EJPD
Staatssekretariat für Migration SEM
sandrine.favre@sem.admin.ch
helena.schaer@sem.admin.ch
fedpol
simone.rusterholz@fedpol.admin.ch
anna.wolf@fedpol.admin.ch

Sozialdemokratische Partei
der Schweiz

Theaterplatz 4
Postfach · 3001 Bern

Telefon 031 329 69 69
Telefax 031 329 69 70

info@spschweiz.ch
www.spschweiz.ch

Bern, 9. Januar 2020

Stellungnahme zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität (Weiterentwicklungen des Schengen-Besitzstands)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Zustellung der Vernehmlassungsunterlagen zum Bundesbeschluss über die Genehmigung und die Umsetzung der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität. Gerne nehmen wir dazu Stellung.

Zusammenfassung: Die SP unterstützt die Übernahme der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität, fordert in der Umsetzung aber deutliche Nachbesserungen: Grundrechts- und Datenschutz müssen gestärkt, die Normendichte erhöht und zum Schutz der Freiheitsrechte eine unabhängige und ausreichend dotierte Aufsichtsbehörde eingerichtet werden. Zudem sind mit der EU gleichwertige Verfahren zu den Qualitätssicherungs- und Evaluationsprozessen vorzusehen.

Für die SP ist es inakzeptabel, dass der Bundesrat den objektiv vorhandenen grossen Spielraum der Schweiz zur Umsetzung von Schengen-Recht einmal mehr einseitig zugunsten der «Festung Europa», des repressiven Überwachungsstaates und zulasten der Freiheit der Bürger und Bürgerinnen wahrnimmt. Die Tatsache, dass bei einer Ablehnung einer Schengen-Vorlage durch die Schweiz sehr viel auf dem Spiel stehen würde, darf nicht dazu missbraucht werden, dass der Bundesrat mittels eines schwer verständlichen, spröd-juristischen Sachzwangdiskurses eine offene politische Debatte über Spielräume zugunsten einer Grundrechts-schonenden Umsetzung zu vermeiden versucht.

Die vorgesehene Interoperabilität birgt bedeutende Risiken

Ziel der Vorlage besteht darin, die Schweiz an eine im Aufbau begriffene Infrastruktur gewaltiger Mengen höchst sensibler Daten anzudocken. Rechtliche Grundlage bilden zwei Verordnungen, die Rat und Parlament der EU im Mai 2019 nach dreijähriger Vorbereitung verabschiedet haben. Ihr Ziel ist es, die Interoperabilität zwischen neun Datenbanken aufzubauen: zu drei bestehenden und drei im Aufbau befindlichen Informationssystemen der EU im Bereich Asyl, Migration und Sicherheit sowie zu Europol-Daten und zwei Interpol-Datenbanken. Die beiden EU-Verordnungen sind fast identisch. Eine getrennte Regelung «Grenze» bzw. «Polizei» war nötig, weil nicht alle Informationssysteme auf Schengen-Recht beruhen und je unterschiedliche Staatengruppen daran teilnehmen.

Kaum abschätzbare Folgen: Weil bestehende Informationssysteme weiterentwickelt und andere erst neu aufgebaut werden, werden viele technische Normen und Folgeerlasse erst in den nächsten Jahren erarbeitet. Die Interoperabilität erfordert zudem den Aufbau vier so genannter «Komponenten». Die Auswirkungen des Gesamtsystems lassen sich entsprechend noch kaum abschätzen. Umso wichtiger ist die Einrichtung begleitender Evaluierungsverfahren. Die vier neuen «Komponenten» bilden ihrerseits vier gigantische, neu aufzubauende Datenbanken bzw. Plattformen:

1. Das *Europäische Suchportal* (European Search Portal, ESP) ermöglicht mit einer Abfrage die gleichzeitige Suche in neun Informationssystemen: In sechs EU-Datenbanken (Schengener Informationssystem SIS, Visa-Informationssystem VIS, Fingerabdruck Datenbank von Asylsuchenden Eurodac, Einreise/Ausreisesystem EES, Reiseinformations- und -genehmigungssystem ETIAS und Strafregisterinformationssystem für Drittstaatsangehörige ECRIS-TCN) sowie den Europol-Daten und zwei Interpol-Datenbanken. Die Schweiz hat momentan Zugang zu den fünf erstgenannten EU-Datenbanken, aber noch nicht direkt zum ECRIS-TCN und den Europol/Interpol-Daten. Dies wird zurzeit geprüft bzw. angestrebt. Die Inbetriebnahme des ESP ist auf 2023 geplant.
2. Der *Gemeinsame Dienst für den Abgleich biometrischer Daten* (Biometric Matching Service, BMS) speichert systematisch die mathematischen Abbilder («templates») aller biometrischen Daten aus dem SIS, VIS, Eurodac und EES. Mittels eines biometrischen Datensatzes können so mit einer einzigen Anfrage gleichzeitig alle vier Datenbanken durchsucht werden (in Betrieb 2021).
3. Der *Gemeinsame Speicher für Identitätsdaten* (Common Identity Repository, CIR). Alle Identitätsdaten aus VIS, Eurodac, EES, ETIAS und ECRIS-TCN werden im CIR gespeichert einschliesslich Daten zu Reisedokumenten und biometrische Daten von Drittstaatenangehörigen (in Betrieb 2022).
4. Der *Detektor für Mehrfachidentitäten* (Multiple Identity Detector, MID). Der MID ist erforderlich, weil polizeiliche Identitätsdaten aus dem SIS aus rechtlichen Gründen nicht in den CIR aufgenommen werden können (SIS ist strafrechtlich, CIR nicht). MID deckt Zusammenhänge zwischen neuen und bestehenden Identitätsdaten in allen EU-Informationssystemen auf (in Betrieb 2023).

Zusätzlich wird ein *Zentraler Speicher für Berichte und Statistiken* (Central Repository for Reporting and Statistics, CRRS) eingerichtet. Dieser wird aus allen genannten Datenbanken systematisch gefüttert. Er speichert also gigantische Mengen höchst sensibler Daten, freilich allein zu Statistikzwecken.

Der Europäische Datenschutzbeauftragte wies in seiner Stellungnahme[1] auf folgende Risiken hin:

Immenses Schadenpotenzial: Aufgrund der Grösse der zentralen Datenbanken CIR und BMS und der hochsensiblen Art der darin gespeicherten Daten kann jeder Verstoss gegen Datenschutzvorschriften einen immensen Schaden zufügen, und zwar potenziell für Millionen von Menschen.

Erhöhte Vulnerabilität: Je grösser Datenbanken, desto attraktiver werden sie für Hackerangriffe und Geheimdienste beispielsweise aus den USA, Russland, China oder Nordkorea.

Unverhältnismässiges Misstrauen gegen Drittstaatangehörige: Die EU-Verordnungen gehen davon aus, dass Drittstaatsangehörige die Sicherheit a priori bedrohen und Identitätsbetrug weit verbreitet sei. Die mitwirkenden Staaten speichern in den Systemen konsequent sämtliche Daten von Drittstaatsangehörigen, unabhängig davon, ob es sich um blosse Reisende wie Touristen und Geschäftsleuten handelt. Um die Verhältnismässigkeit der Massnahme zu überprüfen, forderte der Europäische Datenschutzbeauftragte, zunächst das Ausmass von Identitätsbetrug unter Drittstaatsangehörigen abzuklären. Diese Zahlen sind nie vorgelegt worden und fehlen auch im erläuternden Bericht.

Verstoss gegen den Grundsatz der Zweckbindung: Laut Artikel 20 sind Abfragen im zentralen Speicher für Identitätsdaten CIR bereits erlaubt, «wenn Zweifel an den von einer Person vorgelegten Identitätsdaten bestehen». Derart vage Kriterien könnten, so der Datenschutzbeauftragte, zu einem routinemässigen Abruf der Daten führen, was gegen den Grundsatz der Zweckbindung verstosse.

[1] Europäischer Datenschutzbeauftragter, Stellungnahme 04/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Grosssystemen der EU
https://edps.europa.eu/sites/edp/files/publication/18-04-16_edps-opinion-on-interoperability_de.pdf

Aushebelung von rechtsstaatlichen Grundsätzen der Strafverfolgung: Artikel 22 erleichtert den Strafverfolgungsbehörden den Zugriff auf Systeme, die nichts mit Strafverfolgung zu tun haben. Strafverfolgungsbehörden aus über dreissig Staaten könnten so Zugriff auf Millionen von Identitätsdaten irgendwelcher Personen erhalten, die allein eine Reise gemacht haben.

Gegenseitige Vertrauensbasis ist brüchig geworden: Die Interoperabilität und der erleichterte Austausch sehr grosser Mengen an hoch sensiblen Daten beruht auf dem Grundsatz des gegenseitigen Vertrauens, einem tragenden Pfeiler der europäischen Zusammenarbeit. Dieses Vertrauen ist aktuell aber erheblich erschüttert, wenn wir an Korruption in höchsten Regierungskreisen[2], Mängel bei der Rechtsstaatlichkeit[3] und der Unabhängigkeit der Justiz[4] in einzelnen Mitgliedstaaten denken. Umso wichtiger sind Sicherungsmassnahmen in der nationalen Umsetzungsgesetzgebung der Schweiz.

Wer das Schengen-Recht einseitig umsetzt, gefährdet die Assoziation an Schengen

JA zur Übernahme der Verordnungen (EU) 2019/817 und 2019/818 zur Interoperabilität: Würde die Schweiz die beiden Interoperabilität-Verordnungen «Grenze» bzw. «Polizei» nicht übernehmen, so würde dies die Schweizer Assoziation an Schengen in höchstem Masse gefährden. Es müsste ein in den Verträgen nicht vorgesehenes Wunder passieren, damit die Assoziation der Schweiz an Schengen nicht nach Ablauf von sechs Monaten automatisch erlöschen würde. Es wäre nicht einmal eine Kündigung erforderlich. Ohne Schengen fiele aber die grossartige Errungenschaft der europaweiten Reisefreiheit dahin. Und ohne Zugriff auf die erwähnten Datenbanken hätte die Schweiz rasch sehr grosse Probleme mit der Sicherheit, der Ein- und Ausreise, der Migration und dem Asylwesen.

NEIN zu einer einseitigen Umsetzung zugunsten der «Festung Europa», des repressiven Überwachungsstaates und zulasten der Freiheit der Bürger und Bürgerinnen: Trotz der erwähnten (und weiteren) Risiken der Interoperabilität-Verordnungen tritt die SP deshalb für ein Andocken der Schweiz an die vier «Komponenten» ein, welche die Interoperabilität gewährleisten. Für die SP ist es aber inakzeptabel, dass der Bundesrat den objektiv vorhandenen grossen Spielraum der Schweiz zur Umsetzung von Schengen-Recht einseitig umsetzt

- zugunsten der «Festung Europa»: Identifizierende biometrische Daten von Drittstaatsangehörigen werden ohne jeden Anfangsverdacht gegen eine bestimmte Person bei jeder Ein- und Ausreise systematisch erfasst, unbeschränkt lange gespeichert und aufgrund der neuen Interoperabilitätskomponenten in einem Hit/No-Hit-Verfahren erleichtert routinemässig systematisch abgefragt. Namentlich der systematische Gebrauch biometrischer Daten von Drittstaatsangehörigen bedeutet für diese eine deutliche Schlechterstellung gegenüber EU/EFTA-Bürger und Bürgerinnen.
- zugunsten des repressiven Überwachungsstaates: die Effizienz der Instrumente von Grenzschutzbehörden, Justiz, Polizei und Nachrichtendiensten wird durch die neue Interoperabilität deutlich erhöht. Der Vernehmlassungsentwurf ignoriert aber im EU-Recht ebenfalls enthaltene Vorgaben für eine Stärkung der Datenschutzbehörden, die Einrichtung einer unabhängigen Aufsichtsbehörde sowie Qualitätssicherungs- und Evaluationsmechanismen systematisch.

---

[2] Joseph Muscat, Premierminister von Malta, musste aufgrund schwerer Korruptionsvorwürfe im Gefolge der Ermordung der Journalistin Daphne Caruana Galizia seinen Rücktritt per 18. Januar 2020 bekanntgeben. Der ehemalige slowakische Staatspräsident der Slowakei, Andrej Kiska, bezeichnete sein Land im Sommer 2019 als «Mafia-Staat», nachdem bekannt wurde, dass Premierminister Robert Fico in die Ermordung des Journalisten Ján Kuciak und seine Verlobte Martina Kusnirova verwickelt war und deswegen zurücktreten musste. Der ehemalige rumänische Premierminister Liviu Dragnea ist zweifach rechtskräftig wegen Korruption verurteilt worden und sitzt jetzt im Gefängnis. Dennoch wurde die vorgängige Entlassung von Laura Kövesi als Leiterin der obersten Korruptionsbekämpfungsbehörde sowie die von Dragnea veranlassten weiteren massiven Erschwerungen zur Korruptionsbekämpfung bisher nicht rückgängig gemacht. Die Vorstellung, dass die Behörden von Malta, Polen oder der Slowakei noch einfacheren Zugriff auf Daten aus der Schweiz zugreifen könnten, trägt nicht wirklich zur Stärkung des Vertrauens und des Sicherheitsgefühls bei.

[3] Vgl. Vertragsverletzungsverfahren gegen Polen, EuGH, Rs. C-619/18, Kommission/Polen, ECLI:EU:C:2019: 531; Kommission eröffnet Debatte zur Stärkung der Rechtsstaatlichkeit in der EU, Medienmitteilung, 3.4.2019.

[4] Die Grosse Kammer des Europäischen Gerichtshofs EuGH urteilte am 27. Mai 2019 in einem Vorabentscheidungsverfahren, die deutschen Staatsanwaltschaften böten keine hinreichende Gewähr für Unabhängigkeit gegenüber der Exekutive, um zur Ausstellung eines Europäischen Haftbefehls befugt zu sein. Es bestehe die strukturelle Gefahr, dass Entscheide der Staatsanwaltschaft durch Anordnungen der Exekutive beeinflusst werden könnten (Urteil vom 27.05.2019, Az. C-508/18).

- zulasten der Freiheit der Bürgerinnen und Bürger: es fehlen planmässige und konsequente Vorkehrungen, um die Grundrechte der Bürgerinnen und Bürger im Gegenzug zur Stärkung der polizeilich-repressiven Instrumente zu schützen und so das Gleichgewicht zwischen Freiheit und Sicherheit zu wahren.

Für die SP ist klar: Die Tatsache, dass bei einer Ablehnung einer Schengen-Vorlage durch die Schweiz sehr viel auf dem Spiel stehen würde, darf nicht dazu missbraucht werden, dass mittels eines schwer verständlichen, spröd-juristischen Sachzwangdiskurses versucht wird, eine offene politische Debatte über die vorhandenen grossen Spielräume zugunsten einer Grundrechts-schonenden Umsetzung zu vermeiden. Es gibt bei der Umsetzung von Schengen-Recht Grenzen, die aus Sicht der SP nicht überschritten werden dürfen.

Ungenügende Verfassungsgrundlage, unklare Zuständigkeiten und Rechtsgrundlagen

Ungenügende materielle Verfassungsgrundlage: Gemäss Kapitel 7.1 des erläuternden Berichtes stützt sich die Übernahme der Rechtsgrundlagen zur Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenze, Migration und Polizei auf Artikel 54 Absatz 1 der Bundesverfassung (BV) (die auswärtigen Angelegenheiten sind Sache des Bundes), auf Artikel 184 Absatz 2 BV (der Bundesrat unterzeichnet und ratifiziert völkerrechtliche Verträge) und Artikel 166 Absatz 2 BV (die Bundesversammlung ist für die Genehmigung völkerrechtlicher Verträge zuständig). Die Umsetzung der EU-Verordnungen geht aber weit über Aussenpolitik hinaus. Die materielle Verfassungsgrundlage bleibt im erläuternden Bericht ungeklärt.

Weit mehr als Aussenpolitik: Es geht beim Anschluss der Schweiz an die EU-Informationssysteme um weit mehr als um Aussenpolitik. Es geht um grundlegende Weichenstellungen, wie die Schweiz ihre Politik im Bereich Asyl, Migration und Sicherheit gestaltet. Diese Bereiche greifen tief in die Funktionsweise der Gesellschaft ein, die teilweise europäisiert wird. Es gibt kein lupenreines „Drinnen“ und „Draussen“, wie die Verfassungsartikel über die Zuständigkeiten zur Gestaltung der Aussenpolitik nahelegen. Vielmehr gibt es nur noch einen einzigen europaweiten Raum der Freiheit, der Sicherheit und des Rechts sowie die Tendenz, den repressiv-polizeilichen Schutz der Aussengrenzen massiv auszubauen. Je stärker die Schweiz in diesen Raum eingebunden ist, desto schwerer wiegt das demokratiepolitische Defizit, so lange dessen Gestaltung allein unter dem Titel „Aussenpolitik“ abgehandelt wird. Dieses Defizit würde sich im Falle eines EU-Beitritts der Schweiz deutlich verkleinern, denn dann könnten Schweizer EU-Parlamentsmitglieder, die solchen Verordnungen zustimmen, gewählt oder abgewählt werden. Solange dies nicht der Fall ist, sollte zumindest bei der Umsetzung von Schengen-Recht alles daran gesetzt werden, keine zusätzlichen demokratiepolitischen Probleme zu schaffen. Auch dazu könnte eine materielle Verfassungsgrundlage beitragen.

Ungeklärtes Verhältnis Bund-Kantone: Eine direkte Folge der ungenügenden Klärung der Zuständigkeiten auf Verfassungsstufe besteht in einer ungeklärten Ausscheidung von Rechten und Pflichten zwischen Bund und Kantonen. Obschon die Kantone im Bereich der öffentlichen Sicherheit und der Migration bedeutende Zuständigkeiten haben, sieht der Bundesrat nach aktueller Planung eine einseitige Überwälzung der hohen Investitionskosten an den Bund vor. Salami-Taktik[5], Vermeidung von ordentlichen Vernehmlassungsverfahren mit luftigen Begründungen[6] und fehlende explizite Klärung der Kostenausscheidung dürften alle dem Ziel dienen, kritische Rückfragen und eine politische Diskussion aus dem Weg zu gehen: solange der Bund einfach bezahlt, schweigen die Kantone. All dies geht zulasten der demokratischen Legitimität des Vorhabens, was grosse politische Risiken birgt.

[5] Im vorliegenden Erläuternden Bericht werden allein Kosten von 21.6 Millionen Franken ausgewiesen. In seiner Botschaft zu einem Verpflichtungskredit zur Weiterentwicklung des Schengen/ Dublin-Besitzstands vom 4. September 2019 (19.049) beantragt der Bundesrat aber einen Verpflichtungskredit von 98.7 Millionen Franken und betont, weitere 23 Millionen würden aus Eigenmitteln finanziert. Dies bedeutet in der Summe **Schengen-Informatik-Investitionen von 122 Millionen Franken**.

[6] Beim Verpflichtungskredit von 98.7 Millionen Franken bzw. geplanten Informatik-Investitionen von 122 Millionen Franken handelt es sich laut Bundesrat „nicht um ein Vorhaben von grosser finanzieller Tragweite“. Es könne deshalb auf „die Durchführung einer Vernehmlassung ... verzichtet werden“. Siehe Botschaft 19.049, Kapitel 2, Seite 6198.

Unklarheit über das anwendbare Recht: Übernimmt die Schweiz eine EU-Richtlinie oder eine EU-Verordnung, so wird diese in der Schweiz zum direkt anwendbaren Recht. Nach einem fast nicht nachvollziehbaren Filter werden einzelne Bestimmungen des EU-Rechts in einem Schweizer Bundesgesetz wiederholt, andere nicht. Im Vernehmlassungsentwurf ausführlich wiederholt wird etwa im neuen 14b. Kapitel des Ausländer- und Integrationsgesetzes (AIG), auf welcher Grundlage und mit welcher Funktion die vier neuen europäischen Datenbanken bzw. Plattformen ESP, BMS, CIR und MID errichtet werden. Dies wird selbst dann umschrieben, wenn das gleiche bereits in den beiden EU-Verordnungen zur Interoperabilität geregelt ist. Bedeutende Bestimmungen dieser Verordnungen über Grundrechte, Datenschutz, Aufsichtsbehörden, Evaluations- und Qualitätssicherungsmassnahmen usw. werden aber nirgends wiederholt. Sind sie deswegen in der Schweiz nicht anwendbar, obschon es sich bei den EU- Verordnungen um direkt anwendbares Recht handelt? Wie werden diese Bestimmungen in der Schweiz angewendet, wenn der Bundesrat darauf verzichtet zu klären, welche Behörden für deren Umsetzung zuständig sind? Warum schaffen es alle Bestimmungen mit repressivem Inhalt systematisch in die Schweizer Gesetzgebung und alle Bestimmungen über den Grundrechts- und Menschenrechtsschutz nicht? Diese Problematik wird verschärft, indem die Vernehmlassungsentwurf an mehreren Stellen eine Delegationskompetenz an den Bundesrat vorsieht (siehe erläuternder Bericht, Kapitel 7.4 unter Verweis auf Art. 110h AIG und Art. 22 BPI; weiter hinten findet sich freilich kein Art. 22 BPI: der aktuelle Art. 22 BPI regelt dessen Inkrafttreten) bzw. in Kapitel 4.3.1 wird betont: «Zahlreiche Neuerungen haben demgegenüber nur Auswirkungen auf das später zu erlassende Verordnungsrecht und bleiben im Folgenden unberücksichtigt». Es wird also angekündigt, dass «zahlreiche» Bestimmungen aus den EU-Verordnungen direkt im Schweizer Verordnungsrecht umgesetzt werden. Auch dies entzieht sie einer politischen Diskussion im Schweizer Parlament.

Interne Kontrollstelle für Datenschutz einrichten (AIG Art. 101)

Auch in anderen Gesetzen ging es darum, zwischen Sicherheitsanforderungen und dem Schutz der Freiheit der Bürgerinnen und Bürger eine ausgewogene Balance zu wahren. Diese Herausforderung wird im Nachrichtendienstgesetz (u.a. in Art. 45) sowie Ziffer 73 im erwähnten Bericht des Europäischen Datenschutzbeauftragten darin gesucht, dass starke institutionelle Mechanismen der Qualitätskontrolle geschaffen werden. Entsprechend regt die SP an, den Datenschutzartikel E-AIG Art. 101 um einen neuen Absatz 3 und 4 wie folgt zu ergänzen:

AIG Art. 101 Datenschutz

[3] Die für die Bearbeitung der Daten zuständige Behörde setzt eine interne Kontrollstelle ein. Sie wacht über

a. für die Einhaltung hoher Qualitätsstandards;
b. ein umfassendes Risikomanagement für Informationssicherheit;
c. die Rechtmässigkeit, Zweckmässigkeit, Wirksamkeit und Richtigkeit der Datenbearbeitungen und überprüft stichprobenweise die Protokolle über die Nutzung der Schengen-Dublin-Informationssysteme und die Einhaltung des Datenschutzgesetzes.

[4] Die interne Kontrollstelle erstellt jährlich Bericht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Normendichte für Abfragen des CIR zwecks Identifikation erhöhen (E-AIG Art. 110b)

Aus Sicht des Datenschutzes gilt es namentlich zu vermeiden, dass es zu routinemässige Abfragen des CIR zwecks Identifikation kommt. Solche Abfragen müssen auf begründete Fälle beschränkt werden. Ein Grundsatz des Datenschutzes besteht darin, dass in heiklen Fragen des Datenschutzes eine ausreichende Normendichte erforderlich ist, um Fragen der Verhältnismässigkeit und Angemessenheit des Grundrechtseingriffes zu klären. Die SP erachtet die Normendichte in den sehr allgemeinen Formulierungen von Art. 110b E-AIG als zu klein und schlägt in Anlehnung an die Ziffern 48 und 83 der Empfehlungen des Europäischen Datenschutzbeauftragten folgende Ergänzung vor:

Art. 101b E-AIG Abfrage des CIR zwecks Identifikation
[2] ...sowie des Schutzes der inneren Sicherheit. Die Abfrage des CIR erfolgt grundsätzlich in Anwesenheit der Person, und a. wenn die Person zur Kooperation nicht in der Lage ist und kein Dokument vorlegen kann, aus dem ihre Identität hervorgeht, oder b. wenn sie die Kooperation verweigert, oder c. wenn der berechtigte und begründete Verdacht besteht, dass vorgelegte Dokumente falsch sind oder dass die Person über ihre Identität nicht die Wahrheit sagt. [2bis] Eine Duplizierung personenbezogener Daten aus dem CIR ist untersagt.

Beschleunigungsgebot für die manuelle Verifizierung von Verknüpfungen im MID

Der Europäische Datenschutzbeauftragte empfiehlt in Ziffer 92 seines Berichtes die Einführung eines festen Zeitrahmens mit konkreten Fristen und die Festlegung eines klaren Verfahrens, das eine rechtzeitige Verifizierung von Verknüpfungen im MID gewährleistet. Ungeklärte Verknüpfungen können für die betreffende Person nachteilige Folgen nach sich ziehen. Die SP regt deshalb an, im MID-Artikel 18d in einem neuen Absatz 3bis vorzusehen, dass ungeklärte Verknüpfungen innert nützlicher Frist verifiziert werden und die betreffende Person entsprechend informiert wird.

E-AIG Art. 18d Manuelle Verifizierung von Verknüpfungen im MID
[3bis] Die manuelle Verifizierung verschiedener Identitäten erfolgt wenn immer möglich innerhalb von zwölf Stunden nach der Feststellung und Meldung einer ungeklärten Verknüpfung. Die betreffende Person wird umgehend informiert, sofern einer solchen Mitteilung keine überwiegenden Sicherheitsinteressen entgegenstehen.

Schnittstellen zum Europäischen Datenschutzbeauftragten und der nationalen unabhängigen Aufsichtsbehörde klären

Die Interoperabilitäts-Verordnungen fordern in Artikel 53 im Rahmen ihrer jeweiligen Zuständigkeiten eine aktive Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten, dies im Sinne einer koordinierten Aufsicht über die Nutzung der Interoperabilitätskomponenten und der Anwendung anderer Bestimmungen dieser Verordnung. Auch wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde grössere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellen oder unrechtmässige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten bemerken, soll diese koordinierte Aufsicht einschreiten. Erstmals bis zum 12. Juni 2021 und danach alle zwei Jahre übermittelt der Europäische Datenschutzausschuss zudem einen gemeinsamen Bericht über seine Tätigkeiten bezüglich der Interoperabilitäts-Verordnungen an das Europäische Parlament, den Rat, die Kommission, Europol, die Europäische Agentur für die Grenz- und Küstenwache und eu-LISA. «Dieser Bericht enthält für jeden Mitgliedstaat ein Kapitel, das von der Aufsichtsbehörde des betreffenden Mitgliedstaats erstellt wird.», schreibt Artikel 53 der EU-Verordnungen vor. Es muss sichergestellt werden, dass dieser Bericht auch von den Schweizer Behörden und dem Schweizer Parlament zur Kenntnis genommen wird und die Schweiz ihrerseits zu diesem Bericht angemessen beiträgt.

Für die SP ist es unverständlich, weshalb diese zentrale Vorgabe der Interoperabilitäts-Verordnungen im Entwurf nicht umgesetzt wird. Namentlich ist zu klären, wer als nationale Aufsichtsbehörde die geforderte Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten wahrnimmt und worin dessen Kompetenzen und Aufgaben bestehen. U.a. ist zu klären, wer zuhanden des erwähnten periodischen EU-Rechenschaftsberichtes das Schweizer Kapitel verfasst und wer den Gesamt-Bericht in der Schweiz anschliessend in welcher Form zur Kenntnis nimmt.

Diese Frage ist umso dringender, als auch innerhalb der Schweiz die Vorarbeiten zur Schaffung einer nationalen Abfrageplattform zur Verbesserung des nationalen polizeilichen Informationsaustauschs

weit vorangeschritten sind (siehe Motion 18.3592). Dies wirft auch auf nationaler Ebene die Frage auf, wie angesichts der fortschreitenden Interoperabilität von polizeilichen und anderen Informationssystemen innerhalb der Schweiz und im Verkehr mit den Schengen-Dublin-Informationssystemen eine gleichmässige Kontrolle der Verarbeitung personenbezogener Daten sichergestellt werden kann.

Der Europäische Datenschutzbeauftragte hat seine rechtliche Grundlage in Artikel 75 Absatz 1 der *Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten*[7]. Gleichzeitig hat diese Datenschutz-Grundverordnung in Artikel 51 Absatz 1 auch die Mitgliedstaaten zur Errichtung nationaler Aufsichtsbehörden verpflichtet. Allerdings hat die Schweiz diese Verordnung nie übernommen, sondern allein die gleichzeitig erlassene *Richtlinie (EU) 2016/ 680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts*[8]. Dies erfolgte im Rahmen der «Schengen-Revision des Datenschutzgesetzes» (17.059).

Weil die Schweiz die EU-Datenschutz-Grundverordnung nicht übernahm, blieb ungeklärt, wer die nationale Aufsichtsbehörde im Sinne des EU-Rechts sei und ob die sanfte Stärkung des EDÖB in Ziffer 1 des Bundesgesetzes über die Umsetzung der Richtlinie (EU) 2016/680[9] ausreichend sei, um in der Schweiz ein mit der EU gleichwertiges, «angemessenes Datenschutzniveau» zu schaffen.

Erschwerend kommt hinzu, dass sich die Stärkung des EDÖB im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 allein auf Daten zum Aufdecken und Verfolgen von Straftaten bezog, nicht aber in Bezug auf alle weiteren Dublin-Schengen-Informationssysteme, die mit Strafverfolgung nichts zu tun haben. Diese Frage spitzte sich anlässlich des Beitritts der Schweiz zum Ein- und Ausreisesystem EES im Jahre 2018 zu.[10] Die SP forderte deshalb bereits damals in ihrer Stellungnahme zum EES-Vernehmlassungsentwurf die Aufwertung des EDÖB zu einer eigentlichen unabhängigen Aufsichtsbehörde, die auf Augenhöhe mit ihren Schwesterbehörden in den EU Mitgliedstaaten sowie mit dem Europäischen Datenschutzbeauftragten kommunizieren kann.[11]

Mit der hier vorliegenden weiteren massiven Ausweitung der Schengen-Dublin-Informationssysteme sowie der parallelen Errichtung einer nationalen Abfrageplattform für den polizeilichen Informationsaustausch wird eine solche Aufsichtsbehörde noch dringender. Ein Präzedenzfall bildet die Umsetzung der EU-VIS-Verordnung 767/2008[12], die dannzumal eine «nationale Kontrollstelle» verlangte. Diese wurde gestützt auf Art. 109e Bst. f, g und i AIG in Art. 37 Abs. 3 VISA-Informationssystem-Verordnung umgesetzt, indem der EDÖB als solche bezeichnet wurde.

Aus Sicht der SP sollte eine so wichtige Frage allerdings auf Gesetzesstufe geregelt werden. Neben der Interoperabilitäts- und VIS-Verordnungen fordern auch das EES und das ETIAS eine Benennung einer Aufsichtsbehörde. Die Regelung allein auf Stufe verstreuter Einzel-Verordnungen ist der Transparenz nicht förderlich und kann dazu verleiten, den damit verbunden zusätzlichen Ressourcenbedarf beim EDÖB nicht ausreichend zu erkennen. Eine einheitliche Regelung dieser Frage für sämtliche Schengen-Dublin-Informationssysteme erleichtert zudem die Umsetzung der Berichterstattungspflichten an den Europäischen Datenschutzbeauftragten (Interoperabilitäts-Verordnung Art. 53 Abs. 3) und eine – bis heute fehlende – parallele Rechenschaftsablage an das Schweizer Parlament. Während in der EU ein mehrstufiges Aufsichts- und Oberaufsichtssystem unter Einbezug des Parlamentes besteht, fehlt in der Schweiz eine solche Aufsicht/Oberaufsicht über die Nutzung von Schengen-Dublin-Informationssystemen weitestgehend, obschon deren Risikopotenzial riesig ist.

---

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.DEU
[9] Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands) vom 28. September 2018, https://www.admin.ch/opc/de/official-compilation/2019/625.pdf
[10] Bundesgesetz zur Genehmigung und Umsetzung der Notenaustausche zwischen der Schweiz und der EU betreffend die Übernahme der Rechtsgrundlagen zur Errichtung und Nutzung des Einreise-und Ausreisesystems (EES) (Verordnungen [EU] 2017/2226 und 2017/2225
[11] https://www.sp-ps.ch/sites/default/files/documents/18-418_einreise_ausreise-system_sp.pdf
[12] EU-VIS-Verordnung Art. 41, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008R0767

Die SP fordert gestützt auf diese Überlegungen folgende Ergänzung:

E-AIG Art. 111k (neu) Nationale Aufsichtsbehörde und Berichterstattung

[1] Nationale Aufsichtsbehörde gemäss Artikel 51 Absatz 1 der Datenschutz-Grundverordnung (EU) 2016/679 ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB).

[2] Er ist im Rahmen seiner Zuständigkeiten gegenüber den Behörden weisungsberechtigt, die in der Schweiz für die Bearbeitung der Daten in den Schengen-Dublin-Informationssystemen zuständig sind.

[3] Er veröffentlicht jährlich die Zahl der Anträge auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung personenbezogener Daten, die getroffenen Folgemassnahmen und die Zahl der Berichtigungen, Löschungen und Einschränkungen der Verarbeitung, die auf Antrag der betroffenen Personen vorgenommen wurden (Artikel 51 Absatz 2 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).

[4] Er arbeitet mit dem Europäischen Datenschutzbeauftragten und den übrigen nationalen Aufsichtsbehörden zusammen. Er erstattet diesen Bericht, falls er grössere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten oder unrechtmässige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten feststellt und zieht Schlussfolgerungen für die Schweiz aus dem Evaluierungsbericht, den die Europäische Kommission jedes Jahr zur Umsetzung der Datenqualität durch die Mitgliedstaaten erstellt (Artikel 37 Absatz 5 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).

[5] Der EDÖB erstattet dem Schweizer Parlament und dem Europäischen Datenschutzbeauftragten alle zwei Jahre über die Bearbeitung der Daten in den Schengen-Dublin-Informationssystemen Bericht.

[6] Er wacht im Bereich seiner Zuständigkeiten über die Umsetzung der EU-Empfehlungen über die Evaluation der Umsetzung und Anwendung des Schengen-Rechts in der Schweiz.

[7] Der Bundesrat stellt sicher, dass der EDÖB als nationale Aufsichtsbehörde über ausreichende Ressourcen und Fachkenntnisse zur Wahrnehmung der Aufgaben verfügt, die ihm hier übertragen werden (Artikel 51 Absatz 4 der Verordnungen (EU) 2019/8177 und (EU) 2019/8187).

Der Europäische Datenschutzbeauftragte misst der Forderung in Absatz 7 in seinem Bericht (Ziffer 23) besondere Bedeutung zu. In Ziffer 141 betont er erneut, «dass eine Aufsicht nur wirksam sein kann, wenn für sie angemessene Ressourcen bereitstehen». Auch Artikel 51 Absatz 4 der Interoperabilitäts-Verordnungen schreibt allen mitwirkenden Staaten – also auch der Schweiz – vor, dass die nationalen Aufsichtsbehörden über ausreichende Ressourcen zur Wahrnehmung ihrer Aufgaben verfügen sollten, die ihnen gemäss dieser Verordnung übertragen werden. Der Europäische Datenschutzbeauftragte empfiehlt in Ziffer 137 ausdrücklich, eine entsprechende Bestimmung ins nationale Recht aufzunehmen. Auch dieser wichtige Passus über eine angemessene Ressourcenausstattung wird im vorliegenden Vernehmlassungsentwurf einfach ignoriert. Die SP fordert, diese Lücke zu schliessen.

Wir danken Ihnen, geschätzte Damen und Herren, für die Berücksichtigung unserer Anliegen und verbleiben mit freundlichen Grüssen

Sozialdemokratische Partei der Schweiz

Christian Levrat
Präsident

Peter Hug
Politischer Fachsekretär