Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)268 G

STIFTUNG DATENSCHUTZ

Ass. Jur. Kirsten Bock

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Stellungnahme

zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat
zum Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens
BT-Drucksachen 20/6519, 20/7076

Die Bundesregierung hat dem deutschen Bundestag den „Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens“ vorgelegt. Änderungen durch das Artikelgesetz sollen für das Passgesetz (Art. 1), Das Personalausweisgesetz (Art. 2), des eID-Karte-Gesetzes (Art. 3), des Aufenthaltsgesetzes (Art. 4) sowie des Beurkundungsgesetzes (Art. 5) erfolgen. Durch Änderungen im Europarecht zur Gültigkeitsdauer von Kinderreisepässen sind diesbezügliche Änderungen im Passgesetz erforderlich. Darüber hinaus sollen u.a. Änderungen vorgenommen werden, um rechtliche Voraussetzungen für Standardisierungen zur Kommunikation von Daten aus Identitätsdokumenten sowie um weitere Möglichkeiten zur Kontrolle und Weiterverarbeitung dieser Daten nach einer Identitätsfeststellung zu schaffen. Ziel des Gesetzes ist die Anpassung der Verfahren an die „Möglichkeiten der modernen Datenerfassung“.[1]

Zu dem Gesetzentwurf hat der Bundesrat und die Bundesregierung in einer Gegenäußerung Stellung genommen.[2] Zudem liegt ein Änderungsantrag der Fraktionen der SPD , Bündnis 90 / Die Grünen und der FDP im 4. Ausschuss (Innenausschuss) des Deutschen Bundestages zu dem Gesetzentwurf der Bundesregierung zur Modernisierung des Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesens[3] sowie ein Antrag auf eine Entschließung des 4. Ausschusses für Inneres und Heimat[4] vor.

Diese Stellungnahme beschränkt sich auf datenschutzrechtliche Aspekte und erfolgt angesichts der kurzen Frist thesenartig zusammengefasst:

---

[1] Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens, BT-Drs. 20/6519, S. 2, 17.
[2] Drucksache 20/6519.
[3] Ausschussdrucksache 20(4)257.
[4] Ausschussdrucksache 20(4)258.

1. Verarbeitungsbefugnisse von personenbezogenen Daten aus Ausweisdokumenten eingrenzen

Der vorgelegte Gesetzentwurf zielt darauf ab, die Verarbeitungsbefugnisse von öffentlichen Stellen für die auf Pässen und Personalausweisen aufgedruckten und den im Chip der Dokumente gespeicherten Daten zu erweitern. Bisherige Beschränkungen sollen gelockert werden, um den Zugriff auf diese Daten für alle öffentlichen Stellen, und nicht nur für Echtheits- und Identifizierungszwecke, sondern auch für weitere Zwecke zu ermöglichen. Für eine solche Erweiterung der Befugnisse gilt grundsätzlich, dass nur solche Daten ausgelesen und gespeichert werden dürfen, die für die Zwecke der Aufgabenerfüllung erforderlich sind (Grundsatz der Zweckbindung, Art. 5 Abs. 1 lit. b, Art. 6 Abs. 1 lit. c, Abs. 3 s. 2, Abs. 4 DSGVO). Kann technisch nicht sichergestellt werden, dass nur erforderliche Daten verarbeitet werden, weil nur ein kompletter Datensatz ausgelesen werden kann, ist sicherzustellen, dass zumindest eine Speicherung nicht erforderlicher Informationen unterbleibt.

Durch die Gesetzesänderung soll es den Polizeivollzugsbehörden, der Zollverwaltung sowie den Pass-, Personalausweis- und Meldebehörden sowie den öffentlichen Stellen mit Zustimmung der sich ausweisenden Person ermöglicht werden, die bei einer Identitätsfeststellung aus dem Chip erhobenen Daten aus Pässen und Personalausweisen automatisiert zu speichern und damit für eine weitere Verwendung zu übernehmen, ohne dass die gesetzlichen Regelungen die weitere Verwendung näher bestimmen oder einschränken. Der Grundsatz der Zweckbindung als Kernelement des Grundrechts auf Datenschutz aus Art. 8 GRCh verlangt jedoch stets eine hinreichend konkrete Beschreibung des Zweckes des Grundrechtseingriffs, d.h. der Verarbeitung personenbezogener Daten. Dies gilt gem. Art. 6 Abs. 3 S. 2, Abs. 4 DSGVO auch für Regelungen durch die Mitgliedstaaten. Bereits der Bundesbeauftragte für Datenschutz hat in seiner Stellungnahme[5] darauf hingewiesen, dass weitergehende Regelungen hinsichtlich der Zwecke und Dauer der Verarbeitung erforderlich sind. So müssen insbesondere

- ausdrückliche gesetzliche Rechtsgrundlagen im Fachrecht vorliegen, die eine Erhebung und Weiterverarbeitung gestatten,
- die weiteren Zwecke unmittelbar vorliegen und es darf keine Verarbeitung auf Vorrat erfolgen,
- die erhobenen Daten für die weiteren Zwecke zwingend erforderlich sein und keine darüberhinausgehenden Daten verarbeitet werden,
- eine über die Dauer der weiteren Zwecke hinausgehende Verarbeitung ausgeschlossen werden und
- die betroffene Person über die weitere Verarbeitung informiert werden.

2. Keine Speicherung biometrischer Daten

Die Ausnahme der Speicherung in § 16a Abs. 2 Satz 1 PassG-E und § 16 Abs. 2 PAuswG-E der im Chip gespeicherten biometrischen Daten ist zu begrüßen. Eine - wie vom Bundesrat vorgeschlagene - Streichung der Ausnahme der Speicherung biometrischer Daten hätte einen schweren Grundrechtseingriff zur Folge, der einer besonderen Rechtfertigung bedarf. Gem. Art. 9 Abs. 2 DSGVO ist an die Verarbeitung besonderer Kategorien personenbezogener

[5] Stellungnahme des Bundesbeauftragten für Datenschutz und Informationsfreiheit zum Entwurf eines Gesetzes zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens vom 2.06.2023.

Daten, zu denen die biometrischen Daten zählen, besonders hohe Anforderungen zu stellen. § 48 BDSG lässt eine solche Verarbeitung nur zu, wenn sie zur Aufgabenerfüllung zwingend erforderlich ist. Der in der Begründung des Bundesrates genannte Beispielsfall (Vorliegen des Passes bei Nichtauffindbarkeit der Person) lässt eine Verhältnismäßigkeit des Eingriffs durch eine allgemeine Speicherbefugnis nicht erkennen.

3. Verarbeitung sicher gestalten

Es wird begrüßt, dass der Gesetzentwurf Echtheits- und Identitätskontrollen zumindest über **öffentliche Kommunikationswege ausgeschlossen** werden. Das Ansinnen des Bundesrates, Echtheits- und Identitätskontrollen auch über öffentliche, gesicherte Kommunikationswege zuzulassen, verkennt, dass dabei der für diese Daten notwendige hohe Schutzbedarf, bei der Nutzung von Smartphones und Apps nicht durchgängig gewährleistet werden kann. Auch eine Beschränkung auf die Nutzung von Diensttelefonen kann einen hohen Schutzbedarf insbesondere für die Vertraulichkeit und die Sicherstellung der Zugriffsberechtigung nicht gewährleisten.

Der Bundesrat möchte weitergehend auch eine sichere oder automatisierte Verarbeitung der Daten aus dem sichtbaren Bereich zulassen. Damit wären technische Möglichkeiten wie etwa das Scannen, Kopieren oder Fotografieren zulässig. Insofern wäre eine automatisierte Verarbeitung zumindest auf den maschinenlesbaren Bereich zu begrenzen. Weiterhin zu beachten ist, dass bei einem optischen Auslesen die Fehleranfälligkeit höher ist, als bei einem Auslesen aus dem Chip. Soll ein optisches Auslesen überhaupt zugelassen werden, fehlen an dieser Stelle, wie auch insgesamt, **Regelungen zur Intervention** durch die verarbeitende Stelle wie auch durch die Betroffenen selbst. Insbesondere Art. 25 DSGVO verlangt technische und organisatorische Maßnahmen zur Umsetzung der Grundsätze aus Art. 5 Abs. 1 DSGVO i.V.m. Art. 16 DSGVO.

Anzumerken ist zudem, dass für die Sicherheit der Verarbeitung ein pauschaler Verweis auf die Art. 24, 25 und 32 DSGVO sowie auf Verschlüsselungs- und Pseudonymisierungsmaßnahmen unzureichend sind, um eine Gewährleistung des Grundrechtsschutzes im Anwendungsbereich der zu ändernden Gesetze sicherzustellen. Wünschenswert wäre die weitere Ermöglichung von **Wahrheitswertabfragen** in Ausweisdokumenten. Solche Abfragen (z.B. Altersverifizierungen) erlauben die Bestätigung (wahr/falsch) eines bereits bekannten Datums und sind daher besonders datensparsam. Informationen, die nicht benötigt werden oder nicht bekannt gegeben oder verwendet werden dürfen, wie etwa die Seriennummer, würden gar nicht erhoben und müssten dann auch nicht nachträglich gelöscht werden.

4. Kein automatisierter Lichtbildabruf für öffentliche Stellen

Der Gesetzentwurf soll es öffentlichen Stellen ermöglichen, auf das biometrische Lichtbild im Chip zuzugreifen, um die Identität der ausweisführenden Person zu prüfen, wenn dies durch Gesetz oder aufgrund eines Gesetzes ermächtigt wird und die Pass- oder Personalausweisinhaber*in dem zustimmt. Zwar liegt mit dem Pass- und Personalausweisdatenabrufverordnung ein einheitlicher Kommunikationsstandard vor, doch durften bislang nicht alle öffentlichen Stellen auch einen automatisierten Lichtbildabruf durchführen. Dies war bislang nur für bestimmte Sicherheitsbehörden zulässig, die dies zwingend für ihre Aufgabenerfüllung benötigten.

Eine Beschränkung des Online-Abrufs von Lichtbildern war einstmals eingeführt worden, um zu verhindern, dass die verpflichtend in Pässen und Personalausweisen aufgenommenen biometrischen Gesichtsbilder zur Massenüberwachung genutzt werden.[6] Schon bei der Einführung eines auf Sicherheitsbehörden begrenzten Zugriffs bestanden erhebliche **grundrechtliche Bedenken**. So führte beispielsweise Konstantin von Notz aus, dass die „Einführung des automatisierten Pass- bzw. Personalausweisphotoabgleichs durch alle bundesdeutschen Geheimdienste [...] nichts anderes als der offene Einstieg in eine bundesweite biometrische Bilddatenbank aller Bundesbürger" sei.[7]

Biometriedaten enthalten Identifizierungsmerkmale, die mittels Gesichtserkennungssystemen für Überwachungsmaßnahmen besonders geeignet sind. In der Vergangenheit wurde wiederholt versucht, mit Hilfe von Videoüberwachungsanlagen und dem elektronischen Abgleich von Gesichtsbildern öffentlicher Raum großflächig zu kontrollieren.[8]

Die Verarbeitung biometrischer Daten stellt einen schwerwiegenden Eingriff in die Rechte der betroffenen Person dar. Daher müssen erhebliche öffentliche Interessen erfüllt sein, um einen solchen Zugriff zu rechtfertigen und besonders hohe technische Anforderungen an die Sicherheit der Übermittlung gestellt werden. Der Zugriff sollte insofern nur solchen Stellen gewährt werden, die klar geregelte gesetzliche Aufgaben von erheblichem öffentlichem Interesse wahrnehmen und dafür einen Zugriff auf biometrische Lichtbilder zwingend benötigen. Für andere öffentliche Stellen bietet der Personalausweis schon jetzt die Möglichkeit, eine Person zuverlässig zu identifizieren.

5. Einführung einer registerführenden Behörde

Bei Wohnungsumzügen in einen anderen räumlichen Zuständigkeitsbereich sind die bisherige sowie die neue Behörde über den neuen Wohnsitz zu informieren. Als sog. registerführende Behörde, soll nunmehr für Pass- Personalausweisangelegenheiten und eID-Karte diejenige Behörde zuständig sein, die das Ausweisdokument ursprünglich ausgestellt hat. Damit werden zukünftig nach einem Umzug die örtlich zuständige Behörde und die registerführende Behörde auseinanderfallen und eine **Doppelzuständigkeit** entstehen. Da die Register stets aktuell zu halten sind, macht diese Doppelzuständigkeit eine ganze Reihe von Übermittlungs- und Abrufvorgängen zwischen den Behörden notwendig, für die der Gesetzentwurf die rechtlichen Grundlagen schaffen soll. Die Gründe für diese Regelung sind aus praktischer Sicht wenig nachvollziehbar, da zum einen viele Übermittlungen auch zu einer erhöhten Fehleranfälligkeit führen und zum anderen doch die Registermodernisierung gerade eine medienbruchfreie Kommunikation zwischen den Behörden sicherstellen soll. Es ist kaum zu erwarten, dass die technischen Voraussetzungen, die zur Umsetzung der Neuregelung erforderlich sind, schneller und fehlerfreier erfolgen kann, als die Registermodernisierung.

Auf lange Sicht würde eine solche Änderung dazu führen, dass die registerführende Behörde zukünftig die Behörde des Geburtsortes ist, bzw. die Behörde, bei der Eltern erstmalig einen Ausweis beantragen. Besonders schwerwiegend kann diese Regelung für Personen werden, die aufgrund einer Bedrohungssituation ihren ursprünglichen Heimatort verlassen müssen oder

[6] Peter Schaar, Mai 2017, https://www.eaid-berlin.de/das-neue-big-brother-gesetz/
[7] https://netzpolitik.org/2017/morgen-im-bundestag-automatisierter-zugriff-auf-biometrische-passbilder-fuer-alle-geheimdienste/
[8] Ibid.

aufgrund von Mißbrauchserfahrungen umziehen. Fälle, in denen in der Regel eine Auskunftssperre im Einwohnermelderegister eingetragen ist, werden zukünftig weiterhin im Register diese Ursprungsortes geführt. Dies kann zu einer hohen psychischen Belastung der Betroffenen führen. Zudem könnte die Einführung einer registerführenden Stelle Marginalisierungen von Bevölkerungsgruppen verstärken, da über die registerführende Behörde zukünftig die Zugehörigkeit zu einer Volks- oder Gesellschaftsgruppe naheliegen könnte. **Intersektionale Benachteiligungen** würden so verstärkt werden.

Für den Informationsaustausch zwischen den Behörden fehlen bislang standardisierte Nachrichtenformate und standardisierte Kommunikationsprozesse. Standardisierungen im Bereich der Datenübermittlung sind im Rahmen der Registermodernisierung grundsätzlich zu begrüßen. Ein Augenmerk sollte hier auf **offene und verbindliche Standards** gelegt werden. Dies sowie die Einbindung in das Konzept der Registermodernisierung - hier vor allem dem Once-Only-Prinzip - lässt der Gesetzentwurf bislang nicht ausdrücklich erkennen. Insofern greift die Regelung der Registermodernisierung vor und schafft Grundlagen für zusätzliche Verarbeitungsvorgänge statt solche zu reduzieren.

Begrüßt wird der Ansatz zur Aufrechterhaltung einer **dezentralen, föderalen Registerstruktur**. Eine dezentrale Registerhaltung ist am ehesten geeignet, möglichen Angriffsszenarien[9] standzuhalten. Zum einen, sind kleine Registerbestände weniger attraktive Angriffsziele, weil ein möglicher Schaden nur begrenzte Auswirkungen hat. Andererseits können in einer föderalen Registerstruktur Register selektiv aus dem Verbund genommen werden und die Integrität des Verbundes sowie der einzelnen Register wirksamer und als Teil einer verwaltungskritischen Infrastruktur resilient geschützt werden.

6. Datenschutzcockpit als Steuerungswerkzeug

Zu begrüßen ist der Antrag der Regierungsparteien[10], das Datenschutzcockpit nicht nur als Transparenz-, sondern auch als Steuerungswerkzeug für die Bürgerïnnen auszubauen. Erst die Implementierung von Interventions- und Steuerungsmöglichkeiten gewährleistet einen umfassenden Grundrechtsschutz und macht Betroffenen zu Akteuren. Das diese Gewährleistung aber erst in einer dritten Ausbaustufe des Datenschutzcockpits erfolgen soll, erscheint zu spät. Das Grundrecht auf Datenschutz aus Art. 8 GRCh beinhaltet das durch das BVerfG konkretisierte Recht auf informationelle Selbstbestimmung. Diesem Recht wird nur dann genüge getan, wenn einhergehend mit einer Vernetzung der Register und erweiterten digitalen Zugriffs- und Verarbeitungsfunktionalitäten der Verwaltung auch die Betroffenen über die Transparenz hinaus ebensolche Möglichkeiten erhalten, Verwaltungshandeln anzustoßen, zu kontrollieren und zu intervenieren.

[9] Die Prüfsteine aus der Zivilgesellschaft, Superrr Lab, https://feministtechpolicy.org/fallbeispiele/pruefsteine-regmod/
[10] Ausschussdrucksache 20(4)258.