Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Deutscher Bundestag
An die Vorsitzende des
Rechtsausschusses
Frau Elisabeth Winkelmeier-Becker

Ausschließlich per E-Mail an:
rechtsausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat12@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 31.05.2024
GESCHÄFTSZ. 12-221/098#1769

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

BETREFF **Regierungsentwurf eines Vierten Gesetzes zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (Viertes Bürokratieentlastungsgesetz)**

Sehr geehrte Frau Vorsitzende,

sehr geehrte Mitglieder des Rechtsausschusses,

das Ihnen vorgelegte sog. vierte Bürokratieentlastungsgesetz wurde meinerseits bereits im Rahmen der durchgeführten Ressortabstimmung geprüft. Leider wurden meine Bedenken bezüglich der Änderung des Passgesetzes (PassG) in Artikel 8 und zur Änderung des Luftverkehrsgesetzes (LuftVG) in Artikel 9 des Regierungsentwurfs nicht aufgegriffen. Ich wende mich daher an Sie, da gegen den Vorschlag zur Einführung eines neuen § 18 Abs. 5 bis 7 PassG sowie eines neuen § 19d LuftVG meinerseits weiterhin grundsätzliche Bedenken bestehen.

Zunächst möchte ich nochmals die Historie der rechtlichen Möglichkeit zur Verarbeitung der im Chip des Passes gespeicherten personenbezogenen Daten skizzieren. Sodann werden die durch die Einführung des § 18 Abs.5 PassG-E, 18 Abs. 6-7 PassG-E und § 19d LuftVG-E entstehenden Risiken dargelegt.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

1. Historie

Nach der bis zum 12. Oktober 2023 geltenden Rechtslage war die Verarbeitung der im Chip des Passes gespeicherten Daten (1.) nur durch Polizeivollzugsbehörden, durch die Zollverwaltung sowie durch Pass-, Personalausweis- und Meldebehörden zulässig und (2.) nur soweit dies zur Prüfung der Echtheit des Passes und zur Prüfung der Identität des Passinhabers erforderlich war. Die Daten waren unverzüglich nach Beendigung der Prüfung zu löschen (§ 16a PassG a. F.).

Die Regelung trug dem Umstand Rechnung, dass die Verarbeitung insbesondere der biometrischen Daten im Chip des Passes zu einem erheblichen Eingriff in die Grundrechte der betroffenen Personen führt. Das biometrische Lichtbild unterfällt den besonderen Kategorien personenbezogener Daten, an deren Verarbeitung die Datenschutz-Grundverordnung besonders hohe Anforderungen stellt. Nach Art. 9 Abs. 1 DSGVO unterliegen diese einem generellen Verarbeitungsverbot, es sei denn einer der in Art. 9 Abs. 2 Datenschutz-Grundverordnung (DSGVO) genannten Erlaubnistatbestände ist einschlägig.

Die Schwere des Grundrechtseingriffs folgt auch daraus, dass Bürgerinnen und Bürger zur Bereitstellung dieser Daten mindestens dann gezwungen sind, wenn sie zum Mitführen eines Passes verpflichtet sind (§ 1 PassG), und es daher nicht in ihrer Entscheidungsgewalt liegt, ob und wie die Daten verarbeitet werden. Mit dieser staatlich auferlegten Pflicht gehen umgekehrt erhöhte Anforderungen an die Rechtfertigung des Grundrechtseingriffs einher. Das Bundesverfassungsgericht (BVerfG) hat zu der in § 4 PassG angeordneten Pflicht, biometrische Daten preiszugeben, ausgeführt[1], dass sich die Verhältnismäßigkeit eines solchen Eingriffs danach bestimmt, ob die Verwendung der Daten in einem angemessenen Verhältnis zu dem Gewicht ihrer Erhebung und Speicherung steht. Die Voraussetzungen für die Datenverwendung und deren Umfang müssten umso enger begrenzt sein, je schwerer der Eingriff wiege. Entscheidend für die Verhältnismäßigkeit des § 4 PassG sei damit das Nutzungsregime der gemäß § 4 Abs. 3 und 4 PassG zu speichernden biometrischen Daten.

Mit dem Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens vom 8. Oktober 2023 wurde der Kreis der grundsätzlich zugriffsberechtigten Stellen für Zwecke der Identitätsprüfung auf alle öffentlichen Stellen erweitert.

[1] BVerfG, Beschluss v. 30. Dezember 2012 zu Az. 1 BvR 502/09, Rn. 7 f.

Mit der vorliegenden Regelung sollen nunmehr erstmalig auch nichtöffentliche Stellen Zugriff auf die im Chip des Passes gespeicherten Daten erhalten.

2. Zu § 18 Abs. 5 PassG-E

Insbesondere sogenannte „Advance Passenger Informations“ (API-Daten) sollen künftig nicht nur über die maschinenlesbare Zone (MLZ), sondern auch über den Chip ausgelesen werden können. Der Datenkranz ebenso wie die Löschfrist sollen weiterhin durch das Fachrecht, also § 31a BPolG definiert sein. Im Ergebnis ist damit das Auslesen des Chips statt der MLZ neu. Eine Begründung hierfür ist nicht bekannt. Ich weise darauf hin, dass sich durch den Wechsel des Erhebungsverfahrens der Umfang der potentiell auslesbaren Daten ändert, weil über den Zugriff auf den Chip auch auf biometrische Daten zugegriffen werden kann. Die bisherige Einschränkung des Ausleseverfahrens (nur MLZ, nicht Chip) stellt sicher, dass keine Daten erhoben werden, die für den konkreten Zweck nicht erforderlich sind. Hinweise darauf, dass das Auslesen der MLZ fehleranfällig ist, liegen mir nicht vor. Auch ist nicht ersichtlich, dass der Vorgang für das Auslesen aus der MLZ sich wesentlich in Geschwindigkeit und Komfort vom Auslesen des Chips unterscheidet. In beiden Fällen muss der Fluggast seinen Pass nahe an ein Lesegerät bringen und die Daten sollten in einer im Vergleich zum Gesamtvorgang vernachlässigbaren Zeit ausgelesen sein.

Das Auslesen des Chips statt der MLZ birgt zudem signifikant erhöhte Risiken, wie insb. die Vorgabe des § 18 Abs. 7 PassG-E zeigt. Das erhöht die Eingriffstiefe der Verarbeitung. Soweit § 18 Abs. 5 PassG zur Erhebung von Daten verpflichtet, die auch über die MLZ auslesbar sind, ist das Auslesen des Chips nach § 18 Abs. 5 PassG-E nicht erforderlich und damit unzulässig.

3. Zu § 18 Abs. 6-7 PassG-E, § 19d LuftVG-E

Mit der Regelung sollen nunmehr Luftfahrtunternehmen, Betreiber von Flugplätzen und Bodenabfertigungsdienstleister Zugriff auf die im Chip des Passes gespeicherten Daten erhalten. Ziel soll sein, die Prozesse der Passagierabfertigung an Flughäfen zu beschleunigen und „das Reiseerlebnis des Fluggastes“ zu verbessern. Die zur Erfüllung rein hoheitlicher Aufgaben erhobenen Daten sollen damit für das Angebot optionaler Komfortleistungen nichtöffentlicher Stellen freigegeben werden. Dies würde zu einer grundlegenden Verschiebung des Nutzungsregimes der im Chip der amtlichen Ausweisdokumente gespeicherten Daten führen. Die Freigabe würde einen gänzlich neuen Verarbeitungszweck bereits für die Erhebung und Speicherung der Daten auf dem Chip für kommerzielle Zwecke begründen.

a. Mangelnde Erforderlichkeit

Zwar haben Flughafenbetreiber, Luftfahrtunternehmen und Bodenabfertigungsdienstleister unbestritten ein berechtigtes Interesse, die Prozesse der Bodenabfertigung zu beschleunigen. Dabei dürfen sie selbstverständlich auch neue, digitale Angebote einführen. Der Zugriff auf die im Chip gespeicherten Daten ist für die angegebenen Zwecke jedoch schon nicht erforderlich.

Der Zugriff auf das biometrische Lichtbild im Chip soll nach dem vorliegenden Gesetzentwurf allein der automatisierten Identitätsprüfung beim Check-in dienen. Inwieweit eine solche automatisierte Identitätsprüfung im Vergleich zu der bisher üblichen, nur Sekunden dauernden Sichtkontrolle des Passes zu einer Beschleunigung der Abfertigungsprozesse führt, ist nicht erkennbar.

Auch aus Sicherheitsgründen ist das Auslesen des Lichtbilds durch Luftfahrtunternehmen, Flughafenbetreiber und Bodenabfertigungsdienstleister nicht erforderlich. Für Serviceangebote zur Verbesserung des Reiseerlebnisses ist eine Identitätsprüfung per Sichtvergleich des aufgedruckten Lichtbilds ausreichend. Erhöhte Sicherheitsanforderungen bestehen hier gerade nicht, anders als bei hoheitlichen Grenzkontrollen, die nicht Gegenstand der Regelung sind, so dass es der Übertragung hoheitlicher Befugnisse der Sicherheitsbehörden auf nichtöffentliche Stellen nicht bedarf. Zumal der behauptete Sicherheitsgewinn schon deshalb nicht eintreten kann, weil den Passagieren freistehen soll, ob sie das Verfahren nutzen. Hinzu kommt, dass im weiteren Abfertigungsprozess an die Stelle des bislang (und bei Weigerung auch weiterhin möglichen) bloßen Vorzeigens der Bordkarte ohne weitere Identitätsprüfung eine Identifizierung von Passagieren mittels biometrischer Verfahren treten soll. Damit soll das bisher eingriffsarme Verfahren durch einen wesentlich grundrechtssensibleren Prozess ersetzt werden.

Für die Wiedererkennung des Passagiers bei der weiteren Bodenabfertigung nach dem Check-in, um das wiederholte Vorzeigen von Reisedokumenten zu vermeiden, soll von vornherein ein erst beim Check-in erzeugtes biometrisches Muster genutzt werden. Des Auslesens des biometrischen Lichtbilds aus dem Pass bedarf es hierfür nicht.

b. Zugriffseröffnung durch Gesetzgeber

Dass die betroffenen Personen in das Auslesen und die weitere Verarbeitung der Daten im Einzelfall einwilligen sollen, berührt nicht die hier vom Gesetzgeber zu treffende Entschei-

dung, ob nichtöffentlichen Stellen Zugriff auf für hoheitliche Zwecke gespeicherte Daten gewährt wird, um diese für Serviceangebote nichtöffentlicher Stellen nutzbar zu machen – wenngleich mit klarer Zweckbegrenzung.

Bei der Entscheidung der Passinhaber im Einzelfall, ob sie Zugriff auf die Daten im Chip des Passes gewähren, sind die Anforderungen an die Wirksamkeit erteilter Einwilligungen zu berücksichtigen. Zwar sieht § 19d Abs. 2 LuftVG-E vor, dass das bisher übliche Verfahren der Fluggastabfertigung ohne Einschränkung als gleichwertiges Verfahren ermöglicht werden muss. An der hierfür notwendigen Freiwilligkeit nach Art. 4 Nr. 11 DSGVO kann es aber fehlen, wenn die Weigerung eines Passagiers, den Zugriff auf die im Chip des Passes gespeicherten Daten freizugeben, aus Sicht der betroffenen Person zu Nachteilen bei den Abfertigungsprozessen führen kann (etwa längere Wartezeit, die im Einzelfall dazu führen kann, dass das Flugzeug nicht rechtzeitig erreicht wird). Dass es sich hierbei um einen vom Gesetzgeber nicht intendierten Nachteil handelt, ist unerheblich. Nach Erwägungsgrund 42 DSGVO ist eine Einwilligung nur dann freiwillig erteilt, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“. Auch faktische Nachteile lassen die Freiwilligkeit entfallen, wenn sich die betroffene Person hierdurch einer Drucksituation ausgesetzt sieht. Vorzugswürdig wären Lösungen, die die Abfertigungszeit für alle Passagiere gleichermaßen verkürzen.

c. Missbrauchsrisiken

Es ist anzuerkennen und zu begrüßen, dass versucht wird, unter anderem durch technische Vorgaben des BSI und die notwendige Feststellung des BSI, dass diese Vorgaben eingehalten sind, Missbrauchsrisiken zu senken (§ 18 Abs. 7 PassG-E, auch § 19d Abs. 1 Satz 4 LuftVG-E). Die Risiken, denen hier begegnet werden soll, entstehen aber erst dadurch, dass nichtöffentliche Stellen ermächtigt werden sollen, auf in amtlichen Pässen gespeicherte, hoheitlich angefertigte biometrische Lichtbilder zuzugreifen. Diese Risiken stehen außer Verhältnis zu der intendierten Verbesserung des individuellen Reiseerlebnisses.

d. Regelungssystematik

Die Separierung der Regelungsteile in verschiedene Gesetze, wobei die Regelungen aufeinander bezogen sind und der Regelungsinhalt sich erst in der Zusammenschau vollständig erschließt, ist wenig überzeugend. Es werden nicht etwa passrechtliche und luftverkehrliche Sachverhalte bzw. Regelungen getrennt, sondern vielmehr wird beispielsweise das Anfertigen einer Bildaufnahme des Passagiers am Flughafen (das mit dem auf dem Pass

gespeicherten biometrischen Lichtbild abgeglichen werden soll) und die Erzeugung eines biometrischen Musters hieraus sowie schließlich dessen Löschung im Passgesetz geregelt und nicht etwa im Luftverkehrsgesetz. Dagegen soll das Erfordernis einer ausdrücklichen Einwilligung in das Auslesen der auf dem Chip des Passes gespeicherten Daten im Luftverkehrsgesetz geregelt werden.

4. Fazit

Aufgrund der grundsätzlichen Bedenken gegen eine solche Regelung, die Begehrlichkeiten auch bei anderen nichtöffentlichen Stellen wecken wird, auf durch staatliche Stellen verarbeitete biometrische Daten zugreifen zu dürfen, halte ich die vorgesehenen Regelungen für höchst problematisch. Für das Auslesen der API-Daten existiert mit § 18 Abs. 4 PassG bereits eine hinreichende Regelung, so dass es des § 18 Abs. 5 PassG-E nicht bedarf. In Hinblick auf § 18 Abs. 6-7 PassG-E und § 19d LuftVG-E sollten alternative Verfahren erwogen werden, die keines Zugriffs auf die Daten im Chip des Passes bedürfen.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber