Bayerischer Landtag

18. Wahlperiode 18.07.2023 **Drucksache** 18/**30091**

Beschluss

des Bayerischen Landtags

Der Landtag hat in seiner heutigen öffentlichen Sitzung beraten und beschlossen:

Konsultationsverfahren der Europäischen Union

Inneres
Reisen – Digitalisierung von Reisedokumenten zur Erleichterung des Reisens
05.04.2023 - 28.06.2023

Drs. 18/**28821**, 18/**29950**

Der Bayerische Landtag nimmt das Konsultationsverfahren zum Anlass, folgende Stellungnahme abzugeben:

Die Digitalisierung von Reisedokumenten ist grundsätzlich zu begrüßen und birgt großes Potenzial hinsichtlich der Vereinfachung von Prozessen insbesondere im Rahmen von Kontrolltätigkeiten, womit perspektivisch Erleichterungen bei den Reisebewegungen sowohl für EU-Bürger als auch für das Kontrollpersonal verbunden sind. Allerdings sind weder die konkrete Ausgestaltung noch die einzelnen Modalitäten abschließend bekannt, sodass derzeit nur folgende Überlegungen an die Hand gegeben werden können:

1. Blickwinkel Sicherheit und Datenschutz

   – Das Risiko gefälschter oder manipulierter Dokumente kann mit einer Digitalisierung von Reisedokumenten verringert werden.

     Bezüglich der Sicherheit digitalisierter Reisedokumente ergeben sich neue Möglichkeiten, hochsichere Verschlüsselungstechnologien und biometrische Daten wie Fingerabdrücke oder Gesichtserkennungstechnologien zu verwenden (Multi-Faktor-Authentifizierung), um die Echtheit der Dokumente zu überprüfen und einen Missbrauch durch unberechtigte Personen zu verhindern. Im Rahmen der visuellen und elektronischen Dokumentenprüfung sind derzeit zumeist lediglich physikalisch vorhandene Personal- und Reisedokumente relevant. Neben der herkömmlichen und unabdingbaren visuellen Prüfung kann beispielsweise eine technisch unterstützte Prüfung mittels Dokumentenlese- und -prüfgeräten erfolgen. Diese zielt einerseits auf eine optische Prüfung (Weißlicht, Infrarot und UV-Licht) ab und eröffnet andererseits die Möglichkeit, die Chips elektronischer Dokumente oder Barcodes zu prüfen. Je nach Schutzstandard des Chips erfolgt dies in unterschiedlicher Ausprägung.

     Über die EAC-PKI-Anbindung (Extended Access Control Public Key Infrastruktur) an die Bundespolizei ist bei elektronischen Dokumenten von insgesamt zehn EU-Mitgliedstaaten sowie der Schweiz auch das Auslesen und Anzeigen von besonders geschützten Datengruppen (EAC-Daten) aus dem integrierten Chip von elektronischen Dokumenten möglich. Mit der EAC-PKI-Anbindung ist

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de - Dokumente abrufbar. Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de – Aktuelles/Sitzungen zur Verfügung.

auch der Zugriff auf personenbezogene Daten des neuen deutschen Personalausweises (nPA) sowie die Nebenbestimmungen des deutschen elektronischen Aufenthaltstitels (eAT) möglich.

Somit könnte das Risiko gefälschter oder manipulierter Dokumente erheblich reduziert und die Sicherheit an den Grenzen gestärkt werden.

– Digitale Dokumente eröffnen schnellere Handlungsmöglichkeiten für die Sicherheitsbehörden.

  Je nach Ausgestaltung des digitalisierten Reisedokuments könnten exemplarisch zusätzliche Hintergrundinformationen, wie Einreisehistorien oder Visa-Status, hinterlegt werden, um die Identität und Rechtmäßigkeit der reisenden Person zu verifizieren. Dies ermöglicht es Behörden zudem, schneller und effektiver auf verdächtige Aktivitäten zu reagieren und mögliche Risiken für die öffentliche Sicherheit zu minimieren. Verbesserungen sind insbesondere in den Bereichen wie der Dokumentenkriminalität, Menschenhandel, Menschenschmuggel, Geldwäsche, Terrorismus etc. zu erwarten.

– In Verbindung mit E-Wallets sind zusätzliche Effizienzgewinne für die Sicherheitsbehörden möglich.

  Nach allgemein zugänglichen Informationen sollen künftig in sogenannten E-Wallets sowohl Personal- und Reisedokumente als auch Führerscheine digitalisiert mitgeführt werden können und bei Kontrollen, und damit auch Grenzkontrollen, zur Verwendung gelangen. Nach Einschätzung des Bayerischen Landeskriminalamts (BLKA) ist dieses zur Erleichterung des Reiseverkehrs und der Kontrolltätigkeit grundsätzlich zu befürworten. Jedoch muss sichergestellt werden, dass nur auf Echtheit geprüfte Dokumente in diese elektronischen Brieftaschen hochgeladen werden können bzw. müsste die zur Verwendung gebrauchte Anwendung selbstständig eine Echtheitsprüfung der hochzuladenden Dokumente durchführen. Aktuell können nur tatsächlich physikalisch vorliegende Dokumente vollständig und umfassend einer Echtheitsprüfung unterzogen werden. Eine Digitalisierung von Identitätsdokumenten kann hier künftig Vorteile bzgl. der Fälschungssicherheit und der Möglichkeit zur automatisierten Echtheitsprüfung bringen. Voraussetzung hierfür ist aber – analog zu klassischen Sicherheitsmerkmalen – die fachgerechte Umsetzung. Diese muss hohen Anforderungen genügen, um die Nachahmung/Manipulation durch Fälscher zu erschweren. Das gilt sowohl gleichermaßen für das Einbringen zusätzlicher digitaler Sicherheitsmerkmale in klassische Dokumente (z. B. elektronisch prüfbare Chips, online prüfbare Barcodes usw.) als auch für vollständig digitale (Identitäts-)Nachweise (z. B. mithilfe von Smartphones oder Chipkarten).

– Der sicherheitsrechtliche Mehrwert von digitalen Reisedokumenten ist nur realisierbar bei entsprechender personeller und sachlicher Ausstattung der Kontrollbehörden.

  Es sollte von Anfang an berücksichtigt werden, dass entsprechende Möglichkeiten (und insbesondere im polizeilichen Bereich auch hochmobile Möglichkeiten) zur Prüfung der digitalen Nachweise geschaffen werden müssen, z. B. an Grenzen, Flughäfen, bei Polizeibehörden oder Verwaltungsämtern. Die elektronische Dokumentenprüfung stellt hier ein gutes Hilfsmittel dar, jedoch ist derzeit eine abschließende Echtheitsbewertung nur durch finale visuelle Prüfung dokumentensachkundiger Fachpersonen möglich.

– Die technischen Voraussetzungen zur Umsetzung eines digitalen Reisedokuments müssen europaweit, unter Beachtung der bereits vorhandenen bzw. zu beschaffenden Infrastruktur, definiert werden.

– Das Verfahren zur Ausstellung von digitalen Dokumenten muss sicher sein.

  Beispielhaft wird die Einrichtung einer sogenannten E-Wallet bereits bei Ausstellung/Aushändigung entsprechender Dokumente durch die Ausstellungsbehörden präferiert bzw. es sollte vor Verwendung eines Dokuments in einer

E-Wallet eine gesicherte Echtheitsprüfung vorangestellt werden. Hier darf zudem darauf hingewiesen werden, dass aus dokumentenfachlicher Sicht zwingend die Lichtbilderstellung künftiger digitaler Dokumente ausschließlich bei den autorisierten Ausstellungsbehörden und durch persönliche Vorsprache – Stichwort Morphing (computergeneriertes Lichtbild einer Person, z. B. zur Fälschung oder Verfälschung einer Identität) – erfolgen sollte. Lediglich elektronisch oder physikalisch übermittelte Lichtbilder ohne nachträglichen, ggf. elektronisch unterstützten, Lichtbild-Echtbildvergleich stellen aus dokumentenfachlicher Sicht ein erhebliches Sicherheitsrisiko dar.

– Es ist eine besondere datenschutzrechtliche Vorsorge zu treffen.

  Aufgrund der Verarbeitung hochsensibler (biometrischer) Daten nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ist ein besonderes Augenmerk auf die Sicherheit der Daten zu legen. Es sind daher geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere die Gefahren eines Identitätsdiebstahls zu minimieren. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat sich bereits bei der Einführung der Online-Ausweisfunktion des Personalausweises mit der Thematik befasst. Die Argumente sind u. E. auf die vorgesehene Digitalisierung der Reisedokumente übertragbar: „Die Sicherheit des Ausweises allein reicht aber nicht aus, um den Datenschutz zu gewährleisten…. [Es] sind auch die Systeme, die auf den Ausweis elektronisch zugreifen und die Daten weiterverarbeiten, kritisch zu sehen. Bei der Verwendung der eID-Funktion ist dies in der Regel der PC des Nutzers mit angeschlossenem Lesegerät, der den bekannten Angriffsszenarien wie Viren und Spyware ausgesetzt ist. Ein sicherer PC ist Grundvoraussetzung für einen sicheren Einsatz der eID Funktion über das Internet.“ (24. Tätigkeitsbericht 2010 des BayLfD, Nr. 2.3.1)

  Im Übrigen ist darauf hinzuweisen, dass die Sicherheit der personenbezogenen Daten der Reisedokumente keinesfalls allein oder wesentlich von der IT-Sicherheit des jeweiligen Endgeräts abhängen darf, auf dem das Reisedokument gespeichert wird.

  Die Verwendung sicherer Kommunikationswege zur Unterbindung missbräuchlicher Datenzugriffe ist sicherzustellen. Um Datenschutzverletzungen und Missbrauch zu verhindern, müssen klare Richtlinien und Verfahren für den Umgang mit persönlichen Daten festgelegt werden, um die Privatsphäre der Bürgerinnen und Bürger zu schützen. Die Kontrolle über die Daten muss bei den betroffenen Personen liegen, um sicherzustellen, dass ihre Daten nur für autorisierte Zwecke verwendet werden.

  Soweit biometrische Daten, insbesondere biometrische Fotos und Fingerabdrücke in den Dokumenten verarbeitet werden sollen, muss diese Befugnis gemäß Art. 9 DSGVO gesondert und konkret geregelt werden. Für polizeiliche Zwecke lässt sich dies aus Gründen des besonderen öffentlichen Interesses begründen, es wäre aber wohl eine konkrete Zweckbindung für diese Daten sowie klare Schutzmaßnahmen gegen Missbrauch erforderlich. So eine Regelung würde dann voraussichtlich (nach den Maßstäben des Europäischen Datenschutzausschusses) auch die Erforderlichkeit einer Datenschutz-Folgenabschätzung nach sich ziehen, welche idealerweise bereits im Rahmen eines EU-Rechtsakts durchgeführt werden sollte. Die Vorgaben der noch nicht abschließend konsolidierten KI-Verordnung zur biometrischen Fernidentifizierung müssten ggf. beachtet werden.

– Digitale Reisedokumente haben Potenzial für mehr Datensicherheit.

  Eine verstärkte Digitalisierung auch unter Verwendung biometrischer Daten bringt aus Datenschutzsicht aber nicht nur Risiken mit sich: Sie trägt insbesondere auch in erheblichem Maß dazu bei, dass Datenpannen vermieden werden und so der Grundsatz der Datenrichtigkeit gewährleistet wird. Insbesondere kann dadurch verhindert werden, dass Unschuldige ins Visier von Polizeibehörden geraten, weil entweder ihre Daten missbraucht werden oder Daten nicht-automatisiert/manuell falsch übertragen werden. Die sichere Authentifizierung von Personen (häufig sogar über mehrere Faktoren) ist gerade zum Schutz von

personenbezogenen Daten sowohl beim Zugang zu diesen als auch bei einer Änderung regelmäßig auch im allgemeinen Geschäftsverkehr erforderlich, bei polizeilichen Maßnahmen muss an die Authentifizierung ein besonders hoher Maßstab angelegt werden.

2. Blickwinkel Grenzkontrollen

– Der reibungslose grenzüberschreitende Reiseverkehr sowie eine reibungslose Passagierabfertigung können grundsätzlich mit digitalen Reisedokumenten gefördert werden.

Schon heute wird eine effizientere und sicherere Grenzkontrolltechnik angestrebt. Bei einer Digitalisierung von Reisedokumenten müssten die bestehenden Prozesse dann an die dann neuen Gegebenheiten angepasst werden.

Gemäß Verwaltungsabkommen zwischen dem Bundesministerium des Innern und der Bayerischen Staatsregierung über die Wahrnehmung von Aufgaben des grenzpolizeilichen Einzeldienstes in Bayern vom 17. April 2008 führt die Bayerische Polizei insbesondere an den zwei Verkehrsflughäfen Nürnberg und Memmingen und zehn Verkehrslandeplätzen mit Status Grenzübergangsstellen (GüG) Grenzkontrollen durch.

Drittstaatsangehörige, aber auch Angehörige eines Schengen-Staates, unterliegen bei der Ein- bzw. Ausreise in den/aus dem Schengenraum der Verpflichtung, sich einer Grenzübertrittskontrolle zu unterziehen. Der Umfang der grenzpolizeilichen Kontrolle steht in Abhängigkeit von der jeweiligen Situation (Ein-/Ausreise) und der Statusfeststellung des Reisenden (Drittstaatsangehöriger oder Freizügigkeitsberechtigter).

Bereits jetzt wird im Rahmen der „Smart Borders Initiative“ der Europäischen Kommission zur Verbesserung des Managements der Schengen-Außengrenzen sowie der „Erneuerung der europäischen Informationslandschaft in den Bereichen Sicherheit, Migration und Grenzen“ der Einsatz von leistungsstarker Hard- und Software erforderlich. Um grenzpolizeiliche Kontrollprozesse zu optimieren, aber auch zur Einführung eines gemeinsamen Grenzkontrollstandards in der Bundesrepublik Deutschland hat sich die Bayerische Polizei hier entschieden, die Grenzkontrolltechnik der Bundespolizei zu übernehmen. Die birgt u. a. auch Vorteile im Hinblick auf die Einführung von EES (Entry-Exit-System) und ETIAS (European Travel Information and Authorisation System).

Eine Inbetriebnahme der Grenzkontrolltechnik der Bundespolizei an den Flughäfen Nürnberg und Memmingen sowie an zehn weiteren Verkehrslandeplätzen ist, abhängig von noch zu unterzeichnenden Vereinbarungen mit der Bundespolizei und dem Bundesverwaltungsamt, noch in diesem Jahr vorgesehen.

Mit Inbetriebnahme der in Rede stehenden Technik steht neben der eingesetzten Hardware (bspw. Fingerscanner, Dokumentenprüfgerät, Gesichtserkennungssysteme) eine leistungsstarke Software zur Verfügung. Dadurch wird eine Bündelung aller notwendigen Datenbanken, die automatisierte Übernahme von eingelesenen Ausweisdaten und Darstellung in einer übersichtlichen und intuitiv zu bedienender Oberfläche den Grenzkontrollbeamten zur Verfügung gestellt. Dies führt nachhaltig zu einer Verbesserung in der Qualität der grenzpolizeilichen Sachbearbeitung (z. B. Vermeidung von Schreibfehlern, Einmalerfassung und schnellen Zugriff auf Daten bei der Ausstellung von Ausnahmevisa). Weiterhin lässt der Einsatz der in Rede stehenden Grenzkontrolltechnik eine Optimierung der zeitlichen Abläufe erwarten.

Zusammenfassend führen die o. g. Maßnahmen insgesamt zu einer Minimierung der Wartezeiten sowie zu einer Erhöhung der Sicherheit und Effizienz an den Grenzübergangsstellen unter Gewährleistung des Schutzes der personenbezogenen Daten und Grundrechte des betroffenen Personenkreises. Dies kommt sowohl den Drittstaatsangehörigen als auch insbesondere den EU-Bürgern zugute und fördert eine reibungslose Passagierabfertigung. Die Einführung der Grenzkontrolltechnik der Bundespolizei ist ein weiterer Beitrag zur stärkeren Digitalisierung der Grenzen.

3. Blickwinkel Pass- und Personalausweiswesen

– Digitale Pässe und Personalausweise sollten wie die Papierdokumente als hoheitliche Aufgabe bei den Pass- und Personalausweisbehörden in den Gemeinden verbleiben und nicht privatisiert werden, damit Vertrauen in diese Dokumente besteht und die bewährten etablierten Verfahren und Strukturen genutzt werden können. Denn es gilt Identitätsmissbrauch vorzubeugen und die Bürgerinnen und Bürger für eine Verwendung zu gewinnen.
– Für die Ausstellung bzw. Herstellung digitaler Dokumente wird nach wie vor eine persönliche Vorsprache der späteren Dokumenteninhaber erforderlich sein, um eine zweifelsfreie Identitätsfeststellung sicherzustellen.
– An die Ausgestaltung der Dokumente werden in Bezug auf das Missbrauchspotenzial bzw. die Dokumentenfälschung und die Sicherheit der Daten sowie eine effektive Kontrolltätigkeit hohe Anforderungen zu stellen sein, die noch in europarechtlichen und nationalen Regelungen festzulegen sind.
– Der Umstand, dass solche Dokumente auch von außerstaatlichen Stellen (z. B. Banken, Hotelgewerbe) akzeptiert werden sollten, um eine flächendeckende Verbreitung und Nutzung zu erreichen, könnte ggf. weiteren zu berücksichtigenden Gestaltungsbedarf auslösen.
– Auf physische Reisedokumente wird mit Blick auf die Bürgerfreundlichkeit und die Einreisebestimmungen von Staaten außerhalb der EU nicht verzichtet werden können. Deshalb wird hinsichtlich der noch festzulegenden Gültigkeitsdauer von digitalen – optionalen – Dokumenten ein Gleichlauf mit Papierdokumenten anzustreben sein, damit der hieraus resultierende Verwaltungsaufwand bewältigt werden kann.
– Für die Ausstellung und Verwendung digitaler Dokumente wird sich ein enormer zusätzlicher Verwaltungsaufwand ergeben, dessen Finanzierbarkeit insbesondere auf Ebene der Länder und Kommunen sichergestellt werden muss.

Der Beschluss des Bayerischen Landtags wird unmittelbar an die Europäische Kommission, das Europäische Parlament, den Ausschuss der Regionen und den Deutschen Bundestag übermittelt.

Die Präsidentin

Ilse Aigner