der Daten der maschinenlesbaren Zone nach § 4 Absatz 2 Satz 2 findet ausschließlich Absatz 2 Anwendung.“

b) Artikel 2 Nummer 7 ist wie folgt zu ändern:

aa) In § 16 Absatz 1 Satz 2 ist das Wort „öffentliche“ durch das Wort „ungesicherte“ zu ersetzen.

bb) § 17 Absatz 1 ist wie folgt zu ändern:

aaa) Das Wort „verwenden“ ist durch die Wörter „diese verarbeiten“ zu ersetzen.

bbb) Folgende Sätze sind anzufügen:

„Sie dürfen unter den Voraussetzungen des Satzes 1 die sicht-

bar auf dem Personalausweis aufgedruckten Daten mit Ausnahme des Lichtbildes durch optoelektronische Verfahren erheben und diese verarbeiten. Für das automatisierte Auslesen der Daten der maschinenlesbaren Zone nach § 5 Absatz 4 Satz 2 findet ausschließlich Absatz 2 Anwendung.“

- cc) In § 17 Absatz 2 Satz 1 ist die Angabe „§ 5 Absatz 2 Satz 2“ durch die Angabe „§ 5 Absatz 4 Satz 2“ zu ersetzen.

Begründung:

Der Vorschlag hat die Aufnahme einer Regelung zur Erhebung der sichtbaren Daten (mit Ausnahme des Lichtbildes) auf Pässen und Personalausweisen mittels optoelektronischer Verfahren durch sog. polizeiliche „Scan-Apps“ und deren weitere Verarbeitung mittels automatisierter Verfahren sowie die Vereinheitlichung des Anwendungsbereiches der im übrigen wortgleichen Regelungen von § 16b Absatz 1 PassG-E und § 17 Absatz 1 PAuswG-E zum Gegenstand. Darüber hinaus betrifft der Antrag die Regelung zur Unzulässigkeit der Datenübertragung durch öffentlichen Kommunikationswege im Rahmen der Identitäts- und Echtheitsfeststellung.

Der Gesetzentwurf enthält u. a. Anpassungen der Bestimmungen des bereichsspezifischen Datenschutzrechts im Pass- und Personalausweisgesetz. Dabei regelt der Gesetzentwurf nur die Erhebung und Verwendung bzw. Speicherung der Daten aus dem Pass bzw. Personalausweis

- a) auf herkömmliche Weise, d. h. durch nicht-automatisierte Erhebung und Verwendung der sichtbar aufgedruckten Daten – § 16b Absatz 1 PassG-E, § 17 Absatz 1 PAuswG-E,
- b) durch Auslesen der maschinenlesbaren Zone (MRZ) – § 16b Absatz 2 PassG-E, § 16 Absatz 2, § 17 PAuswG-E – sowie
- c) durch Auslesen des Chips – § 16a PassG-E, § 16 PAuswG-E.

Eine optoelektronische Erfassung und weitere Verarbeitung in einem polizeilichen Vorgangsbearbeitungssystem bestimmter sichtbar aufgedruckter Daten, wie es die sog. „Scan-Apps“ vorsehen, wird hingegen nicht geregelt.

Zu Buchstabe a Doppelbuchstabe aa und
Buchstabe b Doppelbuchstabe aa:

Der Gesetzentwurf sieht seinem Wortlaut nach sowohl in § 16a Absatz 1 Satz 2 PassG-E als auch in § 16 Absatz 1 Satz 2 PAuswG-E vor, dass Echtheits- und Identitätskontrollen über öffentliche Kommunikationswege unzulässig sind. In der Entwurfsbegründung wird diese Regelung dahingehend konkretisiert, dass Daten -sofern sie aus dem Chip eines Dokuments für eine Echtheits- und Identitätskontrolle ausgelesen werden- nur über gesicherte Kommunikationswege übermittelt werden sollen. Mit Blick auf eine rechtssichere Anwendung der neuen Regelungen zur Verarbeitung der auf dem Chip gespeicherten Daten im Rahmen der Identitäts- und Echtheitsfeststellung wird der Wortlaut des Geset-

zes auf ungesicherte Kommunikationswege konkretisiert. Andernfalls wäre jedenfalls für den Rechtsanwender nicht eindeutig erkennbar, was unter der Begrifflichkeit „öffentliche Kommunikationswege“ subsumiert werden soll.

Zu Buchstabe a Doppelbuchstabe bb Dreifachbuchstabe aaa und
Buchstabe b Doppelbuchstabe bb Dreifachbuchstabe aaa:

Es handelt sich um eine redaktionelle Anpassung, um unter Berücksichtigung der Änderungen zu § 16b Absatz 1 Satz 2 und 3 PassG bzw. § 17 Absatz 1 Satz 2 und 3 PAuswG die Verwendung gleichlautender Formulierungen zu erreichen. Der Gesetzentwurf differenziert im Hinblick auf die Nutzung der sichtbaren Personendaten durch nicht automatisierte Verfahren auf dem Pass und auf Personalausweis. Während § 16b Absatz 1 PassG-E vorsieht, dass die in § 16a Absatz 1 Satz 1 PassG-E genannten Behörden die auf dem Pass sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren verarbeiten dürfen, regelt § 17 PAuswG-E, dass die § 16 Absatz 1 Satz 1 PAuswG-E genannten Behörden die auf dem Personalausweis sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren erheben und verwenden dürfen. Aus der Entwurfsbegründung ist nicht erkennbar, aus welchem Grund die Daten aus Pässen verarbeitet, die Daten aus Personalausweisen indes erhoben und verwendet werden dürfen. Nicht nur der durch Einfügung der neuen Sätze 2 und 3 zum Ausdruck gebrachte Regelungsbedarf spricht dafür, in beiden Regelungen den Begriff der Verarbeitung der erhobenen Daten zu verwenden, da jeweils die Überführung in die Datenverarbeitungssysteme der Polizeivollzugsbehörden im Sinne einer Verarbeitung erforderlich ist. Die Differenzierung zwischen Erhebungsmethode (nicht automatisiertes Verfahren / automatisiertes Verfahren mittels Optoelektronik) und Verwendungsart der Daten dient der rechtssicheren Klarstellung zwischen den Verarbeitungsmodalitäten.

Zu Buchstabe a Doppelbuchstabe bb Dreifachbuchstabe bbb und
Buchstabe b Doppelbuchstabe bb Dreifachbuchstabe bbb:

Mit den Änderungen soll eine gesetzliche Regelung zur Erhebung und Verarbeitung der sichtbaren Daten des PASSES und des Personalausweises mittels optoelektronischer Verfahren durch sog. polizeiliche „Scan-Apps“ eingeführt werden.

Der Bedarf für eine Überarbeitung der bereichsspezifischen Datenschutzvorschriften im Pass- und Ausweiswesen wurde insbesondere vor dem Hintergrund der Entwicklung sog. „Scan-Apps“ zum Einlesen von Daten aus Personalausweisen und Reisepässen im Rahmen der polizeilichen Sachbearbeitung von einigen Ländern bereits im Rahmen der Länderbeteiligung zum Referentenentwurf zum Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens benannt. Der vorliegende Gesetzentwurf weist in seiner Einzelbegründung ausdrücklich darauf hin, dass die bestehenden gesetzlichen Regelungen und Befugnisse zur Erhebung und Verarbeitung von Personendaten –mit Ausnahme der biometrischen Daten- an die Möglichkeiten der modernen Datenerfassung angepasst werden müssen, priorisiert im Bereich der automatisierten Verfahren jedoch nur das Auslesen des Chips des PASSES und des Personalausweises, wobei das Auslesen des Chips darüber hinaus nur zum Zweck der Identitäts- und Echtheitsprüfung zulässig sein soll, vgl. § 16a Absatz 1 PassG-E, § 16 PAuswG-E. Die Befugnis zum Auslesen der

maschinenlesbaren Zone soll nur für den Fall zulässig sein, dass der Chip nach § 16a Absatz 1 PassG-E nicht ausgelesen werden kann. Damit bleibt der Gesetzentwurf hinter dem praktischen Anwendungsbereich der täglichen Arbeit insbesondere der Polizeivollzugsbehörden zurück. Diese sind nach dem Gesetzentwurf weiterhin vorrangig lediglich befugt, die auf dem Personalausweis sichtbar aufgedruckten Daten durch nicht automatisierte Verfahren zu verarbeiten.

Der ausdrückliche Zweck des Gesetzes, die Anpassung der gesetzlichen Regelungen und Befugnisse zur Erhebung und Verarbeitung von Personendaten an die Möglichkeiten der modernen Datenerfassung, wird daher nicht umfassend erreicht.

Der Anwendungsbereich optoelektronischer Verfahren zur Erhebung und Verarbeitung von sichtbaren Daten des Passes bzw. des Personalausweises umfasst eine Vielzahl von Massenverfahren im Aufgabenbereich der Polizeivollzugsbehörden, insbesondere im Bereich von Maßnahmen im Zusammenhang mit dem Straßenverkehr (Fahrzeug- und Verkehrskontrollen), aber auch Maßnahmen der Gefahrenabwehr und Störungsbeseitigung (Vollzug des Gewaltschutzgesetzes und länderspezifischer Polizeigesetze). Diese Maßnahmen erfordern regelmäßig die Verarbeitung der sichtbaren Daten des Passes bzw. des Personalausweises, welche nach aktueller Rechtslage händisch erfolgen muss.

Durch eine Regelung zum Einsatz optoelektronischer Verfahren wird die Möglichkeit geschaffen, den Prozess des Abschreibens der personenbezogenen Daten von Legitimationspapieren und der ggf. darauffolgenden manuellen Übertragung der Daten in die polizeilichen Datenverarbeitungssysteme durch ein medienbruchfreies und automatisiertes Verfahren zu ersetzen. Hierdurch wird den Erfordernissen der Polizeivollzugsbehörden nach einer schnellen und fehlerfreien Datenerfassung vor Ort und deren sicheren Übertragung Rechnung getragen.

Die Schaffung einer Regelung zur Nutzung optoelektronischer Verfahren führt zu einer erheblichen Reduzierung von Zeitaufwand bei der Vorgangssachbearbeitung und zur Schonung polizeilicher Ressourcen zugunsten anderer, insbesondere präventiver Aufgaben. Darüber hinaus steigert das optoelektronische Verfahren die Datenqualität, da Fehlerquellen durch die manuelle Erhebung und Übertragung von Daten in polizeiliche Datenverarbeitungssysteme reduziert werden.

Die im Antrag vorgesehenen Regelungen ergänzen lediglich das im Gesetzentwurf angelegte abgestufte Verfahren um das für den Einsatz der sog. „Scan-Apps“ erforderliche optoelektronische Erfassen nur bestimmter sichtbar aufgedruckter Daten, von denen das Lichtbild ausdrücklich ausgenommen wird. Den Datenschutzinteressen der betroffenen Ausweisinhaberinnen und -inhaber wird damit hinreichend Rechnung getragen. Da die maschinenlesbare Zone zu den sichtbar aufgedruckten Daten des Ausweises gehört, ihr Auslesen aber nach dem Gesetzentwurf einen engeren Anwendungsbereich (nur Identitätsfeststellung, Überprüfung der Echtheit des Dokuments) haben soll als die Erfassung der sichtbaren Daten, stellt jeweils Satz 3 in 16b Absatz 1 PassG-E und § 17 Absatz 1 PAuswG-E klar, dass für das automatisierte Auslesen der MRZ andere Voraussetzungen gelten, nämlich die des Absatzes 2.

Zu Buchstabe b Doppelbuchstabe cc:

Es handelt sich um eine redaktionelle Änderung, da die Daten der maschinenlesbaren Zone in § 5 Absatz 4 Satz 2 PAuswG aufgeführt werden.

4. Zu Artikel 1 Nummer 13 (§ 22 Absatz 1a Satz 2 PassG)

Artikel 1 Nummer 13 § 22 Absatz 1a Satz 2 ist zu streichen.

Begründung:

Der Gesetzentwurf stellt darauf ab, die Verwaltungsabläufe zu modernisieren und durch angepasste Verfahren den Aufwand für die Pass-, Ausweis- und Ausländerbehörden sowie die Bürgerinnen und Bürger zu reduzieren. Darüber hinaus soll mit dem Gesetzentwurf die Sicherheit und Integrität der Daten in Pässen, Personalausweisen und elektronischen Aufenthaltstiteln gesichert und somit das hohe Vertrauen in diese Dokumente aufrechterhalten werden. Dazu sollen mittels eines neuen Absatzes 1a in § 22 PassG und § 24 PAuswG alle erforderlichen Daten der jeweiligen Register auch bei der neu zuständig gewordenen Behörde für die Aufgabenwahrnehmung vorgehalten werden können. Notwendig ist dazu insbesondere, dass die Pass- und Personalausweisbehörden sich gegenseitig standardisierte Mitteilungen übermitteln bzw. Registerdaten austauschen und abrufen können.

Warum in der Kabinettsfassung – in Abkehr vom Referentenentwurf – die biometrischen Daten, die auch dem Dokumentenhersteller übersandt werden, im neuen jeweiligen Satz 2 ausgenommen werden, geht insbesondere aus der Begründung nicht hervor und ist nicht nachvollziehbar. Denn die Aufgaben und Befugnisse der ausstellenden Behörde gehen bei einem Auseinanderfallen von ausstellender und zuständiger Behörde (z. B. im Rahmen eines Umzugs) auf die neu zuständige Behörde über. Hier geht es also nicht um eine Datenübermittlung an fachfremde bzw. andere Behörden. Vielmehr wird lediglich eine örtlich neue Pass-/Personalausweisbehörde zuständig, die in die Lage versetzt werden soll, wie die bisher zuständige Behörde einfach und schnell über die Daten zu verfügen, um einerseits im Interesse des Bürgers Unterlagen nicht wiederholt anzufordern und andererseits ggf. auch einer missbräuchlichen Dokumentenbeantragung entgegenzuwirken. So kann es beispielsweise zur Identifizierung von Pass-/Personalausweisbewerbern bei einer Neuausstellung bei einem vorher verlustigen Dokument erforderlich sein, das Lichtbild (oder auch Augenfarbe und Größe) im damaligen, nun verlustigen und somit nicht mehr verfügbaren Dokument mit der Person, die persönlich für ein neues Dokument vorstellig wird, abzugleichen, um einen Missbrauch zu verhindern.

Nachdem Reisepässe und Personalausweise nur ausgestellt werden dürfen, wenn die Identität der antragstellenden Person zweifelsfrei festgestellt ist und dazu hierzu insbesondere mitgeführte Identitätsdokumente wie frühere Pässe oder Ausweise oder frühere Pass- oder Personalausweisbeanträge heranzuziehen sind (vgl. Nummer 6.3.1.1 der Passverwaltungsvorschrift), erschließt sich diese Einschränkung, die im Ergebnis die Identitätsprüfung erschwert, nicht.

Die Digitalisierung von Prozessen darf nicht dazu führen, dass bestehende Prozesse und Befugnisse, die zur Aufgabenwahrnehmung erforderlich sind, beschnitten werden. Es leuchtet nicht ein, warum die zuständige Behörde (wenn sie nicht zugleich die ausstellende Behörde ist) die Daten des Dokuments, für das sie nunmehr zuständig ist, nicht erhalten soll bzw. darf. Ein derartiges Vorgehen ist mit einer effektiven Aufgabenwahrnehmung unter Wahrung der Sicherheitsinteressen nicht in Einklang zu bringen.

5. Zu Artikel 1 Nummer 14 Buchstabe b (§ 22a Absatz 4 PassG),
Artikel 2 Nummer 12 Buchstabe b (§ 25 Absatz 4 PAuswG)

- a) In Artikel 1 Nummer 14 Buchstabe b § 22a Absatz 4 ist vor der Angabe „§ 64“ das Wort „und“ durch ein Komma zu ersetzen und sind nach dem Wort „Bundesdatenschutzgesetzes“ die Wörter „oder den entsprechenden landesgesetzlichen Regelungen“ einzufügen.
- b) In Artikel 2 Nummer 12 Buchstabe b § 25 Absatz 4 ist vor der Angabe „§ 64“ das Wort „und“ durch ein Komma zu ersetzen und sind nach dem Wort „Bundesdatenschutzgesetzes“ die Wörter „oder den entsprechenden landesgesetzlichen Regelungen“ einzufügen.

Begründung:

Es handelt sich um eine klarstellende Änderung zu den für die einzelnen abrufberechtigten Stellen jeweils geltenden datenschutzrechtlichen Regelwerken.

Gemäß Artikel 4 Absatz 2 Satz 3 EUV i. V. m. Artikel 2 Absatz 2 Buchstabe a 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, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2, L 74 vom 4.3.2021, S. 35) unterfällt die Verarbeitung personenbezogener Daten durch die Nachrichtendienste des Bundes und der Länder bei der Erfüllung ihrer fachspezifischen Aufgaben (z. B. § 3 BVerfSchG) nicht dem Anwendungsbereich des Unionsrechts. Vielmehr stellen die nationalen fachspezifischen Regelungen der Nachrichtendienste in Verbindung mit einzelnen für anwendbar erklärten Regelungen des allgemeinen Datenschutzrechts ein abschließendes Datenschutzvollregime dar, sodass auch bezüglich geeigneter technischer und organisatorischer Maßnahmen für diese abrufberechtigten Stellen nicht auf die Datenschutzgrundverordnung sondern allein auf die nationalen fachspezifischen Regelungen der Nachrichtendienste und einzelne für anwendbar erklärte Regelungen des allgemeinen Datenschutzrechts zurückzugreifen ist (z.B. § 27 Nummer 2 BVerfSchG i. V. m. § 64 BDSG). Zudem war aufgrund des Anwendungsbereichs des Bundesdatenschutzgesetzes für abrufberechtigte Stellen in den Ländern eine Bezugnahme auf die dortigen landesrechtlichen Regelungen aufzunehmen (z.B. § 36 ThürVerfSchG i. V. m. § 54 ThürDSG).

6. Zu Artikel 1 Nummer 17a – neu – (§ 27a Satz 2 PassG),
Artikel 2 Nummer 17 – neu – (§ 34a Satz 2 PAuswG)

a) In Artikel 1 ist nach Nummer 17 folgende Nummer einzufügen:

„17a. In §27a Satz 2 wird die Angabe ‚§ 22a Absatz 2 Satz 6 bis 9‘ durch die Angabe ‚§ 22a Absatz 2 Satz 7 bis 11‘ ersetzt.“

b) In Artikel 2 ist nach Nummer 16 folgende Nummer anzufügen:

„17. In §34a Satz 2 wird die Angabe ‚§ 25 Absatz 2 Satz 5 bis 8‘ durch die Angabe ‚§ 25 Absatz 2 Satz 6 bis 10‘ ersetzt.“

Begründung:

Es handelt sich um redaktionelle Änderungen.

Aufgrund Artikel 7 Nummer 3 und Artikel 8 Nummer 3 des Registermodernisierungsgesetzes vom 28. März 2021 (BGBl I S. 591) wurde in § 22a Absatz 2 PassG ein neuer Satz 5 und in § 25 Absatz 2 PAuswG ein neuer Satz 4 eingefügt. Diese Satzverschiebungen sind im Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät vom 5. Juli 2021 (BGBl I S. 2281) in Artikel 1 bei der Regelung in § 27a Satz 2 PassG sowie in Artikel 2 bei der Regelung in § 34a Satz 2 PAuswG, redaktionell nicht berücksichtigt worden. Es ist daher eine redaktionelle Berichtigung geboten, damit auch nach Gesetzeswortlaut, die in § 22a Absatz 2 Satz 10 und 11 im PassG und § 25 Absatz 2 Satz 9 und 10 im PAuswG enthaltenen ergänzenden Protokollierungsregelungen nicht nur für örtliche, sondern auch für zentrale Pass- und Personalausweisregisterdatenbestände anwendbar sind.

7. Zu Artikel 1 Nummer 18 (§ 28 PassG),
Artikel 7 Absatz 3 (Inkrafttreten)

a) In Artikel 1 Nummer 18 § 28 sind die Angabe „1. Januar 2024“ durch die Angabe „1. November 2025“ und die Angabe „31. Dezember 2023“ durch die Angabe „31. Oktober 2024“ zu ersetzen.

b) Artikel 7 Absatz 3 ist wie folgt zu fassen:

„(3) Artikel 1 Nummer 1 Buchstabe a, Nummer 3 Buchstabe b, e, f, Nummer 4, 14 Buchstabe b und Nummer 18 sowie Artikel 2 Nummer 12 Buchstabe b treten am 1. November 2025 in Kraft.“

Als Folge ist

Artikel 7 Absatz 5 zu streichen.

Begründung:

Der Kinderreisepass soll nicht bereits zum 1. Januar 2024, sondern erst zum 1. November 2025 abgeschafft werden.

Für die Ausstellung von regulären Personalausweisen und Reisepässen für Kinder von 0 bis 6 Jahren werden aufgrund der raschen äußerlichen Veränderung der Kinder die Eltern höhere Kosten aufbringen müssen. Denn die Dokumente werden aus diesem Grund bereits vor Ablauf der Gültigkeitsdauer ungültig und somit die Ausstellung eines neuen gebührenpflichtigen Dokuments erforderlich. Zudem können Kinderreisepässe unmittelbar vor Ort sofort ausgestellt werden.

Um die Bürgerinnen und Bürger, aber auch die Verwaltungen auf die Abschaffung des Kinderreisepasses und den damit erforderlichen zeitlichen Vorlauf, der bei der künftigen Beantragung von regulären Dokumenten anfällt, vorzubereiten, ist im Zuge der Kundenfreundlichkeit ein späteres Inkrafttreten der Abschaffung des Kinderreisepasses geboten. Zudem kann in dieser Zeit die vom BMI im Informationsschreiben vom 6. April 2023, Az. DVI4.20105/47#5, angekündigte Prüfung einer Erweiterung der Voraussetzungen zur Ausstellung eines vorläufigen Reisepasses beispielsweise um Fälle, in denen die Namensführung des Kindes noch nicht feststeht, geprüft werden.

8. Zu Artikel 2 Nummer 11 (§ 24 Absatz 1a Satz 2 PAuswG)

Artikel 2 Nummer 11 § 24 Absatz 1a Satz 2 ist zu streichen.

Begründung:

Der Gesetzentwurf stellt darauf ab, die Verwaltungsabläufe zu modernisieren und durch angepasste Verfahren den Aufwand für die Pass-, Ausweis- und Ausländerbehörden sowie die Bürgerinnen und Bürger zu reduzieren. Darüber hinaus soll mit dem Gesetzentwurf die Sicherheit und Integrität der Daten in Pässen, Personalausweisen und elektronischen Aufenthaltstiteln gesichert und somit das hohe Vertrauen in diese Dokumente aufrechterhalten werden. Dazu sollen mittels eines neuen Absatzes 1a in § 22 PassG und § 24 PAuswG alle erforderlichen Daten der jeweiligen Register auch bei der neu zuständig gewordenen Behörde für die Aufgabenwahrnehmung vorgehalten werden können. Notwendig ist dazu insbesondere, dass die Pass- und Personalausweisbehörden sich gegenseitig standardisierte Mitteilungen übermitteln bzw. Registerdaten austauschen und abrufen können.

Warum in der Kabinettsfassung – in Abkehr vom Referentenentwurf – die biometrischen Daten, die auch dem Dokumentenhersteller übersandt werden, im neuen jeweiligen Satz 2 ausgenommen werden, geht insbesondere aus der Begründung nicht hervor und ist nicht nachvollziehbar. Denn die Aufgaben und Befugnisse der ausstellenden Behörde gehen bei einem Auseinanderfallen von ausstellender und zuständiger Behörde (z. B. im Rahmen eines Umzugs) auf die neu zuständige Behörde über. Hier geht es also nicht um eine Datenübermittlung an fachfremde bzw. andere Behörden. Vielmehr wird lediglich eine

örtlich neue Pass-/Personalausweisbehörde zuständig, die in die Lage versetzt werden soll, wie die bisher zuständige Behörde einfach und schnell über die Daten zu verfügen, um einerseits im Interesse des Bürgers Unterlagen nicht wiederholt anzufordern und andererseits ggf. auch einer missbräuchlichen Dokumentenbeantragung entgegenzuwirken. So kann es beispielsweise zur Identifizierung von Pass-/Personalausweisbewerbern bei einer Neuausstellung bei einem vorher verlustigen Dokument erforderlich sein, das Lichtbild (oder auch Augenfarbe und Größe) im damaligen, nun verlustigen und somit nicht mehr verfügbaren Dokument mit der Person, die persönlich für ein neues Dokument vorstellig wird, abzugleichen, um einen Missbrauch zu verhindern.

Nachdem Reisepässe und Personalausweise nur ausgestellt werden dürfen, wenn die Identität der antragstellenden Person zweifelsfrei festgestellt ist und dazu hierzu insbesondere mitgeführte Identitätsdokumente wie frühere Pässe oder Ausweise oder frühere Pass- oder Personalausweisaneträge heranzuziehen sind (vgl. Nr. 6.3.1.1 der Passverwaltungsvorschrift), erschließt sich diese Einschränkung, die im Ergebnis die Identitätsprüfung erschwert, nicht.

Die Digitalisierung von Prozessen darf nicht dazu führen, dass bestehende Prozesse und Befugnisse, die zur Aufgabenwahrnehmung erforderlich sind, beschnitten werden. Es leuchtet nicht ein, warum die zuständige Behörde (wenn sie nicht zugleich die ausstellende Behörde ist) die Daten des Dokuments, für das sie nunmehr zuständig ist, nicht erhalten soll bzw. darf. Ein derartiges Vorgehen ist mit einer effektiven Aufgabenwahrnehmung unter Wahrung der Sicherheitsinteressen nicht in Einklang zu bringen.

9. Zu Artikel 4 Nummer 1 Buchstabe a₁ – neu – (§ 78 Absatz 6 AufenthG)

Nach Artikel 4 Nummer 1 Buchstabe a ist folgender Buchstabe einzufügen:

„a₁. Absatz 6 wird wie folgt gefasst:

„(6) Die mit der Ausführung dieses Gesetzes betrauten oder zur hoheitlichen Identitätsfeststellung befugten Behörden dürfen die im elektronischen Speicher- und Verarbeitungsmedium gespeicherten Daten sowie sichtbar aufgedruckten und die in der Zone für das automatische Lesen enthaltenen Daten zur Erfüllung ihrer gesetzlichen Aufgaben automatisiert verarbeiten, sofern und soweit sie dazu durch ein Gesetz oder aufgrund eines Gesetzes berechtigt sind.“

Begründung:

§ 78 Absatz 6 AufenthG bestimmt derzeit, dass ausschließlich die Daten aus der Zone für das automatische Lesen durch zur Identitätsfeststellung berechnigte Behörden zur Erfüllung ihrer gesetzlichen Aufgaben verarbeitet werden dürfen. Die übrigen zur weiteren Verfahrensbearbeitung benötigten Daten, welche im elektronischen Speicher- und Verarbeitungsmedium vorhanden sowie sicht-

bar auf dem Dokument aufgedruckt sind, müssen manuell übertragen werden.

Im Hinblick auf die Auslegung des § 49 Absatz 1 AufenthG (analog § 8 Absatz 2 FreizügG/EU und § 16 Absatz 1a AsylG), wonach die Erhebung der aus dem elektronischen Speicher- und Verarbeitungsmedium gespeicherten biometrischen und sonstigen Daten ausschließlich zur IDF und Echtheitsprüfung der Identitätsdokumente ausgelesen werden dürfen, ist die automatisierte und elektronische Speicherung dieser Daten nicht zulässig. Ferner sieht auch § 89 Absatz 3 Satz 1 AufenthG ausdrücklich vor, dass die nach § 49 Absatz 1 AufenthG erhobenen Daten von allen Behörden unmittelbar nach Beendigung der Prüfung der Echtheit des Dokuments oder der Identität der Inhaber zu löschen sind. Somit müssten die bereits erhobenen Daten für die polizeiliche Sachbearbeitung nochmals manuell erhoben und gespeichert werden.

Dieses Vorgehen ist längst überholt und entspricht nicht den Ansprüchen einer modernen Aufgabenerfüllung durch staatliche Behörden. Das Verfahren produziert nicht nur einen unnötigen Aufwand für die zuständigen Behörden, der sich auch in unnötigen Wartezeiten ausdrückt. Es ist zudem hoch fehleranfällig, da bei dem händischen Übertrag der Personendaten leicht Ungenauigkeiten entstehen können.

Die Neufassung des Absatzes 6 gewährleistet ein automatisiertes Verfahren zum Auslesen der notwendigen Daten aus dem elektronischen Speichermedium oder mittels optoelektronischer Methoden aus dem Dokument sowie die medienbruchfreie Übertragung der auf diese Weise erhobenen Daten insbesondere auch in die polizeilichen Datenverarbeitungssysteme zur weiteren Verarbeitung für polizeiliche Zwecke zulassen.

Die für die Verarbeitung erforderlichen Rechtsgrundlagen müssen sich aus dem jeweiligen Fachrecht ergeben.

Durch die Norm wird somit keine zusätzliche Befugnis für die Verarbeitung von Daten geschaffen.

10. Zum Gesetzentwurf allgemein

Am 1. Januar 2021 ist eine auf Europarecht basierende Änderung in Kraft getreten, nach der die Gültigkeitsdauer von Kinderreisepässen bei Neuausstellung oder bei Gültigkeitsverlängerung beziehungsweise Lichtbildaktualisierung auf maximal ein Jahr zu begrenzen ist. Unter Berücksichtigung des mit dem kurzen Gültigkeitszeitraum verbundenen Aufwandes einer regelmäßigen Neubeantragung oder Verlängerung eines Kinderreisepasses sowie einer gegenüber dem Reisepass eingeschränkten Nutzbarkeit, soll für alle deutschen Staatsangehörigen, unabhängig vom Alter, eine einheitliche Lösung für Passdokumente erzielt und der Dokumententyp Kinderreisepass abgeschafft werden. In § 28 PassG-E ist eine Übergangsfrist vorgesehen: „Für vor dem 1. Januar 2024 ausgegebene Kinderreisepässe ist § 5 Absatz 2 in der bis zum 31. Dezember 2023 geltenden Fassung weiter anzuwenden.“

Es wird darauf hingewiesen, dass es in der jüngeren Zeit auch in Deutschland Entführungsfälle von (Klein-)Kindern – nicht selten durch einen der Erziehungsberechtigten – gegeben hat. Werden Personaldokumente in einem Lebensalter von 12 oder jünger ebenfalls für eine Gültigkeitsdauer von sechs Jahren ausgestellt, kann dies eine sichere Identifizierung erheblich erschweren oder unmöglich machen. Die Aufnahme von biometrischen Daten von Kinder in Form von Fingerabdrücken könnte dabei einen Lösungsansatz darstellen.

Begründung:

Die Aufnahme von biometrischen Daten in Form von Fingerabdrücken kann grundsätzlich auch bei Kindern einen erheblichen Mehrwert bieten, wenn es gilt, das Dokument sicher an die sich damit ausweisende Person zu binden. Die Leistenhaut der Hand unterliegt – wie der Körper in seiner Gesamtheit – einem proportionalen Größenwachstum vom Kind zum Erwachsenen. Dieses wird sich auch in der Größe der erfassten Fingerabdrücke widerspiegeln, jedoch sind die kriminaltechnisch relevanten – und auch IT-verwertbaren – Informationen darin selbst von keinen Veränderungen betroffen, so dass eine Zuordnung eines „kindlichen“ Fingerabdrucks mit der gleichen Person im Erwachsenenalter möglich ist.

Das zentrale AFIS des BKA ist technisch in der Lage, dieses Größenwachstum in seinem IT-Vergleichsprozess zu berücksichtigen. Eine manuelle Auswertung durch einen Experten wird immer zum korrekten Resultat kommen.

Bezüglich der Erfassung sollte geprüft werden, ob die verwendeten Geräte in der Lage sind, die in der Gesamtheit kleineren Strukturen der Leistenhaut bei Kindern ausreichend detailliert abzubilden. Aus der polizeilichen Erfahrung heraus ist bekannt, dass die elektronische Erfassung von kleinen Kindern mitunter erschwert sein kann.

B

**11. Der Finanzausschuss und
der Rechtsausschuss**

empfehlen dem Bundesrat, gegen den Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes keine Einwendungen zu erheben.