23.xxx

Botschaft zum Flugpassagierdatengesetz

vom …

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Frau Ständeratspräsidentin
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf des Flugpassagierdatengesetzes.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrte Frau Ständeratspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Viola Amherd
Der Bundeskanzler: Viktor Rossi

Übersicht

Mit dieser Gesetzesvorlage soll die Schweiz, wie zahlreiche andere Länder auch, systematisch Flugpassagierdaten bearbeiten können, um Behörden des Bundes und der Kantone bei der Bekämpfung von Schwerstkriminalität zu unterstützen.

Ausgangslage

Das Passagieraufkommen im Luftverkehr ist in den letzten Jahrzehnten international massiv angestiegen. Dies ist nicht nur eine Herausforderung für die Infrastruktur der Flughäfen, sondern auch für die Behörden, die für die Kontrollen bei der Ein- und Ausreise zuständig sind. Nach dem Reisestopp während der Corona-Pandemie weisen provisorische Daten des BAZL für das Jahr 2023 bereits wieder mehr als 53 Millionen Passagiere aus, die mit Linien- und Charterflügen in die Schweiz einreisten oder die Schweiz auf diesem Weg verliessen.

Trotz dieser hohen Zahl von Ein- und Ausreisen müssen Personen, die den Luftverkehr zur Verfolgung krimineller Ziele nutzen, erkennbar bleiben, vor allem, wenn es um Schwerstkriminalität geht. Als solche gelten terroristische und andere schwere Straftaten.

Terrorismus und Schwerstkriminalität sind meistens grenzüberschreitend.

Deshalb nutzen heute bereits 69 Staaten die Informationen über Flugpassagierinnen und -passagiere als Instrument zur Bekämpfung von Schwerstkriminalität.

Bei der Buchung eines Flugtickets fallen Flugpassagierdaten an, die von den Luftverkehrsunternehmen für die Reservation und Abfertigung des Fluges benötigt werden. Dieser Flugpassagierdatensatz, international bekannt als «Passenger Name Record» (PNR), setzt sich aus 19 Datenkategorien zusammen und umfasst unter anderem den Namen und die Adresse der Flugpassagierin oder des Flugpassagiers, Angaben zum mitgeführten Gepäck und zu den Zahlungsmodalitäten.

Mit der Bearbeitung von Flugpassagierdaten können nicht nur Personen ermittelt werden, die den Strafverfolgungsbehörden bereits bekannt sind. Es lassen sich auch Personen identifizieren, die den Strafverfolgungsbehörden bislang nicht bekannt waren, die aber mit Schwerstkriminalität in Zusammenhang stehen. So lassen sich beispielsweise Datenkombinationen feststellen, die häufig in Zusammenhang mit Menschenhandel oder Drogenschmuggel auftreten.

Die Nutzung von PNR wird derzeit global vorangetrieben. Drei auch für die Schweiz bindende Resolutionen des UNO-Sicherheitsrats weisen die internationale Gemeinschaft an, die Bearbeitung von Flugpassagierdaten zur Verhinderung von Terrorismus einzusetzen.

Die EU hat ihre Mitgliedstaaten mit der Richtlinie (EU) 2016/681 verpflichtet, nationale PNR-Systeme aufzubauen.

Die PNR-Richtlinie der EU ist keine Weiterentwicklung des Schengen-Besitzstands. Dennoch ist die Schweiz von deren Umsetzung betroffen, denn alle Luftverkehrsunternehmen sind bei Flügen aus der Schweiz in die EU und umgekehrt zur Bekanntgabe der PNR-Daten ihrer Passagiere verpflichtet.

Heute werden zwar PNR-Daten von Flügen aus der Schweiz den EU-Mitgliedstaaten, dem Vereinigten Königreich, Norwegen sowie den USA bekanntgegeben. Die Schweiz selber kann aber PNR-Daten nicht systematisch bearbeiten, solange sie nicht über die nötige gesetzliche Grundlage und ein nationales PNR-System verfügt.

Ohne PNR-System fehlen der Schweiz – im Vergleich zu anderen Schengen-Staaten – für die Wahrung der öffentlichen Sicherheit entscheidende Hinweise über Personen, die in die Schweiz und damit in den Schengen-Raum einreisen.

Zudem drohen immer mehr Staaten den Schweizer Luftverkehrsunternehmen ohne PNR-Datenbekanntgabe mit hohen Geldstrafen und sogar mit dem Entzug Landerechte. Dies hätte für die Schweiz fatale wirtschaftliche Folgen.

Die Nutzung von PNR ist schliesslich auch eine Bedingung der USA zum Verbleib der Schweiz im Visa Waiver Program. Dieses erlaubt es Schweizer Staatsangehörigen, zu geschäftlichen oder touristischen Zwecken für bis zu 90 Tage ohne Visum in die USA zu reisen.

Inhalt der Vorlage

Das Flugpassagierdatengesetz liefert die gesetzliche Grundlage, die den Bund zur Bearbeitung von Flugpassagierdaten berechtigt. Mit PNR verfügt die Schweiz künftig im Vorfeld einer Ein- oder Ausreise per Flugzeug über Informationen, ob eine Passagierin oder ein Passagier möglicherweise gefährlich oder zur Fahndung ausgeschrieben ist. Aufgrund dieser Informationen entscheiden die zuständigen Behörden, insbesondere die Polizei- und Strafverfolgungsbehörden, ob eine Flugpassagierin oder ein Flugpassagier näher geprüft werden muss oder gar zu verhaften ist.

Eine neu zu schaffende, beim Bundesamt für Polizei angesiedelte Stelle soll die Flugpassagierdaten für die zuständigen Behörden bearbeiten. Die Passenger Information Unit (PIU) erhält die Daten von den Luftverkehrsunternehmen 24 bis 48 Stunden sowie kurz vor Abflug eines Flugzeugs in die und aus der Schweiz. Diese Daten werden unmittelbar nach ihrem Eingang automatisch mit verschiedenen polizeilichen Informationssystemen sowie mit Risikoprofilen und Beobachtungslisten abgeglichen.

Die PIU gibt die dabei erzielten Übereinstimmungen («Treffer») nach einer manuellen Prüfung den zuständigen Behörden von Bund und Kantonen bekannt, sodass diese rechtzeitig die notwendigen Massnahmen in die Wege lei-

ten können. Welche Straftatbestände eine Bekanntgabe der Flugpassagierdaten an eine Behörde legitimieren, ergibt sich aus dem Deliktskatalog, der im Anhang des Flugpassagierdatengesetzes enthalten ist.

Der Entwurf des Flugpassagierdatengesetzes berücksichtigt entsprechend dem Ergebnis der Vernehmlassung verschiedene Kerninhalte des Urteils des Gerichtshofs der Europäischen Union, so insbesondere die reduzierte Aufbewahrungsdauer für Flugpassagierdaten ohne Anhaltspunkte auf Schwerstkriminalität und die Straffung des Deliktskatalogs.

Die Hälfte der Mitarbeitenden, die bei der PIU tätig sein werden, sollen von den Kantonen entsendet und finanziert werden. Damit wird dem Umstand Rechnung getragen, dass die PIU zu einem bedeutenden Teil auch für die Kantone tätig ist.

Beispiele für den Nutzen von PNR-Daten bei der Bekämpfung von Terrorismus und schwerer Kriminalität

Beispiel 1: Verhinderung der Einreise bei Verdacht auf Terrorismus

Frau X bucht im Internet einen Flug von einer kanadischen Stadt in die Schweiz. Sie gibt die bei der Buchung verlangten Informationen ein – darunter ihren Namen, ihre Kontaktdaten und ihr Geburtsdatum.

Die Fluggesellschaft übermittelt diese Informationen 48 bis 24 Stunden vor dem Flug an die PIU des Abflugs- und des Ziellandes.

Die PIU gleichen diese Daten automatisch mit den polizeilichen Informationssystemen ab, auf die sie Zugriff haben. Bei diesem Abgleich kommt es bei der Schweizer PIU zu einer Übereinstimmung. Die Spezialisten der PIU überprüfen die Übereinstimmung nun zur Sicherheit zusätzlich manuell, um diese zu bestätigen. Das Ergebnis: Frau X ist im Schengener Informationssystem (SIS) wegen Unterstützung und Zugehörigkeit zu einer terroristischen Organisation verzeichnet.

Die PIU übermittelt daraufhin die Übereinstimmung der zuständigen Behörde in der Schweiz (in der Regel eine Kantonspolizei oder fedpol). Die zuständige Schweizer Behörde schickt umgehend ein Ersuchen an die Behörden des Abfluglandes: Sie soll verhindern, dass Frau X den Flug in die Schweiz nimmt.

Einen Tag später begibt sich Frau X zum Flughafen, um ihren Flug zu nehmen. Da sie kein Gepäck hat, geht sie direkt zum Gate. Als sie boarden möchte, wird Frau X von der Polizei angehalten, am Einsteigen gehindert und verhaftet.

Mithilfe von PNR-Daten können Personen vor dem Abflug in polizeilichen Informationssystemen identifiziert und die internationale Polizeikooperation verstärkt werden.

Beispiel 2: Verhinderung von Menschenhandel zum Zweck der sexuellen Ausbeutung.

Eine Kantonspolizei ermittelt gegen einen Menschenhändler und weiss, dass regelmässig junge Frauen zum Zwecke der sexuellen Ausbeutung von einer Stadt in Ostereuropa nach Zürich fliegen. Ihre Begleitung: eine noch unbekannte Person. Die Kantonspolizei weiss auch, dass die Flugtickets für die jungen Frauen immer durch das gleiche Reisebüro gebucht und mit der gleichen Kreditkarte bezahlt werden. Der Verdacht: Die unbekannte Begleitung ist ein Menschenhändler und jene Person, die die Tickets für sich und die jungen Frauen immer im gleichen Reisebüro bucht und mit derselben Kreditkarte bezahlt.

Die Kantonspolizei nimmt nun Kontakt mit der PIU auf und stellt einen Antrag, die aktuell bekannten Daten der Begleitperson – Kreditkartennummer und Reisebüro – auf eine Beobachtungsliste zu setzen. Die PIU prüft den Antrag und vergleicht zukünftig die Angaben der Passagiere, die von dieser osteuropäischen Stadt nach Zürich fliegen, mit der Beobachtungsliste.

Einige Wochen später stellt die PIU bei einem Passagier eine Übereinstimmung mit der Beobachtungliste fest – ein Treffer. Die PIU überprüft den Treffer manuell und gibt anschliessend die Information an die Kantonspolizei weiter. Die Kantonspolizei bereitet sich vor: Der noch unbekannte Mann wird bei der Einreise angehalten und befragt. Diese Befragung und andere Ermittlungen erhärten den Verdacht, dass er ein Menschenhändler ist.

Die Kantonspolizei stellt bei der PIU nun den Antrag zu überprüfen, ob der Mann in den letzten sechs Monaten mit anderen jungen Frauen auf der gleichen Strecke geflogen ist. Der Datenschutzbeauftragte der PIU prüft, ob der Antrag die nötigen rechtlichen Bedingungen erfüllt und leitet ihn dann weiter an das Bundesverwaltungsgericht. Dieses entscheidet, dass auf die Daten der in Frage kommenden Flüge der letzten sechs Monaten zugegriffen und eine Abfrage gemacht werden darf.

Die PIU macht die Einzelabfragen und es zeigt sich: Der Mann ist in den vergangenen sechs Monaten mehrfach auf dieser Flugstrecke und mit anderen potentiellen Opfern unterwegs gewesen.

Dank den zusätzlichen Informationen kann die Kantonspolizei gezielt ermitteln und es gelingt ihr, weitere Opfer zu identifizieren und aus dem Menschenhändlerring zu befreien.

Unter anderem mit Hilfe von PNR-Daten kann Menschenhandel aufgeklärt, verhindert und die Opfer geschützt werden.

Inhaltsverzeichnis

Übersicht **2**

1 Ausgangslage **8**
1.1 Übersicht 8
1.2 Handlungsbedarf und Ziele 9
1.3 Geprüfte Alternativen und gewählte Lösung 11
1.4 PNR und andere Flugpassagierdaten 13
1.5 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates 17
1.6 Erledigung parlamentarischer Vorstösse 17

2 Vorverfahren, insbesondere Vernehmlassungsverfahren **17**
2.1 Vernehmlassungsvorlage 17
2.2 Zusammenfassung der Vernehmlassungsergebnisse 18
2.3 Würdigung der Vernehmlassungsergebnisse 19

3 Rechtsvergleiche, insbesondere mit dem europäischen Recht **20**

4 Grundzüge der Vorlage **24**
4.1 Die beantragte Neuregelung 25
4.2 Abstimmung von Aufgaben und Finanzen 31
4.3 Umsetzungsfragen 32

5 Erläuterungen zu einzelnen Artikeln **33**

6 Auswirkungen **87**
6.1 Auswirkungen auf den Bund 87
6.2 Auswirkungen auf Kantone und Gemeinden, insbesondere auch auf Städte, Agglomerationen und Bergebiete 90
6.3 Auswirkungen auf die Volkswirtschaft 92
6.4 Auswirkungen auf die Gesellschaft 92

7 Rechtliche Aspekte **93**
7.1 Verfassungsmässigkeit 93
7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz 94
7.3 Erlassform 95
7.4 Unterstellung unter die Ausgabenbremse 95
7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz 95
7.6 Delegation von Rechtsetzungsbefugnissen 96
7.7 Datenschutz 97

Beilage **xx**

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)
(Entwurf) BBl **2024** …

Botschaft

1 Ausgangslage

1.1 Übersicht

Wer einen Flug bucht, stellt dem Luftverkehrsunternehmen direkt oder indirekt über die Reiseagentur zahlreiche Informationen zur Verfügung, die bis nach der Reise im jeweiligen Reservierungssystem gespeichert werden. Diese Informationen geben nicht nur über den Namen der Flugpassagierin oder des Flugpassagiers und seine Kontaktdaten (Wohnadresse, Telefon und E-Mail) Auskunft, sondern liefern auch Angaben zu den Zahlungsmodalitäten, der Anzahl Gepäckstücke oder zu Begleitpersonen. Diese Daten bilden den sogenannten Flugpassagierdatensatz, auch «Passenger Name Record» oder PNR genannt.

Aktuell verlangen 69 Staaten von den Luftverkehrsunternehmen diese Daten, um vor der Ein- oder Ausreise Hinweise auf Personen zu erhalten, die in Zusammenhang mit Terrorismus und anderen schweren Straftaten (Schwerstkriminalität) national oder international gesucht werden. Weitere Staaten stehen kurz davor, die Nutzung von PNR-Daten einzuführen.

Drei Resolutionen[1] des UNO-Sicherheitsrats weisen die Mitgliedstaaten an, Kapazitäten zur Sammlung, Verarbeitung und Analyse von PNR aufzubauen und diese für die Bekämpfung von Terrorismus zu nutzen. Diese Resolutionen sind auch für die Schweiz verbindlich.

Auf europäischer Ebene drängt die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) – bei der die Schweiz auch Mitglied ist – auf die Nutzung von PNR. Die OSZE bezeichnet die Bearbeitung von PNR-Daten als wichtige Massnahme zur Bekämpfung terroristischer Straftaten und unterstützt Staaten im Aufbau nationaler PNR-Systeme.

Mit der Richtlinie (EU) 2016/681 vom 27. April 2016[2] (PNR-Richtlinie) verpflichtete die EU ihre Mitgliedstaaten zum Aufbau nationaler PNR-Systeme. Die Richtlinie ist keine Weiterentwicklung des Schengen-Besitzstands und damit für die Schweiz rechtlich nicht verbindlich. Dennoch ist die Schweiz

1 Resolution 2178 (2014) Adopted by the Security Council at its 7272nd meeting, on 24 September 2014; Resolution 2396 (2017) Adopted by the Security Council at its 8148th meeting, on 21 December 2017; Resolution 2482 (2019) Adopted by the Security Council at its 8582nd meeting, on 19 July 2019.

2 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. L 119 vom 4.5.2016, S. 132.

von der Umsetzung betroffen, da die Luftverkehrsunternehmen für Flüge aus der Schweiz in die EU zur Übermittlung der PNR-Daten verpflichtet sind.

Auch die Schweiz soll künftig PNR-Daten zur Bekämpfung von Schwerstkriminalität nutzen. Die nötige Rechtsgrundlage soll mit dem vorliegenden Gesetz geschaffen werden. Damit kommt die Schweiz ihren internationalen Verpflichtungen nach und leistet nicht nur national, sondern auch international einen wichtigen Beitrag zur Bekämpfung von Schwerstkriminalität.

Die Schweizer Luftverkehrsunternehmen übermitteln PNR-Daten zwar bereits heute für Flüge aus der Schweiz in andere Staaten. Zu den Empfängern von PNR-Daten aus der Schweiz gehören neben den EU-Mitgliedstaaten auch das Vereinigte Königreich, Norwegen und Kanada sowie die USA.

Im Juni 2018 erklärten die USA erstmals, dass die Schweiz nur dann weiterhin im *Visa Waiver Program* (VWP) verbleiben könne, wenn sie künftig selber PNR-Daten zur Bekämpfung von Schwerstkriminalität nutze. Das VWP erlaubt es Schweizer Staatsangehörigen, zu geschäftlichen oder touristischen Zwecken für bis zu 90 Tage visumsfrei in die USA einzureisen.

Damit erhält PNR für die Schweiz zusätzlich zur sicherheitspolitischen eine wirtschaftliche Dimension. Ausserdem drohen immer mehr Staaten den Schweizer Luftverkehrsunternehmen ohne PNR-Datenbekanntgabe mit hohen Geldstrafen und sogar mit dem Entzug Landerechte.

1.2 Handlungsbedarf und Ziele

International ist die Schweiz zur Einführung eines PNR-Systems und damit zu diesem Beitrag zur weltweiten Bekämpfung von Schwerstkriminalität verpflichtet. Auch nationale Sicherheitsüberlegungen sprechen für die Einführung eines PNR-Systems. Hinzu kommen zunehmend volkswirtschaftliche Überlegungen, welche die Einführung in der Schweiz nahelegen.

In jedem Fall gilt es aber, die Balance zwischen den sicherheits- und wirtschaftspolitischen Anliegen und den Anliegen des Datenschutzes zu wahren. Dies zeigte die im Jahr 2022 durchgeführte Vernehmlassung.

Unter den Begriff der Bearbeitung fällt jeder Umgang mit (Personen-)Daten, so insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden und Verändern. Selbst das Archivieren, Löschen oder Vernichten von Daten fällt darunter. Schliesslich umfasst dieser Begriff auch die Bekanntgabe von (Personen-)Daten, worunter deren Übermittelung oder deren Zugänglichmachen zu verstehen ist (vgl. Art. 5 Bst. d und e des Datenschutzgesetzes vom 25. September 2020[3] [DSG]).

3 SR **235.1**

Viele Staaten, darunter die meisten wichtigen Wirtschaftspartnerländer der Schweiz, verlangen seit Längerem von den Luftverkehrsunternehmen PNR-Daten.

Mit den USA hat die Schweiz erstmals 2003 ein Abkommen abgeschlossen, das die Datenbekanntgabe vorsieht. Die Datenbekanntgabe für Flüge von der Schweiz nach Kanada basiert auf einem Memorandum of Understanding aus dem Jahr 2006.

PNR-Daten für Flüge aus der Schweiz werden auch in die EU bekanntgegeben. Die Datenbekanntgabe an den EU-Mitgliedstaat, in dem der Flug aus der Schweiz landet, basiert auf einer Übergangslösung, die unter Mitwirkung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) erarbeitet worden ist. Das Bundesamt für Zivilluftfahrt (BAZL) informierte die betroffenen Luftverkehrsunternehmen im Mai 2018 darüber, dass die Bekanntgabe von Flugpassagierdaten an ersuchende EU-Mitgliedstaaten bis zur Schaffung einer gesetzlichen Grundlage zulässig sei. Allerdings müssten die Fluggäste in den Beförderungsbestimmungen der Luftverkehrsunternehmen über die Datenbekanntgabe informiert werden und damit einverstanden sein. In einem analogen Vorgehen wurde auch die Datenbekanntgabe an Norwegen ermöglicht.

Der EDÖB hat seither verschiedentlich darauf hingewiesen, dass die nötigen Rechtsgrundlagen in der Schweiz rasch erstellt werden müssten. Die gegenseitige Datenbekanntgabe wird im Rahmen von völkerrechtlichen Verträgen zu regeln sein.

Damit die Schweiz künftig PNR-Daten zur Bekämpfung von Terrorismus und anderen schweren Straftaten systematisch bearbeiten kann, benötigt sie sowohl eine formelle Rechtsgrundlage, die mit dem vorliegenden Gesetzesentwurf geschaffen werden soll, wie auch ein PNR-Informationssystem.

Der Bundesrat hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) am 12. Februar 2020 beauftragt, in Zusammenarbeit mit dem Eidgenössischen Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) ein Bundesgesetz über die Erhebung und Nutzung von PNR-Daten zu erarbeiten. Zudem sollte in Zusammenarbeit mit dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) ein Mandat für die Aufnahme von Verhandlungen mit der EU über ein Abkommen zu PNR erarbeitet werden.

Am 13. April 2022 eröffnete der Bundesrat die Vernehmlassung zum Vorentwurf des Flugpassagierdatengesetzes. Sie dauerte bis Ende Juli 2022.

1.3 Geprüfte Alternativen und gewählte Lösung

Orientierung am Recht der EU

Der in die Vernehmlassung geschickte Vorentwurf des Flugpassagierdatengesetzes lehnte sich eng an die PNR-Richtlinie der EU an. Damit sollte sichergestellt werden, dass sich mit der EU problemlos ein Abkommen über den gegenseitigen Austausch von PNR-Daten abschliessen lässt. Denn die Zahl der Passagiere, die aus der EU in die Schweiz fliegen, macht mehr als einen Drittel des Gesamtpassagieraufkommens an Schweizer Flughäfen aus. Der Erhalt dieser Daten ist für die Schweiz somit wichtig.

Das Interesse am Austausch von PNR-Daten ist gegenseitig. Dies erklärt sich auch mit dem Status der Schweiz als assoziierter Mitgliedstaat des Schengen-Raums: Die Schweiz soll nicht ein Schlupfloch sein, das Reisen in den Schengen-Raum ohne PNR-Daten ermöglicht.

Am 21. Juni 2022, während der Vernehmlassung des Flugpassagierdatengesetzes, fällte der Gerichtshof der Europäischen Union (EuGH) ein Urteil[4] (EuGH-Urteil), in dem er die Bestimmungen der PNR-Richtlinie dahingehend auslegte, dass sie mit den einschlägigen Normen der Charta der Grundrechte der Europäischen Union[5] (Charta der Grundrechte) konform sei.

Der EuGH stellte insbesondere klar, dass:

- nur die Bekämpfung von *schwerer* Kriminalität nach dem Grundsatz der Verhältnismässigkeit die in Zusammenhang mit PNR möglichen schweren Eingriffe in garantierte Grundrechte zu rechtfertigen vermag;[6]
- eine Speicherdauer von sechs Monaten für alle Daten als zulässig zu betrachten ist;
- sich eine Speicherung bis zu fünf Jahren rechtfertigt, wenn sich aus den Daten objektive Anhaltspunkte für eine terroristische oder andere schwere Straftat ableiten lassen.

Das EuGH-Urteil ist für die Schweiz rechtlich nicht verbindlich. Insofern ist die Schweiz grundsätzlich frei, wie sie mit dem Urteil umgeht. Würde allerdings die Schweiz an der Absicht festhalten, das Flugpassagierdatengesetz vollumfänglich auf die PNR-Richtlinie der EU abzustimmen, hätte sie auch deren Auslegung und damit das EuGH-Urteil zu berücksichtigen.

4 Rechtssache C-817/19, ECLI:EU:C:2022:491.
5 Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391.
6 Rechtssache C-817/19, ECLI:EU:C:2022:491, Rz. 148.

Verschiedene Stellungnahmen aus der Vernehmlassung zum Flugpassagierdatengesetz berufen sich auf dieses Urteil und leiten ihre Forderungen daraus ab. Sie sind im vorliegenden Gesetzesentwurf weitgehend berücksichtigt.

Mit den verschiedenen Anpassungen bleibt eine Orientierung des Flugpassagierdatengesetzes an der PNR-Richtlinie erhalten.

Gewählte Lösung

Die nun gewählte Lösung basiert auf dem Vorentwurf des Flugpassagierdatengesetzes und ist entsprechend den Ergebnissen der Vernehmlassung weiterentwickelt worden.

Berücksichtigt wurden dabei auch verschiedene Forderungen aus der Vernehmlassung, die sich aus dem EuGH-Urteil ableiten.

Der vorliegende Entwurf berücksichtigt

- eine Reduktion der Aufbewahrungsdauer für Daten, die keine Anhaltspunkte für Schwerstkriminalität aufweisen;
- eine Straffung des Deliktskatalogs (Beschränkung auf Schwerstkriminalität);
- einen verstärkten Datenschutz;
- ein ausgedehnteres Auskunftsrecht betroffener Personen.

Mit dieser Lösung sind wichtige Elemente des EuGH-Urteils in den Entwurf des Flugpassagierdatengesetzes eingeflossen, ohne die Effizienz und die Wirksamkeit von PNR als Instrument zur Bekämpfung von Schwerstkriminalität erheblich zu beeinträchtigen.

Der Entwurf bringt damit das öffentliche Bedürfnis nach Sicherheit mit den privaten Interessen an einem ausreichenden Schutz der persönlichen Daten in ein Gleichgewicht.

Rechtsetzungstechnische Überlegungen

Der Bundesrat hat geprüft, die für PNR nötigen Rechtsgrundlagen nicht in einem neuen Gesetz, sondern in geltenden Bundesgesetzen zu schaffen, so im Luftfahrtgesetz vom 21. Dezember 1948[7] (LFG) oder im Ausländer- und Integrationsgesetz vom 16. Dezember 2005[8] (AIG).

Im Ergebnis würde damit aber eine unübersichtliche Rechtslage geschaffen, die weder im Interesse der durch dieses Gesetz verpflichteten Luftverkehrsunternehmen noch im Interesse betroffener Flugpassagierinnen und -passa-

7 SR **748.0**
8 SR **142.20**

giere wäre. Zudem stehen beim Flugpassagierdatengesetz nicht nur sicherheits-, sondern auch wirtschaftspolitische Zielsetzungen im Vordergrund, was sich nur beschränkt mit den Zielsetzungen der genannten Gesetze vereinbaren lässt. Deshalb wurden diese Möglichkeiten verworfen.

Ein neues Gesetz, das die Bearbeitung der Flugpassagierdaten umfassend regelt, bietet insbesondere Personen die grösstmögliche Transparenz, die im Luftverkehr unterwegs sind und von der vorgesehenen Datenbearbeitung betroffen sein werden. Für sie ist einfacher erkennbar, wofür und unter welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen.

Auch aufgrund der internationalen Dimension von PNR lässt sich dieser Lösungsansatz rechtfertigen. Auf einen Blick lässt sich erkennen, wie PNR in der Schweiz geregelt ist. Damit wird die Kommunikation mit ausländischen Partnerstaaten erleichtert.

Mit einem Flugpassagierdatengesetz, das alle relevanten Bestimmungen zu PNR umfasst, ist die Rechtslage schliesslich auch für die betroffenen Luftverkehrsunternehmen klar erkennbar.

Auf sie kommen nun beschränkt neue Pflichten zu. Denn sie müssen die PNR-Daten künftig nicht nur ausländischen, für PNR zuständigen Stellen bekanntgeben, sondern auch der nationalen *Passenger Information Unit* (PIU). Von dieser Ausdehnung der Datenbekanntgabe auf die nationale PIU wären 237 Luftverkehrsunternehmen betroffen gewesen. Mit Charter- und Linienflügen beförderten sie mehr als 53 Millionen Passagierinnen und Passagiere von der Schweiz ins Ausland und vom Ausland in die Schweiz.

1.4 PNR und andere Flugpassagierdaten

API-Daten

Vor der Jahrtausendwende verzeichnete das Passagieraufkommen im Linien- und Charterflugverkehr in allen Regionen der Welt einen enormen Anstieg, der die bauliche Infrastruktur an den Flughäfen und die personellen Ressourcen der für die Grenzkontrolle zuständigen Behörden an den Anschlag brachte. Zunehmend zeigte sich, dass sich nicht mehr *alle* Passagiere und deren Gepäck kontrollieren lassen.

Mit den API-Daten, die von den Luftverkehrsunternehmen «vorab» *(in advance)* übermittelt werden müssen, erhalten die Grenzkontrollbehörden vor einer Ein- und Ausreise die nötigen Informationen über die Flugpassagierinnen und -passagiere, um auf der Grundlage einer Risikobewertung selektiv eine Kontrolle durchzuführen.

Im Zuge von 9/11 begannen die USA, API-Daten auch zur Bekämpfung von Terrorismus zu nutzen.

Mit der Richtlinie 2004/82/EG[9] (API-Richtlinie) verpflichtete die EU die Mitgliedstaaten, die nötigen Rechtsgrundlagen für die Nutzung von API-Daten zur Erleichterung der Grenzkontrolle und zur Bekämpfung der illegalen Einwanderung zu schaffen.

Da die API-Richtlinie zum Schengener Besitzstand gehört, ist sie für die Schweiz rechtlich verbindlich. Seit 2008 verpflichtet sie die Luftverkehrsunternehmen zur Erhebung der API-Daten und zu deren Bekanntgabe an die zuständige Behörde. Die Grundlage bildet Artikel 104 AIG.

Erst seit 2019 lassen sich die API-Daten in der Schweiz auch zur Bekämpfung des Terrorismus sowie des organisierten und international tätigen Verbrechens einsetzen (vgl. Art. 104*a* Abs. 1 Bst. c AIG).

API-Daten	
Personalien	Name, Vorname, Geschlecht, Geburtsdatum, Staatsangehörigkeit
Reisedokument	Nummer, Ausstellerstaat, Art und Ablaufdatum
Visum oder Aufenthaltstitel, soweit verfügbar	Nummer, Ausstellerstaat, Art und Ablaufdatum
Gebuchte Flugroute, soweit bekannt	Abgangsflughafen, Umsteigeflughäfen / Zielflughafen in der Schweiz
Beförderungs-Codenummer	
Anzahl der mit dem betreffenden Flug beförderten Personen	
Datum und Zeit des geplanten Abflugs und der geplanten Ankunft	

Anders als die PNR-Daten fallen die API-Daten nicht automatisch bei der Buchung von Flugtickets an, sondern müssen von den Luftverkehrsunternehmungen zur staatlichen Nutzung unmittelbar vor dem Abflug erhoben werden. Die Schweiz verpflichtet die Luftverkehrsunternehmen zudem nur auf spezifischen, als risikobehaftet eingestuften Flügen aus Drittstaaten, die API-Daten zu erheben und zu übermitteln.

9 Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, ABl. L 261 vom 6.8.2004, S. 24.

Mit der Nutzung von PNR-Daten sollen die API-Daten künftig in Kategorie 18 des Flugpassagierdatensatzes (vgl. Anhang 1 des Gesetzesentwurfs) ausgewiesen werden. Dies gilt allerdings nur, wenn die API-Daten auch tatsächlich verfügbar sind. Verfügbar sind sie nur, wenn ihre Vorab-Übermittlung durch den Staat, in dem die Landung eines Fluges erfolgen soll, verlangt wird. Für API-Daten, die als Kategorie 18 des PNR-Datensatzes an die PIU übermittelt werden, gilt das auf PNR-Daten anwendbare Recht.

API-Novelle

Ende 2022 legte die EU-Kommission mit zwei Verordnungsentwürfen einen Vorschlag für die Neuregelung der API-Daten vor.[10] Der eine Verordnungsentwurf (API Border), der den Einsatz der API-Daten für die Einreisekontrolle regelt, ist für alle Staaten verbindlich, die zum Schengen-Raum gehören – somit auch für die Schweiz. Dieser Verordnungsentwurf ist vorliegend nicht von Interesse.

Der andere Verordnungsentwurf (API Police), der die Erhebung und Bekanntgabe von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität vorsieht, ist nicht Schengen-relevant und lediglich für die EU-Mitgliedstaaten verbindlich.

Die EU-Kommission geht davon aus, dass sich die API-Novelle *frühestens* 2030 umsetzen lässt.

Die API Police sieht vor, dass die API-Daten in der EU künftig nur noch im Rahmen von PNR bearbeitet werden sollen. Zudem sollen die Luftverkehrsunternehmen verpflichtet werden, die API-Daten automatisiert zu erheben, soweit dies aufgrund der Dokumente möglich ist.

Inwieweit auch die Schweiz dies einführen will, ist derzeit offen. Die API Police ist als nicht Schengen-relevanter Rechtsakt für die Schweiz rechtlich unverbindlich.

Allerdings stellt sich für die Schweiz die Frage, ob API-Daten – anders als in der EU angedacht – weiterhin auch ausserhalb von PNR bearbeitet werden sollen. Dies dürfte sich insbesondere für Flüge aus Staaten rechtfertigen, die über kein PNR-System verfügen und der Schweiz somit lediglich die API-

[10] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung vorab übermittelter Fluggastdaten (API) zur Verbesserung und Erleichterung der Kontrollen an den Aussengrenzen, zur Änderung der Verordnung (EU) 2019/817 und der Verordnung (EU) 2018/1726 sowie zur Aufhebung der Richtlinie 2004/82/EG des Rates, COM/2022/729 final; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Erhebung und Übermittlung von API-Daten zur Verhütung, Aufdeckung, Untersuchung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und zur Änderung der Verordnung (EU) 2019/818, COM/2022/731 final.

Daten systematisch bekanntzugeben haben. Zu jenen Staaten gehören aktuell unteranderem Russland und verschiedene Staaten aus dem Nahen Osten.

Neben der fehlenden zeitlichen Abstimmung mit dem laufenden PNR-Rechtsetzungsprozess in der Schweiz lässt sich *aus heutiger Sicht* auch rechtlich kein Abstimmungsbedarf zwischen der API-Novelle und dem Flugpassagierdatengesetz erkennen. Deshalb bleibt sie im vorliegenden Entwurf des Flugpassagierdatengesetzes unberücksichtigt.

Passagierlisten

Artikel 21*f*[11] LFG berechtigt die Strafverfolgungsbehörden, zur «Verhinderung oder Verfolgung von Verbrechen und Vergehen» bei den Luftverkehrsunternehmen «Passagierlisten» einzufordern. Die folgenden Daten haben die Luftverkehrsunternehmen auf Verlangen der Strafverfolgungsbehörden zu liefern, soweit sie diese «im Rahmen ihrer normalen Geschäftstätigkeit bereits erhoben haben»:

a. Name, Vorname, Adresse, Geburtsdatum, Staatsangehörigkeit und Nummer des Reisedokuments;

b. Datum, Zeit und Nummer des Fluges;

c. Abgangs-, Transit- und Enddestination der Beförderung;

d. allfällige Mitreisende;

e. Informationen zur Zahlung, namentlich Zahlungsmethode und verwendetes Zahlungsmittel;

f. Angabe der Stelle, über welche die Beförderung gebucht worden ist.

Die Passagierlisten lassen sich nicht systematisch bearbeiten, wie dies bei PNR der Fall ist.

In der Botschaft vom 31. August 2016[12] führte der Bundesrat dazu aus:

«Ergänzend zu den heute flächendeckend und standardisiert angewendeten Kontrollmechanismen zur Verhinderung von Anschlägen auf die Luftfahrt soll künftig im Interesse der Luftsicherheit und zur Bekämpfung der Kriminalität auch eine risikoabhängige, individuelle Prüfung von Passagieren anhand von Passagierlisten möglich sein. Ähnliche Instrumente sind heute bereits in der Zollgesetzgebung und im Ausländerrecht vorgesehen, um Zollwiderhandlungen und illegale Migration zu bekämpfen. Zur Verhinderung und Ermittlung von kriminellen Handlungen sollen die Luftverkehrsunternehmen verpflichtet werden, den zuständigen Strafverfolgungsorganen auf Verlangen Passagierlisten herauszugeben.»

11 SR **748.0**
12 BBl **2016** 7133 S. 7140

1.5 Verhältnis zur Legislaturplanung und zur Finanzplanung sowie zu Strategien des Bundesrates

Bereits in der Strategie der Schweiz zur Terrorismusbekämpfung vom 18. September 2015[13] nannte der Bundesrat die Nutzung von PNR als mögliche Massnahme, um Ein-, Aus- und Durchreisen von Terrorverdächtigen verhindern zu können.

Der nun vorliegende Gesetzesentwurf ist in der Botschaft vom 29. Januar 2020[14] zur Legislaturplanung 2019–2023 als weiteres Geschäft zur Umsetzung von Ziel 14 «Die Schweiz beugt Gewalt, Kriminalität und Terrorismus vor und bekämpft sie wirksam», angekündigt.

Die Nutzung von PNR leistet daneben auch einen Beitrag zur Umsetzung von Ziel 12 «Die Schweiz verfügt über geregelte Beziehungen mit der EU» sowie von Ziel 15 «Die Schweiz kennt die Bedrohungen ihrer Sicherheit und verfügt über die notwendigen Instrumente, um diesen wirksam entgegenzutreten».

Da der finanzielle Entwicklungsrahmen der Departemente neu basierend auf den Legislaturzielen festgelegt wird, wurden die Mittel für das Projekt und den künftigen Einsatz von PNR über die Bedarfsplanung für den Entwicklungsrahmen des EJPD für die Jahre ab 2025 beantragt.

1.6 Erledigung parlamentarischer Vorstösse

Es sind keine parlamentarischen Vorstösse hängig, die mit der vorliegenden Botschaft zu erledigen wären.

2 Vorverfahren, insbesondere Vernehmlassungsverfahren

2.1 Vernehmlassungsvorlage

Vom 13. April bis zum 31. Juli 2022 hatten die Kantone, die politischen Parteien und die interessierten Kreise Gelegenheit, sich im Rahmen der Vernehmlassung zum Vorentwurf des Flugpassagierdatengesetzes zu äussern.

Der Vorentwurf orientierte sich an der PNR-Richtlinie der EU. Damit sollten optimale Voraussetzungen für ein Abkommen über den gegenseitigen Austausch von PNR-Daten zwischen der Schweiz und der EU geschaffen werden. Denn die EU ist die wichtigste Wirtschafts- und Sicherheitspartnerin der

13 BBl **2015** 7492
14 BBl **2020** 1777 S. 1897

Schweiz. Zudem existiert zwischen der EU und der Schweiz ein reger Personenverkehr, der auch mit Blick auf PNR von Bedeutung ist.

2.2 Zusammenfassung der Vernehmlassungsergebnisse

Im Rahmen der Vernehmlassung vom 13. April bis Ende Juli 2022 haben sich 49 Teilnehmerinnen und Teilnehmer geäussert.

40 Teilnehmerinnen und Teilnehmer würdigten den Vorentwurf positiv bis neutral:

25 Kantone	Als einziger Kanton äusserte sich Uri nicht zur Vorlage
2 Parteien	Die Mitte, FDP
13 Organisationen/Vereinigungen	Aerosuisse, BVGer, easyJet, economiesuisse, Flughafen ZRH, KKJPD, KKPKS, SGB, SSK, STV, SWISS, VSPB, VSF

Die Kantone betonten die sicherheitspolitische Seite von PNR und begrüssten in ihrer Mehrzahl die mit der Nutzung von PNR erwarteten Verbesserungen bei der Bekämpfung von Schwerstkriminalität. Kritischer äusserten sie sich teilweise dazu, die Hälfte der Mitarbeitenden der PIU entsenden und finanzieren zu müssen.

Sicherheitspolitisch neutral fielen demgegenüber die Stellungnahmen seitens der Vertreter der Luftfahrtbranche aus. Mit ihren Anliegen sprachen sie sich für eine pragmatische und sich an internationalen Standards orientierende Regelung aus. Auf einen *Swiss finish* sei unter allen Umständen zu verzichten.

Kritisch bis ablehnend äusserten sich dagegen neun Teilnehmerinnen und Teilnehmer:

4 Parteien	SP, GRÜNE, SVP, Piratenpartei
3 Organisationen	Schweizerischer Anwaltsverband, Digitale Gesellschaft, AlgorithmWatch
2 Private	R.S., LAW FIRM

Unter Verweis auf das EuGH-Urteil lehnten die meisten dieser Vernehmlassungsteilnehmerinnen und -teilnehmer vor allem die einheitliche Speicher-

dauer (gemäss Vorentwurf 5 Jahre) für *alle* Daten und den Umfang des Deliktskatalogs ab. Verschiedene kritisierten zudem, dass der Datenschutz zu wenig Gewicht erhalte. Ihrer Kritik stellten sie mehrheitlich und unter Verweis auf das vorerwähnte EuGH-Urteil Verbesserungsvorschläge gegenüber.

Detaillierte Ausführungen finden sich im Bericht vom 1. März 2024[15] über das Ergebnis des Vernehmlassungsverfahrens.

2.3 Würdigung der Vernehmlassungsergebnisse

Es ist das erklärte Ziel des Bundesrates, mit PNR ein wichtiges sicherheitspolitisches Zeichen zu setzen – national und international: Schwerstkriminalität darf unsere Gesellschaft nicht destabilisieren.

Dies soll allerdings nicht auf Kosten des Datenschutzes gehen. Die Vernehmlassung zeigt, dass eine Balance zwischen den mit der Nutzung von PNR verfolgten sicherheitspolitischen Interessen der Allgemeinheit und den grundrechtlich geschützten Persönlichkeitsrechten der Einzelnen unabdingbar ist.

Einen nicht unwesentlichen Einfluss auf den Ausgang der Vernehmlassung hatte das EuGH-Urteil, auf das sich mehrere Vernehmlassungsteilnehmerinnen und -teilnehmer beriefen.

Auch wenn dieses Urteil für die Schweiz keine bindende Wirkung entfaltet, berücksichtigt der Bundesrat im vorliegenden Gesetzesentwurf zentrale Inhalte dieses Urteils, soweit dies auch in der Vernehmlassung verlangt worden ist und die Wirksamkeit der Nutzung von PNR nicht grundsätzlich in Frage stellt. Im Übrigen anerkennt das Urteil, dass sich PNR-Daten grundrechtskonform nutzen lassen.

Wie das Urteil besagt, muss bei der Aufbewahrungsdauer zwischen Daten unterschieden werden, die objektive Anhaltspunkte vermitteln, dass von der betroffenen Flugpassagierin oder dem betroffenen Flugpassagier eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität ausgehen könnte, und Daten, die keine Anhaltspunkte für eine solche Gefahr geben. Gemäss dem EuGH lässt sich eine Aufbewahrungsdauer von fünf Jahren nur für Daten mit objektiven Anhaltspunkten auf Schwerstkriminalität rechtfertigen. Alle anderen Daten seien dagegen nach sechs Monaten zu löschen.

Einzelne Stellungnahmen aus der Vernehmlassung weisen zu Recht auch auf die wirtschaftliche Bedeutung des Flugpassagierdatengesetzes hin: Die Schweiz muss weiterhin Teil des internationalen Luftverkehrs bleiben, um die hiesigen Arbeitsplätze in der Luftfahrtbranche und im Tourismus sowie die

15 www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > EJPD.

internationale Attraktivität des Standorts Schweiz im Allgemeinen erhalten zu können. Die Nutzung von PNR ist eine wichtige Voraussetzung dafür. Denn vermehrt drohen Staaten damit, die Bewilligung von Flügen in ihr Land von der Nutzung von PNR abhängig zu machen.

Ebenfalls wirtschaftlich motiviert ist schliesslich die Forderung, dass die Schweiz bei der technischen Umsetzung die internationalen Standards beachten soll, sodass den Luftverkehrsunternehmen und den Flughäfen nicht Mehrkosten aufgrund von teuren Sonderlösungen erwachsen. Allerdings stehen diesem Anliegen teilweise wiederum datenschutzrechtlich motivierte Forderungen aus der Vernehmlassung entgegen.

Für den Bundesrat zentral sind die Forderungen nach einer Differenzierung bei der Aufbewahrungsdauer der Flugpassagierdaten und nach einer Straffung des Deliktskatalogs.

Vor allem die Differenzierung bei der Aufbewahrungsdauer der Flugpassagierdaten setzt verschiedene weitere Anpassungen des Gesetzes voraus, ohne dass diese explizit gefordert worden wären. Dazu gehören insbesondere:

- die Unterscheidung zwischen markierten Daten, die objektive Anhaltspunkte für einen Bezug zu Schwerstkriminalität aufweisen, und Daten, die keine solchen Anhaltspunkte aufweisen und demnach auch nicht zu markieren sind,
- die Möglichkeit, dass die Markierung von Daten wieder aufgehoben werden kann, wenn sich aufgrund der weiteren Abklärungen seitens der zuständigen Behörden die Anhaltspunkte nicht bestätigen oder wenn sich der ursprüngliche Verdacht einer zur Fahndung ausgeschriebenen Person als gegenstandslos erweist,
- eine Differenzierung beim Auskunftsrecht, wenn es Daten einer Flugreise betrifft, die länger als sechs Monate zurückliegt.

3 Rechtsvergleiche, insbesondere mit dem europäischen Recht

EU

Etliche EU-Mitgliedstaaten haben PNR-Daten bereits vor 2016 nach ihrem jeweiligen Landesrecht bearbeitet. Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat die Richtlinie (EU) 2016/681. Die Richtlinie trat am 24. Mai 2016 in Kraft und bezweckt, die PNR-Vorschriften der EU-Mitgliedstaaten zu harmonisieren, Rechtsunsicherheit und Sicherheitslücken zu beheben und zugleich den Datenschutz auf einem gemeinsamen Niveau zu gewährleisten. Dänemark ist der einzige EU-Mitgliedstaat, der nicht

an diese Richtlinie gebunden ist.[16] Es hat sich jedoch mittlerweile freiwillig dem PNR-Informationsaustausch der übrigen EU-Mitgliedstaaten angeschlossen.

Die PNR-Richtlinie harmonisiert unter anderem die Zuständigkeiten der sogenannten PNR-Zentralstellen, die für den operationellen Betrieb in den jeweiligen EU-Mitgliedstaaten verantwortlich sind (Art. 4), die zulässige Datenbearbeitung (insb. Art. 6) sowie die Pflichten der Fluggesellschaften zur Datenbekanntgabe (Art. 8).

Nach zwei Jahren überprüfte die EU-Kommission die PNR-Richtlinie. Die Ergebnisse hielt sie im Bericht vom 24. Juli 2020[17] an das Europäische Parlament und den Rat fest. Insgesamt gelangte die Kommission zum Schluss, dass sich PNR als effektives Instrument bei der Bekämpfung von Terrorismus und schwerer Kriminalität einsetzen lassen. Verschiedene weiterführende Ermittlungshandlungen oder Verhaftungen wären ohne PNR nicht möglich gewesen. Die EU-Mitgliedstaaten bestätigten im Übrigen, dass eine verdachtsunabhängige Speicherung der PNR-Daten über fünf Jahre aus operativer Sicht nötig sei. Allerdings bleibe die Verbesserung der Datenqualität eine Herausforderung.

Mit dem Urteil vom 21. Juni 2022 bestätigt der EuGH die Vereinbarkeit der PNR-Richtlinie mit der Charta der Grundrechte. Der EuGH legte die Bestimmungen der PNR-Richtlinie dahingehend aus, dass sie mit den einschlägigen Normen der Charta der Grundrechte konform sind.

Bislang hat die EU mit den USA[18] und Australien[19] Abkommen über den gegenseitigen Austausch von PNR-Daten abgeschlossen.

Der EuGH hat sich 2017 im Rahmen eines Gutachtens auch mit Fragen rund um solche Abkommen der EU mit Drittstaaten befasst.[20] Dabei ging es um ein geplantes Abkommen mit Kanada. Der EuGH verlangte unter anderem, dass Kanada PNR-Daten aus der EU sofort nach der Ausreise der betroffenen

16 PNR-Richtlinie, Erwägung 40.

17 Bericht der EU-Kommission an das Europäische Parlament und den Rat über die Überprüfung der Richtlinie (EU) 2016/681 über die Verwendung von Flugpassagierdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, COM/2020/305 final.

18 Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, ABl. L 215 vom 11.8.2012, S. 5.

19 Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service, ABl. L 186 vom 14.7.2012, S. 4.

20 EuGH, Gutachten 1/15 vom 26. Juli 2017; ECLI:EU:C:2017:592

Person löscht. Das Abkommen mit Kanada wurde bis heute nicht abgeschlossen.

Im Februar 2020 wurde die EU-Kommission beauftragt, Verhandlungen mit Japan aufzunehmen.

Im gleichen Jahr signalisierte die EU-Kommission auch gegenüber der Schweiz ihr Interesse an einem bilateralen PNR-Abkommen. Ende 2020 nahmen die EU-Kommission und die Schweiz, vertreten durch das EDA, das BAZL und das fedpol, exploratorische Gespräche auf, die sehr konstruktiv verliefen.

Bei der EU-Kommission auf ein positives Echo stiess hingegen die Absicht der Schweiz, das EuGH-Urteil hinsichtlich der reduzierten Aufbewahrungsdauer und der Straffung des Deliktskatalogs zu berücksichtigen.

Am 8. Februar 2023 hat die EU-Kommission der Schweiz, Norwegen und Island Verhandlungen für bilaterale PNR-Abkommen vorgeschlagen, die sie mit den drei Schengen-assoziierten Staaten parallel, aber separat zu führen beabsichtigt. Die Schweiz benötigt dazu ein Verhandlungsmandat. Der Bundesrat hat es in seiner Sitzung vom 1. November 2023 unter Vorbehalt der Zustimmung der Aussenpolitischen Kommissionen der Eidgenössischen Räte und der Konferenz der Kantonsregierungen Aussenpolitischen Räte und der Kantone verabschiedet. Diese haben dem Verhandlungsmandat zugestimmt.

Vereinigtes Königreich

Das Vereinigte Königreich verfügte als erster EU-Mitgliedstaat über ein funktionierendes PNR-System und bearbeitet seit 2004 PNR-Daten.

Im Rahmen der Verhandlungen zum Brexit vereinbarte das Vereinigte Königreich mit der EU, den Austausch von PNR-Daten fortzuführen. Das Vereinigte Königreich und die EU haben dazu ein PNR-Abkommen ausgehandelt, das in den Art. 542 ff. des Handels- und Kooperationsabkommens zwischen der EU und Grossbritannien/TCA aufgenommen wurde.[21]

Die Schweiz hat mit dem Vereinigten Königreich nach dem Brexit ein Polizeiabkommen[22] abgeschlossen. Da dieses jedoch keine Grundlage für einen umfassenden gegenseitigen Informationsaustausch zu PNR-Daten bietet, wird die Schweiz mit dem Vereinigten Königreich voraussichtlich ein separates Abkommen zu PNR abschliessen.

21 Abkommen über Handel und Zusammenarbeit zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, ABl. L 149 vom 30.4.2021, S. 10, Art. 542–562.

22 SR **0.360.367.1**

Vereinigte Staaten

Die USA verpflichteten die Luftverkehrsunternehmen im Anschluss an die Terroranschläge vom 11. September 2001 durch den «Aviation and Transportation Security Act»[23], den US-Behörden Zugriff auf die PNR-Daten aller Flüge in die, aus den und über die USA zu gewähren.

Das erste PNR-Abkommen, das die USA mit der Schweiz abschloss, trat am 29. März 2005 in Kraft und galt aufgrund seiner Befristung lediglich dreieinhalb Jahre. Am 23. Dezember 2008 trat das Folge-Abkommen in Kraft.[24]

Die US-Regierung verpflichtet sich in diesem Abkommen, den PNR-Daten aus der Schweiz den gleichen Schutz zukommen zu lassen wie den Daten aus der EU.[25]

Kanada

Seit 2009 werden PNR- und API-Daten von Flügen aus der Schweiz nach Kanada den dort zuständigen Behörden bekanntgegeben. Die Datenbekanntgabe stützt sich auf das Memorandum of Understanding between the Canada Border Services Agency and the Swiss Federal Office for Civil Aviation Concerning Advance Passenger Information/Passenger Name Record vom 17. März 2006[26].

Die PNR-Daten dürfen nur zur Identifikation von Personen verwendet werden, bei denen die Gefahr besteht, dass sie:

- Waren im Zusammenhang mit Terrorismus oder terrorismusbezogenen Straftaten einführen,
- andere schwere Straftaten begehen, die grenzüberschreitend sind (einschliesslich organisierter Kriminalität), oder
- eine mögliche Verbindung zu solchen Verbrechen haben.

PNR-Daten werden von den kanadischen Behörden nach 24 Monaten pseudonymisiert und nach insgesamt 42 Monate gelöscht, sofern die betreffende Person nicht Gegenstand eines Verfahrens wird.

Das Abkommen stellt der Schweiz die Bekanntgabe von PNR- und API-Daten aus Kanada in Aussicht, sobald die nötige Rechtsgrundlage für die Bearbeitung von PNR-Daten in der Schweiz geschaffen ist.

23 www.congress.gov/bill/107th-congress/senate-bill/1447
24 SR **0.748.710.933.6**
25 Vgl. Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, ABl. L 215 vom 11.8.2012, S. 5.
26 www.admin.ch > Dokumentation > Medienmitteilungen > Vereinbarung mit Kanada über Fluggastdaten vom 17. März 2006.

4 Grundzüge der Vorlage

PNR-Daten werden weltweit in 69 Ländern genutzt: seit rund 20 Jahren in den USA, in Kanada sowie im Vereinigten Königreich und seit einigen Jahren in den Mitgliedstaaten der EU.

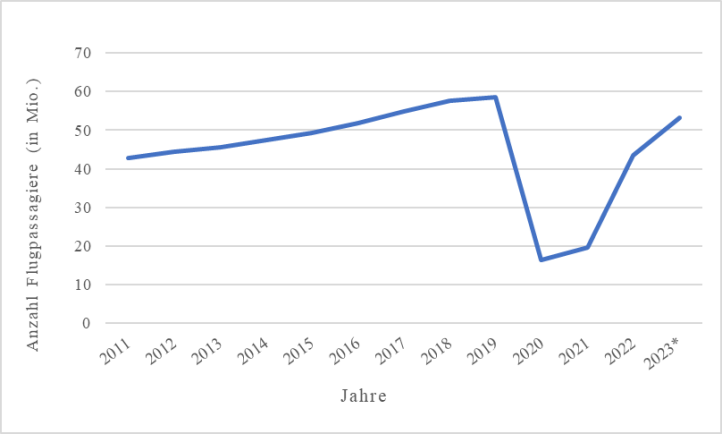
Mit dem Flugpassagierdatengesetz soll künftig auch die Schweiz PNR als bewährtes Instrument im Kampf gegen Schwerstkriminalität einsetzen und damit ihren internationalen Verpflichtungen nachkommen können.

Verpflichtend sind insbesondere die drei bindenden Resolutionen des UNO-Sicherheitsrates[27], welche die Mitgliedstaaten auffordern, zur Bekämpfung von Terrorismus PNR aufzubauen.

Weiter hat die International Civil Aviation Organization (ICAO) im Auftrag des UNO-Sicherheitsrates zusammen mit der Weltzollorganisation (WZO) sowie Regierungen der Mitgliedstaaten, Fluggesellschaften und Dienstleistern Standards für die Bekanntgabe von Flugpassagierdaten entwickelt. Diese *PNR Reporting Standards* sind für alle Mitgliedstaaten der ICAO – und somit auch für die Schweiz – verbindlich.

Verschiedene Staaten, darunter auch die meisten der wichtigen Wirtschaftspartnerländer der Schweiz, verlangen seit Längerem von den Luftverkehrsunternehmen mit Flugverbindungen in die Schweiz die Übermittlung von PNR-Daten. Zur Datenbekanntgabe verpflichtet können die Luftverkehrsunternehmen auch bei Flügen aus der Schweiz sein. Einige Staaten stellen neuerdings den Entzug der Landerechte in Aussicht, wenn sie nicht vorgängig die PNR-Daten erhalten. Damit droht der Schweiz mittel- bis langfristig eine deutlich reduzierte Einbindung in den internationalen Luftverkehr. Dessen Bedeutung für die Schweiz zeigt sich an den Passagierzahlen, die jährlich an Schweizer Flughäfen auf grenzüberschreitenden Linien- und Charterflügen verzeichnet werden.

27 Resolution 2178 (2014) Adopted by the Security Council at its 7272nd meeting, on 24 September 2014, Resolution 2396 (2017) Adopted by the Security Council at its 8148th meeting, on 21 December 2017, Resolution 2482 (2019) Adopted by the Security Council at its 8582nd meeting, on 19 July 2019.



Zahl der Flugpassagierinnen und -passagiere, die in Charter- und Linienflügen aus der Schweiz aus- oder in die Schweiz einreisten (Quelle: BAZL).
*2023: Die Anzahl der Flugpassagierinnen und -passagiere ist provisorisch.

Die USA schliesslich machen den Verbleib der Schweiz im VWP (siehe Ziff. 1.1) von PNR abhängig.

Der Entwurf des Flugpassagierdatengesetzes orientiert sich an der PNR-Richtlinie und berücksichtigt zentrale Inhalte des EuGH-Urteils, soweit diese in der Vernehmlassung verlangt wurden und die Wirksamkeit von PNR nicht grundsätzlich in Frage stellen.

4.1 Die beantragte Neuregelung

Die Luftverkehrsunternehmen erheben die Flugpassagierdaten bei der Buchung eines Flugtickets und nutzen sie zur Abwicklung der Flüge. Die staatliche Nutzung dieser Daten ist nachgelagert.

Das Flugpassagierdatengesetz (E-FPG) bildet die rechtliche Grundlage, damit der Bund die Passagierdaten der Linien- und Charterflüge aus der Schweiz und in die Schweiz systematisch zur Bekämpfung von Schwerstkriminalität bearbeiten kann. Die massgeblichen Straftatbestände sind in Anhang 2 des Gesetzes ausgewiesen.

Zuständig für die Bearbeitung der Flugpassagierdaten ist die PIU, die beim fedpol angesiedelt werden soll. Die PIU lässt sich damit als eine staatliche Dienstleisterin im Sicherheitsbereich verstehen.

Die Artikel 2–4 des Gesetzesentwurfs regeln die Pflichten der Luftverkehrsunternehmen.

Die Luftverkehrsunternehmen haben insgesamt 19 verschiedene Kategorien von Flugpassagierdaten bekanntzugeben, die in Anhang 1 des Gesetzesentwurfs ausgewiesen sind und zusammen den Flugpassagierdatensatz bilden. Bekanntzugeben sind die Datensätze *aller* Passagierinnen und -passagiere von Charter- und Linienflügen, die von der Schweiz ins Ausland und umgekehrt unterwegs sind. Bekanntzugeben sind die Daten jeweils innerhalb gesetzlich definierter Zeitfenster vor dem Abflug aus der Schweiz beziehungsweise in die Schweiz. Empfängerin der Daten in der Schweiz ist die PIU (Art. 2).

Von den Luftverkehrsunternehmen wird erwartet, dass sie die zumutbaren Massnahmen treffen, damit die Datenbekanntgabe rechtzeitig und entsprechend den technischen Vorgaben erfolgt (Art. 3).

Zudem haben die Luftverkehrsunternehmen ihre Passagierinnen und Passagiere bei der Buchung des Tickets angemessen und damit in präziser, transparenter, verständlicher und leicht zugänglicher Form über die staatliche Bearbeitung ihrer Daten nach diesem Gesetz zu informieren (Art. 4).

Kommt ein Luftverkehrsunternehmen diesen Verpflichtungen nicht oder nur unvollständig nach, greifen die Sanktionen nach Artikel 31. Davon befreien kann es sich mit dem Nachweis, alle zumutbaren technischen und organisatorischen Massnahmen zur Erfüllung der gesetzlichen Pflichten getroffen zu haben.

Die Artikel 5–11 des Gesetzesentwurfs regeln die Datenbearbeitung durch die PIU.

In ihrer Gesamtheit werden die bei der PIU eintreffenden Flugpassagierdaten ausschliesslich beim automatischen Datenabgleich nach Artikel 6 aktiv bearbeitet. Dieser Bearbeitungsschritt ermöglicht eine frühe Triage der Daten.

Sobald die Flugpassagierdaten bei der PIU eingetroffen sind, werden sie automatisch mit polizeilichen Informationssystemen sowie mit den hinterlegten Risikoprofilen und Beobachtungslisten abgeglichen (Art. 6).

Allfällige dadurch erzielte Übereinstimmungen («Treffer», «Hits») sind sodann manuell durch die PIU zu überprüfen. Erst danach darf die PIU die Übereinstimmungen einer zuständigen Behörde nach Artikel 1 Absatz 2 bekanntgeben. Übereinstimmungen, die bei der manuellen Überprüfung nicht bestätigt werden, sind umgehend zu löschen (vgl. Art. 22).

Ergebnisse des automatischen Datenabgleichs ermöglichen den zuständigen Behörden:

- auf Straftaten nach Anhang 2 aufmerksam zu werden, die bisher nicht Gegenstand von laufenden Ermittlungs- und Strafverfolgungsverfahren waren (vgl. Art. 5 Abs. 1 Bst. a);
- Informationen in Zusammenhang mit laufenden Ermittlungs- oder hängigen Strafverfahren wegen einer Straftat nach Anhang 2 sowie mit ungeklärten Straftaten nach Anhang 2 zu vervollständigen (vgl. Art. 5 Abs. 1 Bst. a);
- national und international wegen einer Straftat nach Anhang 2 gesuchte Personen anzuhalten und allenfalls zu verhaften (vgl. Art. 5 Abs. 1 Bst. a sowie Bst. b Ziff. 1);
- Personen dem Vollzug einer Freiheitsstrafe zuzuführen, zu der sie wegen einer Straftat nach Anhang 2 rechtskräftig verurteilt worden sind (vgl. Art. 5 Abs. 1 Bst. b Ziff. 2).

Sobald diese Bekanntgabe erfolgt ist, markiert die PIU die betroffenen Daten. Die markierten Daten unterliegen danach automatisch einer längeren Speicherfrist als jene Daten, die nicht markiert und bekanntgegeben worden sind (vgl. Art. 21).

Nach diesem Bearbeitungsschritt können die Flugpassagierdaten nur noch einer zuständigen Behörde bekanntgegeben und danach markiert werden:

- auf Antrag einer solchen Behörde nach Artikel 8; oder
- zusammen mit einem bei der PIU eingegangenen Hinweis nach Artikel 9.

Eine Sonderform der Bekanntgabe von Flugpassagierdaten, die *nicht* zur Markierung der bekanntgegebenen Daten führt, sieht Artikel 11 vor: Der Nachrichtendienst des Bundes (NDB) soll die Flugpassagierdaten bestimmter Flugstrecken zur selbständigen Bearbeitung erhalten, soweit dies der Erfüllung seiner Aufgaben nach Artikel 6 Absatz 1 Buchstabe a Ziffern 1–5 des Nachrichtendienstgesetzes vom 25. September 2015[28] (NDG) dient und es dabei um die Bekämpfung einer Straftat nach Anhang 2 des vorliegenden Gesetzes geht. Die Einzelheiten der Bearbeitung durch den NDB, wie die zulässige Aufbewahrungsfrist, bestimmt sich nach dem NDG (vgl. Anhang 3 Ziff. 1 E-FPG).

Die Unterscheidung zwischen markierten Daten und Daten ohne Markierung ermöglicht es, dem Anliegen aus der Vernehmlassung zu entsprechen, wonach Flugpassagierdaten ohne Anhaltspunkte für eine Straftat nach Anhang 2 (Daten ohne Markierung) nicht so lange aufbewahrt werden sollen wie markierte Daten.

28 SR **121**

Eine zuständige Behörde nach Artikel 1 Absatz 2 kann zur Erkenntnis gelangen, dass sie die von der PIU bekanntgegebenen Daten nicht mehr benötigt. Dies kann der Fall sein, wenn sich die Anhaltspunkte, die zur Bekanntgabe der Daten geführt haben, nicht bestätigt haben oder wenn sich der ursprüngliche Verdacht einer zur Fahndung ausgeschriebenen Person als gegenstandslos erweist. Sobald die PIU die Information der Behörde erhalten hat, hebt sie die Markierung der betreffenden Daten auf (Art. 10). Die Daten sind danach wieder ohne Markierung und unterliegen den für diese Daten geltenden Rechtsfolgen (vgl. Art. 18 und 21).

Die Artikel 12–15 legen die Einzelheiten für den Einsatz von Risikoprofilen und Beobachtungslisten beim automatischen Datenabgleich fest. Der Bundesrat überwacht den Einsatz dieser Instrumente.

Mit dem Risikoprofil lässt sich in den Flugpassagierdaten nach Datenkombinationen suchen, die bei einzelnen Straftaten nach Anhang 2 und insbesondere beim organisierten Verbrechen (Menschenhandel) verbreitet sind (Art. 12). Da nicht in Zusammenhang mit einer den Behörden bereits bekannten Straftat nach Anhang 2 gesucht wird, finden sich im Risikoprofil auch keine Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen und damit Personendaten im Sinne von Artikel 5 Buchstabe a DSG darstellen.

Daten, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen, gelangen dagegen bei den Beobachtungsliste nach den Artikeln 13 und 14 zum Einsatz. Mit den Beobachtungslisten wird in den Flugpassagierdaten nach konkreten Angaben gesucht, die in Zusammenhang mit einer den Behörden bekannten Straftat nach Anhang 2 von Bedeutung sind: beispielsweise nach dem Namen einer Person, nach der gefahndet wird, oder nach der Nummer einer Kreditkarte, die von einer kriminellen Organisation wiederholt eingesetzt worden ist.

In Ausnahmefällen und nur, sofern ein zuständiges Zwangsmassnahmengericht dies genehmigt hat, dürfen auch Daten von Drittpersonen Gegenstand einer Beobachtungsliste sein (Art. 14). Mit Hilfe dieser Daten soll der vorerst noch unbekannte Aufenthalt einer Person im Ausland ausfindig gemacht werden, die einer Straftat nach Anhang 2 beschuldigt oder wegen einer solchen Straftat rechtskräftig verurteilt ist und zur Verbüssung ihrer Freiheitsstrafe gesucht wird.

Der Einsatz dieser Instrumente soll vom Bundesrat überprüft werden (Art. 15).

Die Artikel 17–26 konkretisieren den Datenschutz, der bei der Bearbeitung der Flugpassagierdaten durch die PIU zu beachten ist.

Mit dem totalrevidierten Datenschutzrecht adaptiert die Schweiz datenschutzrechtliche Entwicklungen der EU.[29] Der vorliegende Gesetzesentwurf berücksichtigt das neue Datenschutzrecht, das am 1. September 2023 in Kraft getreten ist.

Das Flugpassagierdatengesetz sieht mit den Artikeln 17–26 Regelungen vor, die in ihrer Mehrzahl das DSG präzisieren und diesem vorgehen. Einzelne Bestimmungen weisen aus Transparenzgründen Regelungen des DSG aus oder verweisen darauf.

Artikel 17 legt dar, welche datenschutzrechtlichen Grundlagen für die PIU sowie für jene Behörden gelten, die Daten nach dem vorliegenden Gesetzesentwurf erhalten und bearbeiten.

Die Daten ohne Markierung, wozu auch solche gehören, deren Markierung nach Artikel 10 wieder aufgehoben worden ist, werden einen Monat nach ihrem Eingang bei der PIU pseudonymisiert und erfahren damit einen technisch erhöhten Schutz (Art. 18).

Die Zeit, in der Daten ohne Markierung einer bestimmten Person zuordenbar sind, beschränkt sich somit auf einen Monat. Anders als die Anonymisierung kann die Pseudonymisierung rückgängig gemacht werden. Dazu ist die Genehmigung des Bundesverwaltungsgerichts erforderlich (Art. 19 und 20).

Nach Ablauf von insgesamt sechs Monaten werden die Daten ohne Markierung automatisch gelöscht. Diese kurze Aufbewahrungsdauer entspricht einem Anliegen, das in der Vernehmlassung wiederholt geäussert worden ist.

Demgegenüber dürfen markierte Daten fünf Jahre aufbewahrt werden, sofern ihre Markierung nicht nach Artikel 10 vorher aufgehoben worden ist. Danach werden auch sie automatisch gelöscht (Art. 21).

Die weiteren Daten, die nach diesem Gesetz bei der PIU anfallen können, unterstehen den Löschfristen, die sich aus Artikel 22 ergeben.

Artikel 24 legt fest, dass von allen automatisierten Bearbeitungen elektronisch ein Protokoll zu erstellen ist. Dieses gibt auch im Nachhinein darüber Auskunft, wer, wann, welchen automatisierten Bearbeitungsschritt vorgenommen hat und welche Daten davon betroffen sind. Die Protokolle müssen ausserhalb des PNR-Informationssystems gespeichert werden (zum Ort der Speicherung siehe Ziff. 6.1) und sind nur den wenigen Personen zugänglich, die dies zur

[29] Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 6941, S. 6943.

Wahrnehmung ihrer Sicherheits- sowie Überwachungs- und Aufsichtsaufgaben zwingend benötigen.

Artikel 26 räumt einer Flugpassagierin oder einem Flugpassagier das Recht ein, Auskunft über die sie oder ihn betreffenden Daten zu erhalten, die gestützt auf das vorliegende Gesetz bearbeitet werden. Eine betroffene Person soll allerdings nicht über die Auskunftserteilung über ein gegen sie laufendes Verfahren informiert werden können.

Dieses Risiko besteht, wenn die Auskunft Daten einer Flugreise betrifft, die länger als sechs Monate zurückliegt. Zu diesem Zeitpunkt sind die meisten Daten dieses Fluges gelöscht. Übrig bleiben nur jene, die markiert sind und deshalb fünf Jahre aufbewahrt werden dürfen (Art. 21).

Im Falle von Auskunftsbegehren, die Daten von Flugreisen betreffen, die länger als sechs Monate zurückliegen, teilt das fedpol der antragstellenden Person deshalb *immer* den Aufschub der Auskunft mit und weist sie auf die Möglichkeit hin, vom EDÖB zu verlangen, dass er prüfe, ob allfällige Daten über sie rechtmässig bearbeitet werden und ob überwiegende Geheimhaltungsinteressen den Aufschub der Auskunft rechtfertigen.

Alle Auskünfte, die Daten von Flugreisen betreffen, die höchstens sechs Monate zurückliegen, richten sich dagegen uneingeschränkt nach dem DSG.

Datenschutzrechtlich relevant sind schliesslich auch jene Bestimmungen, die nicht in diesem, sondern in einem anderen Abschnitt des Gesetzes geregelt sind, so insbesondere:

- Artikel 5 Absatz 1: Zweckbindung der Datenbearbeitung;
- Artikel 5 Absatz 2: Beschränkung der PIU bei der Bearbeitung besonders schützenswerter Personendaten;
- Artikel 6 Absätze 2 und 3, Artikel 7 sowie die Verweise in den Artikeln 8 und 9 auf Artikel 7: Pflicht zur manuellen Überprüfung von Bearbeitungsergebnissen vor deren Bekanntgabe an eine zuständige Behörde;
- Artikel 16 Absatz 2: eingeschränkter Zugriff auf das PNR-Informationssystem.

Den technischen Massnahmen zur Wahrung des Datenschutzes (vgl. Art. 7 Abs. 2 DSG) zuordenbar sind insbesondere:

- der Automatismus, der für den Abgleich (Art. 6), die Pseudonymisierung (Art. 18) und die Löschung der Flugpassagierdaten (Art. 21) vorgesehen ist; sowie
- die Protokollierung der Datenbearbeitung (Art. 24).

Organisatorische Massnahmen zur Wahrung des Datenschutzes sehen schliesslich Artikel 27 Absatz 2 sowie Artikel 28 Absatz 4 vor, um das Risiko eines informellen Austauschs von datenschutzrechtlich relevanten Inhalten einzugrenzen.

Als technische Massnahmen zur Wahrung der Datensicherheit (vgl. Art. 7 DSG) gelten die Pseudonymisierung (Art. 18) und die Anonymisierung der Daten (Art. 23).

Die Artikel 27 und 28 widmen sich der Organisation und dem Personal der PIU.

Die PIU ist beim fedpol angesiedelt (Art. 27). Sie setzt sich je hälftig aus Mitarbeitenden des Bundes und aus Mitarbeitenden zusammen, welche die Kantone entsenden. Die Kantone kommen während der Dauer des Einsatzes ihrer Mitarbeitenden für deren Lohnkosten auf und entrichten die sozialversicherungsrechtlichen Beiträge. Damit wird dem Umstand Rechnung getragen, dass die PIU zu einem überwiegenden Teil einen Nutzen für die Kriminalitätsbekämpfung in den Kantonen bringt. Die Einzelheiten der Entsendung von Personal in die PIU werden Bund und Kantone in einer Vereinbarung festlegen. Der Bundesrat wird berechtigt, mit den Kantonen eine solche Vereinbarung abzuschliessen (Art. 28).

Die Artikel 31 und 32 regeln die administrativen Sanktionen.

Luftverkehrsunternehmen, die ihren Pflichten nach den Artikeln 3 und 4 nicht oder ungenügend nachkommen, können sanktioniert werden. Weisen sie indes nach, dass sie alle zumutbaren technischen und organisatorische Massnahmen getroffen haben, um ihren Pflichten nachzukommen, entfällt die Sanktion (Art. 31 Abs. 4).

4.2 Abstimmung von Aufgaben und Finanzen

Der Schaden, den (Schwerst-)Kriminalität bei Betroffenen und volkswirtschaftlich verursacht, ist immens. Die Aufklärung solcher Straftaten und die Verurteilung der Täterinnen und Täter sind zentrale Elemente in einem Rechtsstaat. Für Opfer ist die Bestrafung der Täterin oder des Täters vielfach Voraussetzung für einen persönlichen Neubeginn.

Sicherheit ist ein wichtiges Gut, damit sich eine Gesellschaft zum Wohle aller entwickeln und Wohlstand erfahren kann. Sicherheit hat jedoch ihren Preis.

Dieser Preis ist nicht nur monetärer Natur, was sich auch in Zusammenhang mit dem vorliegenden Gesetz zeigt: Kontrollen leisten einen wichtigen Beitrag zur öffentlichen Sicherheit, können jedoch punktuell zu Beschränkungen unserer Persönlichkeitsrechte führen, auch wenn kein sicherheitsrelevanter Anlass vorliegt.

Die Nutzung von PNR-Daten gilt als international bewährtes Instrument zur Bekämpfung von Schwerstkriminalität. Mit seiner Einführung leistet die Schweiz nicht nur national, sondern auch international einen Beitrag zu mehr Sicherheit.

Früher wurde jede Person bei der Ein- und Ausreise kontrolliert. Angesichts des rasanten Wachstums, das Flugreisen in den letzten 30 Jahren erfuhren, musste die vor Ort durchgeführte systematische Kontrolle der Reisenden risikobasiert eingegrenzt werden. Zur Wahrung der Sicherheit bleibt das Erkennen von Personen, welche sich der Schwerstkriminalität schuldig gemacht haben oder entsprechende Ziele verfolgen, jedoch unabdingbar.

Mit PNR ist dies möglich. Dies zeigen die Erfolge, welche die EU-Mitgliedstaaten vorweisen können. Im Übrigen hat der EuGH mit dem Urteil vom 21. Juni 2022 anerkannt, dass sich die Nutzung von PNR zur Bekämpfung von Schwerstkriminalität auch mit dem Schutz der Grundrechte vereinbaren lässt.

Die Nutzung von PNR-Daten löst keinen erheblichen Regulierungsaufwand bei den Luftverkehrsunternehmen aus. Ihr Aufwand beschränkt sich auf die rechtzeitige Bekanntgabe verfügbarer Daten an die zuständige staatliche Stelle und die Information der Reisenden. Die Nutzung von PNR verlangt damit von den Luftverkehrsunternehmen keinen spürbaren Mehraufwand.

Die Nutzung von PNR ist nicht nur effizient, sondern auch effektiv. Anders lässt sich nicht erklären, dass dieses Instrument seit rund 20 Jahren und mittlerweile von 69 Staaten, darunter den USA, Kanada, der EU, Australien und dem Vereinigten Königreich, zur Bekämpfung von Schwerstkriminalität eingesetzt wird. Statistiken und Fallberichte einzelner Länder belegen dies klar.

Es ist vorgesehen, dass die Kantone die Hälfte der Mitarbeitenden der PIU entsenden und dafür die Personalkosten tragen. Diese Kostenteilung zwischen Bund und Kantonen widerspiegelt, dass die Sicherheit des Landes und der Schutz der Bevölkerung vor Schwerstkriminalität eine Aufgabe ist, die Bund und Kantonen gemeinsam zu erfüllen haben. Die Kosten für den Aufbau der technischen Infrastruktur sowie die Betriebskosten trägt dagegen alleine der Bund.

4.3 Umsetzungsfragen

Neben den PNR-Daten, die der Bund auf der Grundlage des Flugpassagierdatengesetzes künftig erhält, liefern die Luftverkehrsunternehmen dem Bund bzw. dem Staatssekretariat für Migration (SEM) bereits heute die API-Daten von bestimmten Flügen aus Drittstaaten in die Schweiz, die als risikobehaftet beurteilt werden. Seit 2015 werden diese Daten automatisiert auf der Grundlage der Artikel 104*a* und 104*b* AIG bearbeitet.

Gemäss den internationalen technischen Standards der ICAO, WZO und IATA ist für die Bekanntgabe von PNR- und API-Daten ein sogenanntes *single window* vorzusehen. Gemeint ist damit eine gemeinsame Schnittstelle für die Bekanntgabe der beiden Arten von Daten. Damit soll den Luftverkehrsunternehmen unnötiger Aufwand erspart werden.

Bei der Umsetzung des PNR-Systems muss somit für die API- und die PNR-Daten auf technischer Ebene ein solches *single window* bereitgestellt werden. Explizit wurde diese Lösung vom Verband Schweizer Flugplätze und von der Swiss im Rahmen der Vernehmlassung begrüsst.

5 Erläuterungen zu einzelnen Artikeln

1. Abschnitt: Gegenstand

Artikel 1 Gegenstand und Zweck

Diese Bestimmung weist die wichtigsten Inhalte sowie den Zweck aus, der mit diesem Gesetz verfolgt wird.

Absatz 1

Buchstabe a

Die Luftverkehrsunternehmen haben die Flugpassagierdaten sowohl beim Flug in die Schweiz als auch beim Flug von der Schweiz ins Ausland der PIU bekanntzugeben.

Diese Pflicht ist für Luftverkehrsunternehmen grundsätzlich nicht neu. Sie erfüllen sie seit Jahren zum Beispiel gegenüber den USA, Kanada und gegenüber den EU-Mitgliedstaaten. Neu wird für die Luftverkehrsunternehmen lediglich die Pflicht sein, die Flugpassagierdaten auch der PIU bekanntzugeben.

Buchstabe b

Neben den Pflichten der Luftverkehrsunternehmen regelt das Gesetz auch die Bearbeitung der Flugpassagierdaten durch die zuständigen Stellen.

Flugpassagierdaten dürfen bearbeitet werden, wenn damit Schwerstkriminalität bekämpft wird (vgl. Abs. 4).

Buchstabe c

Das vorliegende Gesetz legt zusätzlich auch die Organisation der nationalen Stelle fest, die für die Bearbeitung der Flugpassagierdaten in der Schweiz zuständig sein wird. Die international übliche Bezeichnung dieser Stelle, *Passenger Information Unit* oder kurz *PIU*, soll auch in der Schweiz Anwendung finden.

Die PIU soll beim fedpol angesiedelt werden (vgl. Art. 27) und sich sowohl aus Mitarbeitenden des Bundes wie der Kantone zusammensetzen (vgl. Art. 28).

Absatz 2

Der Zweck des vorliegenden Gesetzes besteht darin, Behörden von Bund und Kantonen bei der Bekämpfung von Schwerstkriminalität (vgl. Anhang 2) zu unterstützen.

Behörden, welche Leistungen der PIU nach diesem Gesetz erhalten, sind die Polizei- und Strafverfolgungsbehörden von Bund und Kantonen, die Nachrichtendienste des Bundes, bestehend aus dem Nachrichtendienst des Bundes (NDB) und dem Nachrichtendienst der Armee, sowie die kantonalen Vollzugsbehörden nach Artikel 9 NDG.

Zu den Strafverfolgungsbehörden des Bundes gehört unter anderem auch der Bundessicherheitsdienst (Art. 4 Bst. b des Strafbehördenorganisationsgesetzes vom 19. März 2010[30]).[31]

Absatz 3

Im geltenden Recht findet sich keine Definition der *Luftverkehrsunternehmen*. Deshalb werden sie hier näher umschrieben. Die Umschreibung orientiert sich an jener, die im CO_2-Gesetz vom 25. September 2020[32] (Art. 2 Bst. i) vorgesehen war. Luftverkehrsunternehmen ist, wer als Unternehmen Personen gewerbsmässig mit einer Betriebsbewilligung oder einer anderen gleichwertigen Bewilligung auf dem Luftweg transportiert.

Nicht als Luftverkehrsunternehmen gilt die sogenannte Leichtaviatik. Darunter fallen Schul-, Übungs- und Kontrollflüge, Touristikflüge, Luftsport sowie Privatflüge. Vom Anwendungsbereich des Gesetzes ausgenommen sind auch militärische und andere hoheitliche Flüge sowie Such- und Rettungsflüge.

Die begriffliche Umschreibung der Luftverkehrsunternehmen ist insofern wichtig, als diese durch das vorliegende Gesetz verpflichtet werden. In- und ausländische Luftverkehrsunternehmen haben die Flugpassagierdaten rechtzeitig und entsprechend den technischen Vorgaben der PIU bekanntzugeben (vgl. Art. 2 und 3). Zudem haben sie ihre Passagierinnen und Passagiere angemessen über die Datenbearbeitung nach dem vorliegenden Gesetz zu informieren (vgl. Art. 4). Allfällige Verletzungen dieser Pflichten können nach Artikel 31 sanktioniert werden.

Absatz 4

Anhang 1 dieses Gesetzes weist die Flugpassagierdaten aus, die von den Luftverkehrsunternehmen bekanntzugeben sind und nach dem vorliegenden Gesetz bearbeitet werden.

30 SR **173.71**
31 Botschaft vom 10. September 2008 zum Bundesgesetz über die Organisation der Strafbehörden des Bundes (Strafbehördenorganisationsgesetz, StBOG), BBl **2008** 8125 S. 8150.
32 BBl **2020** 7847 S. 7848; abgelehnt in der Volksabstimmung vom 13. Juni 2021.

Die Flugpassagierdaten gliedern sich in insgesamt 19 verschiedene Datenkategorien, die zusammen den Flugpassagierdatensatz bilden. Die Datenkategorien entsprechen der PNR-Richtlinie und berücksichtigen im vorliegenden Wortlaut die Auslegung, welche der EuGH in seinem Urteil vom 21. Juni 2022 von den EU-Mitgliedstaaten verlangt.

Die Luftverkehrsunternehmen erheben die Flugpassagierdaten bei der Buchung von Flugtickets. Sie benötigen diese Daten zur Abwicklung des Fluges. Ihre Bearbeitung nach dem vorliegenden Gesetz beschränkt sich auf bereits verfügbare Daten ist damit nur nachgelagert.

Einen Sonderfall bilden die API-Daten, die – soweit verfügbar – von den Luftverkehrsunternehmen als Teil des Flugpassagierdatensatzes in Kategorie 18 bekanntzugeben sind. Die API-Daten fallen nicht bei der Buchung an, sondern müssen von den Luftverkehrsunternehmen erhoben werden, wenn dies staatlich verlangt wird (vgl. Art. 104 AIG). Deshalb sind sie nur dann als Kategorie 18 im Rahmen von PNR an die PIU bekanntzugeben, wenn sie *verfügbar* sind.

Viele der 19 Datenkategorien weisen keine Daten auf, die Rückschlüsse auf eine Person geben. Weil sie damit keine Personendaten sind (vgl. Art. 5 Bst. a DSG), fällt ihre Bearbeitung auch nicht in den Geltungsbereich des revidierten Datenschutzgesetzes (Art. 2 DSG).

Personendaten finden sich in den folgenden Kategorien des Flugpassagierdatensatzes:

- *Kategorie 4:* Name(n) sowie Zahl und Namen der mitreisenden Personen;
- *Kategorie 5:* Adresse und Kontaktdaten einschliesslich E-Mail, Telefon-Nummern;
- *Kategorie 6:* Angaben zur allenfalls eingesetzten Kreditkarte sowie Rechnungsadresse;
- *Kategorie 8:* Vielfliegerprogramm: Status und Nummer der Flugpassagierin oder des Flugpassagiers;
- *Kategorie 9:* Name der Sachbearbeiterin oder des Sachbearbeiters des Reisebüros, das die Buchung des Tickets vorgenommen hat;
- *Kategorie 12:* Angaben zu unbegleiteten Personen unter 18 Jahren, Name und Kontaktdaten der Begleitpersonen beim Abflug, bei der Ankunft sowie der begleitenden Flughafenmitarbeitenden vor dem Abflug und nach der Landung;
- *Kategorie 17:* Zahl, Vornamen und Nachnamen von Mitreisenden im Flugpassagierdatensatz;
- *Kategorie 18:* API-Daten (vgl. Art. 104 Abs. 3 AIG), die zugleich Personendaten sind: (a) Personalien (Name, Vorname, Geschlecht, Geburtsdatum, Staatsangehörigkeit) der Flugpassagierin / des Flugpassagiers; (b) Nummer, Ausstellerstaat, Art und Ablaufdatum des

mitgeführten Reisedokuments; (c) Nummer, Ausstellerstaat, Art und Ablaufdatum des mitgeführten Visums oder Aufenthaltstitels, soweit das Luftverkehrsunternehmen über diese Daten verfügt.

- *Kategorie 19:* Sie enthält alle Änderungen des Flugpassagierdatensatzes. Personendaten enthält diese Kategorie, wenn solche im Nachgang zur Buchung Änderungen erfahren haben.

Die Flugpassagierdaten dürfen nach diesem Gesetz ausschliesslich zur Bekämpfung von Schwerstkriminalität bearbeitet werden. Als Schwerstkriminalität gelten jene Straftaten, die im Deliktskatalog nach Anhang 2 unter Angabe der massgeblichen Straftatbestände des Strafgesetzbuches[33] (StGB) oder des Nebenstrafrechts ausgewiesen sind. Anhang 2 unterteilt sie in terroristische (Ziff.1) und andere schwere Straftaten (Ziff. 2).

Ursprünglich orientierte sich der Deliktskatalog an den Deliktskategorien der PNR-Richtlinie und ordnete diesen die massgeblichen Straftatbestände zu, welche der im Rahmen von PRÜM[34] erweiterte Anhang 1 des Schengen-Informationsaustausch-Gesetzes vom 12. Juni 2009[35] (SIaG) vorsieht. Obschon die Erweiterung noch nicht in Kraft ist, wird sie vorliegend bereits berücksichtigt. Gleiches gilt für eine weitere Ergänzung des SIaG-Anhangs, die sich derzeit in Vorbereitung befindet. Abweichend von Anhang 1 SIaG berücksichtigt der für PNR massgebende Deliktskatalog neu auch schwere Formen des verbotenen Nachrichtendienstes.

Als *terroristisch* im Sinne des Flugpassagierdatengesetzes gelten die Straftaten, die unter die Tatbestände nach Ziffer 22 Anhang 1 SIaG fallen. Nicht mehr in dem für PNR massgebenden Deliktskatalog aufgeführt ist der Straftatbestand des Landfriedensbruchs (vgl. Art. 260 Abs. 1 StGB). Damit wird Forderungen aus der Vernehmlassung entsprochen.

Die meisten dieser Straftaten sind Verbrechen. Die angedrohte Maximalstrafe beläuft sich auf *mehr* als drei Jahre (vgl. Art. 10 Abs. 2 StGB). Dagegen handelt es sich bei den folgenden Straftatbeständen um Vergehen (vgl. Art. 10 Abs. 3 StGB). Sie sind mit einer Höchststrafe von maximal drei Jahren bedroht:

- Schreckung der Bevölkerung (Art. 258 StGB),
- öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit (Art. 259 StGB).

33 SR **311.0**

34 Bundesbeschluss über die Genehmigung und die Umsetzung des Abkommens zwischen der Schweiz und der EU zur Vertiefung der grenzüberschreitenden Zusammenarbeit (Prümer Zusammenarbeit) und des Eurodac-Protokolls zwischen der Schweiz, der EU und dem Fürstentum Liechtenstein betreffend den Zugang zu Eurodac für Gefahrenabwehr- und Strafverfolgungszwecke, BBl **2021** 2332 S. 10–16.

35 SR **362.2**

Als terroristisch gelten die Mehrzahl der in dieser Kategorie aufgeführten Straftaten nur, wenn sie auch tatsächlich terroristisch motiviert sind (vgl. Anhang 2 Ziff. 1). Terroristisch motiviert ist eine Straftat insbesondere, wenn durch ihre Begehung oder Androhung die staatliche Ordnung verändert oder beeinflusst werden soll (vgl. Art. 23*e* des Bundesgesetzes vom 21. März 1997[36] über Massnahmen zur Wahrung der inneren Sicherheit [BWIS]).

Als *andere schwere Straftaten* weist Anhang 2 des vorliegenden Gesetzes aus:

- unter Ziffer 2.1: Verbrechen aus dem bereits erwähnten Anhang 1 des SIaG, sowie
- unter Ziffer 2.2: Verbrechen in Zusammenhang mit dem verbotenen Nachrichtendienst.

Der Katalog der anderen schweren Straftaten wurde aufgrund verschiedener Anliegen aus der Vernehmlassung, die Bezug auf das EuGH-Urteil nahmen, deutlich gestrafft. Insbesondere wurde auf die Straftaten in der Strafverfolgungskompetenz des Bundesamts für Zoll und Grenzsicherheit (BAZG) verzichtet, da es sich hierbei nicht um Schwerstkriminalität handelt.

Der Deliktskatalog umfasst jetzt nur noch jene Straftatbestände, die:

a) gemäss EuGH *explizit* einen «unbestreitbar hohen Schweregrad» (Rz. 149), als Schwerstkriminalität einen unmittelbaren Bezug zu Flugreisen (Rz. 154) oder einen grenzüberschreitenden Charakter (Rz. 155) aufweisen; oder

b) nach Schweizer Recht eine gesetzliche Mindeststrafe vorsehen, die als vom EuGH erwähnte Besonderheit des nationalen Rechts verstanden werden kann und Rückschluss auf eine besondere Schwere der Straftat zulässt (e contrario aus Rz. 151 f.).

Mit Blick auf die veränderte geopolitische Lage sieht der Deliktskatalog zusätzlich drei Straftatbestände in Zusammenhang mit dem verbotenen Nachrichtendienst vor (Ziff. 2.2). Diese schweren Formen des verbotenen Nachrichtendiensts sind allesamt Verbrechen im Sinne von Artikel 10 Absatz 2 StGB und sehen zusätzlich eine gesetzliche Mindeststrafe vor.

2. Abschnitt: Pflichten der Luftverkehrsunternehmen

Artikel 2 Bekanntgabe der Flugpassagierdaten

Als Bekanntgabe gelten jede Übermittlung und jedes Zugänglichmachen von Personendaten (vgl. Art. 5 Bst. e DSG).

Artikel 2 legt die Einzelheiten fest, nach denen die Bekanntgabe von Flugpassagierdaten durch die Luftverkehrsunternehmen zu erfolgen hat. Verletzungen dieser Pflichten können Sanktionen zur Folge haben (vgl. Art. 31).

36 SR **120**

In der Vernehmlassung wurde die Aufnahme einer Bestimmung angeregt, welche die zulässige Nutzung und die Löschung der Flugpassagierdaten durch die Luftverkehrsunternehmen regelt. Dem kann nicht entsprochen werden. Denn die Flugpassagierdaten sind Daten, welche die Luftverkehrsunternehmen zur Abwicklung der Buchung und des Flugs benötigen. Vor diesem Hintergrund bestimmt sich die für diese Daten bei den Luftverkehrsunternehmen geltende Aufbewahrungsdauer nach deren betrieblicher Notwendigkeit und nach den dabei zu beachtenden Grundsätzen des Datenschutzes.

Absatz 1

Artikel 2 legt fest, dass alle Luftverkehrsunternehmen (vgl. Art. 1 Abs. 3), die die Schweiz anfliegen, der Schweizer PIU die Flugpassagierdaten bekanntzugeben haben (Abs. 1).

Auch Flüge, die unter schweizerischem Recht (mit IATA-Flughafencode «BSL») auf dem Euroairport Basel Mulhouse Freiburg landen, gelten als Flüge in die Schweiz, obschon sich der Flughafen auf einem Terrain befindet, das ausserhalb der Schweiz liegt. Gleiches gilt für Flüge, die mit dem entsprechenden IATA-Flughafencode ab dem Euroairport Basel Mulhouse Freiburg einen nicht schweizerischen Flughafen anfliegen.

Keine Flugpassagierdaten bekanntzugeben sind demgegenüber bei Inlandflügen, selbst wenn sie von Luftverkehrsunternehmen nach Artikel 1 Absatz 3 durchgeführt werden.

Absatz 2

Flugpassagierdaten fallen bei der Buchung eines Flugtickets an. Wird das Ticket bei einem Schweizer Luftverkehrsunternehmen gebucht, befinden sich die entsprechenden Daten in der Schweiz. Wird das Ticket dagegen von der Schweiz aus bei einem im Ausland ansässigen Luftverkehrsunternehmen gebucht, befinden sich die Flugpassagierdaten nicht mehr in der Schweiz, sondern in jenem Staat, in dem das Luftverkehrsunternehmen seinen Sitz hat. Mit dieser Ticketbuchung gibt eine Flugpassagierin oder ein Flugpassagier ihre Daten selber «ins Ausland» bekannt oder stimmt dieser Datenbekanntgabe zu.

Absatz 2 gilt deshalb nur für Schweizer und nicht für ausländische Luftverkehrsunternehmen. Schweizer Luftverkehrsunternehmen dürfen die Daten ihrer Passagierinnen und Passagiere nur einer PIU im Ausland bekanntgeben, wenn ein völkerrechtlicher Vertrag mit der Schweiz dies vorsieht (vgl. Art. 29).

Wurde der Flug dagegen von der Schweiz aus bei einem ausländischen Luftverkehrsunternehmen gebucht, bestimmt sich die grenzüberschreitende Datenbekanntgabe durch das ausländische Luftverkehrsunternehmen nach dem auf dieses anwendbaren (ausländischen) Recht.

Vertragspartner der Schweiz kann ein ausländischer Staat oder eine internationale Organisation sein. Als internationale Organisation zu erwähnen ist im vorliegenden Zusammenhang insbesondere die EU.

Handelt die Schweiz einen solchen Vertrag mit einem Vertragspartner aus, der über einen angemessenen Datenschutz (vgl. Art. 16 Abs. 1 DSG) verfügt, müssen seitens der Schweiz keine spezifischen Regelungen für den Schutz der bekanntgegebenen Daten aus der Schweiz vereinbart werden. Zur Datenbekanntgabe nach Absatz 2 reicht somit ein völkerrechtlicher Vertrag, der sich auf die Gegenseitigkeit der Datenbekanntgabe beschränkt.

Wird dem Vertragspartner dagegen kein angemessener Datenschutz attestiert, muss der völkerrechtliche Vertrag zusätzlich zur Gegenseitigkeit der Datenbekanntgabe auch Regelungen vorsehen, die bei der Bearbeitung der Flugpassagierdaten aus der Schweiz einzuhalten sind. Damit gewährleistet der Vertragspartner einen geeigneten Schutz der Daten aus der Schweiz (vgl. Art. 16 Abs. 2 Bst. a DSG).

Bereits heute liefern Schweizer Luftverkehrsunternehmen Flugpassagierdaten an Staaten, die das Ziel von Flügen aus der Schweiz sind, so an die USA und an Kanada. In beiden Fällen bilden Abkommen mit der Schweiz die Grundlage der Datenbekanntgabe. Beide Abkommen sichern im Übrigen die Datenbekanntgabe an die Schweizer PIU zu, sobald mit dem vorliegenden Gesetz die nötige Rechtsgrundlage für die Bearbeitung von Flugpassagierdaten geschaffen ist.

Weitere Abkommen sind geplant. Ein Mandat für Verhandlungen mit der EU ist in Vorbereitung. Mit dem Abkommen soll die heute geltende Übergangsregelung abgelöst werden (vgl. Ziff. 1.2).

Absatz 3

Die Flugpassagierdaten sind der PIU innerhalb von zwei Zeitfenstern bekanntzugeben: frühestens 48 bis spätestens 24 Stunden vor dem planmässigen Abflug sowie nach Abschluss des Boardings. Die Bekanntgabe von Daten im ersten Zeitfenster liefert zwar erst provisorische Angaben, erlaubt der PIU aber eine gewisse Vorlaufzeit bis zur Landung, was gerade bei kurzen Flügen unabdingbar ist. Die Bekanntgabe der Daten unmittelbar nach Abschluss des Boardings *aktualisiert* die bereits eingegangenen Daten und liefert ein abschliessendes Bild der Flugpassagierinnen und -passagiere, die tatsächlich in die Schweiz einreisen oder sie verlassen. Die in den vorherigen Zeitfenstern an die PIU bekanntgegebenen Daten jener Flugpassagierinnen und -passagiere, die den Flug schliesslich nicht angetreten haben, sind für die PIU nicht mehr einsehbar und können deshalb von ihr auch nicht mehr bearbeitet werden.

Dank der gestaffelten Bekanntgabe kann sich die PIU nach dem Boarding auf jene Daten konzentrieren, die eine Aktualisierung erfahren haben oder neu dazugekommen sind.

Die Luftverkehrsunternehmen lösen die Bekanntgabe der Flugpassagierdaten an die PIU selber aus. Diese sogenannte PUSH-Methode entspricht nicht nur

der Empfehlung der ICAO[37], sondern auch Artikel 8 der PNR-Richtlinie der EU.

Absatz 4

Zuständig für Festlegung der Einzelheiten, die bei der Bekanntgabe zu beachten sind, soll der Bundesrat sein. Zu den *technischen* Einzelheiten, die es zu regeln gilt, gehören unter anderem die zulässigen Formate, die bei der Bekanntgabe der Flugpassagierdaten Anwendung finden dürfen.

Der Bundesrat wird sich an den Vorgaben der ICAO orientieren, die für alle Mitgliedstaaten – und damit auch für die Schweiz – verbindlich sind. Diese internationalen Standards stellen sicher, dass die Datenbekanntgabe weltweit nach einheitlichen Grundsätzen erfolgt, so dass den Luftverkehrsunternehmen kein Mehraufwand durch länderspezifische Sonderregelungen erwächst. Sind internationale Vorgaben zu präzisieren, wird sich der Bundesrat möglichst an Lösungen der EU orientieren. Damit entspricht er den nachvollziehbaren Forderungen, die Vertreterinnen und Vertreter der Luftfahrtbranche in der Vernehmlassung geäussert haben: Auf einen *Swiss finish* und damit auf spezifisch schweizerische Sonderreglungen sei zu verzichten.

Artikel 3 Sorgfaltspflicht

Die Luftverkehrsunternehmen haben der PIU die Daten aller Passagierinnen und Passagiere rechtzeitig und entsprechend den technischen Vorgaben bekanntzugeben (vgl. Art. 2 Abs. 3 und 4).

Sie haben die zumutbaren Massnahmen zu treffen, um dieser Pflicht nachzukommen. Andernfalls greifen die Sanktionsmöglichkeiten nach Artikel 31.

Artikel 4 Informationspflicht

Artikel 4 verpflichtet die Luftverkehrsunternehmen, die Flugpassagierinnen und -passagiere bei der Buchung des Flugtickets *angemessen* darüber zu informieren, dass ihre bei der Buchung des Flugs bekanntgegebenen Daten nicht lediglich für die Abwicklung ihrer Flugreise bearbeitet werden, sondern zusätzlich auch nach dem Flugpassagierdatengesetz.

Artikel 13 der Datenschutzverordnung vom 31. August 2022[38] (DSV) präzisiert den Begriff der Angemessenheit: Die Information muss in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen.

Im erläuternden Bericht zur DSV hält das Bundesamt für Justiz fest: «Mit anderen Worten muss der Verantwortliche bei der Wahl der Informationsform sicherstellen, dass die betroffene Person bei der Beschaffung ihrer Personendaten die wichtigsten Informationen stets auf der ersten Kommunikationsstufe

37 ICAO, Guidelines on Passenger Name Record (PNR) Data, Ziff. 2.7.3, abrufbar unter www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf.

38 SR **235.11**

erhält. Erfolgt die Kommunikation zum Beispiel über eine Internetseite, kann eine gute Praxis darin bestehen, dass alle wesentlichen Informationen auf einen Blick, z. B. in Form einer gegliederten Übersicht, verfügbar sind. Um weitere Informationen zu erhalten, kann die betroffene Person danach auf diese zuerst angezeigten Informationen klicken, worauf sich ein Fenster mit detaillierteren Angaben öffnet. Es ist allerdings festzuhalten, dass die Kommunikation über eine Website nicht immer genügt: Die betroffene Person muss wissen, dass sie die Informationen auf einer bestimmten Website findet.»[39]

Damit die Passagierinnen und Passagiere ihre Rechte wahrnehmen können, müssen die Luftverkehrsunternehmen ihnen gestützt auf Artikel 4 des vorliegenden Gesetzes mindestens die folgenden Informationen abgeben:

- den Hinweis, dass die Flugpassagierdaten dem fedpol bekanntgegeben werden;
- den vollständigen Titel des vorliegenden Gesetzes als rechtliche Grundlage für die Bearbeitung der Flugpassagierdaten;
- den Hinweis auf das Auskunftsrecht nach Artikel 26;
- die Kontaktdaten des fedpol;
- den Namen der ausländischen Stelle, wenn die Daten ins Ausland bekanntgegeben werden.

Kommt ein Luftverkehrsunternehmen der Informationspflicht nach Artikel 4 nicht oder nur ungenügend nach, muss es mit Sanktionen nach Artikel 31 rechnen.

Auf die Informationspflicht liesse sich verzichten, da die Bearbeitung der Flugpassagierdaten gesetzlich vorgesehen ist (vgl. Art. 19 DSG). Dass sie trotzdem im Flugpassagierdatengesetz vorgesehen ist, rechtfertigt sich, weil die Flugpassagierdaten wie folgt bearbeitet werden:

- in zwei vollständig verschiedenen tatsächlichen und rechtlichen Kontexten (technische Abwicklung Flugbuchung / Umsetzung Flugpassagierdatengesetz);
- zu unterschiedlichen Zwecken (Flugbuchung / Bekämpfung Schwerstkriminalität); und
- unter unterschiedlicher Verantwortung (Luftverkehrsunternehmen / fedpol).

Mit Blick auf die in Artikel 11 gesetzlich geregelte automatisierte Weiterleitung von Streckenlisten an den NDB hätte der EDÖB eine weitergehende In-

39 Erläuternder Bericht des Bundesamtes für Justiz vom 31. August 2022 zur Datenschutzverordnung, S. 37; www.bj.admin.ch > Neues Datenschutzrecht > Neues Datenschutzrecht > 1. Bisherige Etappen, 2022 – Verabschiedung der neuen Verordnungen (DSV und VDSZ).

formationspflicht der Luftverkehrsunternehmen bevorzugt. Er macht in diesem Zusammenhang darauf aufmerksam, dass die automatisierte Weiterleitung von Informationen über einen dafür eingesetzten Dienst nicht zu einer Verwässerung der Informationspflicht führen darf.

3. Abschnitt: Datenbearbeitung durch die PIU

Artikel 5 Grundsätze

Absatz 1

Absatz 1 regelt den Zweck der *Datenbearbeitung*.

Sowohl präventiv wie auch repressiv sollen PNR-Daten zur Bekämpfung von Schwerstkriminalität eingesetzt werden können. Dies bringt die Aufzählung in Absatz 1 zum Ausdruck:

- *präventiv:* im Erkennen und Verhindern solcher Straftaten (vgl. u. a. Art. 6 Abs. 1 Bst. a NDG, Art. 2*a* Bst. f des Bundesgesetzes vom 7. Oktober 1994[40] über die kriminalpolizeilichen Zentralstellen des Bundes und gemeinsame Zentren für Polizei- und Zollzusammenarbeit mit anderen Staaten [ZentG], kantonale Polizeigesetze);
- *repressiv:* im Aufklären solcher Straftaten sowie in der Fahndung nach Beschuldigten (vgl. u. a. Art. 15–21 der Strafprozessordnung[41] [StPO]) und nach rechtskräftig wegen einer solchen Straftat Verurteilten, die die verhängte Strafe nicht oder noch nicht vollständig verbüsst haben.

Einschränkungen dieses Zwecks finden sich beim Einsatz von Risikoprofilen (Art. 12) und von Beobachtungslisten (Art. 13 und 14).

Absatz 2

Besonders schützenswerte Personendaten (vgl. Art. 5 Bst. c DSG) sind weder in Risikoprofilen noch in Beobachtungslisten zu finden. Auch in den Flugpassagierdaten nach Anhang 1 sind keine besonders schützenswerten Personendaten vorgesehen.

Auf solche Daten kann die PIU aber bei der Überprüfung von Übereinstimmungen stossen, die aufgrund des automatischen Abgleichs erzielt worden sind (vgl. Art. 6 Abs. 2 und 3).

Die PIU darf solche Daten nur bearbeiten, wenn es sich um die in Absatz 2 genannten handelt. Es sind dies:

- biometrische Daten, die eine natürliche Person identifizieren, so zum Beispiel der digitale Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme;

40 SR **360**
41 SR **312**

- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen; diesen Daten gleichgestellt sind Angaben über polizeiliche Realakte (Sicherheits- und Schutzmassnahmen).[42]

Alle weiteren besonders schützenswerten Daten, die bei der Bearbeitung der Flugpassagierdaten anfallen können, hat die PIU umgehend zu löschen (vgl. Art. 22 Bst. a).

Artikel 6 Automatischer Datenabgleich

Der automatische Datenabgleich, den alle Flugpassagierdaten durchlaufen, ist zeitlich eingegrenzt. Er hat *unmittelbar* nach ihrem Eingang bei der PIU zu erfolgen und wird automatisch ausgelöst (Abs. 1).

Mit dem Datenabgleich erfahren die Flugpassagierdaten eine erste Triage in:

- Daten, die keine Übereinstimmung erzielt haben und – vorbehältlich der Artikel 8−11 − nicht mehr vertieft weiterzubearbeiten sind, und
- Daten, die eine Übereinstimmung erzielt haben, deshalb näher zu prüfen (Abs. 2 und 3) und allenfalls der zuständigen Behörde zur weiteren Bearbeitung bekanntzugeben sind (vgl. Art. 7).

Verläuft diese Prüfung nach Absatz 2 positiv, gibt die PIU die Übereinstimmung und die betroffenen Flugpassagierdaten als Ergebnis des automatischen Abgleichs der zuständigen Behörde bekannt (vgl. Art. 7) und markiert die bekanntgegebenen Daten. Die Behörde, welche die Daten von der PIU erhält, entscheidet sodann über allfällige Massnahmen.

Die markierten Daten unterliegen einer fünfjährigen Aufbewahrungsfrist. Demgegenüber werden die Daten ohne Markierung nach einem Monat pseudonymisiert (vgl. Art. 18) und nach fünf weiteren Monaten automatisch gelöscht (vgl. Art. 21).

Absatz 1

Die Flugpassagierdaten werden bei ihrem Eintreffen im Informationssystem der PIU automatisch abgeglichen:

- mit den Daten der polizeilichen Informationssysteme nach den Artikeln 15 und 16 des Bundesgesetzes vom 13. Juni 2008[43] über die polizeilichen Informationssysteme des Bundes (BPI) sowie gestützt auf Artikel 351 StGB[44] mit dem polizeilichen Informationssystem von Interpol;

42 Gemäss BGE 130 I 369, S. 380 ist unter einem Realakt das «tatsächliche und informelle Verwaltungshandeln» zu verstehen. Es «zeichnet sich u.a. dadurch aus, dass es an sich nicht auf Rechtswirkungen, sondern auf die Herbeiführung eines Taterfolges ausgerichtet ist, indessen gleichwohl die Rechtsstellung von Privaten berühren kann».

43 SR **361**

44 SR 311.0

- mit den Risikoprofilen nach Artikel 12; und
- mit den Beobachtungslisten nach den Artikeln 13 und 14.

Finden sich Inhalte eines Flugpassagierdatensatzes (vgl. Anhang 1), beispielsweise der Name der Person, die Telefonnummer oder die E-Mail-Adresse, auch in einem der beiden polizeilichen Informationssystemen oder in einer Beobachtungsliste, führt der automatische Datenabgleich zu einer Übereinstimmung.

Nachfolgend wird näher auf die beiden polizeilichen Informationssysteme eingegangen, mit deren Daten die Flugpassagierdaten automatisch abgeglichen werden.

Das *automatisierte Polizeifahndungssystem (RIPOL; vgl. Art. 15 BPI)* enthält Angaben zu Personen, die zur Verhaftung oder Fahndung ausgeschrieben sind, Informationen zu ungeklärten Straftaten oder zu an einer Straftat beteiligten Personen sowie weitere zur Aufklärung von Straftaten dienende Informationen. Es unterstützt die zuständigen Behörden von Bund und Kantonen bei der Verhaftung von Personen und bei der Abwehr von Gefahren für die öffentliche Sicherheit. Der Abgleich der Flugpassagierdaten mit dem RIPOL kann nicht nur zu Fahndungserfolgen beitragen, sondern auch zu Ermittlungsfortschritten bei ungeklärten terroristischen und anderen schweren Straftaten nach Anhang 2 E-FPG. Wer zum Abgleich mit dem RIPOL berechtigt ist, erhält beim Abgleich automatisch auch Übereinstimmungen mit der Interpol-Datenbank «Automated Search Facility» (ASF) gemeldet. Diese Datenbank enthält Informationen zu international gesuchten Personen sowie zu gestohlenen oder verlorenen Identifikationsdokumenten.

Der nationale Teil des Schengener Informationssystems (N-SIS; vgl. Art. 16 BPI) umfasst Ausschreibungen von Personen und Sachen (z. B. zu gestohlenen Ausweisdokumenten), die im Schengen-Raum gesucht werden. Der Abgleich der Flugpassagierdaten mit dem N-SIS kann dazu führen, dass den zuständigen Behörden die Verhaftung von Personen bei der Ein- und Ausreise gelingt, die international gesucht werden.

Näheres zu den beim automatischen Abgleich eingesetzten Risikoprofilen und Beobachtungslisten findet sich in den Erläuterungen zu den Artikeln 12–14.

Absatz 2

Die Meldung einer im Rahmen des automatischen Datenabgleichs erzielten Übereinstimmung durch das PNR-Informationssystem allein reicht nicht, um eine Bekanntgabe an die zuständige Behörde und die Markierung der Daten zu legitimieren (vgl. Art. 7 Abs. 1).

Vielmehr muss die PIU jede einzelne Übereinstimmung manuell überprüfen. Damit stellt die PIU sicher, dass keine Bearbeitungsergebnisse an eine zuständige Behörde bekanntgegeben werden, die:

- ausserhalb des für die Datenbearbeitung zulässigen Zwecks (vgl. Art. 5 Abs. 1) liegen; oder

- sich – beispielsweise aufgrund einer fehlerhaften Erfassung des Namens – auf eine falsche Person beziehen.

Oftmals lassen sich diese Fragen nur klären, indem manuell auf zusätzliche Angaben in polizeilichen und weiteren Informationssystemen des Bundes zugegriffen wird.

Absatz 3

Absatz 3 nennt die Informationssysteme, auf welche die PIU zur Überprüfung der Übereinstimmungen zugreifen darf.

Buchstabe a

Ob bei der Übereinstimmung tatsächlich ein Straftatbestand nach Anhang 2 vorliegt, muss die PIU klären, indem sie manuell auf Hintergrundinformationen zu den Tatumständen im RIPOL und N-SIS (vgl. Erläuterungen zu Abs. 1) sowie in den folgenden polizeilichen Informationssystemen zugreift:

- *Das Nationale Ermittlungssystem (NES, Art. 10 und 11 BPI)* umfasst Informationen zu gerichtspolizeilichen Ermittlungen des Bundes sowie zu Vorermittlungen und gerichtspolizeilichen Ermittlungen der Kantone. Von Bedeutung können zudem die Informationen zur Zusammenarbeit der Bundeskriminalpolizei mit Strafverfolgungsbehörden und Kriminalpolizeien der Kantone sowie mit ausländischen Behörden im Kampf gegen internationale und organisierte Kriminalität sein.
- *Das System internationale und interkantonale Polizeikooperation (IPAS, Art. 12 BPI)* enthält unter anderem Informationen zu laufenden Ermittlungen in- oder ausländischer Polizei- und Strafverfolgungsbehörden.
- *Nationaler Polizeiindex (Art. 17 BPI):* Er umfasst Hintergrundinformationen zu Ausschreibungen der Kantone.
- *SIRENE-IT (gestützt auf Art. 18 BPI):* Darin finden sich Hintergrundinformationen zu Ausschreibungen im Schengen-Informationssystem in den Bereichen der organisierten Kriminalität und des Terrorismus.
- *Interpol-Informationssystem (I-24/7, Art. 350–352 StGB):* Dieses System der Internationalen Kriminalpolizeilichen Organisation (Interpol) enthält Informationen, die Rückschlüsse auf die Gründe internationaler Ausschreibungen ermöglichen.

Buchstabe b

Zur Klärung der Identität werden vor allem hinterlegte Angaben zur Person und zu ihren Reiseinformationen von Bedeutung sein. Dazu muss die PIU nicht nur auf das RIPOL und das N-SIS zugreifen können, sondern auch auf die folgenden Informationssysteme des Bundes:

- *Nationales Visumsystem (ORBIS, Art. 109b AIG):* Das nationale Visumsystem liefert Angaben zu Visumsgesuchen und weist alle Personen aus, die über ein Visum für den Schengen-Raum verfügen. Eine Person kann anhand der überprüfbaren Passnummer identifiziert werden.
- *Zentrales Migrationsinformationssystem (ZEMIS, Bundesgesetz vom 20. Juni 2003[45] über das Informationssystem für den Ausländer- und den Asylbereich, BGIAA):* Das Zentrale Migrationsinformationssystem enthält Personendaten von Ausländerinnen und Ausländern in der Schweiz (z. B. Name, Vorname, Geburtsdatum) und deren Aufenthaltsstatus. Über das ZEMIS abrufbar sind neu auch die Daten aus dem Informationssystem zur Ausstellung von schweizerischen Reisedokumenten und Bewilligungen zur Wiedereinreise an Ausländerinnen und Ausländer ISR (bisher Art. 111 Abs. 1 AIG). Damit lassen sich über das ZEMIS auch Angaben aus Reisedokumenten wie Name, Heimatort von in der Schweiz registrierten Ausländerinnen und Ausländern mit einem von der Schweiz ausgestellten Reisedokument (z. B. Flüchtlingsreisepass) abrufen.
- *Informationssystem Ausweisschriften (ISA, Art. 11 des Ausweisgesetzes vom 22. Juni 2001[46]:* ISA wird vom fedpol betrieben und enthält die in Schweizer Reisepässen und Identitätsdokumenten aufgeführten Daten einer Person wie Name, Heimatort, sowie die ausstellende Behörde und die Ausfertigungsstelle.

Aufgrund des automatischen Abgleichs erzielte Übereinstimmungen, deren Überprüfung durch die PIU negativ ausfällt, sind umgehend zu löschen (vgl. Art. 22 Bst. b). Bestätigt die Überprüfung die Übereinstimmung, gibt die PIU diese sowie die betroffenen Flugpassagierdaten der zuständigen Behörde bekannt und markiert die betroffenen Daten (vgl. Art. 7).

Artikel 7 Bekanntgabe im Fall einer Übereinstimmung

Absatz 1

Nur im Rahmen des automatischen Datenabgleichs erzielte Übereinstimmungen, die von der PIU gestützt auf Artikel 6 Absatz 2 positiv überprüft worden sind, dürfen zusammen mit den betroffenen Flugpassagierdaten als Ergebnisse des automatischen Abgleichs an die zuständige Behörde nach Artikel 1 Absatz 2 bekanntgegeben werden.

Empfängerin eines solchen Bearbeitungsergebnisses ist jene Behörde, die in der für die Übereinstimmung massgeblichen Ausschreibung im polizeilichen Informationssystem als zuständig ausgewiesen ist oder deren Risikoprofil oder Beobachtungsliste die Übereinstimmung ausgelöst hat.

45 SR **142.51**
46 SR **143.1**

Wann eine Überprüfung der Übereinstimmung andere Schritte als eine Bekanntgabe an die zuständige Behörde nach sich zieht, ergibt sich aus Artikel 22 Buchstabe b. Sofort zu löschen – statt an eine Behörde bekanntzugeben − sind Übereinstimmungen:

- die sich nicht oder nicht eindeutig einer Straftat nach Anhang 2 zuordnen lassen (Art. 6 Abs. 3 Bst. a); oder
- bei denen sich die Identität als unrichtig erweist (Art. 6 Abs. 3 Bst. b).

Denn in diesen Fällen fiel die Überprüfung der aufgrund des automatischen Abgleichs erzielten Übereinstimmungen negativ aus, was einer Bekanntgabe an eine zuständige Behörde entgegensteht und die sofortige Löschung bedingt.

Absatz 2

Wurde ein Risikoprofil durch die PIU initialisiert (vgl. Art. 12 Abs. 3 Bst. b), fehlt eine antragstellende Behörde. Gleiches gilt, wenn die PIU einen Hinweis auf eine drohende Straftat weiterzugeben hat (vgl. Art. 9). Denkbar ist auch der Fall, dass eine Ausschreibung ausnahmsweise keine zuständige Behörde ausweist.

In diesen Fällen gibt die PIU die Daten jener Behörde nach Artikel 1 Absatz 2 bekannt, die am ehesten für die weitere Bearbeitung zuständig ist. Im Zweifelsfall gibt die PIU die Daten der Bundeskriminalpolizei (BPK) bekannt. Erachtet sich die BKP in der Sache als nicht zuständig, leitet sie die Daten an jene Behörde weiter, die sie als zuständig betrachtet. Lässt sich auch aus Sicht der BKP keine zuständige Behörde finden, was eher unwahrscheinlich sein dürfte, hat die BKP die Daten zu löschen. Sobald die PIU davon Kenntnis genommen hat, hebt sie die Markierung der entsprechenden Daten gestützt auf Artikel 10 Absatz 1 auf.

Absatz 3

Mit der Bekanntgabe der Daten an eine Behörde nach Artikel 1 Absatz 2 markiert die PIU die bekanntgegebenen Daten *technisch*. In Zusammenhang mit dem vorliegenden Gesetz gelten sie danach als markierte Daten.

Exkurs zu markierten Daten

Der EuGH hält in seinem Urteil vom 21. Juni 2022 unmissverständlich fest, dass sich eine sechsmonatige Aufbewahrung aller Flugpassagierdaten rechtfertigen lässt. Dagegen müsse sich eine darüberhinausgehende Aufbewahrung auf das ermittlungs- und verfolgungstechnisch Notwendige beschränken:

«Gibt es in besonderen Fällen objektive Anhaltspunkte – wie bei den PNR-Daten […], die zu einem überprüften Treffer geführt haben – dafür, dass von bestimmten Fluggästen eine Gefahr im Bereich terroristischer Straftaten oder

schwerer Kriminalität ausgehen könnte, erscheint eine Speicherung ihrer PNR-Daten über den ursprünglichen Zeitraum hinaus jedoch zulässig».[47]

Daten, welche die PIU einer zuständigen Behörde nach Artikel 7 bekanntgegeben hat, werden markiert. Diese technische Massnahme sichert die unterschiedliche *automatische* Bearbeitung, die das Gesetz für Daten vorsieht, die:

- keine Anhaltspunkte auf Schwerstkriminalität aufweisen, deshalb nicht markiert sind und nach einem Monat automatisch pseudonymisiert und nach weiteren fünf Monaten automatisch gelöscht werden vgl. Art. 21 Abs. 1); und
- aufgrund ihrer Anhaltspunkte auf Schwerstkriminalität einer Behörde bekanntgegeben und markiert sowie nach insgesamt fünf Jahren automatisch gelöscht werden (vgl. Art. 21 Abs. 2).

Eine Markierung wird jedoch wieder aufgehoben, wenn die PIU von der zuständigen Behörde informiert wird, dass sie die Daten nicht mehr benötige (vgl. Art. 10). Dies kann der Fall sein, wenn sich die Anhaltspunkte, die zur Bekanntgabe der Daten geführt haben, nicht bestätigen oder wenn sich der ursprüngliche Verdacht einer zur Fahndung ausgeschriebenen Person als gegenstandslos erweist. Mit Aufhebung der Markierung sind die Daten je nach Alter zu pseudonymisieren und danach zu löschen oder werden sofort gelöscht (vgl. Art. 18 und 21).

Absatz 4

Sowohl die Anträge der zuständigen Behörden an die PIU wie auch die Daten, welche die PIU ihnen bekannt gibt, sollen sicher übermittelt werden. Der Bundesrat wird ermächtigt, die dazu nötigen Einzelheiten auf Verordnungsebene zu regeln. Dazu gehört nicht nur die Art und Weise der Bekanntgabe. Zu klären ist auch die Frage, ob sich der Datenaustausch mit den einzelnen Behörden standardisiert und über eine Anlaufstelle abwickeln lässt. Im Falle der Polizeikorps von Bund und Kantonen könnte diese Rolle beispielsweise die jeweilige Einsatz- und Alarmzentrale übernehmen.

Artikel 8 Bekanntgabe auf Antrag

Diese Bestimmung findet nur Anwendung, wenn die beantragten Flugpassagierdaten *nicht* pseudonymisiert sind.

Sind die gewünschten Daten pseudonymisiert, ist zunächst die Aufhebung ihrer Pseudonymisierung zu beantragen (vgl. Art. 19 oder 20).

Absatz 1

Die Datenbekanntgabe nach Artikel 8 muss hinreichend konkret und damit eingegrenzt sein. Generische Abfragen, die nicht spezifiziert sind und zu einer

47 Rechtssache C-817/19, ECLI:EU:C:2022:491; Rz. 248–262.

Vielzahl von unterschiedlichsten Suchergebnissen führen könnten, sind dagegen nicht zulässig. Dies wird mit dem Begriff «einzelfallweise» verdeutlicht.

Der Antrag muss zudem schlüssig darlegen, weshalb die gewünschten Daten zur Bekämpfung einer Straftat nach Anhang 2 notwendig sind.

Absatz 2

Ob die verlangten Flugpassagierdaten tatsächlich in Zusammenhang mit einer Straftat nach Anhang 2 benötigt werden, muss die PIU zumindest aufgrund des Antrags und allenfalls mittels Nachfrage bei der antragstellenden Behörde prüfen (vgl. Art. 7 Abs. 1).

Flugpassagierdaten, die auf Antrag einer zuständigen Behörde bekanntgegeben werden, sind zu markieren (vgl. Art. 7 Abs. 3).

Artikel 9 Weitergabe von Hinweisen

Absatz 1

Hinweise auf eine drohende Straftat nach Anhang 2 kann die PIU von einer ausländischen PIU erhalten (vgl. auch Art. 30).

Die PIU muss einen solchen Hinweis der zuständigen Behörde (vgl. Art. 1 Abs. 2) bekanntgeben, die gestützt darauf vertiefte Abklärungen treffen kann und allenfalls die angezeigten Massnahmen zur Verhinderung dieser Straftat veranlasst.

Absatz 2

Unter die weiteren Angaben, welche die PIU der zuständigen Behörde auf deren Antrag bekanntgibt, fallen die Flugpassagierdaten der vom Hinweis getroffenen Person sowie allfällige überprüfte und diese Flugpassagierdaten betreffende Übereinstimmungen, die aufgrund des Datenabgleichs nach Artikel 6 Absatz 1 erzielt worden sind.

Absatz 3

In dringenden Fällen kann die PIU die Angaben nach Absatz 2 sofort und ohne einen Antrag der zuständigen Behörde abzuwarten, bekanntgeben.

Absatz 4

In sinngemässer Anwendung von Artikel 7 prüft die PIU insbesondere, ob sich der gemeldete Hinweis tatsächlich auf eine Straftat nach Anhang 2 bezieht (vgl. Art. 7 Abs. 1).

Lässt sich für die PIU nicht zweifelsfrei feststellen, welche Behörde für die weitere Abklärung zuständig ist, stellt die PIU die Meldung der Bundeskriminalpolizei zu, welche die Zuständigkeit klärt (vgl. Art. 7 Abs. 2).

Nach der Weiterleitung der Daten an die zuständige Behörde sind diese durch die PIU zu markieren (vgl. Art. 7 Abs. 3).

Artikel 10 Aufhebung von Markierungen

Die zuständige Behörde ist in der Lage, den mit den bekanntgegebenen Daten einhergehenden Verdacht in einem deutlich breiteren Abklärungsrahmen zu prüfen als die PIU. Sie kann dabei auch zum Schluss kommen, dass sich die Anhaltspunkte, die zur Bekanntgabe der Daten geführt haben, nicht bestätigt haben oder dass sich der ursprüngliche Verdacht einer zur Fahndung ausgeschriebenen Person als gegenstandslos erweist.

In diesem Fall hat die zuständige Behörde die PIU darüber zu informieren, dass sie die bekanntgegebenen Daten nicht mehr benötigt.

Sobald die PIU von dieser Mitteilung Kenntnis nimmt, hat sie die Markierung der betroffenen Daten wieder aufzuheben. Danach gelten für diese Daten jene Regelungen, die auf Daten ohne Markierung anwendbar sind (vgl. Art. 18 und 21).

Auf Verordnungsebene wird ein Verfahren festzulegen sein, in dem die zuständigen Behörden in regelmässigen Abständen an ihre Informationspflicht nach Artikel 10 erinnert werden. Bestätigen sie innert einer von der PIU gesetzten Frist (z.B. innert 10 Tagen), dass der Verdacht auf der betroffenen Person wegen Schwerstkriminalität fortbesteht, bleiben die Daten markiert. Geht indes keine solche Bestätigung bei der PIU ein, wird die Markierung aufgehoben und die nun unmarkierten Daten – je nach ihrem Alter − von der PIU pseudonymisiert oder gelöscht. Mit diesem Vorgehen lässt sich verhindern, dass Daten ohne entsprechende Rechtfertigung markiert und damit einer fünfjährigen Aufbewahrungsfrist unterstellt bleiben.

Artikel 11 Bekanntgabe an den Nachrichtendienst des Bundes

Der NDB hat bei der Bekämpfung von terroristischen und anderen schweren Straftaten eine besondere Stellung. Seine Informationsbeschaffung ist der polizeilichen Ermittlung und der Strafverfolgung meistens vorgelagert und dient dem vorzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit.

Die Rohdaten auf bestimmten Flugstrecken sollen deshalb dem NDB zur Weiterbearbeitung zugänglich gemacht werden, nicht jedoch dem Nachrichtendienst der Armee oder den kantonalen Vollzugsstellen nach Artikel 9 NDG.

Die Bearbeitung der Flugpassagierdaten durch den NDB richtet sich nach dem NDG, das entsprechend ergänzt wird (vgl. Anhang 3 Ziff. 1). Im Flugpassagierdatengesetz wird lediglich die Bekanntgabe der Daten und der zulässige Bearbeitungszweck geregelt.

Absatz 1

Absatz 1 hält lediglich fest, dass der NDB die Flugpassagierdaten von im Voraus bestimmter Flugstrecken erhält. Sie werden ihm automatisch bekanntgegeben. Diese Bekanntgabe führt zu keiner Markierung der entsprechenden Daten.

Absatz 2

Der NDB soll Flugpassagierdaten zur Erfüllung seiner Aufgaben nach Artikel 6 Absatz 1 Buchstabe a NDG selbstständig bearbeiten können. Allerdings ist nicht vorgesehen, dass dem NDB ein direkter Zugriff auf das PNR-Informationssystem eingeräumt wird. Die Daten werden ihm automatisch und nur auf im Voraus vom Bundesrat bestimmten Strecken (vgl. Abs. 3) bekanntgegeben.

Der NDB erfährt bei der Bearbeitung der Flugpassagierdaten nach dem vorliegenden Gesetz eine weitere Einschränkung: So darf er die Flugpassagierdaten nur zur Bekämpfung jener Straftaten nach Anhang 2 des Flugpassagierdatengesetzes bearbeiten, die sich seinen Aufgaben nach Artikel 6 Absatz 1 Buchstabe a NDG zuordnen lassen.

Der neue Artikel 16*a* NDG verweist explizit auf diese Zweckbestimmung nach dem vorliegenden Gesetz.

Diese Zweckbestimmung sah bereits der Vorentwurf des Flugpassagierdatengesetzes vor und entspricht auch dem EuGH-Urteil (vgl. Rz. 235). Der EuGH zieht noch einen weiteren Schluss:

«Überdies folgt aus dem abschließenden Charakter der […] genannten Ziele, dass die PNR-Daten auch nicht in einer einheitlichen Datenbank gespeichert werden dürfen, die zur Verfolgung sowohl dieser als auch anderer Ziele konsultiert werden kann. Die Speicherung dieser Daten in einer solchen Datenbank brächte nämlich die Gefahr einer Verwendung der Daten zu anderen als den […] genannten Zwecken mit sich.»

Dass der NDB den Bearbeitungszweck technisch nicht ausweiten darf, ergibt sich aus der Zweckbindung, die in Absatz 2 statuiert ist. Es bedarf damit keiner weiteren gesetzlichen Regelung.

4. Abschnitt: Risikoprofile und Beobachtungslisten

Artikel 12 Risikoprofile

Artikel 12 liefert neben einer begrifflichen Umschreibung die gesetzliche Grundlage, damit ein Risikoprofil erstellt und eingesetzt werden darf.

Dass einzelne, den massgeblichen Behörden bisher unbekannte Personen mit kriminellem Hintergrund aus der Masse der Ein- und Ausreisenden auffallen und näher geprüft, allenfalls eingehend befragt oder gar verhaftet werden, ist auch heute immer noch dank ausgewiesener Berufserfahrung und Intuition von Mitarbeitenden der Kontrollbehörden möglich. Solche persönlichen Momente bei Kontrollen sind allerdings auch kritisch zu hinterfragen, zumal sie subjektiv motiviert sind und ein Einfallstor für unbewusste Diskriminierungen sein können. Deshalb und weil die Zahl der Personen, die Kontrollpunkte passieren, in den vergangenen Jahren rasant gewachsen ist, müssen heute vermehrt elektronische Instrument zum Einsatz gelangen.

Das Risikoprofil im Rahmen von PNR ist eines dieser Instrumente. Es gelangt − wie die Beobachtungsliste − beim automatischen Abgleich nach Artikel 6 zum Einsatz und macht auf Flugpassagierdatensätze aufmerksam, die Datenkombinationen aufweisen, die oft in Zusammenhang mit Schwerstkriminalität auftreten.

Beim Risikoprofil, wie es im Rahmen von PNR Anwendung findet, handelt es sich *nicht* um ein Profiling (vgl. Art. 5 Bst. f und g DSG). Denn der Abgleich von Flugpassagierdaten mit dem Risikoprofil umfasst weder eine Analyse der betroffenen Person noch die Vorhersage ihrer Verhaltensweise.

Beim Einsatz des Risikoprofils wird nach einzelnen Daten gesucht, die sich kombiniert in einem Flugpassagierdatensatz vorfinden. Eine im Rahmen des Abgleichs erzielte Übereinstimmung besagt lediglich, dass sich in dem von der Übereinstimmung betroffenen Datensatz die mittels Risikoprofil gesuchte Datenkombination vorfindet.

Die Entwicklung von Risikoprofilen stellt in der Praxis eine grosse Herausforderung dar. Erfolgreich einsetzen lassen sich Risikoprofile nur, wenn sich bei ihrer Konzeption kriminalistisches Know-how und ausgewiesene Erfahrung in der Datenabfrage vereinen lassen.

Alle automatisierten Bearbeitungsschritte müssen in einem elektronischen Protokoll dokumentiert werden. Dies gilt auch für den Einsatz von Risikoprofilen (vgl. Art. 24).

Risikoprofile müssen gelöscht werden, wenn sie nicht mehr erforderlich sind (vgl. Art. 22 Bst. d).

Der Einsatz von Risikoprofilen wird durch den Bundesrat überprüft (vgl. Art. 15).

Absatz 1

Gewisse Verbrechen führen in Flugpassagierdatensätzen zu typischen Datenkombinationen, so die organisierte Kriminalität und insbesondere der Menschenhandel. Mit dem Einsatz von Risikoprofilen lassen sich die Flugpassagierdaten systematisch nach solchen Datenkombinationen durchsuchen und dadurch objektive Anhaltspunkte auf eine den Behörden bisher noch nicht bekannte Straftat nach Anhang 2 gewinnen.

In der Vernehmlassung wurde wiederholt die Befürchtung geäussert, dass Risikoprofile diskriminierende Inhalte aufweisen könnten. Diese Befürchtung ist unbegründet. Denn das Risikoprofil setzt sich *nicht* aus Daten zusammen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen und damit Personendaten nach Artikel 5 Buchstabe e DSG sind. Entsprechend sind auch besonders schützenswerten Personendaten (vgl. Art. 5 Bst. c DSG) als mögliche Inhalte eines Risikoprofils ausgeschlossen.

Absatz 2

Risikoprofile werden immer durch die PIU erstellt.

Ausgangspunkt eines Risikoprofils kann ein schriftlicher Antrag einer zuständigen Behörde nach Artikel 1 Absatz 2 sein. Darin muss die Behörde darlegen, welche Daten zu welchem Zweck in das Risikoprofil aufgenommen werden sollen.

Die PIU kann Risikoprofile aber auch ohne einen solchen Antrag erstellen. Ausgangspunkt eines solchen Risikoprofils sind Erkenntnisse, welche die PIU aus dem Praxisalltag von Polizei- und Strafverfolgungsbehörden im In- und Ausland gewonnen hat.

In beiden Fällen muss die PIU prüfen, ob die beantragten Inhalte zweckkonform und hinreichend konkret sind. Stellt die PIU fest, dass die Angaben der antragstellenden Behörde noch nicht hinreichend konkret sind, wird sie diese darauf hinweisen und sie bei der zusätzlichen Präzisierung des beantragten Risikoprofils unterstützen.

Absatz 3

Das Erstellen von Risikoprofilen stellt technisch hohe Anforderungen. Erfahrungen aus dem Ausland zeigen, dass mit Risikoprofilen oftmals zu viele Übereinstimmungen erzielt werden.

Dies hängt damit zusammen, dass sie zu wenig präzis sind. Im Idealfall setzen sich Risikoprofile aus be- und entlastenden Daten zusammen.

Eine Vielzahl von Übereinstimmungen, die nicht relevant sind, dürfen nicht das Ziel der Risikoprofile sein, weder aus datenschutzrechtlichen Gründen (vgl. Art. 7 Abs. 3 DSG) noch aus solchen der Verfahrensökonomie.

Deshalb sind Risikoprofile vor ihrem Einsatz zwingend zu testen. Durchgeführt werden die Tests ausschliesslich mit künstlich aufgrund von Simulationen generierten Daten.

Absatz 4

Allein die PIU und damit natürliche Personen dürfen Veränderung der in einem Risikoprofil eingesetzten Daten vornehmen.

Artikel 13 Beobachtungslisten

Artikel 13 liefert neben einer begrifflichen Umschreibung die gesetzliche Grundlage, damit eine Beobachtungsliste erstellt und eingesetzt werden darf.

Wie das Risikoprofil gelangt die Beobachtungsliste beim automatischen Abgleich aller neu eingetroffenen Flugpassagierdaten zum Einsatz (vgl. Art. 6 Abs. 1).

Alle automatisierten Bearbeitungsschritte müssen in einem elektronischen Protokoll dokumentiert werden. Dies gilt auch für den Einsatz der Beobachtungsliste (vgl. Art. 24).

Die Löschung von Inhalten einer Beobachtungsliste nach Artikel 13 bestimmt sich nach Artikel 22 Buchstabe d.

Der Einsatz der Beobachtungsliste wird durch den Bundesrat überprüft (vgl. Art. 15).

Absatz 1

Mit Beobachtungslisten nach Artikel 13 lässt sich gezielt und direkt nach Inhalten in den Flugpassagierdaten suchen, welche in Zusammenhang mit *begangenen* Straftaten nach Anhang 2 stehen und den Behörden bekannt sind.

Anders als die Risikoprofile setzt sich die Beobachtungsliste nur aus Daten zusammen, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen. Diese Umschreibung lehnt sich an die Definition der Personendaten an, die in der Schweiz bis zur Aufhebung des Bundesgesetzes vom 19. Juni 1992[48] über den Datenschutz galt. Mit dieser Ausdehnung lässt sich sicherstellen, dass beispielsweise auch dann nach bestimmten Kreditkartennummern gesucht werden kann, wenn die Kreditkarte nicht einer natürlichen, sondern einer juristischen Person gehört.

Besonders schützenswerten Personendaten gelangen auch bei der Beobachtungsliste nicht zum Einsatz. Denn selbst die in Reisedokumenten hinterlegten biometrischen Daten sind nicht Gegenstand eines Flugpassagierdatensatzes nach Anhang 1 (vgl. Kategorie 18).

Absatz 2

Absatz 2 legt fest, wer eine Beobachtungsliste beantragen kann und welche der in Artikel 5 Absatz 1 definierten Bearbeitungszwecke bei der Erstellung und damit beim Einsatz der Beobachtungsliste zu beachten sind.

Anders als beim Risikoprofil darf die PIU Beobachtungslisten nur auf schriftlichen Antrag einer Behörde nach Artikel 1 Absatz 2 Buchsstabe a erstellen und einsetzen. Die Aufgabe der PIU beschränkt sich darauf, zu prüfen, ob die beantragten Inhalte zweckkonform und hinreichend konkret sind.

Die Beobachtungsliste nach Artikel 13 darf nur zu den folgenden Zwecken erstellt und eingesetzt werden:

- zur Aufklärung einer *behördlich bekannten* terroristischen oder anderen schweren Straftat nach Anhang 2, welche Gegenstand eines laufenden Ermittlungs- oder Strafverfolgungsverfahrens ist (Bst. a); oder
- zur Fahndung nach einer *bestimmten* Person, die entweder in Zusammenhang mit einer bestimmten Straftat nach Anhang 2 als Beschuldigte gesucht wird (Bst. b) oder rechtskräftig verurteilt ist und sich der Verbüssung der Freiheitsstrafe zu entziehen versucht (Bst. c).

Absatz 3

48 AS **2022** 491

Allein die PIU und damit natürliche Personen sind für die Erstellung von Beobachtungslisten und für die Veränderung der eingesetzten Daten zuständig.

Artikel 14 Aufnahme von Daten über Drittpersonen in die Beobachtungsliste

Artikel 14 stellt eine Sonderregelung für die Aufnahme von Daten in eine Beobachtungsliste nach Artikel 13 dar. Denn mit der Aufnahme von Daten Dritter, die keinen Bezug zu einer Straftat nach Anhang 2 haben, wird *indirekt* nach bestimmten Personen gesucht, die den Behörden bekannt sind.

Die Daten Dritter sollen Rückschlüsse auf den Aufenthalt von Personen möglich machen, nach denen wegen einer Straftat nach Anhang 2 gefahndet wird. Dabei muss es sich entweder um Beschuldigte in einem laufenden Strafverfahren oder um rechtskräftig Verurteilte handeln, die der verhängten Freiheitsstrafe für eine Straftat nach Anhang 2 zugeführt werden sollen.

Artikel 270 StPO stellt eine vergleichbare Regelung auf. Denn sie erlaubt die Überwachung des Post- und Fernmeldeverkehrs einer Drittperson. Als Massnahme greift die Überwachung des Post- und Fernmeldeverkehrs aber viel tiefer in die Persönlichkeitsrechte der Drittperson ein als die hier in Artikel 14 vorgesehene Massnahme, die sich auch deutlich kostengünstiger umsetzen lassen dürfte als eine Massnahme nach Artikel 270 StPO. Drittpersonen können auch bei Observationen nach Artikel 282 StPO betroffen sein.

Die Löschung von Inhalten einer Beobachtungsliste nach Artikel 14 bestimmt sich nach Artikel 22 Buchstabe e.

Der Einsatz der Beobachtungsliste wird durch den Bundesrat überprüft (vgl. Art. 15).

Absatz 1

In die Beobachtungsliste dürfen zeitlich beschränkt Daten über eine Drittperson aufgenommen werden, die selber keinen direkten Bezug zu einer terroristischen oder anderen schweren Straftat nach Anhang 2 hat.

Eine Beobachtungsliste nach Artikel 14 kann nur eine Behörde nach Artikel 1 Absatz 2 Buchstabe a schriftlich beantragen.

Der Antrag richtet sich in diesem Fall aber an das für diese Behörde zuständige Zwangsmassnahmengericht. Denn die Daten über eine Drittperson dürfen nur dann in eine Beobachtungsliste aufgenommen werden, wenn das zuständige Zwangsmassnahmengericht dies gutheisst.

Ziel dieser Beobachtungsliste ist es, dass die Behörden aufgrund der Flugpassagierdaten einer Drittperson Rückschlüsse auf den Aufenthaltsort einer Person erhalten, die in Zusammenhang mit einer Straftat nach Anhang 2 entweder als Beschuldigte gesucht wird oder rechtskräftig verurteilt ist und sich der Verbüssung der Freiheitsstrafe zu entziehen versucht (Art. 13 Abs. 2 Bst. b und c).

Als Drittperson im Sinne von Artikel 14 gilt, wer einer gesuchten Person geschäftlich oder privat so nahesteht, dass ein Besuch am Aufenthaltsort der gesuchten Person wahrscheinlich ist.

Dabei muss man sich vergegenwärtigen, dass eine Beobachtungsliste mit Inhalten nach Artikel 14 nur greifen kann, wenn die Drittperson und die gesuchte Person vor Ort miteinander Kontakt haben und die Drittperson *oder* die gesuchte Person sich in der Schweiz aufhält. Halten sich beide Personen in der Schweiz auf, bedarf es keiner grenzüberschreitenden Flugreise für die Kontaktpflege. Halten sich beide im Ausland auf, sind die Daten der Drittperson in einer Beobachtungsliste ebenfalls kaum erfolgsversprechend, verfügt doch die Schweizer PIU im Normalfall nur über Passagierdaten von Flügen in die oder aus der Schweiz.

Absatz 2

Die Aufnahme solcher Daten in eine Beobachtungsliste unterliegt einer zeitlichen Befristung, die ebenfalls durch das Zwangsmassnahmengericht festzusetzen ist.

Bei der Festlegung der zulässigen Laufzeit dürfte sich das Zwangsmassnahmengericht von ähnlichen Kriterien leiten lassen wie bei vergleichbaren Massnahmen nach der StPO.

Die Inhalte der Beobachtungsliste sind von der PIU mit Ablauf der gerichtlich festgelegten Laufzeit zu löschen (vgl. Art. 22 Bst. e).

Absatz 3

Das Zwangsmassnahmengericht teilt seinen Entscheid der antragstellenden Behörde und der PIU mit.

Artikel 15 Überprüfung der Risikoprofile und Beobachtungslisten

Risikoprofile und Beobachtungslisten sind zentrale PNR-Instrumente. Sie ermöglichen mit überschaubarem Aufwand, zeitnah Informationen zu erhalten, die für die Bekämpfung von Schwerstkriminalität von Bedeutung sein können.

Die Vernehmlassung zeigte, dass der Einsatz dieser beiden Instrumente überprüft werden soll. Da diese Überprüfung hauptsächlich die Funktionalität dieser zentralen Instrumente von PNR zum Gegenstand hat, soll der Bundesrat für diese Aufgabe zuständig sein.

Absatz 1

Artikel 15 sieht vor, dass der Einsatz von Risikoprofilen und Beobachtungslisten durch den Bundesrat überprüft werden sollen.

Erforderlich ist der Einsatz dieser Instrumente, wenn sie so erstellt sind, dass sich damit die gesetzlich definierten Zwecke erreichen lassen.

Risikoprofile, die eine Vielzahl von letztlich unnötigen Übereinstimmungen generieren, trüben den Blick für das Wesentliche. Zudem binden sie unnötig

viele Ressourcen. Risikoprofile, die nicht die nötige Bestimmtheit aufweisen, lassen sich nicht durch ihre Erforderlichkeit legitimieren.

Gleiches gilt für Risikoprofile, die sich nicht an aktuellen Verhaltensmustern orientieren. Denn diese ändern sich laufend. Sind Risikoprofile nicht mehr aktuell, ist ihr Einsatz ebenfalls nicht mehr erforderlich und ihre Inhalte sind zu löschen (vgl. Art. 22 Bst. d).

Weniger heikel ist der Einsatz von Beobachtungslisten. Dennoch können auch sie viele unnötige Übereinstimmungen hervorrufen, so wenn beispielsweise geläufige Namen von Personen ohne weitere Kriterien aufgenommen werden, welche die gesuchte Person näher bestimmen.

Der Hauptgrund, weshalb Beobachtungslisten nicht mehr erforderlich sind, dürfte darin liegen, dass sich die gesuchte Person finden liess. Inhalte einer Beobachtungsliste, die nicht mehr erforderlich sind, sind durch die PIU zu löschen (vgl. Art. 22 Bst. d und e).

Absatz 2

Die Einzelheiten dieser Überprüfung sind auf Verordnungsebene festzulegen. Von einer Publikation des Berichts, wie dies in der Vernehmlassung verlangt worden ist, sollte allerdings abgesehen werden. Sicherheitsüberlegungen und Gründe des Persönlichkeitsschutzes legen den Verzicht auf die Publikation eines Berichts mit hoher Aussagekraft nahe.

5. Abschnitt: PNR-Informationssystem

Artikel 16

Absatz 1

Die Bearbeitung der Flugpassagierdaten erfolgt im PNR-Informationssystem. Einzelheiten dazu finden sich unter Ziffer 6.1.

Absatz 2

Als Betreiberin des PNR-Informationssystems kommt dem fedpol die Rolle als Verantwortliche im Sinne von Artikel 5 Buchstabe j DSG zu.

Das fedpol ist damit insbesondere verpflichtet:

- die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden (Art. 7 Abs. 1 DSG);
- mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist (Art. 7 Abs. 3 DSG);
- durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit zu gewährleisten (Art. 8 Abs. 1 DSG);

- ein Verzeichnis der Bearbeitungstätigkeiten zu führen (Art. 12 DSG);
- eine Datenschutz-Folgenabschätzung zu erstellen, sofern die Voraussetzungen zur Erstellung einer solchen gegeben sind (Art. 22 DSG);
- dem EDÖB so rasch als möglich eine allfällige Verletzung der Datensicherheit zu melden, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 24 Abs. 1 DSG);
- soweit vom EDÖB verlangt oder zum Schutz der betroffenen Person, diese über eine Verletzung der Datensicherheit zu informieren (Art. 24 Abs. 4 DSG).

Darüber hinaus hat das fedpol:

- einer Person auf Verlangen Auskunft zu erteilen, ob Personendaten über sie bearbeitet werden (Art. 25 DSG vorbehältlich der Einschränkungen nach Art. 26 des vorliegenden Gesetzes);
- auf Verlangen einer Person – vorbehältlich der Einschränkungen nach Artikel 29 DSG – die automatisiert bearbeiteten Personendaten herauszugeben (Art. 28 DSG);
- Begehren einer betroffenen Person gegen die Bekanntgabe ihrer Personendaten zu behandeln (Art. 37 DSG);
- Gesuche einer betroffenen Person nach Artikel 41 DSG zu behandeln.

Zu diesen Vorgaben finden sich in den Artikeln 17–26 E-FPG zum Teil präzisierende Bestimmungen, die den allgemeinen Bestimmungen des DSG vorgehen.

Absätze 3 und

Ein Zugriff auf die Flugpassagierdaten und auf Ergebnisse ihrer Bearbeitung ist jenen Mitarbeitenden vorbehalten, die dies zur Erfüllung ihrer Aufgabe zwingend benötigen. Zugriffsberechtigt sind in erster Linie die Mitarbeitenden der PIU (Bst. a). Auch die Datenschutzberaterin oder der Datenschutzberater des fedpol muss zur Wahrnehmung der Aufgaben nach dem DSG über eine Zugriffsberechtigung verfügen (Bst. b).

Über eine Zugriffsberechtigung müssen auch Personen verfügen, die für die Entwicklung, Weiterentwicklung oder Wartung des PNR-Informationssystems zuständig sind oder technischen Support leisten (Bst. c). Diese Notwendigkeit ergibt sich nicht zuletzt aus der sehr weiten Umschreibung des Begriffs der Datenbearbeitung.

Denn als Bearbeiten gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren (vgl. Art. 5 Bst. d DSG). Entspre-

chend kann bereits der User-Support zur Datenbearbeitung führen. In technischen Belangen kommen auch bei der Bearbeitung von PNR nur Dienstleister zum Einsatz, die den Zuschlag im Rahmen der WTO-Ausschreibung Alpin.2.0 erhalten haben. Alpin 2.0 sichert für die gesamte Bundesverwaltung einen Pool an Projektdienstleistungen für IKT-Schlüsselprojekte, IKT-Grossprojekte oder komplexe und strategische Vorhaben. Die konkreten Aufträge werden unter den Zuschlagsempfängern in einem elektronischen Mini-Tender Verfahren (Wettbewerb) vergeben. Alle zum Einsatz gelangenden Dienstleister müssen im Übrigen die erweiterte Personensicherheitsprüfung des Bundes erfolgreich absolvieren.

Der Betrieb und die Wartung des PNR-Informationssystems liegen in der Verantwortung des ISC-EJPD und von dessen Mitarbeitenden. Für den Betrieb und die Wartung der Lösung werden keine externen Dienstleister beigezogen.

Nach Buchstabe d sollen schliesslich auch die zuständigen Behörden (vgl. Art. 1 Abs. 2) auf das PNR-Informationssystem zugreifen können, um die ihnen von der PIU bekanntgegebenen Daten empfangen und weiterbearbeiten zu können. Der Zugriff ist auf das «Abholen» dieser Daten beschränkt.

6. Abschnitt: Datenschutz

Artikel 17 Grundsätze

Die Flugpassagierdaten werden nicht nur durch die PIU bearbeitet, sondern auch durch Behörden von Bund und Kantonen, denen sie nach diesem Gesetz bekanntgegeben werden.

Die Vernehmlassung zeigte die Notwendigkeit, gesetzlich auszuweisen, dass sich die Bearbeitung der Daten je nach Behörde, die hierfür zuständig ist, datenschutzrechtlich nach unterschiedlichen Rechtsgrundlagen richtet.

In einem ersten Schritt ist zu prüfen, ob es sich um eine Behörde des Bundes oder eines Kantons handelt und damit eidgenössisches oder kantonales Datenschutzrecht Anwendung findet. Einen Sonderfall stellen dabei allerdings die Strafverfolgungsbehörden dar (siehe Erläuterungen zu Absatz 2).

In einem zweiten Schritt ist sodann zu prüfen, ob für eine bestimmte Behörde eidgenössische beziehungsweise kantonale Sonderregelungen greifen, die dem allgemeinen eidgenössischen beziehungsweise kantonalen Datenschutzrecht vorgehen.

Absatz 1

In der Botschaft vom 15. September 2017[49] über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz führte der Bundesrat aus:

49 BBl **2017** 6941 S. 7010

«Zudem ist darauf hinzuweisen, dass der E-DSG genau wie das bisherige Recht das Datenschutzrecht im Allgemeinen regelt. Falls die Bearbeitung von Personendaten in den Anwendungsbereich anderer Bundesgesetze fällt, gelten aufgrund der Lex-specialis-Regel (besondere Normen gehen der allgemeinen Norm vor) grundsätzlich die bereichsspezifischen Datenschutznormen.»

Die PIU hat als Behörde des Bundes bei der Bearbeitung der Daten das DSG zu beachten, soweit das vorliegende Gesetz keine besondere Regelung vorsieht. Die datenschutzrechtlichen Bestimmungen des vorliegenden Gesetzes und insbesondere die Artikel 17–26 gelten somit als lex specialis und gehen damit dem DSG vor.

Absatz 2

Für Behörden, die von der PIU Daten nach dem E-FPG erhalten, gelten die Datenschutzregelungen nach dem vorliegenden Gesetz nicht. Je nach Behörde sind auch die Regelungen des DSG nicht anwendbar.

Eidgenössische und kantonale Strafverfolgungsbehörden: Bei hängigen Verfahren bestimmt sich der zu gewährleistende Datenschutz nach dem jeweils anwendbaren Verfahrensrecht und insbesondere nach den Artikeln 95–103 StPO. Das eidgenössische und kantonales Datenschutzrecht findet erst wieder Anwendung, wenn solche Verfahren abgeschlossen sind (vgl. Art. 99 Abs. 1 StPO). Zudem findet es Anwendung auf erstinstanzliche Verwaltungsverfahren (vgl. Art. 2 Abs. 3 DSG). Dazu führte der Bundesrat in der Botschaft über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz aus:[50]

«Nach Artikel 2 Absatz 3 E-DSG regelt das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen. Die Norm regelt das Verhältnis des DSG zum Verfahrensrecht und hält als allgemeinen Grundsatz fest, dass ausschliesslich das anwendbare Verfahrensrecht darüber bestimmt, wie Personendaten in laufenden Verfahren zu bearbeiten und wie die Rechte der betroffenen Personen ausgestaltet sind. Das Verfahrensrecht stellt […] ebenfalls den Schutz der Persönlichkeit und der Grundrechte aller Beteiligten sicher und gewährleistet damit einen dem DSG äquivalenten Schutz. Käme in diesem Bereich das DSG zur Anwendung, bestünde die Gefahr von Normkollisionen und Widersprüchen, die das austarierte System der jeweils anwendbaren Verfahrensordnung stören könnten.»

Polizeibehörden des Bundes ausserhalb eines Strafverfolgungsverfahrens: Hier bestimmt sich der Datenschutz nach dem DSG, soweit das Bundesrecht nicht Spezialbestimmungen vorsieht. Entsprechende Bestimmungen ergeben sich aus dem BPI, dem BWIS und der Verordnung vom 30. November 2001[51] über die Wahrnehmung kriminalpolizeilicher Aufgaben im Bundesamt für Polizei.

50 BBl **2017** 6941 S. 7013
51 SR **360.1**

Polizeibehörden der Kantone ausserhalb eines Strafverfolgungsverfahrens: Hier bestimmt sich der Datenschutz nach dem kantonalen Datenschutzgesetz, soweit nicht kantonale Spezialbestimmungen vorgehen.

NDB: Die Artikel 44–67 NDG gehen den Bestimmungen des DSG vor.

Kantonale Vollzugsstellen nach Artikel 9 NDG: Arbeiten diese kantonalen Behörden als Vollzugsstellen nach Artikel 46 Absatz 1 NDG, unterstehen sie dem Datenschutzrecht des Bundes, soweit nicht besondere Bestimmungen des NDG vorgehen. Arbeiten die kantonalen Nachrichtendienste dagegen in ihrem kantonalen Zuständigkeitsbereich, bestimmt sich der zu gewährleistende Datenschutz nach kantonalem Recht.

Artikel 18 Pseudonymisierung der Flugpassagierdaten

Bei der Pseudonymisierung werden Daten, die Rückschlüsse auf eine konkrete Person zulassen, durch neutrale Angaben (Pseudonym) ersetzt. Eine Konkordanztabelle hält fest, welches Pseudonym welchen identifizierenden Daten entspricht. Die Konkordanztabelle muss ausserhalb des PNR-Informationssystems gespeichert werden. Solange diese Tabelle besteht und den berechtigten Personen zugänglich ist, kann die Pseudonymisierung rückgängig gemacht werden (vgl. Art. 19 und 20).

Im Rahmen der Vernehmlassung wurde − zum Teil unter Bezugnahme auf das EuGH-Urteil − eine deutliche Verkürzung der Aufbewahrungsdauer für Daten gefordert, die keinen Anlass für eine längere Speicherung geben.

Damit wird implizit verlangt, dass im gesamten Anwendungsbereich von PNR zwischen Daten zu unterscheiden ist, die objektive Anhaltspunkte dafür liefern, dass von bestimmten Personen eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität ausgehen könnte («markierte Daten»), und Daten, die keine solchen Anhaltspunkte liefern (übrige Flugpassagierdaten). Für die markierten und die übrigen Flugpassagierdaten sieht das vorliegende Gesetz je unterschiedliche Regelungen vor.

Eine dieser Regelungen stellt die Pseudonymisierung dar. Pseudonymisiert werden sollen nach Artikel 18 nur Daten, die keiner zuständigen Behörde bekanntgegeben worden und deshalb nicht nach Artikel 7 Absatz 3 markiert sind. Ihnen gleichgestellt sind Daten, deren Markierung nachträglich aufgehoben worden ist (vgl. Art. 11). Sie sollen einen Monat nach ihrem Eingang im PNR-Informationssystem pseudonymisiert werden.

Gemäss der Botschaft zum neuen Datenschutzgesetz gilt die Pseudonymisierung als geeignete technische Massnahme, um die Datensicherheit (vgl. Art. 8 DSG) zu gewährleisten.[52] Der Bundesrat führt dazu in der Botschaft aus, dass das Datenschutzgesetz nicht für Daten gilt, «… wenn eine Reidentifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre, den

52 BBl **2017** 6941 S. 7031

kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten.»

Mit der Pseudonymisierung werden jene Daten eines Flugpassagierdatensatzes mit einem Pseudonym versehen, die Rückschlüsse auf die betroffene natürliche Person geben. Mit der Pseudonymisierung lassen sich die betroffenen Daten nicht mehr einer bestimmten oder bestimmbaren Person zuordnen und verlieren damit ihren Status als Personendaten.

In der Botschaft zum neuen Datenschutzgesetz schreibt der Bundesrat, dass die Pseudonymisierung eine der technischen Massnahmen sei, um «Verletzungen der Datensicherheit zu vermeiden, d. h. jede Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.»[53]

Folgende Personendaten nach Artikel 5 Buchstabe a DSG lassen sich im Flugpassagierdatensatz (vgl. Anhang 1 des Gesetzes) finden:

- Namen der Flugpassagierin oder des Flugpassagiers sowie Namen der mitreisenden Personen (Kategorien 4 und 17);
- Adresse und Kontaktdaten (Kategorie 5);
- Einzelheiten zu den eingesetzten Kreditkarten und Rechnungsadresse (Kategorie 6);
- Vielflieger-Eintrag (Kategorie 8);
- Name der Sachbearbeiterin oder des Sachbearbeiters des Reisebüros, das die Buchung des Tickets vorgenommen hat (Kategorie 9);
- Angaben zu unbegleiteten Personen unter 18 Jahren: Name und Geschlecht, Alter, Sprachen, Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht, begleitende/r Flughafenmitarbeiter/in bei Abflug und Ankunft (Kategorie 12);
- API-Daten (vgl. Art. 104 Abs. 3 AIG), die zugleich Personendaten sind: (a) Personalien (Name, Vorname, Geschlecht, Geburtsdatum, Staatsangehörigkeit) der Flugpassagierin / des Flugpassagiers; (b) Nummer, Ausstellerstaat, Art und Ablaufdatum des mitgeführten Reisedokuments; (c) Nummer, Ausstellerstaat, Art und Ablaufdatum des mitgeführten Visums oder Aufenthaltstitels, soweit das Luftverkehrsunternehmen über diese Daten verfügt (Kategorie 18);
- nachträgliche Änderungen der im Flugpassagierdatensatz aufgeführten Personendaten (Kategorie 19).

53 BBl **2017** 6941 S. 7031

Die Personendaten in diesen Datenkategorien sind zu pseudonymisieren.

Im Gegensatz zur Anonymisierung kann die Pseudonymisierung unter bestimmten Voraussetzungen rückgängig gemacht werden.

Daten, die objektive Anhaltspunkte für Schwerstkriminalität aufweisen, einer zuständigen Behörde nach Artikel 1 Absatz 2 zur weiteren Abklärung bekanntgegeben und von der PIU deshalb markiert worden sind (vgl. Art. 7), sollen dagegen *nicht* pseudonymisiert werden.

Absatz 1

Flugpassagierdaten, die *keine* Anhaltspunkte auf Schwerstkriminalität geben und deshalb keiner Behörde nach Artikel 1 Absatz 2 bekanntgegeben worden sind, weisen keine Markierung auf (vgl. Art. 7 Abs. 3). Sie werden bereits nach Ablauf von einem Monat seit ihrem Eingang im PNR-Informationssystem automatisch pseudonymisiert und lassen sich damit nicht mehr der betroffenen Flugpassagierin oder dem betroffenen Flugpassagier zuordnen.

Markierte Daten werden dagegen nicht pseudonymisiert.

Absatz 2

Stellt die zuständige Behörde fest, dass die Daten für ihre Verfahren nicht mehr nötig sind, hat sie die PIU davon in Kenntnis zu setzen. Die PIU hebt sodann die Markierung der betroffenen Daten auf (vgl. Art. 10 Abs. 2).

Nach Aufhebung der Markierung sind diese Daten je nachdem durch die PIU:

- *zu pseudonymisieren*, sofern die für die Daten massgebende Flugreise mindestens einen Monat und nicht länger als sechs Monate zurückliegt; oder
- *zu löschen*, sofern die Flugreise länger als sechs Monate zurückliegt (vgl. Art. 21 Abs. 2).

Artikel 19 Ordentliche Aufhebung der Pseudonymisierung

Pseudonymisiert sind nur Personendaten in Flugpassagierdatensätzen ohne Markierung und in solchen, deren Markierung nachträglich aufgehoben worden ist (vgl. Art. 18 Abs. 2).

Trotz des automatischen Abgleichs der Flugpassagierdaten nach Artikel 6 und der daran anschliessenden manuellen Überprüfung erweist sich die einmonatige Frist bis zur Pseudonymisierung jedoch als sehr kurz. Abfragen im PNR-Datenbestand müssen deshalb auch dann möglich sein, wenn die Daten älter als einen Monat und damit, sofern nicht markiert, pseudonymisiert sind. Solche historischen Suchanfragen bedingen, dass die Pseudonymisierung im Bedarfsfall aufgehoben werden kann.

Artikel 19 legt fest, dass die Pseudonymisierung nur aufgehoben werden darf, wenn das Bundesverwaltungsgericht die gesetzlichen Voraussetzungen als erfüllt betrachtet und diesen Bearbeitungsschritt genehmigt.

Systemtechnisch ist sichergestellt, dass die vom Gericht genehmigte Aufhebung der Pseudonymisierung nur vollzogen werden kann, wenn:

- dies durch eine Person erfolgt, die über die dazu nötige Berechtigung verfügt; *und*
- das Urteil des Bundesverwaltungsgerichts hinterlegt oder auf andere Weise hinreichend referenziert wird.

Dieser Schritt wird protokolliert, sodass auch im Nachhinein feststellbar ist, ob die Pseudonymisierung rechtmässig aufgehoben worden ist (vgl. Art. 24).

Nach den Artikeln 19 und 20 ist die Pseudonymisierung aufzuheben, wenn eine zuständige Behörde dies verlangt.

Nicht nach diesen Bestimmungen, sondern ohne gerichtliches Urteil lässt sich die Pseudonymisierung aufheben, wenn ein Auskunftsbegehren der betroffenen Person nach Artikel 26 Absatz 1 diesen Schritt bedingt. Die nötige gesetzliche Grundlage bildet Artikel 25 Absatz 2 Buchstabe b des DSG, wonach der betroffenen Person in der erteilten Auskunft «die bearbeiteten Personendaten als solche» mitzuteilen sind.

Allerdings ist auch die Aufhebung der Pseudonymisierung aufgrund eines Auskunftsbegehrens zu protokollieren (vgl. Art. 24). Im Protokoll muss das Auskunftsbegehren hinterlegt oder in anderer Form hinreichend referenziert werden. Im Einzelnen wird dies auf Verordnungsebene zu regeln sein.

Absatz 1

Behörden nach Artikel 1 Absatz 2 können der PIU die Aufhebung der Pseudonymisierung beantragen.

Absätze 2 und 3

In einem ersten Schritt prüft die PIU, ob der Antrag hinreichend begründet ist.

Hinreichend begründet ist ein Antrag, wenn:

- die Daten, deren Pseudonymisierung aufgehoben werden soll, bestimmt sind; dies ist dann erfüllt, wenn sich die beantragte Aufhebung der Pseudonymisierung beispielsweise auf eine bestimmte Person bezieht; in begründeten Ausnahmefällen kann sich der Aufhebungsantrag aber auch auf einen ganzen Flug beziehen;
- glaubhaft gemacht wird, dass die Aufhebung der Pseudonymisierung massgebliche Informationen zur Bekämpfung einer bestimmten Straftat nach Anhang 2 des Gesetzes liefert; die erwarteten Informationen sind dabei möglichst genau zu umschreiben.

Fehlen im Antrag entsprechende Ausführungen oder sind sie unzureichend, teilt die PIU dies der antragstellenden Behörde mit, die damit die Möglichkeit einer Vervollständigung ihres Antrags hat (Abs. 3).

Die PIU empfiehlt eine Aufhebung der Pseudonymisierung, wenn sich damit die gesuchten Informationen aus technischer Sicht erzielen lassen. Technisch

nicht erzielbar sind Informationen, die nicht Gegenstand eines Flugpassagierdatensatzes sein können. Gleiches gilt für Daten, die älter als sechs Monate sind. Denn solche Daten sind entweder bereits gelöscht (da ohne Markierung) oder nicht pseudonymisiert (da markiert).

Ist der Antrag hinreichend begründet, leitet die PIU ihn zusammen mit ihrer Empfehlung ans Bundesverwaltungsgericht weiter.

Absätze 4 und 5

Über eine allfällige Aufhebung der Pseudonymisierung entscheidet das Bundesverwaltungsgericht. Die Zuständigkeit eines Gerichts sehen grundsätzlich auch das deutsche[54] wie das österreichische Recht[55] in Umsetzung von Artikel 12 Absatz 3 der PNR-Richtlinie der EU vor.

Die dem Bundesverwaltungsgericht eingeräumte Frist beläuft sich auf maximal fünf Arbeitstage. Diese Maximalfrist entbindet das Gericht jedoch nicht davon, je nach Schwere des Verdachts möglichst zeitnah zu entscheiden.

Der Entscheid ist endgültig. Die Unzulässigkeit von Beschwerden ans Bundesgericht auf dem Gebiet der inneren und äusseren Sicherheit der Schweiz ergibt sich aus Artikel 83 Buchstabe a des Bundesgerichtsgesetzes vom 17. Juni 2005[56].

Absatz 6

Das Bundesverwaltungsgericht eröffnet seinen Entscheid sowohl der PIU wie der antragstellenden Behörde.

Art. 20 Aufhebung der Pseudonymisierung bei Dringlichkeit

Das Vorgehen bei nachweislicher Dringlichkeit orientiert sich an Artikel 31 NDG.

In einem dringlichen Fall soll die Aufhebung der Pseudonymisierung durch die Direktorin oder den Direktor des fedpol provisorisch angeordnet werden können. Sie oder er orientiert sodann umgehend die Vorsteherin oder den Vorsteher des EJPD, die oder der die Aufhebung der Pseudonymisierung sistieren lassen kann (vgl. Art. 31 Abs. 1 NDG).

Zu diesem Schritt veranlasst dürfte sie oder er nur sein, wenn die Dringlichkeit fraglich ist. Aufgrund des Sistierungsentscheids sind alle bereits getätigten Schritte zur Aufhebung der Pseudonymisierung wieder rückgängig zu machen und der Entscheid des Bundesverwaltungsgerichts abzuwarten.

54 Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG), § 5 Abs. 2, BGBl 117s1484

55 Bundesgesetz über die Verarbeitung von Fluggastdaten zur Vorbeugung, Verhinderung und Aufklärung von terroristischen und bestimmten anderen Straftaten (PNR-Gesetz – PNR-G), § 6 Abs. 2, BGBl. I Nr. 64/2018

56 SR **173.110**

Dieses entscheidet innerhalb von drei Arbeitstagen über den Antrag der Direktorin oder des Direktors des fedpol (vgl. Art. 31 Abs. 2 und 3 NDG).

Im Fall eines abschlägigen Entscheids des Bundesverwaltungsgerichts sind alle Schritte vollständig rückgängig zu machen, die aufgrund der provisorischen Anordnung durch die Direktorin oder den Direktor des fedpol veranlasst worden sind.

Artikel 21 Aufbewahrungsdauer und Löschung der Flugpassagierdaten

Artikel 21 bezieht sich lediglich auf die Flugpassagierdaten und regelt deren Löschung und damit indirekt deren Aufbewahrungsdauer.

Die Löschung aller anderen Daten, die sich aus der Datenbearbeitung durch die PIU ergeben oder mit der Bearbeitung in Zusammenhang stehen, richtet sich nach Artikel 22. Eine Ausnahme bildet die Löschung der Protokolle (vgl. Art. 24 Abs. 4).

Nach diesem Gesetz gelöscht sind Daten und Informationen, wenn sie unwiderruflich gelöscht sind und damit nicht wiederhergestellt werden können. Dies geschieht automatisch, indem der Speicherplatz mehrfach überschrieben wird.

Der EuGH hält in seinem Urteil vom 21. Juni 2022 unmissverständlich fest, dass sich eine sechsmonatige Aufbewahrung aller Flugpassagierdaten *rechtfertigen lässt*.

Dagegen müsse sich eine darüberhinausgehende Aufbewahrung auf das ermittlungs- und verfolgungstechnisch absolut Notwendige beschränken:

«Gibt es in besonderen Fällen objektive Anhaltspunkte – wie bei den PNR-Daten […], die zu einem überprüften Treffer geführt haben – dafür, dass von bestimmten Fluggästen eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität ausgehen könnte, erscheint eine Speicherung ihrer PNR-Daten über den ursprünglichen Zeitraum hinaus jedoch zulässig.»[57]

Verschiedene Vernehmlassungsteilnehmerinnen und -teilnehmer schlossen sich dieser Sichtweise an und beriefen sich in ihren Stellungnahmen zum Teil auf das genannte Urteil.

Artikel 21 sieht nun je nach Daten unterschiedliche Aufbewahrungsdauern vor:

- für Daten ohne Markierung: sechs Monate;
- für markierte Daten, die älter als sechs Monate sind: bis zur Aufhebung der Markierung und längstens bis fünf Jahre nach ihrem Eingang im PNR-Informationssystem.

Mit dieser indirekten Regelung wird auch klargestellt, dass es sich bei der zulässigen Aufbewahrungsdauer um absolute Fristen handelt.

57 Rechtssache C-817/19, ECLI:EU:C:2022:491, Rz. 259.

Absatz 1

Eine Aufbewahrungsdauer von sechs Monaten gilt für alle Flugpassagierdaten, die nicht markiert sind. Nach Ablauf von sechs Monaten werden diese Daten automatisch gelöscht.

Absatz 2

Markierte Flugpassagierdaten dürfen fünf Jahre aufbewahrt werden. Danach werden auch sie automatisch gelöscht.

Wird die Markierung vor Ablauf der für markierte Daten zulässigen Aufbewahrungsdauer aufgehoben, hat die PIU die nun wieder als Flugpassagierdaten ohne Markierung geltenden Daten je nach Datum ihres Eingangs im PNR-Informationssystem sofort zu pseudonymisieren oder zu löschen (vgl. Erläuterungen zu Art. 18 Abs. 2).

Artikel 22 Löschung von weiteren Daten

Anders als in Artikel 21, der die Löschung der Flugpassagierdaten regelt, geht es in Artikel 22 um die weiteren Daten, die bei der Bearbeitung der Flugpassagierdaten nach diesem Gesetz anfallen können.

«Umgehend» erfolgt eine Löschung, wenn die Löschung zeitlich ohne Verzögerung auf die bewusste Kenntnisnahme des Umstands folgt, der die Löschung bedingt.

Nach diesem Gesetz gelöscht sind Daten und Informationen, wenn sie unwiderruflich gelöscht sind und damit nicht wiederhergestellt werden können. Dies geschieht automatisch, indem der Speicherplatz mehrfach überschrieben wird.

Buchstabe a

Nach Artikel 5 Absatz 2 darf die PIU nur biometrische Daten und Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen bearbeiten. Alle anderen besonders schützenswerten Personendaten muss die PIU umgehend löschen.

Buchstabe b

Alle Übereinstimmungen, die aufgrund des automatischen Datenabgleichs erzielt worden sind, müssen vor ihrer Bekanntgabe an eine zuständige Behörde manuell überprüft werden (vgl. Art. 6 Abs. 2).

Aus Buchstabe b ergibt sich, unter welchen Voraussetzungen die überprüften Übereinstimmungen nicht bekanntgegeben werden dürfen, sondern umgehend zu löschen sind.

Sie sind einerseits zu löschen, wenn sich einer erzielten Übereinstimmung keine Straftat nach Anhang 2 eindeutig zuordnen lässt (vgl. Ziff. 1). Anderseits sind sie zu löschen, wenn die gesuchte Person und die Flugpassagierin oder der Flugpassagier nicht identisch sind (vgl. Ziff. 2).

Buchstabe c

Flugpassagierdaten, die einer Behörde nach Artikel 1 Absatz 2 bekanntgegeben und deshalb markiert worden sind, werden nach Ablauf von fünf Jahren automatisch gelöscht, sofern ihre Markierung nicht vorher aufgehoben worden ist (vgl. Art. 21 Abs. 2).

Buchstabe c legt fest, dass jene Daten, die der zuständigen Behörde zusammen mit den Flugpassagierdaten bekanntgegeben worden sind, zu löschen sind, sobald die betroffenen Flugpassagierdaten gelöscht worden sind.

Buchstabe d

Risikoprofile und Beobachtungslisten bestehen aus Daten, die nicht nach Artikel 21 gelöscht werden. Sie sollen nach Artikel 22 Buchstabe d gelöscht werden, sobald kein Bedarf mehr nach diesen Daten ist.

Buchstabe e

Einen Sonderfall stellen die Daten darf, die nach Artikel 14 Gegenstand einer Beobachtungsliste sind. Diese Daten sind mit Ablauf der Frist zu löschen, die das Zwangsmassnahmengericht festgelegt hat (vgl. Art. 14 Abs. 2). Erweisen sie sich bereits vorher als nicht mehr erforderlich, sind die entsprechenden Daten nach Buchstabe d zu löschen.

Artikel 23 Bearbeitung von anonymisierten Daten

Anonymisiert sind Daten, wenn sie keiner bestimmten oder bestimmbaren Person mehr zugeordnet werden können und dies unwiderruflich ist.

Mit der Anonymisierung verlieren die Daten *unwiderruflich* ihren Status als Personendaten (vgl. Art. 5 Bst. a DSG). Mit der Unwiderruflichkeit unterscheidet sich die Anonymisierung von der Pseudonymisierung. Letztere lässt sich unter bestimmten Voraussetzungen aufheben (vgl. Art. 19 und 20), sodass die Daten wieder einer bestimmten oder bestimmbaren Person zugeordnet werden können.

Anonymisierte Daten darf die PIU zu statistischen Zwecken bearbeiten. Die PIU kann sie aber auch dem Bundesarchiv zur Übernahme anbieten (vgl. Art. 6 des Archivierungsgesetzes vom 26. Juni 1998[58]).

Artikel 24 Protokolle der Datenbearbeitung

Absatz 1

Die Bearbeitungsschritte, die zwingend protokolliert werden müssen, bestimmen sich nach Artikel 4 Absatz 2 DSV: Bei der automatisierten Bearbeitung von Personendaten sind zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten in Protokollen festzuhalten.

Im schweizerischen Datenschutzrecht fehlt eine Legaldefinition des zentralen Begriffs «automatisiert». Nach schriftlicher Auskunft des Bundesamts für Justiz (BJ) vom 23. November 2022 lässt sich der Begriff «automatisiert» als Gegenstück zu «manuell» verstehen. «Eine manuelle Datenbearbeitung beinhaltet das Handeln einer Person, während eine automatisierte Bearbeitung durch einen ‹Automaten› vorgenommen wird. Dabei handelt es sich um eine ‹Maschine, deren mechanische oder elektronische Steuerung bewirkt, dass die von ihr selbsttätig vorgenommenen Arbeitsabläufe zu einer abrufbaren Leistung führen, die von einer vorherigen Arbeitsaufgabe abhängt›.»

Das BJ weist jedoch darauf hin, dass die Protokollierungspflicht auch dann greift, «wenn gewisse Arbeitsschritte manuell vorgenommen werden». Es führt aus, dass eine Protokollierung insbesondere dann erfolgen müsse, «wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.»

Die Protokolle müssen nach Artikel 4 Absatz 4 DSV Aufschluss geben über:

- die Identität der Person, welche die Bearbeitung vorgenommen hat;
- die Art der Bearbeitung;
- das Datum und die Uhrzeit der Bearbeitung;
- die Identität allfälliger Empfängerinnen und Empfänger der Daten.

Dadurch ermöglichen Protokolle, dass die einzelnen Bearbeitungen von Personendaten nachträglich überprüfbar sind.

Absätze 2 und 3

Absatz 2 hält fest, welchen Zwecken die Protokolle dienen.[59] Mit dieser abschliessenden Aufzählung ist eine Nutzung der Protokolle zur Überwachung von Mitarbeitenden nicht erlaubt. Dies zeigt sich auch in der Zugriffsberechtigung nach Absatz 3.

Absatz 4

Protokolle werden automatisch erstellt und müssen ausserhalb des PNR-Informationssystems aufbewahrt werden. Damit wird gewährleistet, dass die Protokolle – selbst im Falle eines Cyberangriffs − nicht manipuliert werden können und sicher sind. Es ist vorgesehen, die Protokolle zu PNR auf der Infrastruktur des ISC-EJPD zu speichern.

Der vorerwähnte erläuternde Bericht zur DSV hält fest, dass die Protokolle ein Jahr aufbewahrt werden müssen (vgl. Art. 4 Abs. 5 DSV). «Dies bedeutet allerdings nicht, dass die Protokolle während einer unverhältnismässig langen

59 Erläuternder Bericht des BJ vom 31. August 2022 zur Datenschutzverordnung, S. 27; www.bj.admin.ch > Neues Datenschutzrecht > Neues Datenschutzrecht > 1. Bisherige Etappen, 2022 – Verabschiedung der neuen Verordnungen (DSV und VDSZ).

Dauer aufbewahrt werden dürfen. Die Aufbewahrungsdauer muss im Vergleich zum Ziel einer angemessenen Datensicherheit in einem angemessenen Verhältnis stehen.»[60]

Das vorliegende Gesetz sieht vor, dass die Protokolle der automatisierten Bearbeitung von Flugpassagierdaten ein Jahr länger verfügbar sein sollen als die Daten, deren Bearbeitung protokolliert worden ist. Danach sind die Protokolle zu löschen.

Bis zu ihrer Löschung sind die Protokolle demnach zu Kontroll- und Aufsichtszwecken verfügbar, nicht jedoch für die PIU.

Artikel 25 Überwachung und Aufsicht

Fachlich unabhängig und weisungsungebunden überwacht die Datenschutzberaterin oder der Datenschutzberater des fedpol amtsintern die Einhaltung der Datenschutzvorschriften (vgl. Art. 26 Abs. 1 und 2 DSV). Diese Aufgabe übt die Datenschutzberaterin oder der Datenschutzberater auch gegenüber der PIU aus.

Zudem fungiert die Datenschutzberaterin oder der Datenschutzberater als Anlaufstelle für den EDÖB (Art. 28 DSV).

Das fedpol hat der Datenschutzberaterin oder dem Datenschutzberater Zugang zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten zu gewähren, die sie oder er zur Erfüllung ihrer oder seiner Aufgaben benötigt, und allfällige Verletzungen der Datensicherheit zur Kenntnis zu bringen.

Trotz der Unterstützungs- und Kontrollfunktion[61], welche der Datenschutzberaterin oder dem Datenschutzberater zukommt, verbleibt die eigentliche Aufsicht beim EDÖB.

Die Verantwortung, dass die Personendaten bei der PIU datenschutzkonform bearbeitet werden, tragen jedoch weder die Datenschutzberaterin oder der Datenschutzberater noch der EDÖB. Sie liegt allein beim fedpol. Dies ergibt sich aus der Botschaft[62] zum neuen Datenschutzgesetz.

60 Erläuternder Bericht des BJ vom 31. August 2022 zur Datenschutzverordnung, S. 27, www.bj.admin.ch > Neues Datenschutzrecht > Neues Datenschutzrecht > 1. Bisherige Etappen, 2022 – Verabschiedung der neuen Verordnungen (DSV und VDSZ).

61 Erläuternder Bericht des Bundesamts für Justiz vom 31. August 2022 zur Verordnung über den Datenschutz (Datenschutzverordnung, DSV), S. 17, Ziff. 4.7; www.bj.admin.ch > Neues Datenschutzrecht > Neues Datenschutzrecht > 1. Bisherige Etappen, 2022 – Verabschiedung der neuen Verordnungen (DSV und VDSZ)

62 BBl **2017** 6941 S. 7033

Artikel 26 Auskunftsrecht

Luftverkehrsunternehmen haben Flugpassagiere bei der Buchung ihrer Tickets über die Bearbeitung ihrer Daten nach dem vorliegenden Gesetz zu informieren (vgl. Art. 4).

Die von den Luftverkehrsunternehmen erhaltene Information ermöglicht es einer betroffenen Person, von ihrem Auskunftsrecht nach Artikel 26 Gebrauch zu machen. Ersuchen um Auskunftserteilung sind an das fedpol zu richten.

Zu unterscheiden sind:

- *das direkte Auskunftsrecht (Abs. 1)*, das bei Daten zum Zuge kommt, die nicht älter als sechs Monate sind, und sich aus den Artikeln 25–28 DSG ergibt und
- *das indirekte Auskunftsrecht (Abs. 2)*, das auf Daten Anwendung findet, die älter als sechs Monate sind, und sich sinngemäss nach Artikel 8 BPI richtet.

Das unterschiedliche Vorgehen je nach Alter der Daten lässt sich damit erklären, dass nach Ablauf von sechs Monaten nur noch markierte Flugpassagierdaten aufbewahrt sind, die sich bei der zuständigen Behörde in Bearbeitung befinden. Eine Auskunft, wonach Daten einer Flugreise bearbeitet werden, die länger als sechs Monate zurückliegt, bestätigt ein laufendes Verfahren und ist ein Hinweis auf den Verdacht, der auf der gesuchstellenden Person lastet.

Eine solche Information kann laufende Vor- und Ermittlungsverfahren empfindlich beeinträchtigen.

Das DSG eröffnet zwar für solche Fälle mit Artikel 26 Absatz 2 Buchstabe b die Möglichkeit, die Auskunft zu verweigern, einzuschränken oder aufzuschieben. Demgegenüber wäre nach dem DSG aber der überwiegenden Zahl der Passagierinnen und Passagiere desselben Flugs eine andere Auskunft zu erteilen: dass ihre Daten nicht oder nicht mehr bearbeitet werden. Denn sie sind nach Artikel 21 Absatz 1 bereits gelöscht.

Im Fall der Flugpassagierdaten kommt somit eine Verweigerung, eine Einschränkung oder ein Aufschub der Auskunft nach Artikel 26 Absatz 2 Buchstabe b DSG der Auskunft gleich, dass die fraglichen Daten auch nach Ablauf von sechs Monaten noch bearbeitet werden. Damit wäre die betroffene Person gewarnt. Denn länger als sechs Monate dürfen Flugpassagierdaten nur bearbeitet werden, wenn sie markiert und damit von einer zuständigen Behörde bekanntgegeben worden sind.

Um diese unerwünschte Information zu verhindern, behilft sich das Flugpassagierdatengesetz mit dem indirekten Auskunftsrecht nach Artikel 8 BPI.

In solchen Fällen verfasst das fedpol stets die gleichlautende Antwort, unabhängig davon, ob Daten vorhanden sind: Die Auskunftserteilung werde aufgeschoben, die gesuchstellende Person habe jedoch das Recht, vom EDÖB

die Prüfung zu verlangen, ob allfällige, ihre Person betreffende Daten rechtmässig bearbeitet werden.

Der EDÖB führt die Prüfung durch, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte (Art. 49 Abs. 1 DSG). Er informiert sodann die um Prüfung ersuchende Person über die unternommenen Schritte und das Ergebnis einer allfälligen Untersuchung.

Diese für eine gesuchstellende Person elementare Auskunft wird auch beim indirekten Auskunftsrecht nach Artikel 8 BPI niemandem verweigert, auch jenen Personen nicht, deren Daten bei der PIU markiert und von einer zuständigen Behörde nach Artikel 1 Absatz 2 bearbeitet werden.

Unabhängig davon hat das fedpol der gesuchstellenden Person nach Ablauf des Geheimhaltungsinteresses und spätestens nach Ablauf der maximal zulässigen Aufbewahrungsdauer von fünf Jahren die Auskunft zu erteilen, um die ersucht wurde. Personen, über die keine Daten bearbeitet wurden, informiert das fedpol drei Jahre nach Eingang ihres Gesuchs über diese Tatsache (vgl. Art. 8 Abs. 6 BPI).

7. Abschnitt: Organisation und Personal der PIU

Artikel 27 Organisation

Absatz 1

Die nationale Stelle für Flugpassagierdaten, die PIU, soll organisatorisch beim fedpol angesiedelt werden. Diese Zuordnung ergibt sich einerseits aus der Zweckbestimmung der Datenbearbeitung. Anderseits lässt sie sich auch mit der breiten Erfahrung des fedpol im Umgang mit Informationssystemen begründen, was sich zweifellos positiv auf den Aufbau und Betrieb des PNR-Informationssystems auswirken wird.

Absatz 2

Angesichts der Besonderheit der Flugpassagierdaten, deren Schutz es zu gewährleisten gilt, rechtfertigt es sich, dass die PIU organisatorisch von den Einheiten getrennt ist, die beim fedpol Ermittlungsaufgaben wahrnehmen. Explizit erwähnt wird auch die personelle Trennung, womit ausgeschlossen wird, dass einzelne Mitarbeitende zeitgleich sowohl bei der PIU als auch bei einer ermittelnden Behörde oder bei den Strafverfolgungsbehörden arbeiten können.

Damit wird verhindert, dass diese Behörden informell einen privilegierten Zugang zu Informationen der PIU erhalten. Für alle zuständigen Behörden nach Artikel 1 Absatz 2 gelten damit die gleichen Voraussetzungen, um Daten von der PIU zu erhalten, unabhängig davon, ob es sich um Behörden des Bundes oder der Kantone handelt.

Hinsichtlich PNR soll die beim fedpol angesiedelte PIU sowohl für die Luftverkehrsunternehmen wie auch für die ausländischen PIU der *Single Point of Contact* sein.

Die PIU kann bei Bedarf einen 24/7-Dienst sicherstellen, um auch die in Randzeiten eintreffenden Flugpassagierdaten rechtzeitig überprüfen zu können.

Artikel 28 Personal

Die PIU soll sich je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzen. Mit der Entsendung der Mitarbeitenden beteiligen sich die Kantone an den Kosten der PIU. Eine weitergehende Beteiligung der Kantone ist nicht vorgesehen.

Da die kantonalen Mitarbeitenden ohne Aufgabe ihres Arbeitsverhältnisses beim Kanton *vorübergehend* in den Betrieb der PIU eingegliedert werden, lässt sich dieses Zusammenarbeitsmodell am ehesten mit einer echten Leiharbeit, einem Typus des Personalverleihs vergleichen. Der Bundesrat schreibt dazu in der Botschaft vom 27. November 1985[63] zu einem revidierten Bundesgesetz über die Arbeitsvermittlung und den Personalverleih:

«Der Arbeitnehmer erbringt die geschuldete Arbeitsleistung nicht im Betrieb seines Arbeitgebers, sondern ausserhalb, in einem Einsatzbetrieb. Dies hat eine Aufspaltung der Arbeitgeberfunktionen zur Folge: Das Weisungsrecht betreffend Ziel- und Fachanweisungen und des Verhaltens des Arbeitnehmers im Betrieb sowie der Anspruch auf Interessenwahrung und Geheimhaltung gehen an den Einsatzbetrieb über, ebenso, damit notwendigerweise verbunden, die betriebliche Fürsorgepflicht; Die übrigen Rechte und Pflichten aus dem Arbeitsvertrag bleiben beim Verleiher, insbesondere die Lohnzahlungs- und die allgemeine Fürsorgepflicht.»

Diese Ausführungen gelten sinngemäss auch für die Entsendung von Mitarbeitenden in den Dienst der PIU.

Die Einzelheiten der Entsendung sollen der Bund und die Kantone in einer Vereinbarung regeln.

Dazu hält der Basler-Kommentar zur Bundesverfassung[64] (BV) fest:

«Da die Bundesverfassung aber die rechtsetzenden Verträge zwischen Bund und Kantonen nicht als eigenständige Erlassform (Art. 163 BV) vorsieht, müssen zumindest die Rahmenbedingungen des Vertrags durch ein Bundesgesetz (Art. 164 BV) oder (bei Bestimmungen von untergeordneter Bedeutung) durch eine Verordnung festgelegt werden. Erst auf der Basis dieser

63 BBl **1985** III 556 S. 565 f.
64 SR **101**

Rechtsgrundlage […] kann der Vertrag mit den Kantonen abgeschlossen werden.»[65]

Artikel 28 bildet die rechtliche Grundlage für die zwischen Bund und Kantonen abzuschliessende Vereinbarung und legt insbesondere fest:

- den Zweck und Umfang der Entsendung (Abs. 1);
- die Finanzierung (Abs. 2);
- wichtige personalrechtliche Sonderbestimmungen (Abs. 3 und 4).

Absatz 5 versteht sich als Delegationsnorm und berechtigt den Bundesrat, die aufgeführten Einzelheiten in der Vereinbarung mit den Kantonen zu regeln.

Ob die Kantone ihre jeweilige Beteiligung untereinander im Rahmen eines Konkordats oder anderweitig regeln, ist derzeit noch offen und bedarf keiner Regelung im Bundesrecht.

Absatz 1

Die Polizeiarbeit und die Strafverfolgung liegen aufgrund des föderalistischen Systems der Schweiz mehrheitlich in der originären Zuständigkeit der Kantone. Der Bund engagiert sich demgegenüber bei der Verfolgung gewisser schwerer Straftaten, so z. B. des Terrorismus und der organisierten Kriminalität sowie diverser Straftaten im Nebenstrafrecht des Bundes, wozu Straftatbestände beispielsweise im Kernenergie-[66], im Transplantations-[67] oder im Waffengesetz[68] gehören.

Vor diesem Hintergrund versteht sich die Bekämpfung von Schwerstkriminalität als eine gemeinsame Aufgabe von Bund und Kantonen mit je spezifischen Schwerpunkten. Mit der Bearbeitung der Flugpassagierdaten unterstützt die PIU Bund und Kantone gleichermassen bei der Wahrnehmung dieser gemeinsamen Aufgabe.

Deshalb soll sich die PIU je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammensetzen.

Absatz 2

Der Einsatz der kantonalen Mitarbeitenden bei der PIU führt nicht zu einer Aufhebung des bisherigen Arbeitsverhältnisses, sondern lediglich zu einer Aufspaltung der Arbeitgeberrolle, wie dies auch beim Personalverleih der Fall ist.[69]

Das Weisungsrecht in fachlichen und betrieblichen Fragen, wozu unter anderem das Festlegen der Einsatzzeiten gehört, geht während des Einsatzes bei

65 Waldmann Bernhard /Belser Eva Maria / Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015, Art. 48 N 37.
66 Kernenergiegesetz vom 21. März 2003; SR **732.1.**
67 Transplantationsgesetz vom 8. Oktober 2004; SR **810.21.**
68 Waffengesetz vom 20. Juni 1997; SR **514.54.**
69 Arbeitsvermittlungsgesetz vom 6. Oktober 1989; SR **823.11.**

der PIU an das fedpol über. Dagegen verbleibt das disziplinarische Weisungsrecht bei der entsendenden Behörde.

Die übrigen Rechte und Pflichten aus dem Arbeitsvertrag, so insbesondere die Lohnzahlungspflicht und die Pflicht, für die sozialversicherungsrechtlichen Arbeitgeberbeiträge aufzukommen, bleiben bei jener Behörde, welche der PIU Mitarbeitende zur Verfügung stellt.

Allein durch den Bund getragen werden die Kosten für die Infrastruktur der Arbeitsplätze bei der PIU sowie für den Aufbau und den Betrieb des PNR-Informationssystems.

Zu beachten bleibt, dass der Bund nicht nur für seine Mitarbeitenden, sondern auch für die kantonal entsandten, bei der PIU im Einsatz stehenden Mitarbeitenden nach dem Verantwortlichkeitsgesetz vom 14. März 1958[70] (VG) einstehen muss. Dies folgt aus Artikel 1 Absatz 1 Buchstabe f VG.

Absatz 3

Die Absätze 3 und 4 sehen arbeitsrechtliche Sonderregelungen vor, die während des Einsatzes bei der PIU Anwendung finden sollen. Sie bedürfen einer gesetzlichen Grundlage.

Konkret geht es bei den Sonderregelungen:

- um das geteilte Weisungsrecht (Abs. 3); sowie
- um die Pflicht der Mitarbeitenden zur Verschwiegenheit (Abs. 4), die auch gegenüber ihrem vertraglichen Arbeitgeber zu wahren ist.

Als geteilt gilt das Weisungsrecht, weil es teilweise vom entsendenden Arbeitgeber und teilweise vom fedpol beziehungsweise durch die PIU wahrgenommen wird. Die PIU nimmt das fachlich-betriebliche Weisungsrecht wahr, das alles umfasst, was sich nicht dem disziplinarischen Weisungsrecht zuordnen lässt. Letzteres verbleibt beim vertraglichen Arbeitgeber.

Zeigt eine entsandte Person beim Einsatz der PIU ein disziplinarisch relevantes Verhalten, wird das fedpol das Gespräch mit dem vertraglichen Arbeitgeber zu suchen haben. Dieser prüft sodann, welche Massnahmen disziplinarisch angezeigt sind. In der überwiegenden Zahl von Fällen wird eine entsprechende Weisung ausreichen. In Ausnahmefällen muss disziplinarisch die fristlose Kündigung ausgesprochen werden. Auch diese Möglichkeit verbleibt in der Zuständigkeit des vertraglichen Arbeitgebers und wird durch die Entsendung nicht tangiert.

Absatz 4

Nach Absatz 4 ist es Mitarbeitenden der PIU untersagt, über Sachverhalte ausserhalb der PIU zu verfügen, von denen sie während ihres Einsatzes bei der PIU Kenntnis erhalten. Dies gilt auch nach Beendigung ihres Einsatzes. Damit

70 SR **170.32**

wird insbesondere der informelle Austausch von Personendaten zwischen der PIU und der entsendenden Einheit untersagt.

Wünschbar ist dagegen, dass die Mitarbeitenden nach der Rückkehr von ihrem Einsatz bei der PIU das dort angeeignete methodische Wissen bei der Bearbeitung von Flugpassagierdaten an ihre Kolleginnen und Kollegen weitergeben. Dazu gehören beispielsweise die Erfahrungen, wie Risikoprofile und Beobachtungslisten möglichst wirksam konzipiert und eingesetzt werden. Damit gewährleistet das Entsendemodell einen Wissenstransfer von der PIU in die entsendenden Behörden.

Absatz 5

In der vom Bundesrat mit den Kantonen abzuschliessenden Vereinbarung gilt es, die Einzelheiten der Entsendung festzulegen.

So gilt es neben der Zahl der entsandten kantonalen Mitarbeitenden auch die erwartete Qualifikation zu vereinbaren. Der Fokus dürfte insbesondere auf kantonalen Mitarbeitenden liegen, die eine hohe Affinität zu digitalen Prozessen haben. Die weiteren finanziellen Ansprüche der Entsandten, die ebenfalls Gegenstand der Vereinbarung sein sollen, betreffen insbesondere die Spesen. Zu ihrer Entrichtung verpflichtet ist grundsätzlich der vertragliche Arbeitgeber beziehungsweise der entsendende Kanton.

8. Abschnitt: Abschluss von Verträgen und Vereinbarungen sowie Amtshilfe

Artikel 29 Abschluss von Verträgen und Vereinbarungen

PNR werden derzeit bereits von 69 Staaten eingesetzt. Sie verlangen die Flugpassagierdaten im Minimum von den landenden Flügen.

Das vorliegende Gesetz sieht in Artikel 2 eine zur PNR-Richtlinie der EU analoge Regelung vor: Die Luftverkehrsunternehmen sollen der PIU in der Schweiz die Flugpassagierdaten sowohl beim Hinflug in die Schweiz wie auch beim Abflug aus der Schweiz bekanntgeben.

Allerdings dürfen Schweizer Luftverkehrsunternehmen ihre Flugpassagierdaten einer im Ausland zuständigen Stelle nur bekanntgeben, wenn ein völkerrechtlicher Vertrag der Schweiz dies vorsieht (vgl. Art. 2 Abs. 2).

Mit Artikel 29, der den Bundesrat zum Abschluss solcher Verträge ermächtigt, entfällt eine parlamentarische Genehmigung (vgl. Art. 166 Abs. 2 BV), soweit sich der Inhalt des Vertrags im Rahmen der Delegationsnorm nach Absatz 2 des vorliegenden Gesetzes bewegt.

Ein solcher Vertrag soll insbesondere mit der EU («internationale Organisation») abgeschlossen werden. Er soll die Übergangslösung ersetzen, die unter Mitwirkung des EDÖB erarbeitet worden ist und derzeit den Schweizer Luftverkehrsunternehmen die Datenbekanntgabe an die EU ermöglicht (vgl. vorne, Ziff. 1.2).

Rund 72 Prozent aller auf Schweizer Flughäfen verzeichneten Passagierinnen und Passagiere fliegen in die EU oder von dort in die Schweiz. Zwar lässt sich daraus nicht direkt auf das Volumen von Daten aus der EU schliessen. Dennoch zeigt dieser hohe Prozentanteil, dass der Luftverkehr zwischen der EU und der Schweiz bedeutend ist. Ein völkerrechtlicher Vertrag über die gegenseitige Bekanntgabe der Flugpassagierdaten ist sowohl für die Schweiz wie auch für die EU zentral. Der Bundesrat hat am 1. November 2023 ein entsprechendes Verhandlungsmandat erteilt.

Weitere Verträge sind unteranderem mit Norwegen und dem Vereinigten Königreich geplant.

Absatz 1

Die in Anhang 1 DSV aufgeführte Liste weist jene Staaten aus, die einen angemessenen Datenschutz gewährleisten. In diese Staaten können Personendaten aus der Schweiz bekanntgegeben werden, ohne dass ein völkerrechtlicher Vertrag abgeschlossen werden müsste. Dennoch sieht das vorliegende Gesetz vor, auch mit diesen Staaten Verträge abzuschliessen. Damit soll die *gegenseitige* Datenbekanntgabe sichergestellt werden. Erachten beide Staaten den vom anderen Staat gewährten Datenschutz als angemessen (vgl. Art. 16 Abs. 1 DSG), wird sich der Vertrag auf die Modalitäten der gegenseitigen Datenbekanntgabe beschränken.

Der erläuternde Bericht des Bundesamts für Justiz (BJ) vom 31. August 2022 zur Datenschutzverordnung führt indes aus, dass die in Anhang 1 der Verordnung aufgeführte Staaten-Liste regelmässig überprüft werde, «um einerseits die Praxis anderer Staaten und andererseits die Entwicklungen auf internationaler Ebene, insbesondere die Ratifizierungen des revidierten Übereinkommens SEV 108, zu berücksichtigen. Die Liste ist folglich nicht endgültig und könnte vor dem Inkrafttreten der Verordnung noch geändert werden.»[71]

In der Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz hielt der Bundesrat fest, dass unter völkerrechtlichem Vertrag «nicht nur ein internationales Datenschutzübereinkommen wie das Übereinkommen SEV 108[72] und sein Zusatzprotokoll zu verstehen [sei], dem der Empfängerstaat angehört und dessen Anforderungen von der Vertragspartei im innerstaatlichen Recht umgesetzt worden sind, sondern auch jedes andere internationale Abkommen, das einen Datenaustausch zwischen den Vertragsparteien vorsieht und materiell den Anforderungen des Überein-

71 www.bj.admin.ch > Neues Datenschutzrecht > Neues Datenschutzrecht > 1. Bisherige Etappen, 2022 – Verabschiedung der neuen Verordnungen (DSV und VDSZ).

72 Übereinkommen 5. Juni 1997 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten; SR **0.235.1.**

kommens SEV 108 entspricht. Dabei kann es sich auch um einen Staatsvertrag handeln, den der Bundesrat im Rahmen von Artikel 61 Buchstabe b E-DSG [entspricht Art. 67 Bst. b DSG] abgeschlossen hat». [73]

Absatz 2

Da die Schweiz nicht alle Vorgaben des EuGH übernommen hat, ist nicht ausgeschlossen, dass das Abkommen mit der EU punktuell vom vorliegenden Gesetz abweichende, strengere Regelungen des Datenschutzes vorsieht. Absatz 2 trägt diesem Umstand insofern Rechnung, als der Bundesrat ermächtigt wird, vertraglich nötigenfalls weniger weitgehende Bearbeitungen für Daten aus der EU zu vereinbaren.

Absatz 3

Mit Absatz 3 erhält das fedpol die Kompetenz, selbstständig Vereinbarungen mit Behörden anderer Staaten abzuschliessen. Diese Kompetenz ist begrenzt auf operative, technische oder administrative Inhalte.

Vereinbarungen über grundsätzliche Belange des Datenschutzes und über Rechte und Pflichten von Behörden sind dagegen immer in einem völkerrechtlichen Vertrag nach Absatz 1 durch den Bundesrat abzuschliessen.

Artikel 30 Amtshilfe

Auch im Fall von PNR soll die Amtshilfe grundsätzlich durch die zuständigen Behörden (vgl. Art. 1 Abs. 2) nach dem für diese Behörden geltenden Recht erfolgen.

Die PIU soll nur in Notfällen Amtshilfe leisten. Dies bringt Absatz 2 mit der «unmittelbaren Gefahr» einer Straftat nach Anhang 2 im Ausland zum Ausdruck. Abweichende Regelungen in einem völkerrechtlichen Abkommen bleiben indes vorbehalten.

Die Amtshilfe, welche die PIU einer ausländischen PIU leistet, ist somit auf begründete Ausnahmesituationen beschränkt, die ein Handeln der PIU – anstelle einer zuständigen Behörde nach Artikel 1 Absatz 2 – rechtfertigen.

Die PIU gibt Flugpassagierdaten einer ausländischen PIU im Rahmen der Amtshilfe nur auf deren begründeten Antrag bekannt. Dieser muss mindestens darlegen:

- die gewünschten, konkret bezeichneten Daten;
- deren Notwendigkeit zur Abwendung einer unmittelbar drohenden Straftat nach Anhang 2.

Die PIU darf die Daten nur einer ausländischen PIU bekanntgeben, die der Verwaltung eines Staates angehört, der:

- nach Anhang 1 DSV Gewähr für einen angemessenen Datenschutz bietet (vgl. Art. 16 Abs. 1 DSG); oder

73 BBl **2017** 6941 S. 7039

- aufgrund spezifischer Regelungen in einem völkerrechtlichen Vertrag mit der Schweiz einen geeigneten Datenschutz gewährleistet (Art. 16 Abs. 2 Bst. a DSG).

Greift keine dieser Voraussetzungen, muss die PIU auf die Bekanntgabe von Flugpassagierdaten verzichten.

Werden Daten verlangt, die pseudonymisiert oder besonders schützenswert sind, ist die Amtshilfe durch die PIU ebenfalls ausgeschlossen.

9. Abschnitt: Administrative Sanktionen

Artikel 31 Sanktionen bei Pflichtverletzung durch Luftverkehrsunternehmen

Die Sanktion nach Artikel 31 gehört zu den sogenannten pekuniären Verwaltungssanktionen. Ausgehend von den im Bundesrecht geltenden Regelungen hat der Bundesrat diese Sanktionen im Bericht vom 1. November 2018[74] wie folgt umschrieben: Eine pekuniäre Verwaltungssanktion kann «vereinfachend als eine finanzielle Belastung der Verfahrenspartei mit einem Betrag beschrieben werden, die als behördliche Reaktion auf eine in der Vergangenheit liegende Verletzung einer verwaltungsrechtlichen Vorschrift erfolgt und in einem Verwaltungsverfahren durchgesetzt wird».

Absatz 1

Eine Verletzung der Sorgfalts- und der Informationspflicht nach den Artikeln 3 und 4 soll unabhängig von einem Verschuldensnachweis seitens des Bundes geahndet werden, wie dies seit dem 1. Oktober 2015 in Artikel 122*b* AIG bei Meldepflichtverletzungen durch Luftverkehrsunternehmen Anwendung findet. Der Bundesrat begründete die damalige Abkehr vom Verschuldensnachweis mit den daraus resultierenden, umfangreichen Abklärungen, die auch im Ausland durchgeführt werden mussten. Faktisch hätte sich dieser Nachweis in der Praxis als unmöglich erwiesen.[75]

Absatz 2

Pflichtverletzungen nach Artikel 3 des vorliegenden Gesetzes werden gesetzlich vermutet, wenn die Bekanntgabe der Flugpassagierdaten:

- nicht oder zu spät;
- unter Nichtbeachtung technischer Vorgaben; oder
- nicht von allen Flugpassagierinnen und -passagieren des Fluges erfolgt ist.

74 Pekuniäre Verwaltungssanktionen. Bericht des Bundesrates in Erfüllung des Postulates 18.4100 SPK-N vom 1. November 2018, BBl **2022** 776 Ziff. 2.1.

75 Botschaft vom 8. März 2013 zur Änderung des Ausländergesetzes (Sorgfalts- und Meldepflichtverletzungen durch Luftverkehrsunternehmen, Informationssysteme), BBl **2013** 2561 S. 2588.

Gleiches gilt, wenn die Luftverkehrsunternehmen ihre Passagierinnen und Passagiere nicht im Sinne von Artikel 4 über die Datenbearbeitung nach diesem Gesetz informiert haben (vgl. Erläuterungen zu Art. 4).

Die PIU muss den Nachweis erbringen, dass die Luftverkehrsunternehmen die Daten nicht entsprechend den rechtlichen Vorgaben bekanntgegeben oder ihre Passagierinnen und Passagiere nicht oder nicht angemessen über die Bearbeitung der Daten nach dem vorliegenden Gesetz informiert hat.

Absatz 3

In leichten Fällen kann von der Eröffnung eines Verfahrens abgesehen werden, so z. B., wenn sich ein Verfahren als unverhältnismässig erweist.

Demgegenüber gilt eine Verletzung der Sorgfaltspflicht dann als schwer, wenn sie wiederholt festgestellt wird oder wenn die gesamten Datensätze eines Fluges nicht geliefert werden.

Absatz 4

Im vorerwähnten Bericht präzisierte der Bundesrat das vom Gesetzgeber vorgesehene Konzept der verschuldensunabhängigen pekuniären Verwaltungssanktion: «Somit muss die Verwaltungsbehörde zumindest ein Organisationsverschulden (objektiver Sorgfaltsmangel) nachweisen [können]. Sofern ein schuldhaftes Verhalten einer verantwortlichen Person vorliegt, kann das Unternehmen ebenfalls ins Recht gefasst werden. Dieser Mittelweg hat sich in der kartellrechtlichen Praxis bewährt und lässt sich auf die anderen Bestimmungen über pekuniäre Verwaltungssanktionen übertragen. Gesamthaft betrachtet besteht somit hinsichtlich des Verschuldens der Sanktionsadressaten auf gesetzlicher Ebene kein grundsätzlicher Anpassungsbedarf».[76]

Kann das Luftverkehrsunternehmen nachweisen, dass es trotz der zumutbaren Sorgfalt zu den Beanstandungen gekommen ist, entfällt eine Sanktion. Ein solcher Fall liegt beispielsweise bei einem unverschuldeten Stromausfall vor, der eine Datenbekanntgabe verunmöglicht hat.

Absatz 5

Absatz 5 stellt sicher, dass auch Sorgfaltspflichtverletzungen im Ausland geahndet werden können. Eine solche liegt unteranderem vor, wenn ein Luftverkehrsunternehmen die Flugpassagierdaten vor dem Abflug in die Schweiz nicht, nicht rechtzeitig oder unvollständig an die PIU in der Schweiz bekanntgibt.

Artikel 32 Verfahren

Absatz 1

Eine Sanktion nach Artikel 31 spricht das fedpol aus.

[76] Pekuniäre Verwaltungssanktionen. Bericht des Bundesrates in Erfüllung des Postulates 18.4100 SPK-N» vom 1. November 2018, BBl **2022** 776 Ziff. 4.3.3.

Absatz 2

Wird eine Verletzung der Meldepflicht nach Artikel 122*b* AIG mit einer Sanktion belegt, soll sie dafür nicht zusätzlich nach dem Flugpassagierdatengesetz sanktioniert werden. Allerdings bleibt eine Sanktion wegen Verletzungen der Informationspflicht nach Artikel 4 vorbehalten.

Absatz 3

Die Frist von zwei Jahren lässt sich nicht erstrecken.

10. Abschnitt: Schlussbestimmungen

Artikel 33 Vollzug

Bei diesen Ausführungsbestimmungen handelt es sich um untergeordnete beziehungsweise Detailvorschriften, die dem Vollzug des vorliegenden Gesetzes dienen. Die Kompetenz des Bundesrates zum Erlass solcher Bestimmungen basiert auf Artikel 182 Absatz 2 BV.

Artikel 34 Änderung anderer Erlasse

Anhang 3 weist aus, welche Änderungen in Zusammenhang mit dem vorliegenden Gesetz in anderen Gesetzen vorgenommen werden müssen. Von solchen Änderungen betroffen sind das NDG, das AIG, das BGIAA, das Verwaltungsgerichtsgesetz vom 17. Juni 2005[77] (VGG), das BPI und das LFG.

Artikel 351 Absatz 1 StGB bildet die gesetzliche Grundlage, damit das fedpol auf das Informationssystem von Interpol (I-24/7) zugreifen kann. Da die PIU eine Einheit des fedpol ist, bedarf es für deren Zugriff keiner zusätzlichen Rechtsgrundlage.

Anhang 1 Flugpassagierdaten

Unter dem *Reisestatus* (Ziff. 10) wird ausgewiesen, welche Strecken bereits abgeflogen sind und welche noch geflogen werden sollen. Anzugeben sind Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge und Flugpassagierinnen und -passagiere mit einem Flugticket, aber ohne Reservierung.

Ein *Splitting* (Ziff. 11) liegt vor, wenn Personen eine gemeinsam gebuchte Reise getrennt vornehmen. In diesem Fall müssen die entsprechenden Flugpassagierdaten nicht nochmals erhoben, sondern aufgeteilt werden.

Ein *Code-Sharing* (Ziff. 15) liegt vor, wenn ein anderes Luftverkehrsunternehmen bei dem für den Streckenflug verantwortlichen Unternehmen Sitze kauft. Bucht eine Flugpassagierin oder ein Flugpassagier einen solchen Sitz, fliegt sie/er mit den Codes beider Flugverkehrsunternehmen.

Einzelheiten zum Flugpassagierdatensatz finden sich auch in den Erläuterungen zu Artikel 1 Absatz 4.

77 SR **173.32**

Anhang 2 Deliktskatalog

Der Deliktskatalog enthält terroristische (Ziff. 1) und andere schwere Straftaten (Ziff. 2), deren Bekämpfung zur Bearbeitung von Flugpassagierdaten nach diesem Gesetz berechtigt.

Ursprünglich orientierte er sich an den Deliktskategorien der PNR-Richtlinie der EU und ordnete diesen die massgeblichen Straftatgestände zu, welche der im Rahmen von PRÜM[78] erweiterte Anhang 1 SIaG vorsieht. Obschon die Erweiterung derzeit noch nicht in Kraft ist, wird sie vorliegend berücksichtigt. Gleiches gilt für eine weitere Ergänzung des SIaG-Anhangs, die sich derzeit in Vorbereitung befindet.

Zusätzlich berücksichtigt werden neu schwere Formen des verbotenen Nachrichtendienstes. Diese Ergänzung ergibt sich aus der geänderten geopolitischen Lage.

Die folgende Tabelle weist die Straftatbestände aus, die im Nachgang zur Vernehmlassung neu im Deliktskatalog aufgenommen worden sind.

1.7	Angriffe auf die verfassungsmässige Ordnung (Art. 275 StGB)
2.1.14.1	Sexuelle Nötigung (Art. 189 Abs. 1 StGB)
2.1.14.3	Schändung (Artikel 191 StGB)
2.1.11.5	Verschwindenlassen (Art. 185bis sowie 260bis Abs. 1 Bst. f*bis* und Abs. 3 StGB)
2.2.1.1	Schwere Fälle von politischem Nachrichtendienst (Art. 272 Ziff. 2 StGB)
2.2.1.2	Schwere Fälle von wirtschaftlichem Nachrichtendienst (Art. 273 dritter Absatz StGB)
2.2.1.3	Schwere Fälle von militärischem Nachrichtendienst (Art. 274 Ziff. 1 vierter Absatz StGB)

Umgekehrt wurde der Deliktskatalog im Nachgang zur Vernehmlassung und unter Mitberücksichtigung der Ausführungen des EuGH deutlich gestrafft. Er umfasst jetzt nur noch jene Tatbestände, die:

a. für Straftaten gelten, die gemäss EuGH einen «unbestreitbar hohen Schweregrad» (Rz. 149), einen unmittelbaren Bezug zu Flugreisen (Rz. 154) oder einen grenzüberschreitenden Charakter (Rz. 155) aufweisen;

78 Bundesbeschluss über die Genehmigung und die Umsetzung des Abkommens zwischen der Schweiz und der EU zur Vertiefung der grenzüberschreitenden Zusammenarbeit (Prümer Zusammenarbeit) und des Eurodac-Protokolls zwischen der Schweiz, der EU und dem Fürstentum Liechtenstein betreffend den Zugang zu Eurodac für Gefahrenabwehr- und Strafverfolgungszwecke, BBl **2021** 2332, S. 10-16

b. nach schweizerischem Recht eine gesetzliche Mindeststrafe vorsehen, die als vom EuGH erwähnte Besonderheit des nationalen Rechts verstanden werden kann und Rückschluss auf eine besondere Schwere der Straftat zulässt (e contrario aus Rz. 151 f.).

Eine gesetzliche Mindeststrafe sehen auch die neu in den Deliktskatalog aufgenommenen Straftatbestände in Zusammenhang mit dem verbotenen Nachrichtendienst vor.

Weitere Ausführungen zu den Straftatbeständen nach Anhang 2 finden sich vorne in den Erläuterungen zu Artikel 1 Absatz 4.

Anhang 3 Änderung anderer Erlasse

1. Nachrichtendienstgesetz vom 25. September 2015[79]

Der NDB hat bei der Bekämpfung von terroristischen und anderen schweren Straftaten eine besondere Stellung. Seine Informationsbeschaffung ist der polizeilichen Ermittlung und der Strafverfolgung meistens vorgelagert und dient dem vorzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit.

Die bekanntgegebenen Flugpassagierdaten werden nach ihrem Eintreffen mit den Daten im IASA NDB und IASA-GEX NDB abgeglichen. Allfällige Übereinstimmungen werden in dem System weiterbearbeitet, dessen Daten die Übereinstimmung ausgelöst haben.

Für die Daten im IASA NDB sieht Artikel 21 der Verordnung vom 16. August 2017[80] über die Informations- und Speichersysteme des Nachrichtendienstes des Bundes (VIS-NDB) je nach Fachbereich eine Aufbewahrungsfrist von 30 bis 45 Jahren vor. Die Übereinstimmungen im IASA-GEX NDB werden spätestens nach 15 Jahre gelöscht (vgl. Art. 28 Abs. 1 VIS-NDB).

Die Flugpassagierdaten, die keine Übereinstimmungen erzielt haben, verbleiben bis zu ihrer Löschung nach einem Monat im Restdatenspeicher.

Artikel 16a Flugpassagierdaten

Der NDB ist die einzige zuständige Behörde, die von der PIU Flugpassagierdaten zur selbstständigen Bearbeitung erhält. Die Bekanntgabe der Flugpassagierdaten ist nur für jene Strecken zulässig, die der Bundesrat in einer nicht öffentlichen Liste im Voraus festgelegt hat. Der hier gewählte Wortlaut orientiert sich an Artikel 20 Absatz 4 NDG.

Bei der Bearbeitung der Flugpassagierdaten ist der NDB an die in Artikel 11 Absatz 2 E-FPG definierte Zweckbestimmung gebunden: Er darf die Flugpassagierdaten im Rahmen von Artikel 6 Absatz 1 Buchstabe a Ziffern 1–5 NDG

79 SR **121**
80 SR **121.2**

mit seinen Daten nur abgleichen und bearbeiten, sofern dies zur Verhinderung von Straftaten nach Anhang 2 E-FPG erforderlich sind (Abs. 2).

Nach Absatz 3 müssen die Daten, die beim automatischen Abgleich mit zwei Informationssystemen des NDB zu keiner Übereinstimmung geführt haben, einen Monat nach der Übermittlung an den NDB automatisch gelöscht werden.

2. Ausländer- und Integrationsgesetz vom 16. Dezember 2005[81]

Artikel 109*b* AIG bildet die gesetzliche Grundlage für das nationale Visumsystem, kurz ORBIS. Es liefert Angaben zu Visumsgesuchen und weist alle Personen aus, die über ein Visum für den Schengen-Raum verfügen. Eine Person kann anhand der überprüfbaren Passnummer identifiziert werden.

Art 109c Bst. i Abfrage des nationalen Visumsystems

Damit wird die PIU berechtigt, zur Abklärung der Identität von Flugpassagierinnen und -passagieren auf die im ORBIS gespeicherten Daten zuzugreifen (vgl. Art. 6 Absatz 3 Bst. b E-FPG).

3. Bundesgesetz vom 20. Juni 2003[82] über das Informationssystem für den Ausländer- und den Asylbereich

Das BGIAA regelt das Informationssystem, das im Ausländer- und Asylbereich eingesetzt wird, kurz ZEMIS. Das ZEMIS enthält Personendaten von Ausländerinnen und Ausländern in der Schweiz (z. B. Name, Vorname, Geburtsdatum) und deren Aufenthaltsstatus. Über das ZEMIS abrufbar sind neu auch die Daten, aus dem Informationssystem zur Ausstellung von schweizerischen Reisedokumenten und Bewilligungen zur Wiedereinreise an Ausländerinnen und Ausländer. Damit lassen sich über das ZEMIS auch Angaben aus Reisedokumenten wie Name, Heimatort von in der Schweiz registrierten Ausländerinnen und Ausländern mit einem von der Schweiz ausgestellten Reisedokument (z. B. Flüchtlingsreisepass) abrufen.

Art. 9 Abs. 1 Bst. q

Damit wird die PIU berechtigt, zur Abklärung der Identität von Flugpassagierinnen und -passagieren auf die im ZEMIS gespeicherten Daten zuzugreifen (vgl. Art. 6 Absatz 3 Bst. b E-FPG).

4. Verwaltungsgerichtsgesetz vom 17. Juni 2005[83]

81 SR **142.20**
82 SR **142.51**
83 SR **173.32**

Nach den Artikeln 19 und 20 E-FPG entscheidet das Bundesverwaltungsgericht über die Aufhebung der Pseudonymisierung. Dies bedingt die beantragten Änderungen.

5. Bundesgesetz vom 13. Juni 2008[84] über die polizeilichen Informationssysteme des Bundes

Das BPI enthält die gesetzlichen Grundlagen für die polizeilichen Informationssysteme, mit deren Daten die Flugpassagierdaten automatisch abgeglichen werden (vgl. Art. 6 Abs. 1 Bst. a). Zudem muss die PIU auf die Daten der einzelnen polizeilichen Informationssysteme manuell zugreifen können, um die Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck prüfen zu können (vgl. Art. 6 Abs. 3 Bst. a).

Der manuelle Zugriff der PIU auf das Geschäfts- und Aktenverwaltungssystem nach Artikel 18 BPI, um die Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck prüfen zu können (vgl. Art. 6 Abs. 3 Bst. a), muss nicht explizit vorgesehen werden, da Artikel 18 Absatz 7 den Zugriff der Mitarbeitenden des fedpol bereits vorsieht.

Zur Überprüfung der Identität muss die PIU zusätzlich auf das RIPOL und auf das N-SIS zugreifen können (vgl. Art. 6 Abs. 3 Bst. b).

Art. 10 Abs. 4 Bst. a^{bis} *System zur Unterstützung gerichtspolizeilicher Ermittlungen des Bundes*

Art. 11 Abs. 5 Bst. b^{bis} *System Bundesdelikte*

Diese beiden Änderungen berechtigen die PIU zum manuellen Zugriff auf die Daten im nationalen Ermittlungssystem, kurz NES, zur Überprüfung der Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck nach Artikel 6 Absatz 3 Buchstabe a.

Art. 12 Abs. 6 Bst. b^{bis} *System internationale und interkantonale Polizeikooperation*

Diese Änderung berechtigt die PIU zum manuellen Zugriff auf das System internationale und interkantonale Polizeikooperation, kurz IPAS, zur Überprüfung der Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck nach Artikel 6 Absatz 3 Buchstabe a.

Art. 15 Abs. 4 Bst. a^{bis} *Automatisiertes Polizeifahndungssystem*

Diese Änderung berechtigt die PIU zum automatischen Abgleich der Flugpassagierdaten mit den Daten des Automatisierten Polizeifahndungssystems, kurz RIPOL, nach Artikel 6 Absatz 1 Buchstabe a E-FPG und zum manuellen

84 SR **361**

Zugriff zur Überprüfung der Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck nach Artikel 6 Absatz 3 Buchstabe a E-FPG.

Art. 16 Abs. 2 Bst. k^bis *Nationaler Teil des Schengener Informationssystems*

Diese Änderung berechtigt die PIU zum automatischen Abgleich der Flugpassagierdaten mit den Daten des Nationalen Teil des Schengener Informationssystems, kurz N-SIS, nach Artikel 6 Absatz 1 Buchstabe a E-FPG und zum manuellen Zugriff zur Überprüfung der Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck nach Artikel 6 Absatz 3 Buchstabe a E-FPG.

Art. 17 Abs. 4 Bst. a^bis *Nationaler Polizeiindex*

Diese Änderung berechtigt die PIU zum manuellen Zugriff auf den nationalen Polizeiindex zur Überprüfung der Vereinbarkeit von automatisch erzielten Übereinstimmungen mit dem gesetzlichen Zweck nach Artikel 6 Absatz 3 Buchstabe a E-FPG.

6. Luftfahrtgesetz vom 21. Dezember 1948[85]

Art. 29 Abs. 5

Luftverkehrsunternehmen sollen nicht unbehelligt in der Schweiz starten und landen können, wenn sie wiederholt erfolglos aufgefordert worden sind, Sanktionen nach Artikel 31 des vorliegenden Gesetzes zu bezahlen.

Eine Betreibung ist insbesondere dort nicht möglich, wo ein ausländisches Luftverkehrsunternehmen über keinen Sitz in der Schweiz verfügt und wo auch die Voraussetzungen einer Betreibung an einem allfälligen Spezialdomizil nicht gegeben sind (Art. 50 des Bundesgesetzes vom 11. April 1889[86] über Schuldbetreibung und Konkurs [SchKG]).

Diese Regelung soll nicht nur im Fall von Sanktionen nach dem Flugpassagierdatengesetz gelten, sondern auch für solche nach dem AIG, das in den Artikeln 122*a* und 122*b* eine sinngemässe Regelung für die Sanktionierung der Luftverkehrsunternehmen vorsieht.

Voraussetzungen für den Entzug der Betriebsbewilligung sind in diesen beiden Fällen:

- eine Sanktion nach Artikel 31 E-FPG oder nach den Artikeln 122*a* und 122*b* AIG ist in Rechtskraft erwachsen;

85 SR **748.0**
86 SR **281.1**

- die Bezahlung der Sanktion wurde wiederholt eingefordert, ohne dass dies erfolgreich war.

Ein Entzug der Betriebsbewilligung soll als ultima ratio, nicht jedoch ohne Abwägung aller weiteren, nicht direkt mit den ausstehenden Zahlungen zusammenhängenden Umstände erfolgen. Deshalb wird von einer gesetzlichen Pflicht zum Entzug der Betriebsbewilligung abgesehen.

6 Auswirkungen

6.1 Auswirkungen auf den Bund

Die Verwendung von PNR bedingt ein Informationssystem sowie den Aufbau der zuständigen Einheit (PIU) bei fedpol.

PNR-Informationssystem

In der Schweiz soll das bereits in verschiedenen Staaten im Einsatz stehende «goTravel» der UNO zum Zuge kommen.

«goTravel» ist eine Weiterentwicklung von «TRIP», das die Niederlande als PNR-Informationssystems entwickelt und anschliessend der UNO zur Verfügung gestellt haben.

Seit mehreren Jahren stellt nun die UNO «goTravel» Mitgliedstaaten zur Verfügung und unterstützt sie bei der Verwendung von PNR im Rahmen des *UN Countering Terrorist Travel Programm*. In Europa stehen «TRIP» in Belgien und «goTravel» in Luxemburg und seit 2022 in Norwegen im Einsatz.

«goTravel» erfährt mit seiner Nutzung in verschiedenen Staaten eine laufende Weiterentwicklung, welche die UNO den anderen Staaten zugänglich macht, die dieses Informationssystem für PNR nutzen.

Allerdings bedingt der Einsatz von «goTravel» in der Schweiz technische Anpassungen. Sie werden von der Schweiz initiiert und von der UNO umgesetzt.

Erst danach wird die auf den hiesigen Einsatz ausgerichtete Version von «goTravel» in die IT-Umgebung des ISC-EJPD integriert und durch das ISC-EJPD und das fedpol auf Funktionalität und Sicherheit überprüft.

In den Tests gelangen keine produktiven, sondern lediglich sogenannte «synthetische» Daten zur Anwendung. Als solche werden Daten bezeichnet, die künstlich erstellt werden. Alle Tests werden intern durchgeführt, ohne dass Testdaten die Testumgebung und damit das ISC-EJPD verlassen. Nach erfolgreicher Prüfung wird «goTravel» sodann zum produktiven Einsatz freigegeben.

Bei dieser Zusammenarbeit gelangt die UNO nie in den Besitz von PNR-Daten oder von Ergebnissen ihrer Bearbeitung aus der Schweiz. Diese Daten werden in der Schweiz bzw. ausschliesslich in der IT-Umgebung des ISC-

EJPD gespeichert, soweit sie nicht einer gesetzlich als zuständig definierten Behörde bekanntgegeben werden (vgl. Art. 7–11 sowie Art. 30).

Die technische Projektabwicklung ist auch beim fedpol nicht ohne die Unterstützung durch externe Dienstleister realisierbar. In technischen Belangen kommen vorliegend nur Dienstleister zum Einsatz, die den Zuschlag hauptsächlich im Rahmen der WTO-Ausschreibung Alpin.2.0 erhalten haben. Alpin 2.0 sichert für die gesamte Bundesverwaltung einen Pool an Projektdienstleistungen für IKT-Schlüsselprojekte, IKT-Grossprojekte oder komplexe und strategische Vorhaben. Die konkreten Aufträge werden unter den Zuschlagsempfängern in einem elektronischen Mini-Tender-Verfahren (Wettbewerb) vergeben. Alle zum Einsatz gelangenden Dienstleister müssen im Übrigen die erweiterte Personensicherheitsprüfung des Bundes erfolgreich absolvieren.

Der Betrieb und die Wartung der von der Schweiz verwendeten Version von «goTravel» liegen in der Verantwortung des ISC-EJPD. Dafür werden keine externen Dienstleister beigezogen.

Zum Datenschutz, der mittels technischer Vorkehrungen und organisatorischen Massnahmen sicherzustellen ist, siehe Ziffer 7.7.

Kosten

Die Projekt- und Betriebskosten des PNR-Informationssystems sowie die Betriebskosten der PIU werden vollumfänglich vom Bund getragen. Das Personal der PIU setzt sich je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammen. Für einen Vollbetrieb der PIU (24 Stunden / 7 Tage) ist mit 30 Vollzeitstellen zu rechnen. Es wird allerdings ein etappenweiser Aufbau vorgesehen, um Erfahrungen mit der Nutzung von PNR-Daten zu sammeln. Für eine Anfangsphase wird deshalb von einem tieferen Personalbestand ausgegangen, mit dem Basisleistungen der PIU ermöglicht werden.

a) Projektkosten

Im Rahmen des Projekts «PNR Schweiz» schafft das fedpol die rechtlichen, technischen und organisatorischen Voraussetzungen für die Bearbeitung der Flugpassagierdaten.

In der Initialisierungsphase des Projekts wurde geprüft, ob das PNR-Informationssystem auf dem Markt beschafft oder im ISC-EJPD selber entwickelt werden soll. Da die Eigenentwicklung als sehr aufwendig und teuer eingeschätzt wird, wurde entschieden, das von der UNO angebotene PNR-Informationssystem «goTravel» in einem «Proof of Concept» (PoC) auf die Erfüllung der Anforderungen und Integrierbarkeit in die IT-Landschaft des ISC-EJPD hin zu evaluieren. Im Juli 2022 entschied sich die PNR-Projektauftraggeberschaft für «goTravel».

Lässt sich «goTravel» in der Schweiz ohne grosse Anpassungen implementieren, belaufen sich die Projektkosten 2020–2026 auf ca. 11,5 Millionen Franken (davon 6,82 Mio. Fr. finanzierungswirksam). Diese Kosten sind im Detail wie folgt budgetiert:

	Projektkosten 2020–2026 ***(in Mio. Fr.)***
Kosten aus externen Dienstleistungen und Vereinbarungen mit dem Leistungserbringer ISC-EJPD	6,82
Fedpol-interne Personalkosten	4,69
Gesamtkosten	**11,51**

Derzeit wird in einem zweiten, umfangreicheren «PoC» vertieft geprüft, wie sich die neuen gesetzlichen Anforderungen der Schweiz im «goTravel» technisch umsetzen lassen. Allenfalls notwendige, finanziell erhebliche Anpassungen und Weiterentwicklungen wären jedoch erst im Rahmen einer Weiterentwicklung ab 2026 umzusetzen.

b) Betriebskosten PNR-Informationssystem und PIU ab 2026 (exklusiv Personalkosten)

Für den Betrieb des PNR-Informationssystems und für die Instandhaltung der IKT-Struktur (Hardware, Software, Netzwerk etc.) beim Leistungserbringer ISC-EJPD ab Aufnahme des operativen Betriebs im Jahr 2026 muss mit jährlichen Kosten von maximal 1,65 Mio. Franken gerechnet werden. Einkalkuliert sind dabei:

- Serverinfrastruktur für den Betrieb von «goTravel» und aller notwendigen Softwarekomponenten sowie die Speicherung der PNR Daten;
- die Speicherung der Protokolle (vgl. Art. 24).

Derzeit klärt das EJPD am Markt ab, mit welchen Kosten für die Beschaffung und den Betrieb des Datengateways für die Übermittlung der Passagierdaten von den Luftverkehrsunternehmen an das PNR-System zu rechnen ist. Ebenfalls in Abklärung begriffen ist die Schaffung von Synergien mit dem Staatssekretariat für Migration, das künftig den gleichen Datengateway zum Erhalt der API-Daten nutzen könnte.

Gemäss aktueller Planung wird die PIU in Bern am fedpol-Hauptsitz eingerichtet werden. Die Räumlichkeiten sind dort bereits vorhanden, daher ist nicht mit erheblichen Mehrkosten zu rechnen. Weitere Kosten fallen pro Arbeitsplatz gemäss dem in der Bundesverwaltung üblichen Ansatz an.

Die konkreten Infrastruktur- und Betriebskosten werden im weiteren Verlauf des Projekts vertieft.

c) Personalkosten

Der Personalbedarf der PIU hängt von ihren Betriebszeiten, der Zahl der angebundenen Flugstrecken und der zu bearbeitenden Datenmenge ab. Geplant ist ein etappenweiser Aufbau. In einer ersten Phase sollen mit Basisleistungen die Nutzung von PNR-Daten ermöglicht und Erfahrungen gesammelt werden. Dafür soll mit einem tieferen Personalbedarf gestartet werden. Damit wird ein eingeschränkter Betrieb der PIU möglich sein (bzl. Betriebszeiten und Leistungsumfang). Für einen Vollbetrieb der PIU (7 Tage / 24 Stunden und voller Leistungsumfang) wären voraussichtlich 30 Vollzeitstellen notwendig.

Bundesseitig stellen das EJDP (fedpol) und das EFD (BAZG) Mitarbeitende. Das BAZG hat sich im Umfang von ein bis zwei Vollzeitstellen zur Mitarbeit in der PIU bereiterklärt, solange es an den Flughäfen Basel und Genf eine delegierte Rolle bei der Personenkontrolle wahrnimmt. Im Gegensatz zu den Mitarbeitenden des BAZG sind jene des fedpol dauerhaft in der PIU tätig und gewährleisten damit die Kontinuität der Arbeit in der PIU und das «operative Gedächtnis» dieser Organisationseinheit. Dazu gehören unter anderem die PIU-Leitung sowie die verantwortlichen Personen für die Betreuung der Fluggesellschaften und die Vertretung der PIU in internationalen Gremien.

6.2 Auswirkungen auf Kantone und Gemeinden, insbesondere auch auf Städte, Agglomerationen und Bergebiete

Viele Straftatbestände, die künftig auch mittels PNR bekämpft werden sollen, fallen in die Strafverfolgungskompetenz der Kantone. Mit PNR gelangen die Polizei- und Strafverfolgungsbehörden der Kantone einfacher, schneller und gezielter an Informationen aus dem Flugverkehr, die für ihre Aufgabenerfüllung relevant sind.

Mit PNR erhalten die kantonalen Strafverfolgungsbehörden Informationen über national oder international gesuchte Personen, die die Schweiz anfliegen oder die sich unmittelbar vor der Ausreise aus der Schweiz befinden. Damit

können die Kantone – allenfalls im Verbund mit anderen Behörden – zeitgerecht die nötigen Massnahmen treffen. Zudem erspart die Verwendung von PNR den Kantonen zeitaufwendige Nachfragen bei Luftverkehrsunternehmen, wenn es darum geht, zu kriminellen Zwecken genutzte Reisewege nachzuverfolgen. Auch nützliche Hinweise auf bisher ungeklärte Straftaten sind mit der Nutzung von PNR zu erwarten.

Wie die Erfahrungen aus dem Ausland zeigen, leisten PNR – und damit künftig das Flugpassagierdatengesetz – einen wichtigen Beitrag zur Steigerung von Effizienz und Effektivität in der Verbrechensprävention und Strafverfolgung. Davon werden die Kantone massgeblich profitieren.

Weil ein Grossteil der aufgrund von PNR zu treffenden Massnahmen bei der Einreise von Personen am Flughafen erfolgt, ist davon auszugehen, dass die Bearbeitung von Flugpassagierdaten für Kantone mit einem internationalen Flughafen tendenziell einen grösseren Aufwand verursachen wird als für die übrigen Kantone. Diesen Umständen ist Rechnung zu tragen.

Personalkosten

Bund und Kantone stellen je zur Hälfte die PIU-Mitarbeitenden und tragen jeweils deren Kosten. Einzelheiten werden Bund und Kantone in einer Vereinbarung festlegen. Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren sowie die Konferenz der Kantonalen Polizeikommandanten der Schweiz haben sich in der Vernehmlassung zustimmend zur personellen Beteiligung der Kantone an der PIU geäussert. Eine entsprechende Vereinbarung wird derzeit mit den Kantonen erarbeitet.

Die entsandten Mitarbeitenden der Kantone werden befristet bei der PIU im Einsatz stehen. Vorrangig werden sie dabei Aufgaben im Kerngeschäft der PIU wahrnehmen. Dazu gehören die Überwachung der Datenbekanntgabe durch die Luftverkehrsunternehmen bzw. des Dateneingangs bei der PIU sowie die Überprüfung der Treffer im Nachgang zum automatischen Abgleich der Flugpassagierdaten mit den Informationssystemen, den Risikoprofilen und Beobachtungslisten. Dieses Vorgehen stellt den Wissenstransfer vom Bund zu den Kantonen sicher und ermöglicht diesen einen maximalen Nutzen aus PNR.

Sinnvollerweise sollten die Kantone mindestens eine Ansprechperson für die PIU bestimmen. Wünschbar wäre, wenn sie auch Spezialisten ausbilden, welche über das nötige Wissen verfügen, um zielführend Anträge an die PIU stellen zu können und mit dieser fallbezogen eng zusammenarbeiten können.

Das Flugpassagierdatengesetz hat keine direkten Auswirkungen auf Gemeinden und Berggebiete.

6.3 Auswirkungen auf die Volkswirtschaft

Mit dem vorliegenden Gesetz kommen grundsätzlich keine neuen administrativen Aufgaben auf die Luftverkehrsunternehmen zu. Denn die Flugpassagierdaten werden unabhängig von diesem Gesetz bei der Buchung von Flugtickets erhoben. Zudem werden PNR bereits heute von 69 Staaten genutzt. Für die Luftverkehrsunternehmen, die zur Datenbekanntgabe an die zuständigen staatlichen Stellen verpflichtet sind, stellt somit auch diese Aufgabe kein Novum mehr dar.

Die Vorlage bezweckt in der Hauptsache eine Erhöhung der Sicherheit.

Ein sicheres gesellschaftliches Umfeld ist eine zentrale Voraussetzung für den Erhalt und die Stärkung des Wirtschaftsstandorts Schweiz. Dies zeigte sich auch in einzelnen Stellungnahmen, die zwischen dem 13. April und dem 31. Juli 2022 im Rahmen der Vernehmlassung eingegangen sind.

Dabei gilt es auch zu berücksichtigen, dass die Bekanntgabe von PNR-Daten durch die Luftverkehrsunternehmen zunehmend zu einer Bedingung für den Anflug gewisser Destinationen erklärt wird. Sollte die Schweiz auf das Flugpassagierdatengesetz und damit auf PNR verzichten, könnten die Schweizer Luftverkehrsunternehmen zunehmend benachteiligt werden und die Schweiz könnte ihre bisher ausgezeichnete internationale Anbindung im Luftverkehr verlieren. Aus volkswirtschaftlicher Sicht ist dies unbedingt zu verhindern.

Die USA haben die Verwendung von PNR zudem zur Bedingung für einen Verbleib in ihrem VWP erklärt. Aufgrund des VWP können sich Schweizerinnen und Schweizer in den USA bis zu 90 Tage ohne Visum zu touristischen oder geschäftlichen Zwecken aufhalten. Ein Ausschluss der Schweiz aus diesem Programm könnte sich auch negativ auf einzelne Bereiche der Schweizer Volkswirtschaft auswirken.

6.4 Auswirkungen auf die Gesellschaft

Allgemeines

Schwerstkriminalität destabilisiert eine Gesellschaft und untergräbt das Vertrauen in den Rechtsstaat. Instrumente, die zur Bekämpfung solcher Verbrechen eingesetzt werden können, sind eine entscheidende Voraussetzung für die Wahrung der öffentlichen Sicherheit und eine positive, gesellschaftliche Entwicklung.

Die Berücksichtigung der datenschutzrechtlichen Vorgaben stellt im Übrigen sicher, dass Personendaten rechtmässig und unter Wahrung der Verhältnismässigkeit bearbeitet werden. Zudem haben Betroffene das Recht, über die Datenbearbeitung informiert zu werden und deren Rechtmässigkeit allenfalls überprüfen zu lassen.

Opfer von Schwerstkriminalität sind auch Kinder. Sie benötigen besonderen Schutz. Erfahrungen anderer Staaten zeigen, dass sich PNR wirksam zu ihrem

Schutz vor der organisierten Kriminalität (z. B. Menschenhandel) oder Pädophilie einsetzen lässt.

Exkurs: Kinder und PNR

Kinder sind im Normalfall mit ihren Eltern oder einem Elternteil unterwegs, insbesondere im Luftverkehr. In diesem Fall sind sie bis zu ihrem 12. Lebensjahr und unter Angabe ihres Geburtstags als Mitreisende im Flugpassagierdatensatz ihrer Eltern oder ihres Elternteils ausgewiesen. Buchen die Eltern das Kind jedoch separat, was bei Kindern ab fünf Jahren zulässig ist, verfügt es auch über einen eigenen Flugpassagierdatensatz. Ab 12 Jahren gelten die Kinder im Luftverkehr als erwachsen und verfügen immer über einen eigenen Flugpassagierdatensatz.

Daneben gibt es aber auch Kinder, die alleine fliegen. Bei der SWISS und der Lufthansa ist dies ab einem Alter von fünf Jahren zulässig, wobei zwingend ein vom Luftverkehrsunternehmen angebotener Betreuungsdienst in Anspruch zu nehmen ist, der das Kind während des ganzen Fluges begleitet. Allein die Lufthansa verzeichnet jährlich rund 70 000 Kinder, die diesen Dienst beanspruchen.

In diesem Fall weist Kategorie 12 des Flugpassagierdatensatzes aus:

- Name und Geschlecht, Alter, Sprachen des unbegleiteten Kindes oder Jugendlichen unter 18 Jahren;
- Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht;
- Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu der oder dem Minderjährigen steht;
- Name und Kontaktdaten der begleitenden Flughafenmitarbeiterin oder des begleitenden Flughafenmitarbeiters bei Abflug und Ankunft.

7 Rechtliche Aspekte

7.1 Verfassungsmässigkeit

Das Flugpassagierdatengesetz unterstellt die Luftverkehrsunternehmen neuen Pflichten. Die BV weist die Kompetenz zum Erlass gesetzlicher Bestimmungen, die den Luftverkehr betreffen, dem Bund zu (vgl. Art. 87 BV).

Das Flugpassagierdatengesetz liefert die gesetzliche Grundlage für den Betrieb eines zentralen Informationssystems, das wichtige Informationen bereitstellt, welche die zuständigen Behörden von Bund und Kantonen bei der Erfüllung ihrer Sicherheitsaufgaben, namentlich der Bekämpfung terroristischer

und anderer schwerer Straftaten, unterstützen. Es handelt sich dabei um Sicherheitsaufgaben, welche die StPO gestützt auf Artikel 123 Absatz 1 BV teilweise dem Bund zuweist (Bekämpfung terroristischer Straftaten sowie anderer schwerer Straftaten, die der Bundesgerichtsbarkeit unterstehen). Diese vorbestehenden Kompetenzen des Bundes sind nicht von marginaler Bedeutung und die vom Flugpassagierdatengesetz geregelten Sicherheitsbelange bedürfen aus Sicht des Bundes einer Koordination unter Leitung des Bundes. Das Flugpassagierdatengesetz kann sich deshalb auch auf Artikel 57 Absatz 2 BV abstützen.[87]

7.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Mit der Errichtung der PIU und der Regelung der Bearbeitung von Flugpassagierdaten setzt die Schweiz als UNO-Mitglied die bindenden Resolutionen des UNO-Sicherheitsrats zur Nutzung von Flugpassagierdaten um (siehe Fussnote 1). Gleichzeitig setzt die Schweiz auch die Standards der ICAO für die Schweizer Luftfahrt um und gewährleistet den Verbleib der Schweiz im VWP der USA. Dieser wichtige Status ist zurzeit nur provisorischer Natur (vgl. Ziff. 1.1).

Der Vorentwurf des Flugpassagierdatengesetzes lehnte sich eng an die PNR-Richtlinie der EU an, ohne dass dazu allerdings eine Pflicht bestand. Im Zuge des EuGH-Urteils erfuhr die PNR-Richtlinie eine teilweise neue Auslegung. Das EuGH-Urteil entfaltet für die Schweiz keine bindende Wirkung. Dennoch sind zentrale Punkte dieses Urteils nun im vorliegenden Entwurf berücksichtigt, namentlich die auf sechs Monate verkürzte Aufbewahrungsfrist für Daten, die keine Anhaltspunkte für Schwerstkriminalität aufweisen, und die Beschränkung des Deliktkatalogs auf Schwerstkriminalität.

Der vorliegende Gesetzesentwurf basiert auf dem Ergebnis der Vernehmlassung und berücksichtigt wichtige Elemente des EuGH-Urteils, sofern sich auch Stellungnahmen in der Vernehmlassung darauf beriefen und die Wirksamkeit und Effizienz der Verwendung von PNR nicht grundlegend in Frage gestellt war.

Nicht vom Gesetzesentwurf betroffen ist das Abkommen vom 21. Juni 1999[88] zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr.

[87] Bericht des Bundesrates in Erfüllung des Postulats Malama 10.3045 vom 3. März 2010. Innere Sicherheit. Klärung der Kompetenzen, BBl **2012** 4459 S. 4486.
[88] SR **0.748.127.192.68**

7.3 Erlassform

Das Erfordernis eines Bundesgesetzes lässt sich hauptsächlich mit der neuen Aufgabe begründen, die der Bund mit der Umsetzung des Flugpassagierdatengesetzes übernimmt (Art. 164 Abs. 1 Bst. e BV).

Zudem kann die Datenbearbeitung das verfassungsmässige Recht auf den Schutz der Privatsphäre von Flugpassagierinnen und -passagieren tangieren, was nur auf der Grundlage eines formellen Gesetzes zulässig ist (Art. 164 Abs. 1 Bst. b BV).

Die Notwendigkeit, die Bearbeitung der Flugpassagierdaten in einem Gesetz im formellen Sinne zu regeln, ergibt sich schliesslich auch aus dem DSG.

7.4 Unterstellung unter die Ausgabenbremse

Mit der Vorlage werden weder neue Subventionsbestimmungen geschaffen, noch neue Verpflichtungskredite oder Zahlungsrahmen beschlossen. Die Vorlage ist somit nicht der Ausgabenbremse (vgl. Art. 159 Abs. 3 Bst. b BV) unterstellt.

7.5 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Subsidiarität

Vorliegend soll der Bund eine neue Aufgabe übernehmen: die Bearbeitung von Flugpassagierdaten, um sie den zuständigen Behörden von Bund und Kantonen zur Bekämpfung von Schwerstkriminalität bekanntzugeben.

Das Prinzip der Subsidiarität (vgl. Art. 5a BV) verlangt nach einer Rechtfertigung, wenn der Bund eine Aufgabe übernehmen soll.

Dafür, dass die Bearbeitung von Flugpassagierdaten beim Bund angesiedelt werden soll, spricht einerseits der internationale Bezug der Aufgabe:

- Sie setzt mehrere internationale Verpflichtungen um, welche die Schweiz eingegangen ist (vgl. Ziff. 1.1).
- Die USA machen den Verbleib der Schweiz im VWP abhängig von einer möglichst baldigen Umsetzung der Nutzung von PNR.
- Der Austausch von Flugpassagierdaten mit dem Ausland bedingt zur Wahrung der Gegenseitigkeit mit allen Staaten und zur Gewährleistung eines geeigneten Datenschutzes mit vielen Staaten völkerrechtliche Verträge. Zuständig für solche Abkommen ist der Bund.

Auch die verfassungsmässige Zuständigkeit des Bundes, gesetzlich den Luftverkehr zu regeln, spricht für die Ansiedelung der neuen Aufgabe beim Bund (vgl. Art. 87 BV). Denn die Verwendung von PNR bedingt, dass die PIU über Daten verfügt, die ihr von den Luftverkehrsunternehmen bekanntgegeben

werden. Das vorliegende Gesetz verpflichtet die Luftverkehrsunternehmen nicht nur zur Bekanntgabe dieser Daten, sondern sieht auch Sanktionen vor, wenn die Daten nicht rechtzeitig oder unvollständig bei der PIU eintreffen. Über die entsprechende Regelungskompetenz verfügt ausschliesslich der Bund.

Fiskalische Äquivalenz

Die fiskalische Äquivalenz leitet sich aus Artikel 43*a* BV ab. Sie besagt, dass Nutzniessung, Kosten und Entscheidkompetenz in einem ausgewogenen Verhältnis stehen.

Die PIU, die für die Bearbeitung der Flugpassagierdaten zuständig ist, lässt sich als eine Dienstleisterin verstehen. Sie stellt die Ergebnisse ihrer Bearbeitung von Flugpassagierdaten sowohl Behörden des Bundes wie der Kantone zur Verfügung. Nutzniesser dieser neuen Aufgabe sind somit sowohl der Bund wie auch die Kantone.

Da den Kantonen verfassungsrechtlich die Hauptverantwortung bei der inneren Sicherheit und insbesondere im polizeilichen Bereich zukommt, darf davon ausgegangen werden, dass die Kantone massgeblich vom Nutzen aus PNR profitieren. Daran ändert auch der im Nachgang zur Vernehmlassung reduzierte Deliktskatalog nicht grundsätzlich etwas. Gestrichen worden sind nämlich vor allem Tatbestände aus dem Nebenstrafrecht des Bundes. Davon sind die Kantone nur am Rande betroffen. Vor diesem Hintergrund rechtfertigt es sich, dass die Hälfte der PIU-Mitarbeitenden von den Kantonen gestellt und finanziert werden.

Die andere Hälfte der Mitarbeitenden stellt und finanziert der Bund. Darüber hinaus trägt er die Kosten des Projekts und der nötigen Infrastruktur sowie die Kosten für den übrigen Betrieb der PIU.

Insgesamt tragen die Kantone damit deutlich weniger als die Hälfte der Kosten, die in Zusammenhang mit dem Aufbau eines PNR-Systems in der Schweiz anfallen.

In der Vernehmlassung verlangten mehrere Kantone die volle Kostentragung durch den Bund. Dies steht indes in klarem Widerspruch zur verfassungsrechtlich verbindlich vorgeschriebenen fiskalischen Äquivalenz. Deshalb kann auf die Forderung dieser Kantone nicht eingegangen werden.

7.6 Delegation von Rechtsetzungsbefugnissen

Artikel 2 Absatz 4 räumt dem Bundesrat die Kompetenz ein, auf Verordnungsebene die für die Luftverkehrsunternehmen bei der Bekanntgabe der Flugpassagierdaten an die PIU zu beachtenden technischen Anforderungen zu regeln. Er orientiert sich dabei an internationalen Standards der ICAO, der WZO und der IATA, die es nötigenfalls auch zu konkretisieren gilt.

Artikel 7 Absatz 4 räumt dem Bundesrat die Kompetenz ein, die Einzelheiten einer sicheren Datenbekanntgabe zwischen der PIU und den zuständigen Behörden zu regeln. Dazu gehört nicht nur die Art und Weise der Bekanntgabe. Zu klären ist auch die Frage, ob sich der Datenaustausch mit den einzelnen Behörden standardisiert über jeweilige *Single Points of Contact* abwickeln lässt. Im Falle der Polizeikorps von Bund und Kantonen könnte dies beispielsweise die jeweilige Einsatz- und Alarmzentrale sein.

Artikel 15 Absatz 2 räumt dem Bundesrat die Kompetenz ein, Einzelheiten der Überprüfung von Risikoprofilen und Beobachtungslisten festzulegen. Zudem soll er die Berichterstattung regeln.

Artikel 29 Absatz 1 räumt dem Bundesrat die Kompetenz ein, selbstständig völkerrechtliche Verträge über die Bearbeitung von Flugpassagierdaten abzuschliessen. Als mögliche Vertragspartner kommen nur Staaten und internationale Organisationen (EU) in Frage, die einen angemessenen oder mittels spezifischer vertraglicher Bestimmungen einen geeigneten Schutz der aus der Schweiz stammenden Daten gewährleisten können. Die Verträge sollen zudem die Gegenseitigkeit der Datenbekanntgabe sicherstellen.

7.7 Datenschutz

Das Flugpassagierdatengesetz orientiert sich vollständig am neuen Datenschutzgesetz, das am 1. September 2023 in Kraft getreten ist. Dies ist umso wichtiger, als der Datenschutz bei der Datenbearbeitung nach dem vorliegenden Gesetz zentral ist. Dies zeigte sich auch in der Vernehmlassung, die in der ersten Hälfte 2022 durchgeführt worden ist. Verschiedene der eingegangenen Stellungnahmen orientieren sich am EuGH-Urteil. Der Gesetzesentwurf berücksichtigt Kerninhalte dieses Urteils, auch wenn es die Schweiz nicht bindet. So sieht es insbesondere die auf sechs Monate verkürzte Speicherfrist für Daten vor, die keine Anhaltspunkte für Schwerstkriminalität aufweisen, sowie die Reduktion des Deliktskatalogs auf tatsächliche Schwerstkriminalität. Nicht berücksichtigt wurden demgegenüber Inhalte des EuGH-Urteils, welche die Effizienz und Effektivität von PNR empfindlich geschmälert hätten.

Personendaten

Der Flugpassagierdatensatz setzt sich aus verschiedenen Kategorien von Daten zusammen. Für den Datenschutz relevant sind einzig die Personendaten (Art. 2 Abs. 1 Bst. b DSG). Es sind dies jene Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 Bst. a DSG). Der Flugpassagierdatensatz enthält solche Daten in den Kategorien 4–6, 8–9, 12, 17 und 18; Kategorie 19 *kann* Personendaten enthalten (vgl. Anhang 1 E-FPG). Zu den Personendaten gehören unter anderem der Name, die Telefonnummer, die Wohn- und die E-Mailadresse einer Flugpassagierin oder eines Flugpassagiers.

Flugpassagierdaten, die keine Anhaltspunkte auf eine Straftat nach Anhang 2 geben und deshalb nicht markiert sind, werden einen Monat nach ihrem Eingang im PNR-Informationssystem automatisch pseudonymisiert (vgl. Art. 18). Mit der Pseudonymisierung lassen sich die Daten nicht mehr einer bestimmten Person zuordnen und verlieren damit ihren Status als Personendaten. Anders als die Anonymisierung, aufgrund der die Daten unwiderruflich ihren Status als Personendaten verlieren, lässt sich die Pseudonymisierung rückgängig machen (vgl. Art. 19 und 20). Das Bundesverwaltungsgericht muss diesen Bearbeitungsschritt genehmigen. Technisch ist vorgesehen, dass nur autorisierte Personen unter Verweis auf das fragliche Urteil diesen Entscheid vollziehen können.

In der Botschaft vom 15. September 2017[89] zum neuen Datenschutzgesetz streicht der Bundesrat hervor, dass die Pseudonymisierung als eine geeignete technische Massnahme gilt, um die Sicherheit von Daten zu gewährleisten (vgl. Art. 8 DSG). Zudem gelte das Datenschutzgesetz *nicht* für Daten, «wenn eine Reidentifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre. Das gilt ebenfalls für pseudonymisierte Daten.»[90]

Besonders schützenswerte Personendaten

Das Gesetz erlaubt nur die Bearbeitung der in Artikel 5 Absatz 2 aufgeführten besonders schützenswerten Daten. In den Besitz solcher Daten gelangt die PIU allenfalls bei der manuellen Überprüfung der mit dem automatischen Abgleich erzielten Übereinstimmungen (vgl. Art. 6 Abs. 3 E-FPG).

Der Gesetzesentwurf berücksichtig die Vorbehalte des EuGH hinsichtlich der Umschreibung einzelner Datenkategorien (vgl. Anhang 1 E-FPG).[91] Damit ist die Möglichkeit gesetzlich ausgeschlossen, dass die PIU über die Flugpassagierdaten in den Besitz von besonders schützenswerten Personendaten gelangt. Dennoch hält Artikel 22 Buchstabe a vorsorglich fest, dass die PIU alle besonders schützenswerten Daten, die nicht in Artikel 5 Absatz 2 genannt sind, umgehend löschen muss.

Aufbewahrungsdauer

Der Gesetzesentwurf sieht vor, dass Daten ohne Markierung nach Ablauf von sechs Monaten automatisch gelöscht werden (vgl. Art. 21 Abs. 1). Damit entspricht das Flugpassagierdatengesetz dem EuGH-Urteil. Der EuGH führt dazu Folgendes aus:

89 BBl **2017** 7031
90 BBl **2017** 7019
91 Rechtssache C-817/19, ECLI:EU:C:2022:491, Rz. 130–140

«Während des ursprünglichen Zeitraums von sechs Monaten ist somit – angesichts der Ziele der PNR-Richtlinie und der Erfordernisse der Ermittlungs- und Verfolgungsmaßnahmen im Bereich terroristischer Straftaten und schwerer Kriminalität – davon auszugehen, dass die Speicherung der PNR-Daten aller Fluggäste, für die das durch die Richtlinie geschaffene System gilt, grundsätzlich auch dann nicht die Grenzen des absolut Notwendigen überschreitet, wenn es keine Anhaltspunkte für ihre Beteiligung an terroristischen Straftaten oder schwerer Kriminalität gibt, da sie es ermöglicht, die nötigen Recherchen zur Ermittlung von Personen anzustellen, die nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein.»[92]

Demgegenüber sollen markierte Daten (vgl. Art. 7 Abs. 3) fünf Jahre gespeichert werden, soweit ihre Markierung nicht vorher aufgehoben worden ist (vgl. Art. 21 Abs. 2). Der EuGH erachtet auch diese Aufbewahrungsdauer als gerechtfertigt. Er führt dazu aus:

«Gibt es in besonderen Fällen objektive Anhaltspunkte – wie bei den PNR-Daten der Fluggäste, die zu einem überprüften Treffer geführt haben – dafür, dass von bestimmten Fluggästen eine Gefahr im Bereich terroristischer Straftaten oder schwerer Kriminalität ausgehen könnte, erscheint eine Speicherung ihrer PNR-Daten über den ursprünglichen Zeitraum hinaus jedoch zulässig (…). Das Vorliegen dieser objektiven Anhaltspunkte wäre nämlich geeignet, einen Zusammenhang mit den Zielen herzustellen, die mit den Verarbeitungen gemäß der PNR-Richtlinie verfolgt werden, so dass die Speicherung der PNR-Daten dieser Fluggäste während des nach der Richtlinie maximal zulässigen Zeitraums von fünf Jahren gerechtfertigt wäre.»[93]

Daten dürfen nur so lange markiert sein und damit der fünfjährigen Aufbewahrungsdauer unterstellt bleiben, wie dies auch tatsächlich nötig ist. Unnötig ist diese Aufbewahrungsdauer, wenn die zuständige Behörde feststellt, dass sie die Daten nicht mehr braucht. Dies ist insbesondere dann der Fall, wenn sich die objektiven Anhaltspunkte aufgrund des laufenden Ermittlungs- oder Strafverfolgungsverfahren als unhaltbar erweisen. Für diesen Fall sieht das Flugpassagierdatengesetz vor, dass die Behörde dies der PIU mitteilt. Die PIU hebt sodann die Markierung auf. Danach sind die betroffenen Daten wieder ohne Markierung und unterstehen den für diese Daten vorgesehenen Regelungen.

Daten dürfen nur zum gesetzlich vorgesehenen Zweck bearbeitet werden (Art. 6 Abs. 4 DSG).

Nach Artikel 5 Absatz 1 dürfen Flugpassagierdaten nur zur Bekämpfung von Schwerstkriminalität bearbeitet werden. Die zulässigen Straftatbestände sind

92 Rechtssache C-817/19, ECLI:EU:C:2022:491, Rz. 255.
93 Rechtssache C-817/19, ECLI:EU:C:2022:491, Rz. 259–260

in Anhang 2 des Gesetzes ausgewiesen. Risikoprofile und Beobachtungslisten dürfen nur zu zusätzlich eingeschränkten Zwecken eingesetzt werden (vgl. Art. 12–14).

Vor jeder Bekanntgabe von Übereinstimmungen, die aufgrund des automatischen Datenabgleichs erzielt worden sind, hat die PIU zu prüfen, ob dabei der gesetzliche Zweck der Datenbearbeitung gewahrt ist (vgl. Art. 6 Abs. 3 Bst. a). Die PIU hat Übereinstimmungen, die diesem Zweck widersprechen, umgehend zu löschen (vgl. Art. 22 Bst. b Ziff. 1).

Diese Überprüfungspflicht gilt sinngemäss auch für die weiteren Daten, bevor sie einer zuständigen Behörde bekanntgegeben werden sollen (vgl. Art. 8 Abs. 2 und Art. 9 Abs. 3).

Werden Personendaten bearbeitet, ist ihre Richtigkeit sicherzustellen (Art. 6 Abs. 5 DSG).

Die PIU ist verpflichtet, die aufgrund des automatischen Datenabgleichs erzielten Übereinstimmungen einzeln und allenfalls unter Zugriff auf weitere Informationssysteme zu überprüfen. Zu überprüfen ist dabei auch die Identität der betroffenen Flugpassagierin oder des betroffenen Flugpassagiers (vgl. Art. 6 Abs. 3 Bst. b). Ist sie oder er nicht identisch mit der gesuchten Person, ist die Übereinstimmung umgehend zu löschen (vgl. Art. 22 Bst. b Ziff. 2). Diese Überprüfungspflicht gilt sinngemäss auch für die weiteren Bearbeitungsergebnisse, bevor sie einer zuständigen Behörde bekanntgegeben werden (vgl. Art. 8 Abs. 2 und Art. 9 Abs. 3).

Der Datenschutz ist mit geeigneten technischen Massnahmen sicherzustellen (Art. 7 DSG).

Technisch wird der Datenschutz durch die Automatismen umgesetzt, welche das Flugpassagierdatengesetz für zahlreiche Bearbeitungsschritte vorsieht, so bei der Pseudonymisierung der Daten ohne Markierung (vgl. Art. 18 Abs. 1), deren Löschung nach insgesamt sechs Monaten sowie bei der Löschung der markierten Daten nach insgesamt fünf Jahren. Diese wichtigen Bearbeitungsschritte sind laufend und zeitgerecht durchzuführen. Deshalb werden sie automatisch ausgelöst (vgl. Art. 18 Abs. 1 sowie Art. 22).

Das Aufstellen von Risikoprofilen stellt technisch hohe Anforderungen. Denn sie sollen nur wenige beziehungsweise die tatsächlich nötigen Übereinstimmungen liefern. Deshalb sind Risikoprofile vor ihrem Einsatz zwingend zu testen. Durchgeführt werden die Tests ausschliesslich mit synthetischen Daten. Ergänzend überprüft der Bundesrat den Einsatz von Risikoprofilen. Diese Überwachung stellt eine zusätzliche Massnahme dar, damit die Anlage von Risikoprofilen aktuell und fokussiert ist und ihre Anwendung auf das tatsächlich Nötige beschränkt bleibt (vgl. Art. 15).

Auch mit organisatorischen Massnahmen sind die Daten zu schützen (Art. 7 DSG).

Zu diesen Massnahmen gehört auf gesetzlicher Ebene einerseits die organisatorische und personelle Trennung der PIU von Einheiten, die potenzielle Empfängerinnen von Bearbeitungsergebnissen der PIU sind (vgl. Art. 27 Abs. 2). Damit und mit der Pflicht zur Verschwiegenheit (vgl. Art. 28 Abs. 4) wird das Risiko eines informellen Austauschs von Mensch zu Mensch organisatorisch und gesetzlich auf ein Minimum reduziert.

In zwei Bereichen sieht das vorliegende Gesetz zudem vor, dass die PIU nicht allein entscheiden kann, sondern abhängig ist von einem gerichtlichen Entscheid:

- Das zuständige Zwangsmassnahmengericht befindet darüber, ob eine Beobachtungsliste mit Daten Dritter (vgl. Art. 14) zum Einsatz kommen darf.
- Das Bundesverwaltungsgericht entscheidet, ob die Voraussetzungen erfüllt sind, welche die Aufhebung der Pseudonymisierung bestimmter Daten erlauben (vgl. Art. 19 und 20).

Eine angemessene Sicherheit der Flugpassagierdaten wird auch durch technische Massnahmen gewährleistet (Art. 8 DSG).

Der individuelle Datenschutz ist nur möglich, wenn zugleich allgemeine technische Vorkehrungen zur Datensicherheit getroffen werden. Die Datensicherheit zielt auf die vorhandenen Daten ab und umfasst den allgemeinen technischen und organisatorischen Rahmen der Datenbearbeitung. Gestützt auf Artikel 8 des DSG ist das fedpol verpflichtet, für das PNR-Informationssystem eine geeignete Sicherheitsarchitektur vorzusehen, sodass die Flugpassagierdaten und die Bearbeitungsergebnisse sicher sind.

Flugpassagierdaten und die Ergebnisse ihrer Bearbeitung werden bundesintern beim ISC-EJPD gespeichert. Gleiches gilt für die Protokolle, die jedoch separat von den operativen Daten zu speichern sind.

Wie der Bundesrat in der Botschaft vom 15. September 2017 zum neuen Datenschutzgesetz ausführt, stellt die Pseudonymisierung eine solche Massnahme dar.[94] Das Flugpassagierdatengesetz sieht die Pseudonymisierung (vgl. Art. 18) für Flugpassagierdaten ohne Markierung vor. Zu den Daten ohne Markierung gehören auch jene Daten, deren Markierung nachträglich aufgehoben worden ist und die mindestens einen Monat alt, jedoch nicht älter als sechs Monate sind (vgl. Art. 18). Mit der Pseudonymisierung werden jene Daten in verschiedenen Kategorien eines Flugpassagierdatensatzes mit einem Pseudonym versehen, die Rückschlüsse auf die betroffene Person geben.

Zwar lässt sich die Pseudonymisierung – anders als die Anonymisierung – rückgängig machen. Dies ist jedoch nur zulässig, wenn das Bundesveraltungsgericht diesen Bearbeitungsschritt genehmigt (vgl. Art. 19 und 20). Technisch lässt sich ein solcher Entscheid des Bundesverwaltungsgerichts nur durch die

94 BBl **2017** 6941 S. 7031

Leitung der PIU umsetzen, die autorisiert ist, auf die Konkordanztafel zuzugreifen, um die Pseudonymisierung im genehmigten Rahmen aufzuheben. Bei diesem Zugriff muss die autorisierte Person auch das hierzu legitimierende Urteil des Bundesverwaltungsgerichts angeben.

All diese Massnahmen erklären die folgende Aussage des Bundesrates in der vorerwähnten Botschaft: «Das Gesetz [gemeint das DSG] gilt nicht für anonymisierte Daten, wenn eine Reidentifizierung durch Dritte unmöglich ist (die Daten wurden vollständig und endgültig anonymisiert) oder wenn dies nur mit einem hohen Aufwand möglich wäre, den kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten.»

Schutzbedarfsanalyse und Datenschutz-Folgenabschätzung

Bei jedem Informatikvorhaben wird in der Bundesverwaltung vorab eine Schutzbedarfsanalyse durchzuführen. Der Zeitpunkt der Analyse richtet sich nach dem Projektvorgehensmodell HERMES und soll während der Initialisierungsphase erstellt werden. Damit ist gewährleistet, dass die Informatiksicherheit von Anfang an berücksichtigt wird.

Für das Projekt PNR Schweiz wurde im Rahmen von HERMES eine Schutzbedarfsanalyse erstellt. Diese wurde vom Sicherheitsbeauftragten des fedpol geprüft und danach im März 2021 unterzeichnet.

Gestützt auf das Bundesgesetz über den Datenschutz wurden die Datenschutzrisiken, welche sich durch die Weitergabe der von den Fluggesellschaften erfassten Personendaten an die Polizei ergeben, identifiziert und entsprechende Massnahmen unter Berücksichtigung der Schutzbedarfsanalyse in einer Datenschutz-Folgenabschätzung (DSFA) festgelegt.

Sie weist 14 potentielle Risiken für Grundrechtsverletzungen («Bruttorisiken») aus, denen mit insgesamt 22 organisatorischen, rechtlichen und technischen Massnahmen begegnet wird. Dadurch lassen sich die Bruttorisiken hinsichtlich Eintretenswahrscheinlichkeit und Schadensausmass von zum Teil «hoch» auf «mittel» bis «gering» reduzieren. Die DSFA weist damit keine potentiellen Restrisiken mehr auf, die als hoch einzustufen wären.

Da das Gesetzgebungsprojekt von den Fluggesellschaften keine Erfassungen von zusätzlichen Personendaten fordert, ergeben sich keine zusätzlichen Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen als die in der DSFA ausgewiesenen Restrisiken.

Der EDÖB hielt in seiner Stellungnahme vom 5. April 2024 zur DSFA fest, dass die DSFA sorgfältig erarbeitet wurde und dass ein Teil der verbleibenden Restrisiken ein hohes Schadensausmass bei einer geringen Eintrittswahrscheinlichkeit indiziert, sodass das bearbeitungsverantwortliche Fachamt die ausgewiesenen Restrisiken insgesamt für vertretbar hält. Angesichts der Nachvollziehbarkeit der fachgerecht erarbeiteten DSFA, sah der EDÖB keine Veranlassung für Einwände, zumal er den Ermessenspielraum, der den Fachämtern bei der Bewertung der Risiken zukommt, nicht ohne Not durch sein eigenes Ermessen ersetzt.

Beilage (Erlassentwurf)