«%ParlID»

Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG)

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

(März 2022)

Übersicht

Mit dieser Gesetzesvorlage soll auch die Schweiz systematisch Flugpassagierdaten bearbeiten können, um Behörden des Bundes und der Kantone bei der Verhinderung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten zu unterstützen.

Ausgangslage

Bei der Buchung eines Flugtickets werden verschiedene Daten von den Passagieren erhoben, die von den Luftverkehrsunternehmen für die Reservation und Abfertigung des Fluges benötigt werden. Dieser Flugpassagierdatensatz, international bekannt als Passenger Name Record (PNR), enthält beispielsweise den Namen und die Anschrift eines Flugpassagiers oder einer Flugpassagierin, aber auch andere Informationen wie Angaben zum mitgeführten Gepäck oder zu Zahlungsmodalitäten.

Mehr als 60 Staaten haben das Potenzial von PNR erkannt und nutzen die Daten seit Jahren als wichtiges Instrument zur Bekämpfung von Terrorismus und anderer Schwerstkriminalität. Mit der Bearbeitung von Flugpassagierdaten und spezifischen Datenanalysen können nicht nur Personen ermittelt werden, die den Strafverfolgungsbehörden bereits bekannt sind. Vielmehr lassen sich über neue Ermittlungsansätze auch Personen identifizieren, die den Strafverfolgungsbehörden bislang nicht bekannt waren, aber mit Terrorismus und anderer Schwerstkriminalität in Zusammenhang stehen könnten.

Die Nutzung von PNR wird derzeit global vorangetrieben. Drei für die Schweiz bindende Resolutionen des UNO-Sicherheitsrats weisen die internationale Gemeinschaft an, Flugpassagierdaten zur Verhinderung von Terrorismus zu verwenden. Die Schweiz ist als Mitglied der Internationalen Zivilluftfahrtorganisation (ICAO) verpflichtet, deren PNR-Standards anzuwenden.

Die EU hat ihre Mitgliedstaaten mit der Richtlinie (EU) 2016/681 verpflichtet, nationale PNR-Systeme aufzubauen. Die Richtlinie ist keine Weiterentwicklung des Schengen-Besitzstandes. Dennoch ist die Schweiz von deren Umsetzung betroffen, denn alle Luftverkehrsunternehmen mit Flügen aus der Schweiz in die EU und umgekehrt sind zur Datenübermittlung verpflichtet.

Heute werden zwar PNR-Daten von Flügen aus der Schweiz in EU-Mitgliedstaaten, ins Vereinigte Königreich, in die USA oder nach Kanada übermittelt, die Schweiz selber kann aber PNR-Daten nicht systematisch bearbeiten, solange sie über keine gesetzliche Grundlage und ein nationales PNR-System verfügt.

Ohne PNR-System stehen der Schweiz - im Vergleich zu anderen Schengen-Staaten - weniger Daten für die Einreisekontrollen zur Verfügung. Damit riskiert sie, dass Personen, die eine Gefahr für die öffentliche Sicherheit darstellen, über die Schweiz unerkannt in den Schengen-Raum gelangen.

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

Inhalt der Vorlage

Mit dem Flugpassagierdatengesetz soll der Bund zur Bekämpfung terroristischer und anderer schwerer Straftaten Flugpassagierdaten bearbeiten dürfen, die bei der Reservation und Abfertigung von Flügen anfallen.

Zuständig für die Bearbeitung der Daten soll eine neu zu schaffende, beim Bundesamt für Polizei (fedpol) angesiedelte Stelle (international als Passenger Information Unit, kurz PIU, bezeichnet) sein. Sie erhält die Daten von den Luftverkehrsunternehmen 24 bis 48 Stunden sowie kurz vor Abflug eines Flugzeuges aus der oder in die Schweiz.

Indem die PIU die Flugpassagierdaten mit polizeilichen Informationssystemen abgleicht, lassen sich im Vorfeld eines Flugs Personen bei der Ein- und Ausreise erkennen, die der Planung oder Begehung terroristischer und anderer schwerer Straftaten verdächtigt oder bezichtigt werden. Nur diese Ergebnisse («Treffer») gibt die PIU den zuständigen Behörden von Bund und Kantonen bekannt, so dass diese rechtzeitig die notwendigen Massnahmen in die Wege leiten können. Im Auftrag dieser Behörden soll die PIU auch gezielte Analysen der Flugpassagierdaten durchführen können. Damit lassen sich Personen oder Verbindungen erkennen, die auf international tätige kriminelle Netzwerke hindeuten.

Die Flugpassagierdaten werden nach Ablauf von sechs Monaten seit ihrem Eingang bei der PIU automatisch pseudonymisiert und nach insgesamt fünf Jahren gelöscht.

Die Hälfte der Mitarbeitenden, die bei der PIU tätig sind, soll von den Kantonen entsendet und von diesen finanziert werden. Damit wird dem Umstand Rechnung getragen, dass die PIU zu einem bedeutenden Teil im Dienste kantonaler Strafverfolgungsbehörden tätig ist.

Inhaltsverzeichnis

1 Ausgangslage

Wer einen Flug bucht, teilt der Fluggesellschaft oder der Reiseagentur zahlreiche Informationen mit, die bis nach der Reise im jeweiligen Reservierungssystem gespeichert werden. Diese Informationen – zusammengefasst in einem Flugpassagierdatensatz[1] (Passenger Name Record, PNR) – geben nicht nur über den Namen des Flugpassagiers und seine Kontaktdaten (Wohnadresse, Telefon und E-Mail) Auskunft, sondern liefern auch Angaben zu den Zahlungsmodalitäten, der Anzahl Gepäckstücke oder zu Begleitpersonen.

Weltweit haben bereits über 60 Staaten das Potenzial von PNR für die Sicherheit erkannt und nutzen die Daten als wirksames Instrument zur Bekämpfung von Terrorismus und anderer Schwerstkriminalität. Damit können sie Straftäter in ihren Reisebewegungen frühzeitig lokalisieren und bei der Ein- und Ausreise erkennen oder Rückschlüsse auf international tätige Netzwerke beispielsweise im Bereich Terrorismus und Menschenhandel ziehen.

Bereits heute liefern Luftverkehrsunternehmen für Flüge von der Schweiz in bestimmte Staaten PNR-Daten. Dazu gehören die USA. Grundlage für die seit 2003 erfolgenden Datenlieferungen an die USA ist das Abkommen vom 23. Dezember 2008[2], das ein entsprechendes, aber zeitlich befristetes Abkommen aus dem Jahr 2003 ersetzt. Die USA erklärten im Juni 2018, dass die Schweiz nur dann weiterhin im Visa Waiver Program (VWP) verbleiben könne, wenn sie künftig auch selber PNR nutze. Das Visa Waiver Program erlaubt schweizerischen Staatsangehörigen, zu geschäftlichen oder touristischen Zwecken für bis zu 90 Tage visumsfrei in die USA einzureisen.

Drei Resolutionen[3] des UNO-Sicherheitsrats weisen die internationale Gemeinschaft an, in allen Mitgliedstaaten Kapazitäten zur Sammlung, Verarbeitung und Analyse von PNR aufzubauen. Diese Resolutionen sind auch für die Schweiz verbindlich.

Auf europäischer Ebene drängt die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE), deren Mitglied die Schweiz ist, zur Nutzung von PNR. Die OSZE bezeichnet die Verwendung von PNR-Daten als wichtige Massnahme zur Verhinderung, Aufdeckung und Verfolgung terroristischer Straftaten und unterstützt Staaten im Aufbau nationaler PNR-Systeme.

Die Europäische Union hat in einem ersten Schritt die Bearbeitung der Advance Passenger Information-Daten (API-Daten), die eine Teilmenge der PNR-Daten sind, in der Richtlinie (EU) 2004/82/EG (API-Richtlinie)[4] festgelegt. Die API-Richtlinie gehört zum Schengener Besitzstand und ist damit für die Schweiz verbindlich.

1 Erklärung siehe Glossar im Anhang
2 SR **0.748.710.933.6**
3 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.
4 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.

Nicht verbindlich für die Schweiz ist dagegen die Richtlinie (EU) 2016/681 vom 27. April 2016 (PNR-Richtlinie)[5], mit der die EU ihre Mitgliedstaaten zum Aufbau nationaler PNR-Systeme verpflichtet. Die Richtlinie ist keine Weiterentwicklung des Schengen-Besitzstandes und verpflichtet die Schweiz damit nicht zur Umsetzung. Dennoch ist die Schweiz von deren Umsetzung betroffen, da die Luftverkehrsunternehmen auch für Flüge aus der Schweiz in die EU zur Datenübermittlung verpflichtet sind.

Die Schweiz verfügt seit dem 1. Oktober 2015 mit den Artikeln 104*a* und 104*b* des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005[6] (AIG) über die nötige Rechtsgrundlage, um API-Daten automatisiert zu bearbeiten. Diese werden jedoch derzeit – wie in der EU – nicht systematisch erhoben, sondern nur auf spezifischen, als risikobehaftet eingestuften Flügen aus Drittstaaten in die Schweiz. Diese Datenbearbeitung soll nicht nur einer verbesserten Grenzkontrolle sowie der Bekämpfung der rechtswidrigen Einreisen in den Schengen-Raum und der Durchreisen durch die internationalen Transitzonen der Flughäfen dienen, sondern auch der Bekämpfung des organisierten und international tätigen Verbrechens sowie des Terrorismus (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 Abfluges und der geplanten Ankunft	

Seit dem 1. Januar 2018 können die Strafverfolgungsbehörden in der Schweiz gestützt auf Artikel 21f des Luftfahrtgesetzes vom 21. Dezember 1948[7] (LFG) Passagierdaten einfordern, soweit diese Daten von den Luftverkehrsunternehmen «im Rahmen der normalen Geschäftstätigkeit» erhoben werden. Damit gelangen die

5 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.
6 SR **142.20**
7 SR **748.0**

Strafverfolgungsbehörden zusätzlich zu den API-Daten in den Besitz der folgenden Flugpassagierdaten:

- allfällige Mitreisende;
- Informationen zur Zahlung, namentlich Zahlungsmethode und verwendetes Zahlungsmittel;
- Angabe der Stelle, über welche die Beförderung gebucht worden ist.

1.1 Handlungsbedarf und Ziele

Die Schweiz verfügt derzeit weder über die gesetzliche Grundlage noch über ein Informationssystem für die Bearbeitung von PNR. Als Bearbeiten gilt jeder Umgang mit Personendaten[8], unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben – das heisst das Übermitteln oder Zugänglichmachen von Personendaten, Archivieren, Löschen oder Vernichten von Daten (Art. 5 des Datenschutzgesetzes vom 25. September 2020[9] [nDSG]).

Verschiedene Staaten, darunter auch wichtige Wirtschaftspartnerländer der Schweiz, verlangen seit längerem von den Luftverkehrsunternehmen, die bei ihnen landen, PNR-Daten.

Die Daten werden zur Bekämpfung von Terrorismus und anderen schweren Straftaten genutzt. Mit der systematischen Bearbeitung von Flugpassagierdaten lassen sich bei der Ein- oder Ausreise Personen lokalisieren, die national oder international gesucht werden. Zudem können die Strafverfolgungsbehörden auf bisher polizeilich unbekannte Personen aufmerksam werden, die mit Terrorismus oder anderer Schwerstkriminalität in Verbindung stehen. PNR kann damit einen wichtigen Beitrag bei der Aufdeckung und Verfolgung international tätiger, krimineller Netzwerke leisten. Von der Verpflichtung zur Lieferung von PNR betroffen sind die Luftverkehrsunternehmen auch bei Flügen aus der Schweiz.

Mit den USA hat die Schweiz erstmals 2003 ein Abkommen abgeschlossen, das die Datenbekanntgabe vorsieht. Die Datenübermittlung für Flüge von der Schweiz nach Kanada basiert auf einem Memorandum of Understanding aus dem Jahr 2006.[10]

Der Datenaustausch zwischen der EU und der Schweiz soll einvernehmlich auf der Grundlage eines völkerrechtlichen Vertrages festgelegt werden. Bis zu dessen Abschluss basiert die Datenübermittlung an die EU-Mitgliedstaaten auf einer Übergangslösung, die unter Mitwirkung des EDÖB erarbeitet worden ist. Das Bundesamt für Zivilluftfahrt (BAZL) informierte die betroffenen Luftverkehrsunternehmen im Mai 2018 darüber, dass eine Übermittlung von Flugpassagierdaten an ersuchende EU-Mitgliedstaaten bis zur Schaffung einer gesetzlichen Grundlage möglich sei, wenn die Flugpassagiere in den Beförderungsbestimmungen der Luftverkehrsunternehmen über die Datenübermittlung informiert würden und damit einverstanden wären. Der EDÖB hat

8 Erklärung siehe Glossar im Anhang
9 BBl **2020** 7639 [es wird im vorliegenden Bericht auf das neue Datenschutzgesetz verwiesen, das bei Inkrafttreten des Flugpassagierdatengesetzes Geltung haben wird].
10 Abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/2242.pdf

seither verschiedentlich darauf hingewiesen, dass die nötigen Rechtsgrundlagen rasch erstellt werden müssten.

Mangels gesetzlicher Grundlage kann die Schweiz keine PNR-Daten selber bearbeiten. Dieser Umstand kann dazu führen, dass Personen, die des Terrorismus oder einer anderen schweren Straftat verdächtigt werden oder eine solche Straftat planen, nach der Landung in der Schweiz – in Umgehung der in den einzelnen Staaten eingesetzten PNR-Systeme – auf dem Landweg im Schengen-Raum weiterreisen könnten.

Damit die Schweiz künftig PNR-Daten zur Bekämpfung von Terrorismus und anderen schweren Straftaten 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 EJPD am 12. Februar 2020 beauftragt, in Zusammenarbeit mit dem UVEK eine Vernehmlassungsvorlage zu einem Bundesgesetz über die Erhebung und Nutzung von PNR-Daten sowie deren Übermittlung an Staaten, deren Datenschutz und Datenbearbeitung dem Standard der PNR-Richtlinie entspricht, auszuarbeiten und dem Bundesrat vorzulegen. Zudem soll in Zusammenarbeit mit dem EDA ein Mandat für die Aufnahme von Verhandlungen mit der EU über ein Abkommen zu PNR erarbeitet werden.

1.2 Geprüfte Alternativen und gewählte Lösung

Rechtsetzungstechnische Überlegungen

Geprüft wurde, die nötigen Rechtsgrundlagen nicht in einem neuen Gesetz, sondern in bereits bestehenden Bundesgesetzen zu schaffen, so im Luftfahrtgesetz (LFG)[11], im Ausländer- und Integrationsgesetz (AIG)[12] oder im Nachrichtendienstgesetz (NDG)[13]. Im Ergebnis würde eine gesplittete und damit unübersichtliche Rechtslage geschaffen, die weder im Interesse der durch dieses Gesetz verpflichteten Flugverkehrsunternehmen noch im Interesse betroffener Flugpassagiere sein kann. Deshalb wurde diese Möglichkeit verworfen.

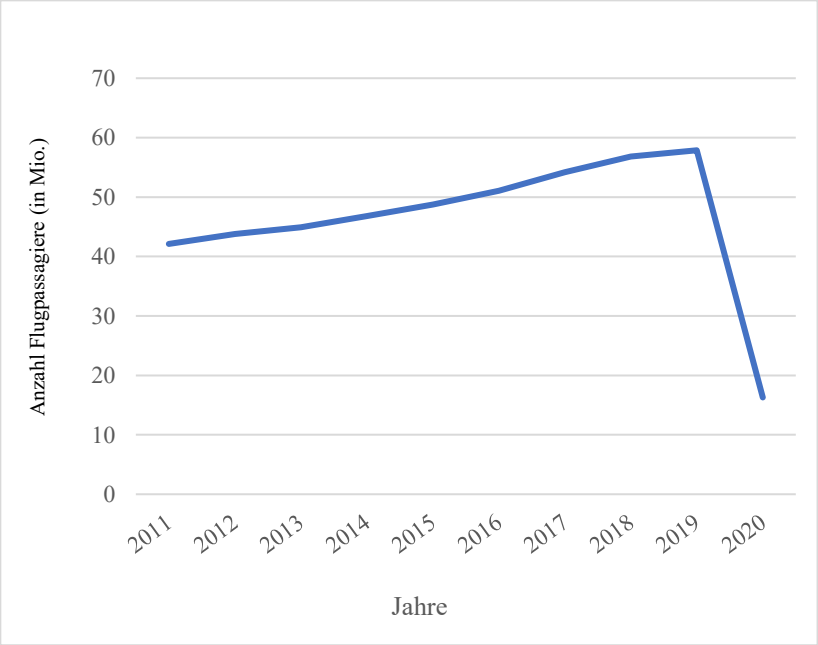
Ein neues Gesetz, das die Bearbeitung von Flugpassagierdaten umfassend regelt, bietet die grösstmögliche Transparenz und Kohärenz. Dies rechtfertigt sich auch mit Blick auf die Einzelheiten, die zu regeln sind. Denn neben der Übermittlung der Flugpassagierdaten durch die Luftverkehrsunternehmen und deren Sanktionierung bei Verletzung dieser Pflicht gilt es auch, die Organisation und die Aufgaben der neu zu schaffenden Nationalen Stelle (PIU) zu regeln. Ihre Aufgabe besteht in der Bearbeitung der Flugpassagierdaten und deren Bekanntgabe an zuständige Behörden im In- und Ausland. Für die Erfüllung ihrer Aufgabe hat die PIU Zugriff auf verschiedene Informationssysteme des Bundes.

Mit der Vorlage entstehen teilweise neue Pflichten für Luftverkehrsunternehmen, die in der Schweiz operieren. Im Jahr 2019 wären bis zu 217 und im Jahr 2020 198 Flugverkehrsunternehmungen betroffen gewesen, die Charter- und Linienflüge

11 SR **748.0**
12 SR **142.20**
13 SR **121**

anbieten. Sie beförderten im Jahr vor der Pandemie rund 60 Millionen Passagiere von der Schweiz ins Ausland und vom Ausland in die Schweiz.

Grafik 1: Zahl der Flugpassagiere, die in Charter- und Linienflügen aus der Schweiz ausreisten und in die Schweiz einreisten (Quelle: BAZL).



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

Auch aus datenschutzrechtlicher Sicht ist es zu begrüssen, ein einheitliches Bundesgesetz zur Hand zu haben. Für Flugpassagiere soll einfach erkennbar sein, wofür und zu welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen.

Nutzung von PNR-Daten für die öffentliche Gesundheit

Fedpol hat auch die Möglichkeit geprüft, Flugpassagierdaten zum Zweck des öffentlichen Gesundheitsschutzes zu nutzen. Im Einvernehmen mit dem Bundesamt für Gesundheit (BAG) wurde beschlossen, diese Möglichkeit nicht weiterzuverfolgen. Bewegungs- und Aufenthaltsdaten zu Gesundheitszwecken sollen bedarfsweise direkt beim jeweiligen Flugpassagier erhoben werden.

Novellierung der API-Richtlinie

API-Daten sind eine Teilmenge von PNR. Auch sie werden weltweit bearbeitet.

In der Schweiz wird die API-Meldepflicht der Luftverkehrsunternehmen in Artikel 104 des Ausländer- und Integrationsgesetzes[14] geregelt. Die Meldepflicht beschränkt sich aktuell auf Flüge in die Schweiz, die als risikobehaftet beurteilt werden.

Die EU überarbeitet derzeit die API-Richtlinie. Die Novellierung ist im Laufe des Jahres 2022 zu erwarten.

Für die Schweiz bedingt die Novelle voraussichtlich eine Ablösung des bestehenden API-Systems (Art. 104*a* AIG) und wahrscheinlich auch eine Anpassung weiterer einschlägiger Bestimmungen im Ausländer- und Integrationsgesetz.

Aufgrund der Parallelen, die API- und PNR-Daten aufweisen, wurde geprüft, ob und inwieweit die Novellierung der API-Richtlinie im vorliegenden Rechtsetzungsvorhaben mitberücksichtigt werden soll.

Gegen eine Mitberücksichtigung spricht die unterschiedliche Zweckbestimmung, unter der eine Datenbearbeitung zulässig ist. So dürfen PNR-Daten lediglich zur Verhinderung und Aufklärung terroristischer und anderer schwerer Straftaten bearbeitet werden. API-Daten dürfen dagegen sowohl zur Verbesserung der Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung als auch − unter bestimmten Bedingungen − zu Strafverfolgungszwecken genutzt werden. Ihre Bearbeitung ist damit zu einem deutlich breiteren Zweck zulässig als dies bei den PNR-Daten der Fall ist.

Die unterschiedlichen Zweckbestimmungen führen denn auch zu unterschiedlichen Zugriffsberechtigungen und Fristen, innerhalb derer eine Bearbeitung zulässig ist.

Die Inhalte der überarbeiteten API-Richtlinie sind derzeit noch nicht abschliessend bestimmt. Auch ist unklar, wann sie in Kraft treten werden. Aus diesem Grund berücksichtigt der Vorentwurf des Flugpassagierdatengesetzes die Novellierung der API-Richtlinie nicht. Die massgeblichenen Bestimmungen im Ausländer- und Integrationsgesetz zur Erhebungs- und Meldepflicht von API-Daten werden deshalb zu gegebener Zeit anzupassen sein.

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

Die Botschaft zu einem nationalen PNR-Informationssystem sowie der dazugehörige Verpflichtungskredit sind in der Legislaturplanung 2019–2023 als weiteres Geschäft zur Umsetzung von Ziel 14, «Die Schweiz beugt Gewalt, Kriminalität und Terrorismus vor und bekämpft sie wirksam», angekündigt.[15]

PNR leistet im Übrigen 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».

Das Flugpassagierdatengesetz liefert die nötige Rechtsgrundlage, um die nationale Stelle bei fedpol (Passenger Information Unit; PIU) aufzubauen, die

14 SR **142.20**
15 Botschaft vom 29. Januar 2020, BBl **2020** 1777

Flugpassagierdaten bearbeitet, um Terrorismus und andere schwere Kriminalität zu bekämpfen. Dazu betreibt die PIU ein PNR-Informationssystem.

Die finanziellen Mittel für den Aufbau des PNR-Informationssystems sind in der Finanzplanung des Bundes eingestellt.[16]

Bereits in der Strategie der Schweiz vom 18. September 2015[17] zur Terrorismusbekämpfung nannte der Bundesrat die Nutzung von PNR als mögliche Massnahme, um unerwünschte Ein-, Aus- und Durchreisen von Terrorverdächtigen verhindern zu können.

2 Rechtsvergleiche, insbesondere mit dem europäischen Recht

EU

Etliche EU-Mitgliedstaaten haben bereits vor 2016 nach einzelstaatlichem Recht PNR-Daten bearbeitet. Am 27. April 2016 verabschiedeten das Europäische Parlament und der Rat die Richtlinie (EU) 2016/681 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (PNR-Richtlinie). Sie trat auf den 24. Mai 2016 in Kraft und bezweckt, die Rechtsvorschriften der EU-Mitgliedstaaten zu harmonisieren, Rechtsunsicherheit und Sicherheitslücken zu beheben und zugleich den Datenschutz auf einem gemeinsamen Niveau zu gewährleisten. Als einziger Mitgliedstaat ist Dänemark nicht an diese Richtlinie gebunden.[18] Dänemark hat seither aber ebenfalls ein umfassendes PNR-System auf der Grundlage nationaler Rechtsvorschriften entwickelt und sich dem PNR-Informationsaustausch der EU-Mitgliedstaaten angeschlossen.

Die Richtlinie regelt neben der Zuständigkeit der sogenannten PNR-Zentralstellen, die für den operationellen Betrieb in den Mitgliedstaaten verantwortlich sind (Art. 4), die Datenbearbeitung (insb. Art. 6) sowie die Pflichten der Fluggesellschaften zur Datenübermittlung (Art. 8). Die Daten werden sechs Monate nach ihrem Eingang depersonalisiert[19] und nach Ablauf von insgesamt fünf Jahren gelöscht (Art. 12). Artikel 13 widmet sich dem Schutz personenbezogener Daten und enthält wichtige Garantien für den Schutz der Grundrechte.

Die Europäische Kommission hat alle Elemente der Richtlinie gemäss Artikel 19 überprüft und die Ergebnisse im Bericht vom 24. Juli 2020[20] an das Europäische Parlament und den Rat erläutert. Konkrete Änderungen der Richtlinie erachtet sie nicht als notwendig. Allerdings sind vor dem Gerichtshof der Europäischen Union (EuGH) zwei Verfahren – eines aus Deutschland und eines aus Belgien – zu Fragen

16 Voranschlag 2022 mit integriertem Aufgaben- und Finanzplan 2023 – 2025, Band 2A, S. 221
17 BBl **2015** 7492
18 PNR-Richtlinie, Erwägung 40
19 Siehe Glossar im Anhang
20 Bericht der 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

des Datenschutzes und der Verhältnismässigkeit der PNR-Richtlinie hängig.[21] Die Europäische Kommission schliesst in ihrem Bericht nicht aus, dass die Gerichtsurteile eine Anpassung der PNR-Richtlinie notwendig machen könnten. Aus ihrer Sicht erweist sich das PNR-System aber als effektives Instrument bei der Bekämpfung von Terrorismus und schwerer Kriminalität. Weiterführende Ermittlungshandlungen oder Verhaftungen wären ohne die Nutzung der PNR-Daten nicht möglich gewesen. Dank der strengen Datenschutzvorkehren werde nur eine sehr geringe Zahl von Personendaten an zuständige Behörden weitergeleitet.

Die EU-Mitgliedstaaten bestätigten, dass die in der PNR-Richtlinie vorgesehene Aufbewahrungsdauer der Daten aus operativer Sicht nötig sei. Darüber hinaus hätten sich die Regelungen des Zugangs von Behörden zu den bei der PNR-Zentralstelle gespeicherten Daten und deren Depersonalisierung als ausreichend erwiesen, um Missbräuche zu verhindern. Die Verbesserung der Datenqualität bleibe aber eine Herausforderung.

In der Mitteilung vom 21. September 2010[22] über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer hat die Europäische Kommission Kriterien festgelegt, die bei der Entscheidungsfindung über künftige Abkommen mit Drittländern berücksichtigt werden sollen. So soll sich die EU auf die Zusammenarbeit mit solchen Drittstaaten beschränken, die einen angemessenen Schutz von Fluggastdaten aus der EU bieten können. Auch die Aussenbeziehungen zwischen der EU und dem Drittland sollen in einer Gesamtbetrachtung von Bedeutung sein. Dazu gehörten namentlich das Funktionieren der Polizei- und Justizbehörden und die Zusammenarbeit mit ihnen sowie Rechtsstaatlichkeit und die allgemeine Achtung der Grundrechte. In der EU-Strategie für eine Sicherheitsunion[23] für den Zeitraum 2020-2025 ist die Überprüfung des geltenden Konzepts für die Übermittlung von PNR-Daten an Drittländer als mittelfristige Massnahme vorgesehen.

Bislang hat die EU mit den USA[24] und Australien[25] Abkommen über die Nutzung von PNR-Daten geschlossen.

Ein mit Kanada ausgehandeltes Abkommen, welches das Abkommen von 2006 ersetzen sollte, musste nach seiner Paraphierung am 6. Mai 2013 neu verhandelt

21 Rechtssache C-817/19, Ligue des droits humains v Conseil des ministres; Rechtssache C-148/20, 149/20, 150/20, AC/DF/BD v Deutsche Lufthansa AG.

22 Mitteilung der Kommission vom 21. September 2010 über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer, COM/2010/492 final

23 Mitteilung der Kommission vom 24. Juli 2020 an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss der Regionen, EU-Strategie für eine Sicherheitsunion, COM/2020/605 final, S. 29

24 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

25 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

werden, nachdem der EuGH im Gutachten vom 26. Juli 2017[26] zum Schluss kam, das anvisierte Abkommen widerspreche der Grundrechtecharta der Europäischen Union[27].

Im Februar 2020 wurde die Europäische Kommission beauftragt, Verhandlungen mit Japan zu eröffnen. Im gleichen Jahr signalisierte die Europäische Kommission gegenüber der Schweiz ihr Interesse an einem bilateralen PNR-Abkommen. 2021 wurden exploratorische Gespräche aufgenommen.

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. Allerdings muss das Vereinigte Königreich Europol und Eurojust sowie den Strafverfolgungsbehörden der EU-Mitgliedstaaten auf deren Ersuchen erstellte Analysen zugänglich machen.[28]

USA

Die USA verpflichtete die Fluggesellschaften im Anschluss an die Terroranschläge vom 11. September 2001 durch den „Aviation and Transportation Security Act“[29] dazu, den US-Behörden Zugriff auf die PNR-Daten aller Flüge in, aus oder über das US-Gebiet zu gewähren. Die US-Regierung strebt seit den Anschlägen vom 11. September 2001 die Sammlung, Übermittlung und Speicherung von PNR-Daten an. Das erste Abkommen mit der Schweiz über den Austausch von PNR-Daten trat am 29. März 2005 in Kraft und galt aufgrund seiner Befristung lediglich dreieinhalb Jahre. Das vom Bundesrat verabschiedete PNR-Abkommen vom 23. Dezember 2008[30] ist im Gegensatz zum ersten Abkommen unbefristet.

Die PNR-Daten werden gemäss den datenschutzrechtlichen Vorgaben des System of Records Notice (SORN) des Automated Targeting System (ATS) bearbeitet. Dieses gehört zum US Department of Homeland Security (DHS), US Customs and Border Protection. Gemäss ATS SORN ist die US-Regierung verpflichtet, für PNR-Daten der Flüge zwischen den USA und der Schweiz im Wesentlichen denselben Datenschutz zu gewährleisten wie gemäss dem Abkommen zwischen den USA und der EU über die Verarbeitung von PNR-Daten von 2007. Seit dem 11. August 2012 regelt ein überarbeitetes Abkommen[31] zwischen den USA und der EU die Verwendung und

26 Gutachten 1/15 des Gerichtshofs (Große Kammer) vom 26. Juli 2017, ECLI:EU:C:2017:592

27 Charta der Grundrechte der Europäischen Union, ABl. C 202 vom 7.6.2016, S. 389

28 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

29 Public Law 107–71, 19. November 2001, 115 STAT. 597, Online: https://www.gpo.gov/fdsys/pkg/PLAW107publ71/pdf/ PLAW107publ71.pdf (28.08.2018)

30 SR **0.748.710.933.6**

31 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

Übermittlung von PNR-Daten. Eine Evaluation des Abkommens wurde im Januar 2021 verabschiedet.[32]

Die Schweiz erhält aufgrund der fehlenden Rechtsgrundlage im nationalen Recht keine PNR-Daten von Flügen aus den USA in die Schweiz.

Kanada

Seit 2009 werden PNR- und API-Daten von Flügen aus der Schweiz nach Kanada den dort zuständigen Behörden übermittelt. Grundlage hierfür ist 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[33]. 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, oder
- sie andere schwere Straftaten begehen, die grenzüberschreitend sind (einschliesslich organisierter Kriminalität), oder
- sie eine mögliche Verbindung zu solchen Verbrechen haben.

Die PNR-Daten werden von den kanadischen Behörden 42 Monate aufbewahrt, sofern die betreffende Person nicht Gegenstand eines Verfahrens wird. Nach 24 Monaten werden sie pseudonymisiert.

Die Bekanntgabe von PNR-Daten von der Canada Border Services Agency an eine andere kanadische Behörde ist nur einzelfallweise und nur nach Bewertung der Relevanz der spezifischen PNR-Informationen, die offengelegt werden sollen, zulässig. Es werden nur diejenigen PNR-Elemente zur Verfügung gestellt, von denen eindeutig nachgewiesen wird, dass sie unter den gegebenen Umständen erforderlich sind. In allen Fällen wird die geringstmögliche Menge an Informationen zur Verfügung gestellt. Die Bekanntgabe von PNR-Daten von den kanadischen Behörden an einen Drittstaat ist zulässig, soweit ein völkerrechtlicher Vertrag dies vorsieht.

Die Schweiz erhält aufgrund der fehlenden Rechtsgrundlage im nationalen Recht keine PNR-Daten von Flügen aus Kanada in die Schweiz.

3 Grundzüge der Vorlage

Mit dem vorgeschlagenen Flugpassagierdatengesetz soll künftig auch die Schweiz PNR als ein bewährtes Instrument zur Bekämpfung von Terrorismus und schweren Straftaten einsetzen können. Dieses steht seit rund 20 Jahren namentlich in den USA, Kanada sowie im Vereinigten Königreich und seit mehreren Jahren in den Mitgliedstaaten der EU im Einsatz.

32 Bericht der Kommission an das Europäische Parlament und den Rat über die gemeinsame Evaluierung des Abkommens 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, COM/2021/18 final

33 Abrufbar unter: https://www.newsd.admin.ch/newsd/message/attachments/2242.pdf

Die EU ist die wichtigste Sicherheitspartnerin der Schweiz und damit auch ihre wichtigste Partnerin im künftigen Austausch von PNR-Daten. Deshalb orientiert sich der Vorentwurf des Flugpassagierdatengesetzes an der PNR-Richtlinie der EU.

Mit dem Flugpassagierdatengesetz kommt die Schweiz ihren internationalen Verpflichtungen nach. Verpflichtend sind insbesondere die drei bindenden Resolutionen des UNO-Sicherheitsrates[34], welche die Mitgliedstaaten anweisen, Kapazitäten zur Sammlung, Verarbeitung und Analyse der PNR-Daten 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 zur Übermittlung von Flugpassagierdaten entwickelt. Diese PNR Reporting Standards sind für alle Mitgliedstaaten der ICAO – auch für die Schweiz – verbindlich. Die USA schliesslich macht den Verbleib der Schweiz im Visa Waiver Program von der Bearbeitung der Flugpassagierdaten abhängig (siehe vorne, Ziff. 1).

3.1 Die beantragte Neuregelung

Das Flugpassagierdatengesetz bildet die rechtliche Voraussetzung, damit auch die Schweiz Flugpassagierdaten bearbeiten und dazu ein Informationssystem betreiben kann.

Flugpassagierdaten fallen – unabhängig von ihrer staatlichen Nutzung zur Bekämpfung von Schwerstkriminalität – bei der Buchung von Flugtickets an. Siee müssen somit nicht speziell für die Zwecke dieses Gesetzes erhoben werden.

Von den Luftverkehrsunternehmen zu übermitteln sind insgesamt 19 verschiedene Datenkategorien Anhang 1 des Flugpassagierdatengesetzes).

Betroffen von dieser staatlichen Datenbearbeitung sind alle Passagierinnen und Passagiere bei Charter- und Linienflügen aus der Schweiz ins Ausland und umgekehrt betroffen.

Die Daten sind von den Luftverkehrsunternehmen zu zwei gesetzlich definierten Zeitpunkten vor dem Abflug in die Schweiz oder aus der Schweiz an die bei fedpol angesiedelte PIU zu übermitteln (Art. 2). Dies ermöglicht den zuständigen Behörden von Bund und Kantonen, rechtzeitig die angezeigten Massnahmen gegen verdächtige Personen bei der An- oder Ausreise veranlassen können.

Die Luftverkehrsunternehmen haben für die Rechtzeitigkeit der Datenübermittlung und die Einhaltung der technischen Vorgaben einzustehen (Art. 4). Zudem haben sie die Flugpassagiere schriftlich über die staatliche Datenbearbeitung zu informieren (Art. 5).

Kommt ein Luftverkehrsunternehmen diesen Verpflichtungen nicht oder unvollständig nach, greifen die Sanktionen nach den Artikeln 23–25. Davon befreien kann sich ein Luftverkehrsunternehmen nur, wenn es nachweist, dass es alle zumutbaren technischen und organisatorischen Massnahmen zur Erfüllung seiner Pflichten getroffen hat.

34 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

Die Artikel 6–12 regeln die Datenbearbeitung.

Flugpassagierdaten dürfen nur zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten bearbeitet werden. Die massgeblichen Straftaten sind im Anhang zu diesem Bericht ausgewiesen. Ergebnisse von Bearbeitungen, die diesen Zweck nicht erfüllen, hat die PIU umgehend zu löschen (Art. 6).

Die Artikel 6–12 regeln die Datenbearbeitung. Dafür zuständig ist die neu zu schaffende nationale Stelle für die Bearbeitung von Flugpassagierdaten (PIU) bei fedpol.

Die von den Luftverkehrsunternehmen übermittelten Daten werden in einem ersten Schritt mit verschiedenen polizeilichen Informationssystemen des Bundes automatisch abgeglichen. Mit diesem Abgleich sollen zum einen national und international gesuchte Personen identifiziert, verhaftet und/oder allenfalls ausgeliefert werden können, zum andern aber auch Informationen vervollständigt werden, die in Zusammenhang mit ungeklärten oder geplanten Straftaten stehen. In einem zweiten Schritt werden sie manuell und allenfalls unter Zugriff auf polizeiliche und weitere Informationssysteme (ZEMIS, ORBIS, Informationssystem BAZG) geprüft (Art. 7).

Ergibt die Prüfung ein positives Ergebnis, wird die Übereinstimmung jener Stelle übermittelt, die für die Ausschreibung verantwortlich ist, welche mit den Flugpassagierdaten eine Übereinstimmung ausgelöst hat. Es können dies Strafverfolgungsbehörden von Bund oder Kantonen und der Nachrichtendienst des Bundes sein (Art. 8). Die für die Ausschreibung verantwortliche Stelle entscheidet sodann über die allenfalls zu treffenden Massnahmen.

Die Flugpassagierdaten können auch mit sogenannten Risikoprofilen und Beobachtungslisten abgeglichen werden, welche die PIU aufgrund eigener Analysen oder auf Antrag der Strafverfolgungsbehörden oder des NDB erstellt. Risikoprofile beschreiben Datenmuster, welche auf kriminelle Aktivitäten im Zusammenhang mit Terrorismus oder Schwerstkriminalität hinweisen. In Beobachtungslisten sind Personen- oder PNR-Datenelemente (z.B. E-Mail-Adressen, Telefonnummern) verzeichnet, welche im Zusammenhang mit terroristischen oder schweren Straftaten nachverfolgt werden sollen. Im Abgleich mit PNR-Daten können diese beide Instrumente die Strafverfolgungsbehörden unterstützen, eine polizeilich noch unbekannte Person zu entdecken, Mitglieder einer kriminellen Organisation zu identifizieren oder beispielsweise potentielle Opfer von Menschenhandel zu erkennen. Beobachtungslisten sollen nur für wenige Straftatbestände eingesetzt werden dürfen, die der Bundesrat in der Verordnung festlegt. Der Fokus liegt auf terroristischen Straftaten und solchen des organisierten Verbrechens (Art. 9).

Das Flugpassagierdatengesetz berücksichtigt bereits das neue, voraussichtlich auf 2023 in Kraft tretende Datenschutzgesetz (nDSG; BBl 2020 7639), womit sich dem rasanten technologischen Wandel Rechnung tragen lässt und eine weitgehende Harmonisierung mit dem Datenschutzrecht der EU erzielt wird.

In ihrer Gesamtheit werden die Flugpassagierdaten lediglich beim Abgleich mit den polizeilichen Informationssystemen, den Risikoprofilen und den Beobachtungslisten (siehe Erläuterungen zu Art. 9) bearbeitet. Danach wird nur noch eine kleine Teilmenge davon weiter bearbeitet. Es sind dies jene Daten, die beim Abgleich eine

Übereinstimmung erzielt haben und damit mit einem gewissen Verdacht behaftet sind. Ob dieser Verdacht berechtigt ist, zeigt sich im nächsten Bearbeitungsschritt, denn die Übereinstimmungen dürfen erst zur Weiterbearbeitung freigegeben werden, wenn sie auf ihre Plausibilität überprüft worden sind. Wird diese bestätigt, handelt es sich um Daten, die im Minimum an den erhärteten Verdacht gekoppelt sind, in einem Bezug zu Terrorismus oder Schwerstkriminalität zu stehen.

Dagegen wird die grosse Mehrzahl der Flugpassagierdaten nach dem Abgleich nicht mehr aktiv weiterbearbeitet und nach Ablauf von sechs Monaten seit ihrem Eingang zusätzlich pseudonymisiert (Art. 14): dabei werden personenbezogene Daten wie zum Beispiel Name, Telefonnummer, E-Mail oder Kreditkartennummer mit einem Pseudonym versehen, so dass sie sich nicht mehr einer bestimmten Person zuordnen lassen. Im Gegensatz zur Anonymisierung kann die Pseudonymisierung allerdings wieder rückgängig gemacht werden. Zuständig für den Entscheid, ob die Umstände einen solchen Schritt rechtfertigen, soll das Bundesverwaltungsgericht sein (Art. 15).

Nach Ablauf von insgesamt fünf Jahren werden die Daten im PNR-Informationssystem gelöscht (Art. 16). Diese Aufbewahrungsdauer ist aus operativer Sicht elementar, da sich die Ermittlungen bei Straftaten, die mit PNR bekämpft werden sollen, häufig über Monate oder gar Jahre hinziehen.[35]

Auch technisch wird der Datenschutz umgesetzt, wie dies Artikel 7 nDSG vorschreibt. So beschränkt sich beispielsweise der Zugriff auf das PNR-Informationssystem auf wenige Personen (Art. 13 Abs. 2). Ausgeschlossen ist insbesondere ein direkter Zugriff der Strafverfolgungsbehörden von Bund und Kantonen auf das PNR-Informationssystem. Verstärkt wird diese Abgrenzung, indem die PIU organisatorisch von ermittelnden Behörden getrennt ist (Art. 19). Zum technischen Datenschutz gehört auch der Automatismus, der für die Pseudonymisierung und die Löschung der Flugpassagierdaten vorgesehen ist.

Die nationale Stelle, die Daten nach dem Flugpassagierdatengesetz bearbeitet, soll bei fedpol angesiedelt werden (Art. 19) und sich je hälftig aus Mitarbeitenden vom Bund und von den Kantonen zusammensetzen (Art. 20).

3.2 Abstimmung von Aufgabe und Finanzen

Der Schaden, den (Schwerst-)Kriminalität bei Betroffenen und volkswirtschaftlich verursacht, ist immens. Die Aufklärung solcher Straftaten und die Verurteilung ihrer Täter sind zentrale Elemente, die in einem Rechtsstaat eng mit Gerechtigkeit gekoppelt sind. Für Opfer sind sie vielfach Voraussetzung für einen Neubeginn.

Noch wichtiger ist die Verhinderung solcher Straftaten. Sicherheit ist ein entscheidendes Gut, damit sich eine Gesellschaft zum Wohle aller entwickeln und Wohlstand erfahren kann.

PNR leistet einen wichtigen Beitrag dazu.

35 Bericht der Kommission an das Europäische Parlament und den Rat über die gemeinsame Evaluierung des Abkommens 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, COM/2021/18 final, S. 9

PNR ermöglicht nicht nur, Schwerstkriminelle effizienter zu verfolgen und die Strafverfolgungsbehörden gezielt zu entlasten. PNR leistet auch einen wichtigen Beitrag dazu, die Planung von schweren Straftaten frühzeitig zu erkennen und ihre Begehung zu verhindern.

- Strafverfolgungsbehörden müssen heute Reiserouten von Schwerstkriminellen im internationalen Luftverkehr zeitaufwändig bei den einzelnen Luftverkehrsunternehmen gezielt erfragen. Wichtige Bezüge organisiert tätiger Krimineller bleiben dabei nicht selten unentdeckt. PNR ermöglicht den Strafverfolgungsbehörden, auf kompakte Datenpakete, die sogenannten PNR-Datensätze, zurückzugreifen, die systematisch erhoben und zentral gespeichert werden. Die PNR-Datensätze zeigen nicht nur Reiserouten auf, sondern können auch Aufschluss geben, wer mit wem wie oft wohin reist. PNR trägt massgeblich dazu bei, dass die Strafverfolgungsbehörden einfacher und schneller an wichtige Informationen über Verdächtige, ihre Reisegewohnheiten und Verbindungsleute gelangen.
- Kriminalität folgt oft gewissen Verhaltensmustern. Diese lassen sich mit PNR einfacher feststellen. Geplante Straftaten können damit frühzeitig erkannt und verhindert werden.

PNR macht sich Daten zunutze, die bei der Buchung von Flugreisen anfallen. Der Aufwand, den Luftverkehrsunternehmen mit PNR zu leisten haben, beschränkt sich auf die Übermittlung dieser Daten an die staatliche Stelle. PNR verlangt von den Luftverkehrsunternehmen keinen erheblichen Mehraufwand. Deshalb kann es als effizientes Instrument bezeichnet werden. PNR ist aber auch effektiv. Anders lässt sich nicht erklären, warum dieses Mittel seit rund 20 Jahren und mittlerweile in über 60 Staaten, darunter den USA, Kanada, Australien, dem Vereinigten Königreich und den EU-Mitgliedstaaten zur Bekämpfung terroristischer und anderer schwerer Straftaten eingesetzt wird.

Für die Einführung von PNR in der Schweiz ist mit wiederkehrenden Aufwendungen zu rechnen, die sich in der Hauptsache auf die Bearbeitung der Daten der Luftverkehrsunternehmen beschränken. Die Ergebnisse der Datenbearbeitung stehen insbesondere den Strafverfolgungsbehörden von Bund und Kantonen zur Verfügung und erleichtern deren Aufgaben.

Es ist vorgesehen, dass die Kantone die Kosten für die Hälfte der Mitarbeitenden tragen, die sie ihrerseits in die PIU entsenden. Diese Kostenteilung wiederspiegelt, dass die Sicherheit des Landes und der Schutz der Bevölkerung eine gemeinsame Aufgabe von Bund und Kantonen sind. Da es sich bei PNR aber um ein kantons- und letztlich auch grenzüberschreitendes Vorhaben handelt, rechtfertigt es sich, dass der Bund allein für die übrigen Kosten aufkommt. Dazu gehören auch die Kosten für den Aufbau des erforderlichen Informationssystems.

3.3 Umsetzungsfragen

Neben den PNR-Daten, die der Bund bei Annahme des Flugpassagierdatengesetzes künftig erhalten würde, 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* des Ausländer- und Integrationsgesetz vom 16. Dezember 2005[36] (AIG) bearbeitet.

Gemäss den internationalen technischen Standards der ICAO, WZO und IATA ist für die Übermittlung von PNR- und API-Daten ein sogenanntes «single window» vorzusehen, also eine einzige Schnittstelle für die Übermittlung beider Datenkategorien. Damit soll den Luftverkehrsunternehmen unnötiger Aufwand erspart werden.

Dies bedeutet, dass bei der Umsetzung des PNR-Systems der Schweiz für die API- und die PNR-Daten auf technischer Ebene ein «single window» zu definieren sein wird. Damit können die Luftverkehrsunternehmen die Daten an eine einzige Schnittstelle liefern, welche sodann automatisch die Datenzuweisung an die PIU bzw. ans SEM vornimmt.

4 Erläuterungen zu einzelnen Artikeln

1. Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten

1. Abschnitt: Gegenstand

Art. 1 Gegenstand

Diese Bestimmung weist die wichtigsten Inhalte des Gesetzes aus. Neben der Bearbeitung und Analyse von Flugpassagierdaten sieht das Gesetz auch Pflichten von Luftverkehrsunternehmen vor. Diese Pflichten sind allerdings nicht neu; die Luftverkehrsunternehmen erfüllen sie seit Jahren zum Beispiel gegenüber den USA und Kanada und seit 2018 gegenüber den Mitgliedstaaten der EU. Neu ist lediglich, dass sie diese Pflichten auch gegenüber der Schweiz zu erfüllen haben.

Die Kategorien von *Flugpassagierdaten*, die bearbeitet werden sollen, finden sich im Anhang 1 des Flugpassagierdatengesetzes. Die 19 verschiedenen Daten-Kategorien entsprechen jenen der PNR-Richtlinie der EU. Die Flugpassagierdaten umfassen nur die Daten der Flugpassagiere, nicht aber die der Flugbesatzung. Zu den Flugpassagierdaten gehören auch Personendaten gemäss Artikel 5 Buchstabe a nDSG. Das Flugpassagierdatengesetz bildet die gesetzliche Grundlage für die Bearbeitung dieser Daten.

Die Bearbeitung soll nur zulässig sein, wenn es um die Bekämpfung von Straftaten geht, die eine besondere Schwere aufweisen und eine ernsthafte Gefährdung der öffentlichen Sicherheit darstellen. Um welche konkreten Tatbestände des Schweizerischen Strafgesetzbuches und des Nebenstrafrechts es dabei geht, bestimmt sich nach Artikel 6 Absätze 2 und 3.

36 SR **142.20**

Artikel 6 Absatz 3 nDSG verlangt, dass die betroffene Person über den Zweck der Datenbearbeitung informiert wird oder die Bearbeitung gesetzlich vorgesehen ist.[37] Deshalb haben die Luftverkehrsunternehmen die Flugpassagierinnen und –passagiere darüber zu informieren, dass ihre Daten nach dem vorliegenden Gesetz bearbeitet werden, um wirksam Terrorismus und andere schwere Straftaten zu bekämpfen (vgl. Art. 5).

Im geltenden Recht findet sich keine Definition der *Luftverkehrsunternehmen*. Deshalb werden sie in Art. 1 Buchstabe b näher umschrieben. Die Umschreibung orientiert sich an jener, die in Zusammenhang mit dem CO_2-Gesetz vom 25. September 2020 (Art. 2 Bst. i) entwickelt worden ist.[38] Für das Flugpassagierdatengesetz ist diese begriffliche Umschreibung notwendig, zumal die Luftverkehrsunternehmen durch dieses Gesetz verpflichtet werden. Luftverkehrsunternehmen haben die Flugpassagierdaten rechtzeitig bekanntzugeben (Art.4). Zudem haben sie ihre Passagiere über die Datenbearbeitung nach diesem Gesetz zu informieren (Art. 5). Pflichtverletzungen werden nach Artikel 23 sanktioniert.

Nicht als Luftverkehrsunternehmen gilt, was unter die sogenannte Leichtaviatik fällt. Dazu gehören Schul-, Übungs- und Kontrollflüge, Touristikflüge, Luftsport sowie Privatflüge.

2. Abschnitt: Pflichten der Luftverkehrsunternehmen

Art. 2 Übermittlung der Flugpassagierdaten an die PIU

Luftverkehrsunternehmen sind verpflichtet, der PIU bei Flügen ab der Schweiz und in die Schweiz die in Anhang 1 des Vorentwurfs aufgeführten Flugpassagierdaten zu übermitteln (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, selbst wenn sich der Flughafen auf einem Terrain befindet, das ausserhalb der Schweiz liegt. Gleiches gilt für Flüge, die entsprechend von dort ins Ausland starten.

Die Flugpassagierdaten sind der PIU zu zwei verschiedenen Zeitpunkten zu übermitteln: frühestens 48 bis spätestens 24 Stunden vor dem planmässigen Abflug sowie unmittelbar nach Abschluss des Boardings (Abs. 2). Die erste Datenübermittlung liefert zwar erst provisorische Angaben, erlaubt der PIU aber eine gewisse Vorlaufzeit bis zum Eintreffen des Fluges, was gerade bei kurzen Flügen von Bedeutung sein dürfte. Die zweite Übermittlung erlaubt die definitive Datenbekanntgabe zu allen sich an Board befindenden Flugpassagieren.

Die Luftverkehrsunternehmen dürfen der PIU keine besonders schützenswerten Personendaten[39] im Sinne von Artikel 5 nDSG übermitteln. Sollten dennoch

37 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz,
BBl **2017** 7025

38 https://www.bafu.admin.ch/dam/bafu/de/dokumente/klima/rechtliche-grundlagen/definition-luftverkehrsunternehmen.pdf.download.pdf

39 Erklärung siehe Glossar im Anhang

fälschlicherweise solche Daten übermittelt werden, sind sie bei Erkennen durch die PIU umgehend zu löschen (Abs. 3).

Die Datenlieferung kann entweder nach der PULL- und nach der PUSH-Methode erfolgen. Bei der PULL-Methode würde die PIU auf das Buchungssystem der Fluggesellschaften greifen, bei der PUSH-Methode lösen die Luftverkehrsunternehmen die Übermittlung selber aus. Die PUSH-Methode bietet ein höheres Datenschutzniveau und soll deshalb bei der Umsetzung des PNR-Systems in der Schweiz Anwendung finden. Dies wird mit dem Begriff der Datenübermittlung zum Ausdruck gebracht. Die Art und Weise der Übermittlung richtet sich im Übrigen nach den einschlägigen Standards der International Civil Aviation Organization (ICAO). Die ICAO hat diese PNR Reporting Standards im Auftrag des UNO-Sicherheitsrates zusammen mit der Weltzollorganisation (WZO) sowie mit Regierungen der Mitgliedstaaten, Fluggesellschaften und Dienstleistern entwickelt. Die Vorgaben sind für alle Mitgliedstaaten der ICAO – und damit auch für die Schweiz – verbindlich. Einer zusätzlichen Regelung auf Gesetzesstufe bedarf es somit nicht. Die laufende technologische Entwicklung macht es jedoch unerlässlich, technische Einzelheiten bei Bedarf präzisieren zu können. Absatz 4 berechtigt fedpol zum Erlass entsprechender Bestimmungen auf Verordnungsstufe (Abs. 4).

Art. 3 Übermittlung der Flugpassagierdaten an ausländische Behörden

Bereits heute liefern Luftverkehrsunternehmen Flugpassagierdaten an Staaten, die das Ziel von Flügen aus der Schweiz sind, so namentlich an die USA und an Kanada. In beiden Fällen bilden Abkommen mit der Schweiz die Grundlage der Datenbekanntgabe. Ein nächstes Abkommen ist mit der EU geplant.

Die Abkommen stellen sicher, dass die übermittelten Daten im Ausland einen vergleichbaren Schutz wie in der Schweiz erfahren. Zudem sichert sich die Schweiz mit den Abkommen auch ihr Gegenrecht auf den Erhalt der Flugpassagierdaten aus jenem Staat.

Art. 4 Sorgfaltspflicht

Die Flugverkehrsunternehmen haben der PIU die Daten *aller* Passagierinnen und Passagiere rechtzeitig (vgl. Art. 2 Abs. 2) und entsprechend den technischen Vorgaben (vgl. Art. 2 Abs. 4) zu übermitteln. Es wird erwartet, dass sie alle zumutbaren Massnahmen treffen, um dieser Pflicht nachzukommen. Andernfalls greifen die administrativen Sanktionsmöglichkeiten nach Artikel 23.

Flugpassagierdaten werden bei der Buchung eines Flugtickets grösstenteils manuell eingegeben – durch die Passagierin oder den Passagier oder durch eine Mitarbeiterin oder einen Mitarbeiter des Flughafens oder des Reisebüros. Entsprechend enthalten die PNR-Daten oft Fehler. Je mehr Fehler sich bei der Datenerhebung einschleichen oder gar bewusst eingebracht werden, desto mehr leidet die Nutzbarkeit von Flugpassagierdaten.

Es wäre indes unverhältnismässig, die Luftverkehrsunternehmen zu verpflichten, sämtliche Flugpassagierdaten auf ihre Richtigkeit hin zu kontrollieren. Weil die Qualität der Daten für eine erfolgreiche Bearbeitung nach dem vorliegenden Gesetz

aber entscheidend ist, sollen die Luftverkehrsunternehmen das Buchungssystem so gestalten, dass offensichtliche Falscheingaben (z.B. Vorname «Aaaaa» oder E-Mail-Adresse ohne @) vom System nicht akzeptiert werden. Solche Massnahmen gelten als zumutbar (vgl. Art. 23 Abs. 2 Bst. b).

Art. 5 Informationspflicht

Die Flugpassagiere sind von den Luftverkehrsunternehmen schriftlich darüber zu informieren, dass ihre Daten nicht lediglich für die Abwicklung ihrer Flugreise, sondern zusätzlich auch nach dem Flugpassagierdatengesetz bearbeitet werden. Die Information kann in den allgemeinen Geschäftsbedingungen der Luftverkehrsunternehmen Eingang finden.

Die Informationspflicht gemäss Artikel 5 rechtfertigt sich, auch wenn damit wiederholt wird, was bereits nach Art. 20 Abs. 1 Bst. b nDSG gilt. Die Wiederholung rechtfertigt sich insbesondere deshalb, weil die Bearbeitung der Flugpassagierdaten

- in zwei vollständig verschiedenen tatsächlichen und rechtlichen Kontexten (technische Abwicklung Flugbuchung / Umsetzung Flugpassagierdaten-gesetz),
- zu unterschiedlichen Zwecken (Flugbuchung / Verbrechensbekämpfung) und
- unter unterschiedlicher Verantwortung (Luftverkehrsunternehmen / fedpol)

erfolgt.

Die Information umfasst nicht nur den Sachverhalt, dass die Daten an die PIU übermittelt werden. Auch der Zweck der Datenbearbeitung muss aus der Information erkennbar sein (vgl. Art. 6 Abs. 3 nDSG). Weitere Einzelheiten, über welche die betroffenen Personen zu informieren sind, werden sich aus der Verordnung zum nDSG ergeben.

3. Abschnitt: Datenbearbeitung

Art. 6 Grundsätze

Die Datenbearbeitung soll nur zulässig sein, wenn es um die Bekämpfung von Straftaten geht, die eine besondere Schwere erreichen und eine ernsthafte Gefährdung der öffentlichen Sicherheit darstellen. Um welche konkreten Tatbestände des Schweizerischen Strafgesetzbuches und des Nebenstrafrechts es dabei geht, bestimmt sich nach Absatz 3.

Die *terroristischen und anderen schweren Straftaten* werden in den Absätzen 2 und 3 umschrieben, ohne diese jedoch konkret zu nennen. Unterschieden werden zwei verschiedene Typen von Straftaten: Die terroristischen und die anderen schweren Straftaten.

Als *terroristisch* im Sinne des Flugpassagierdatengesetzes gelten – unabhängig vom Strafmass – alle Straftaten, die unter die Tatbestände nach Ziffer 22 des Anhangs 1 des SIaG fallen. Die terroristischen Straftaten sind im Anhang 1 zum vorliegenden Bericht ausgewiesen.

Die meisten dieser Straftaten sind Verbrechen und damit mit einer maximalen Freiheitsstrafe von mehr als drei Jahren bedroht (Art. 10 Abs. 2 StGB). Dagegen handelt es sich bei den nachfolgenden Straftatbeständen um Vergehen nach Artikel 10 Abs. 3 StGB.

- Schreckung der Bevölkerung (Art. 258 StGB),
- Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit (Art. 259 StGB),
- Landfriedensbruch (Art. 260 Abs. 1 StGB),
- Rechtswidrige Vereinigung (Art. 275ter StGB).

Sie fallen nur dann in die Kategorie der terroristischen Straftaten, wenn sie auch terroristisch motiviert sind.

Als *schwer* im Sinne des Flugpassagierdatengesetzes gelten zwei Kategorien von Straftaten: einerseits die übrigen Verbrechen gemäss Anhang 1 des SIaG, soweit sich diese einer Deliktkategorie nach der PNR-Richtlinie der EU (vgl. Anhang 2 des Gesetzes) zuordnen lassen, anderseits die Straftaten, die in die Strafverfolgungskompetenz des Bundesamtes für Zoll und Grenzsicherheit (BAZG) fallen und eine Höchststrafe von mindestens drei Jahren vorsehen.

Sowohl die terroristischen wie auch die schweren Straftaten sind gesetzlich bestimmt. In Anhang 2 sind die PNR-Deliktkategorien den entsprechenden Kategorien nach Anhang 1 des SIaG gegenübergestellt. Damit lässt sich nachvollziehen, welche Verbrechen nach dem SIaG-Deliktkatalog als schwere Straftaten gemäss Artikel 6 Abs. 3 Buchstabe a zu gelten haben. Insofern lässt sich zweifelsfrei feststellen, ob ein Verbrechen nach SIaG unter den PNR-Deliktkatalog fällt und damit zur Bearbeitung der Flugpassagierdaten legitimiert.

Trotz ihrer gesetzlichen Bestimmheit sollen dagegen die Straftaten nach Absatz 3 Buchstabe b, die in die Strafverfolgungskompetenz des BAZG fallen, in einer Verordnung ausgewiesen werden. Dieser deklaratorische Ausweis dient der Rechtssicherheit und Transparenz (Abs. 4). Diese Lösung erleichtert allfällige Anpassungen namentlich des Nebenstrafrechts.

Eine aktuelle Übersicht aller massgeblichen Straftaten findet sich im Anhang zum vorliegenden Bericht.

Die Ergebnisse von Bearbeitungen von Flugpassagierdaten, durch die sich andere als die genannten Straftaten verhindern, aufdecken oder verfolgen liessen, sind umgehend zu löschen.

Diese Verpflichtung gilt auch für den Nachrichtendienst des Bundes (NDB). Denn auch er kann Flugpassagierdaten zur Bekämpfung terroristischer und anderer schwerer Straftaten bearbeiten, allerdings nur, wenn diese Bearbeitung zusätzlich der Erfüllung seiner Aufgaben nach Artikel 6 Absatz 1 Buchstabe a Ziffern 1 sowie 3–5 des Nachrichtendienstgesetzes[40] dient.

Die PIU darf nur eingeschränkt besonders schützenswerte Personendaten bearbeiten. Die Luftverkehrsunternehmen dürfen ihr keine solchen Daten liefern (vgl. Art. 2 Abs. 3). Erhält die PIU von ihnen dennoch solche Daten, muss sie diese umgehend löschen.

40 SR **121**

Besonders schützenswerte Personendaten können indes anfallen, wenn die Flugpassagierdaten mit Informationssystemen abgeglichen werden oder wenn die PIU auf solche Systeme zugreift (vgl. Art. 7). Denkbar ist zudem, dass besonders schützenswerte Personendaten bei der Erstellung von Risikoprofilen und Beobachtungslisten auf Antrag einer Behörde zum Zug kommen könnten. Deshalb soll in Artikel 6 Absatz 5 als weiterer Grundsatz festgelegt werden, dass die PIU lediglich die folgenden besonders schützenswerten Personendaten bearbeiten darf:

- biometrische Daten[41], die eine natürliche Person eindeutig identifizieren;
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen.

Erhält die PIU andere besonders schützenswerten Daten, muss sie diese umgehend löschen. Dieser Grundsatz gilt für alle Aufgaben, welche die PIU nach diesem Gesetz wahrnimmt.

Art. 7 Datenabgleich mit Informationssystemen

Die Flugpassagierdaten werden, sobald sie im PNR-Informationssystem eintreffen, automatisch mit verschiedenen Polizeiinformationssystemen abgeglichen (Abs. 1).

Das Gesetz nennt keine spezifischen Technologien, sondern den Zweck des Abgleichs. Die technologieneutrale Formulierung stellt sicher, dass die fraglichen Informationssysteme abgelöst werden können, ohne dass jeweils eine Revision der gesetzlichen Bestimmung erforderlich ist. Neben diesem Vorteil trägt die Technologieneutralität auch zu einer erhöhten Aussagekraft der Regelung bei und grenzt den Abgleich auf das Erforderliche ein. Damit überzeugt die Technologieneutralität auch aus Sicht des Datenschutzes.

Der automatische Abgleich dient der ersten Identifikation, Lokalisierung und allenfalls der Verhaftung von Personen, die auf dem Luftweg in die Schweiz reisen oder aus der Schweiz ausreisen und national oder international in Zusammenhang mit terroristischen oder anderen schweren Straftaten (Art. 6 Abs. 2 und 3) gesucht werden. Daneben kann der automatische Abgleich auch nützliche Informationen in Zusammenhang mit bisher ungeklärten Straftaten liefern. Übereinstimmungen, die ausserhalb des gesetzlich definierten Zweckes liegen, sind umgehend zu löschen (vgl. Art. 6 Abs. 5).

Der automatische Abgleich aller Flugpassagierdaten erfolgt mit den folgenden Polizeiinformationssystemen:

- dem automatisierten Personen- und Sachfahndungssystem (Art. 15 BPI);
- dem nationalen Teil des Schengener Informationssystems (Art. 16 BPI);
- dem Informationssystem der Bundeskriminalpolizei (Art. 10 und 11 BPI)[42];
- dem Informatisierten Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (Art. 18 BPI).

Das *automatisierte Personen- und Sachfahndungssystem (RIPOL)* enthält Angaben zu Personen, die zur Fahndung ausgeschrieben sind, Informationen zu ungeklärten

41 Erklärung siehe Glossar im Anhang
42 SR **361.2**

Straftaten, zu an einer Straftat beteiligten Personen, zu Inhabern von Ausweisen verdächtiger Herkunft sowie weitere zur Aufklärung von Straftaten dienende Informationen. Es unterstützt die zuständigen Behörden von Bund und Kantonen namentlich bei der Verhaftung von Personen und bei der Abwehr von Gefahren für die öffentliche Sicherheit. Der Abgleich der Flugpassagierdaten mit RIPOL kann nicht nur zu Fahndungserfolgen beitragen, sondern auch zu Fortschritten bei ungeklärten terroristischen und anderen schweren Straftaten im Sinne dieses Vorentwurfs. Wer berechtigt zum Abgleich mit dem RIPOL ist, erhält automatisch auch Übereinstimmungen mit der Interpol-Datenbank Automated Search Facility (ASF) gemeldet. Diese Datenbank enthält Informationen zu Personen, gestohlenen Fahrzeugen sowie zu gestohlenen oder verlorenen Identifikationsdokumenten.

Das *Schengener Informationssystems (SIS)* enthält Personen- und Sachausschreibungen (z.B. zu gestohlenen Ausweisdokumenten), welche innerhalb des Schengen-Raums gesucht werden. Der Abgleich der Flugpassagierdaten mit SIS kann zur Verhaftung von Personen führen, die international gesucht und sodann ausgeliefert werden sollen, im Rahmen eines Strafverfahrens vor Gericht erscheinen müssen oder verdeckt registriert sind, weil davon ausgegangen wird, dass sie eine schwere Straftat begangen haben.

Anders als RIPOL und SIS enthalten die nachfolgenden zwei Informationssysteme auch Angaben zu laufenden Ermittlungen von Bund und Kantonen. Deshalb sollen auch sie zum automatischen Abgleich mit den Flugpassagierdaten herangezogen werden:

Das *Informationssystem der Bundeskriminalpolizei* (JANUS) umfasst Informationen zu gerichtspolizeilichen Ermittlungen des Bundes sowie zu Vorermittlungen und gerichtspolizeilichen Ermittlungen der Kantone (Art. 10 BPI). Von Bedeutung sind zudem die Informationen zur Zusammenarbeit der Bundeskriminalpolizei mit Strafverfolgungsbehörden und Kriminalpolizeien der Kantone sowie mit ausländischen Behörden im Kampf gegen internationale und organisierte Kriminalität (Art. 11 BPI).

Das *Informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (IPAS)* enthält Informationen zu laufenden gerichtspolizeilichen Ermittlungen und zu präventiver polizeilicher Tätigkeit von in- oder ausländischen Strafverfolgungs- und Polizeibehörden, namentlich auch der Bundeskriminalpolizei (BKP) oder der zuständigen Stelle bei Interpol.

Übereinstimmungen («Treffer»), die mit dem automatischen Abgleich erzielt werden, sind sodann von der PIU einzeln manuell zu überprüfen, bevor sie der zuständigen Behörde bekanntgegeben werden können (Abs. 3). Damit soll insbesondere verhindert werden, dass Übereinstimmungen bekanntgegeben werden und zu Massnahmen veranlassen, die aufgrund einer gewollten oder ungewollten fehlerhaften Erfassung der Flugpassagierdaten eingetreten sind. Die Pflicht zur Überprüfung ergibt sich auch aus Artikel 6 Absatz 5 des nDSG, wonach sich der Richtigkeit der Daten zu vergewissern hat, wer solche bearbeitet.

Trotz der manuellen Überprüfung können oft nicht alle Fragen geklärt und namentlich auch Zweifel an der Identität der Person nicht vollständig ausgeräumt werden.

Fragen aufwerfen können zudem die Ausschreibungsgründe. Denn Flugpassagierdaten dürfen nur bearbeitet werden, wenn dies der Bekämpfung terroristischer und anderer schwerer Straftaten dient. Ob es bei einer erzielten Übereinstimmung um eine solche Tat geht, lässt sich nur beurteilen, wenn die Straftatbestände bekannt sind oder aufgrund von Hintergrundinformationen aus Datenbanken als vorliegend betrachtet werden können. Anders als RIPOL, aus dem Einzelheiten zur Tat sowie der Tatbestand ersichtlich sind, liefern Treffer, die ein Abgleich mit SIS bringt, lediglich Deliktskategorien (z.B. «Tötung»), nicht jedoch den Sachverhalt und den fraglichen Tatbestand. Dies muss durch Zugriff auf weitere Informationssysteme in Erfahrung gebracht werden. Andernfalls ist der Treffer mangels hinreichender Rückschlüsse auf eine terroristische oder andere schwere Straftat zu löschen. Zu löschen ist er im Übrigen auch, wenn sich hinter der Ausschreibung im SIS ein Straftatbestand herausstellt, der nicht im PNR-Deliktkatalog enthalten ist.

Die Zugriffe im Rahmen der Plausibilisierung ermöglichen, die im ersten Abgleich erzielten Übereinstimmungen hinsichtlich Identität der Person und Ausschreibungsgrund zu verifizieren. Damit wird sichergestellt, dass die Bearbeitung der Flugpassagierdaten im Rahmen des gesetzlichen Zwecks erfolgt und die richtigen Personen an die zuständigen Strafverfolgungsbehörden und den NDB gemeldet werden.

Zur Plausibilisierung der Identität einer Person sowie der Ausschreibungsgründe soll nach dem automatischen Abgleich manuell auf die folgenden Informationssysteme zugegriffen werden können:

a) zur Plausibilisierung der Identität einer Person:

- ZEMIS (BGIAA)[43]: Das Zentrale Migrationsinformationssystem enthält Daten zur Identität der registrierten Personen (z.B. Name, Vorname, Geburtsdatum) und liefert Angaben zum Aufenthaltsstatus von Ausländerinnen und Ausländern, die sich in der Schweiz aufhalten.
- ORBIS (Art. 109c lit. f AIG): Das nationale Visumsystem liefert Angaben zu Visumsgesuchen und Zugang zu allen Personen, die über ein Visum für den Schengen-Raum verfügen. Eine Person kann beispielsweise anhand der überprüfbaren Passnummer identifiziert werden.

b) zur Plausibilisierung der Ausschreibungsgründe:

- Nationaler Polizeiindex (Art. 17 BPI)[44]: Er gibt Informationen über Meldungen der Kantone.
- SIRENE-IT (Art. 5 N-SIS-Verordnung vom 8. März 2013)[45]: Mit Zugriff auf dieses Informationssystem kann anhand von zusätzlichen Hintergrundinformationen eine Ausschreibung im Schengen-Informationssystem im Bereich der organisierten Kriminalität und des Terrorismus einem konkreten Straftatbestand zugeordnet werden.

43 SR **142.51**
44 SR **361.4**
45

- I-24/7 (Art. 352 Abs. 1 StGB): Enthält Informationen, die Rückschlüsse auf die Gründe internationaler Ausschreibungen (Interpol) ermöglichen.
- Informationssystem des BAZG: Es enthält insbesondere relevante Angaben zu den Straftatbeständen in der Strafverfolgungskompetenz dieser Behörde.

Manuell zugegriffen werden muss allenfalls auch auf jene Informationssysteme, mit denen der automatische Abgleich gemacht wurde, so nicht nur zur Plausibilisierung des Ausschreibungsgrundes, sondern auch, um die zuständige Behörde nach Artikel 8 zu eruieren, der die positiv geprüfte Übereinstimmung zu übermitteln ist.

Das zweistufige Vorgehen ermöglicht, dass die Daten so wenig wie möglich bearbeitet werden. Denn ihre Bearbeitung nach dem automatischen Abgleich nach Absatz 1 beschränkt sich nur noch auf jene Daten, die mit einem ersten Verdacht behaftet sind. Nach dem Zugriff gemäss Absatz 3 reduziert sich die Zahl der weiterbearbeiteten Daten auf jene, bei denen sich der erste Verdacht aufgrund der manuellen Überprüfung bestätigt hat. Die übrigen Daten sind davon nicht mehr betroffen.

Der automatische Abgleich und der manuelle Zugriff auf die jeweiligen Systeme bedingt Anpassungen des AIG (ORBIS), des BPI (RIPOL, JANUS, Nationaler Polizeiindex) sowie des Bundesgesetzes vom 20. Juni 2003[46] über das Informationssystem für den Ausländer- und den Asylbereich (ZEMIS). Sie sind in Anhang 3 des Flugpassagierdatengesetzes ausgewiesen. Aufgrund der laufenden Revision der Zollgesetzgebung wird die allenfalls notwendige gesetzliche Grundlage für den manuellen Zugriff auf das Informationssystem des BAZG erst in der Botschaft ausgewiesen.

Artikel 8 Übermittlung

Empfänger von Übermittlungen überprüfter Übereinstimmungen können die Strafverfolgungsbehörden von Bund und Kantonen sowie der NDB sein. Zu den Strafverfolgungsbehörden des Bundes gehören auch das Kommissariat der Sicherheitsbeauftragten Luftverkehr (SIBEL) im Bundessicherheitsdienst (Art. 4 Bst. b Strafbehördenorganisationsgesetz, StBOG[47]) sowie das Bundesamt für Zoll und Grenzsicherheit (Art. 4 Bst. c StBOG).

Die PIU übermittelt die nach Artikel 7 Absatz 3 überprüften Übereinstimmungen jener Behörde, welche

- für die Ausschreibung verantwortlich ist, welche die Übereinstimmung ausgelöst hat oder
- (im Falle von Ausschreibungen eines anderen Staates) entscheiden muss, ob und wenn ja, welche Massnahmen gestützt auf die Übermittlung der PIU zu treffen sind.

46 SR **142.51**
47 SR **173.71**

Art. 9 Datenabgleich mit Risikoprofilen und Beobachtungslisten

Die PIU soll Risikoprofile und Beobachtungslisten zur Bearbeitung der Flugpassagierdaten erstellen können (Abs. 1). Damit der Einsatz dieser Instrumente erfolgreich ist, sind spezifisches Fachwissen, Erfahrungswerte und Hintergrundinformationen unabdingbar. Dies wird gewährleistet, indem

- sich die PIU aus Mitarbeitenden zusammensetzt, die über Fachwissen aus relevanten Behörden von Bund und Kantonen verfügen (siehe Erläuterungen zu Art. 20),
- die Strafverfolgungsbehörden von Bund und Kantonen sowie der NDB Risikoprofile und Beobachtungslisten beantragen können (Abs. 1).

Absatz 2 bildet die gesetzliche Grundlage, damit die PIU die Flugpassagierdaten mit den Risikoprofilen und den Beobachtungslisten abgleichen kann.

Gegenstand von Risikoprofilen und Beobachtungslisten können nur Angaben sein, die sich einer Datenkategorie nach Anhang 1 des Gesetzes zuordnen lassen. Damit ist denn auch ausgeschlossen, dass besonders schützenswerte Personendaten wie beispielsweise die Ethnie oder die Religionszugehörigkeit eingesetzt werden können (vgl. Art. 2 Abs. 3).

Risikoprofile beschreiben Datenmuster, welche erfahrungsgemäss bei kriminellen Aktivitäten im Zusammenhang mit terroristischen oder anderen schweren Straftaten vorkommen. Die Risikoprofile sollen unterschiedliche Straftaten abdecken, die im Deliktkatalog aufgeführt sind. Allerdings dürfen sich die Risikoprofile nur aus solchen Datenkategorien zusammensetzen, die im Anhang 1 dieses Vorentwurfs als Flugpassagierdaten ausgewiesen sind (Abs. 3).

Beobachtungslisten setzen sich aus bereits bekannten, einer Datenkategorie nach Anhang 1 des Gesetzes zuordenbaren Informationen über Personen oder Organisationen zusammen, die im Verdacht stehen, terroristische oder andere schwere Straftaten begangen zu haben oder solche zu planen. Indem die Flugpassagierdaten mit den Beobachtungslisten abgeglichen werden, kann zum Beispiel nach bestimmten E-Mail-Adressen, Telefonnummern oder Kreditkarten-Nummern gesucht werden, um noch unbekannte Zusammenhänge und Beziehungen zu Personen aufzudecken, die im Verdacht stehen, terroristische oder andere schwere Straftaten begangen zu haben. So lassen sich insbesondere Verbindungspersonen von bereits bekannten Straftätern oder Mitglieder krimineller Organisationen identifizieren (Abs. 4).

Risikoprofile und Beobachtungslisten sollen regelmässig auf ihre Begründetheit und Effektivität überprüft werden (Abs. 5). Inhalte, die diesen Erfordernissen nicht mehr genügen, werden von der PIU gelöscht.

Die Einzelheiten der Überprüfung, namentlich die Zuständigkeit und die Periodizität, soll der Bundesrat in einer Verordnung festlegen (Abs. 6 Bst. a). Damit lässt sich gezielter den Erfahrungen entsprechen, die in Zukunft mit diesen Instrumenten bei der Bearbeitung von Flugpassagierdaten gemacht werden.

Ebenfalls in einer Verordnung soll der Bundesrat festlegen können, für welche Straftaten innerhalb des für die Bearbeitung von Flugpassagierdaten massgebenden Deliktkatalogs Beobachtungslisten eingesetzt werden dürfen. Dabei wird der Fokus

auf terroristischen Straftaten sowie Straftaten des organisierten Verbrechens zu legen sein.

Art. 10 Zusammenarbeit mit dem NDB

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

Deshalb soll der NDB die Flugpassagierdaten zur Erfüllung seiner Aufgaben selbständig bearbeiten können. Allerdings soll die selbständige Bearbeitung von Flugpassagierdaten stark eingeschränkt zulässig sein. So ist nicht vorgesehen, dass ihm ein direkter Zugriff auf das PNR-Informationssystem eingeräumt wird. Vielmehr soll die PIU ihm die Daten im automatisierten Verfahren elektronisch übermitteln, wie dies Artikel 104b des Ausländer- und Integrationsgesetzes für die API-Daten vorsieht. Die automatische Übermittlung ist auch angesichts des Datenvolumens angezeigt. Gegenstand der Übermittlung sind Flugpassagierdaten von Abgangs- und Zielflughäfen, die der NDB aufgrund einer eigenen Risikoeinschätzung im Voraus bestimmt hat. Dies erlaubt ihm, die Reisetätigkeit auf Strecken zu überwachen, die mit Sicherheitsrisiken behaftet sind.

Dieser Vorschlag orientiert sich an der Lösung, die in den Artikeln 104*a* und 104*b* des AIG für die Nutzung der API-Daten durch den NDB getroffen worden ist. In der Botschaft vom 3. März 2018[48] zur Revision des Ausländergesetzes (AuG) führte der Bundesrat dazu Folgendes aus:

«Die Geschäftsprüfungsdelegation (GPDel) hat gestützt auf einen internen Bericht und ein Gutachten des Eidgenössischen Datenschutz- und Öffentlichkeitsberaters (EDÖB) im Jahr 2015 die Nutzung der API-Daten ohne Abrufverfahren durch den NDB für rechtmässig erklärt. Mit der vorliegenden Revision soll aus Rechtssicherheitsgründen aber dennoch eine explizite Gesetzesgrundlage für die elektronische Weiterleitung der API-Daten geschaffen werden. Zudem soll neu auch der NDB beim SEM beantragen können, zur Abwehr von Bedrohungen für die innere und äussere Sicherheit, die von Terrorismus, verbotenem Nachrichtendienst und Proliferation ausgehen, die Meldepflicht der Luftfahrtunternehmen auf weitere Abflugorte auszudehnen».

Der NDB erfährt bei der Bearbeitung der Flugpassagierdaten eine weitere Einschränkung: so darf er die Flugpassagierdaten nur zur Bekämpfung jener terroristischen und anderen schweren Straftaten bearbeiten, die sich seinen Aufgaben nach Artikel 6 Absatz 1 Buchstabe a Ziffern 1 und 3–5 des NDG zuordnen lassen (Abs. 2). Die nachfolgende Tabelle weist aus, hinsichtlich welcher Straftatbestände dies der Fall ist. Straftaten nach der Kategorie 1 (Terrorismus) legitimieren im Übrigen nur dann zu einer Bearbeitung der Flugpassagierdaten, wenn sie terroristisch motiviert sind. Dies gilt überall dort, wo der Straftatbestand das terroristische Motiv nicht explizit voraussetzt, wie dies unter anderem beim Landfriedensbruch (Art. 260 StGB) der Fall ist.

48 BBl **2018** 1724

Art. 6 Abs. 1 Bst. a Ziff. 1 und 3–5 NDG	**Straftatbestände nach Art. 6 Abs. 2 und 3, für deren Bekämpfung eine Bearbeitung nach NDG zulässig ist**
Ziff. 1: Terrorismus	Schreckung der Bevölkerung, Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit, Landfriedensbruch, Strafbare Vorbereitungshandlungen, Kriminelle und terroristische Organisationen, Gefährdung der öffentlichen Sicherheit mit Waffen, Finanzierung des Terrorismus, Anwerbung, Ausbildung und Reisen im Hinblick auf eine terroristische Straftat, Rechtswidrige Vereinigung (Art. 258, 259, 260 Abs. 1, 260bis, 260ter, 260quater, 260quinquies, 260sexies, 275ter StGB)
	Organisationsverbot (Art. 74 Nachrichtendienstgesetz[49])
	Strafbestimmungen gemäss Bundesgesetz vom 12. Dezember 2014[50] über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen (Art. 2)
Ziff. 3: der Weiterverbreitung nuklearer, biologischer oder chemischer Waffen, einschliesslich ihrer Trägersysteme, sowie aller zur Herstellung dieser Waffen notwendigen zivil und militärisch verwendbaren Güter und Technologien (NBC-Proliferation) oder dem illegalen Handel mit radioaktiven Substanzen, Kriegsmaterial und anderen Rüstungsgütern,	Vergehen und Verbrechen gemäss Waffengesetz[51] (Art. 33 Abs. 3)
	Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht (Art. 224 Abs. 1 StGB)
	Herstellen, Verbergen, Weiterschaffen von Sprengstoffen und giftigen Gasen (Art. 226 StGB)
	Gefährdung durch Kernenergie, Radioaktivität und ionisierende Strahlen (Art. 226bis StGB)
	strafbare Vorbereitungshandlungen (Art. 226ter StGB)
	Missachtung von Sicherheits- und Sicherungsmassnahmen (Art. 88 Abs. 2 Kernenergiegesetz [KEG][52])
	Widerhandlungen bei nuklearen Gütern und Abfällen (89 Abs. 2 KEG)
Ziff. 4: Angriffen auf Informations-, Kommunikations-, Energie-, Transport- und weitere Infrastrukturen, die für das	Unbefugte Datenbeschaffung (Art. 143 StGB)
	Datenbeschädigung (Art. 144bis Abs. 3 StGB)

49 SR **121**
50 SR **122**
51 SR **514.54**
52 SR **732.1**

Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind (kritische Infrastrukturen),	Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 Abs. 1 und 2 StGB)
	Verursachen einer Überschwemmung oder eines Einsturzes (Art. 227 Ziff. 1 StGB)
	Beschädigung von elektrischen Anlagen, Wasserbauten und Schutzvorrichtungen (Art. 228 Ziff. 1 StGB)
	Sachbeschädigung (Art. 144 Abs. 3 StGB)
	Brandstiftung (Art. 221 Abs. 1 und 2 StGB)
	Verursachung einer Explosion (Art. 223 Ziff. 1 StGB)
Ziff. 5: gewalttätigem Extremismus	Sachbeschädigung (Art. 144 Abs. 3 StGB)
	Brandstiftung (Art. 221 Abs. 1 und 2 StGB)
	Verursachung einer Explosion (Art. 223 Ziff. 1 StGB)
	Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht (Art. 224 Abs. 1 StGB)
	Herstellen, Verbergen, Weiterschaffen von Sprengstoffen und giftigen Gasen (Art. 226 StGB)
	Verursachen einer Überschwemmung oder eines Einsturzes (Art. 227 Ziff. 1 StGB)
	Beschädigung von elektrischen Anlagen, Wasserbauten und Schutzvorrichtungen (Art. 228 Ziff. 1 StGB)
	Gefährdung der öffentlichen Sicherheit mit Waffen (Art. 260quater StGB)

Der NDB hat die Flugpassagierdaten innerhalb 96 Stunden nach ihrem Erhalt zu löschen (Abs. 3). Mit dieser Aufbewahrungsdauer entspricht das Gesetz einer geltenden Regelung des NDB für das Informationssystem «Restdatenspeicher». Die gleiche Regelung findet im Übrigen auch auf die ebenfalls automatisch an den NDB übermittelten API-Daten Anwendung.

Art. 11 Übermittlung von Flugpassagierdaten auf Antrag

Flugpassagierdaten können den Ermittlungen bei terroristischen und schweren Straftaten wesentlich zum Erfolg verhelfen. Sie sollen auch genutzt werden können, wenn es darum geht, Einzelheiten abzuklären. So soll es zulässig sein, dass die PIU auf Antrag gezielte Abfragen im Datenbestand des PNR-Informationssystems durchführt (Abs. 1).

Die anbegehrte Suchabfrage muss hinreichend konkret und damit eingegrenzt sein. Daneben muss der Antrag auch schlüssig darlegen, weshalb die gewünschten Daten für die Aufklärung oder Verhinderung einer terroristischen oder anderen schweren

Straftat notwendig sind. Generische Abfragen, die nicht spezifiziert sind und zu einer Vielzahl von unterschiedlichsten Suchergebnissen führen können, sind dagegen nicht zulässig. Entsprechenden Anträgen darf deshalb nicht Folge geleistet werden.

Dass neben den bereits in Artikel 8 erwähnten Behörden aus der Schweiz auch das Europäische Polizeiamt (Bst. c) als antragsberechtigt gilt, ohne dass die Datenbekanntgabe vom Vorliegen eines völkerrechtlichen Vertrags abhängig gemacht wird, erklärt sich insbesondere mit dem Abkommen, das die Schweiz mit dem Europäischen Polizeiamt (Europol) am 24. September 2004[53] abgeschlossen hat. Es regelt die Zusammenarbeit bei der Bekämpfung schwerwiegender Formen der internationalen Kriminalität. Der Datenaustausch zwischen der Schweiz und Europol ist nur dann zulässig, wenn es um Straftaten geht, die sowohl nach diesem Abkommen wie nach dem Flugpassagierdatengesetz bekämpft werden sollen. Ausgeschlossen ist demnach eine Datenübermittlung an Europol für alle Straftaten, die zwar im Abkommen genannt sind, jedoch nicht in den Anwendungsbereich des Flugpassagierdatengesetzes fallen.

Geht es dagegen um Straftaten, die zwar nicht unter das Abkommen fallen, aber terroristisch oder schwer im Sinne des Flugpassagierdatengesetzes sind, ist eine Datenübermittlung durch die PIU an Europol gestützt auf Artikel 16 Absatz 1 des nDSG zulässig, bestätigt doch der Bundesrat, dass alle Mitgliedstaaten der EU einen hinreichenden Datenschutz gewährleisten.[54] Dies gilt demnach auch für den Verbund der Mitgliedstaaten und damit für das Europäische Polizeiamt.

Art. 12 Meldung bei einem Verdacht

Der Einsatz von Risikoprofilen und Beobachtungslisten kann Rückschlüsse darauf geben, dass eine terroristische oder eine andere schwere Straftat begangen wurde, die Begehung einer solchen Straftat andauert oder aber geplant ist. Die Erkenntnisse, auf denen dieser Verdacht beruht, hat die PIU proaktiv den zuständigen Strafverfolgungsbehörden zu übermitteln. Allerdings soll diese Meldung nur dann erfolgen, wenn der Verdacht der PIU konkret ist. Konkret ist er, wenn er sich auf eine bestimmte Person bezieht und mehrere Indizien nahelegen, dass eine terroristische oder schwere Straftat begangen worden oder geplant ist.

Das weitere Vorgehen entscheiden die Strafverfolgungsbehörden, denen der konkrete Verdacht gemeldet worden ist.

Bei den besonders schützenswerten Personendaten, die gemäss Absatz 2 übermittelt werden dürfen, handelt es sich um biometrische Daten, die eine natürliche Person eindeutig identifizieren, sowie um Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen (vgl. Art. 6 Abs. 5). Andere besonders schützenswerte Personendaten dürfen von der PIU nicht bearbeitet und demnach auch nicht übermittelt werden.

53 SR **0.362.2**
54 https://www.edoeb.admin.ch>edoeb>2017/04

4. Abschnitt: PNR-Informationssystem

Art. 13

Das PNR-Informationssystem wird von der PIU betrieben.

Der Zugriff ist auf die Mitarbeitenden der PIU sowie auf die Personen begrenzt, für die ein Zugriff zur Erfüllung ihrer Wartungs-, Programmierungs- oder Aufsichtsaufgabe unverzichtbar ist.

5. Abschnitt: Datenschutz

Dass dem Datenschutz vorliegend ein so hohes Gewicht zukommen *muss*, erklärt sich damit, dass im Kampf gegen terroristische und schwere Straftaten auch Daten von Personen ohne jeglichen Bezug zu solchen Straftaten zur Bearbeitung herangezogen werden. Dies lässt sich jedoch ohne Infragestellung der gesetzlich festgelegten Zielsetzungen nicht vermeiden.

Gleiches gilt hinsichtlich der vergleichsweise langen Verfügbarkeit der Daten, die erst nach Ablauf von fünf Jahren gelöscht werden. Der Bericht der Europäischen Kommission vom 24. Juli 2020 über die Überprüfung der PNR-Richtlinie führt dazu aus:

«Die Untersuchung und Verfolgung solcher Straftaten erfordert in der Regel monate- und oft jahrelange Arbeit. Diesbezüglich haben die Mitgliedstaaten bestätigt, dass die fünfjährige Speicherfrist aus operativer Sicht notwendig ist. Durch die Verfügbarkeit historischer Daten wird sichergestellt, dass es möglich ist, das Reiseverhalten von Personen, die beschuldigt werden, ein schweres Verbrechen begangen zu haben oder an terroristischen Handlungen beteiligt gewesen zu sein, zu prüfen, etwaige Mitreisende zu ermitteln und potenzielle Komplizen oder andere Mitglieder einer kriminellen Gruppierung sowie potenzielle Opfer zu identifizieren.»[55]

Im Zeichen des Datenschutzes stehen nicht nur die in diesem Abschnitt vorgesehenen Bestimmungen, sondern insbesondere auch die Informationspflicht der Luftverkehrsunternehmen über die Datenbearbeitung nach diesem Gesetz (Art 5), die Zweistufigkeit des Datenabgleichs (Art. 7) sowie die Beschränkung völkerrechtlicher Verträge auf Staaten, die einen mit der Schweiz vergleichbaren Datenschutz gewährleisten (Art. 21).

Art. 14 Pseudonymisierung

Die Flugpassagierdaten enthalten mehrere Datenkategorien, die Rückschlüsse auf die Identität der betroffenen Person geben. Diese Daten sollen nach Ablauf von sechs Monaten seit ihrem Eingang im PNR-Informationssystem automatisch pseudonymisiert werden.

Dies gilt für folgende Elemente im Datensatz einer Person:

55 Bericht der 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

- Name(n) sowie Zahl und Namen der mitreisenden Personen;
- Adresse und Kontaktdaten (E-Mail, Telefon- und Handy-Nummern);
- alle Arten von Zahlungsinformationen einschließlich Rechnungsadresse;
- Vielflieger-Eintrag;
- allgemeine Hinweise, die zur unmittelbaren Feststellung der Identität des Fluggastes beitragen könnten, zu dem die PNR-Daten erstellt wurden,
- allenfalls erhobene API-Daten.

Diese Daten lassen sich somit nicht mehr mit der betroffenen Person in Verbindung bringen, sondern nur noch mit einem Pseudonym. Wer dies rückgängig machen möchte, benötigt die sicher aufbewahrte Konkordanztafel, auf der jedes der verwendeten Pseudonyme mit dem Namen der betroffenen Person verbunden ist.

Gemäss Botschaft zum neuen Datenschutzgesetz gilt die Pseudonymisierung als eine geeignete technische Massnahme, um die Datensicherheit (Art. 8 nDSG) zu gewährleisten.[56] In besagter Botschaft hält der Bundesrat zudem fest, 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 kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten.»[57]

Die Frist von sechs Monaten bis zur Pseudonymisierung entspricht der Lösung, die im Bundesgesetz vom 18. März 2016[58] betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) unter anderem für die Speicherung der Randdaten des Fernmeldeverkehrs (Art. 26 Abs. 5) gewählt worden ist. Auch dort handelt es sich um eine verdachtsunabhängige Speicherung von Daten, die einer bestimmten Person zuordenbar sind und nötigenfalls zu Zwecken der Verbrechensbekämpfung durch den Staat bearbeitet werden können, wie dies bei den Flugpassagierdaten der Fall ist.

Art. 15 Aufhebung der Pseudonymisierung

Wie der oben zitierte Bericht der Europäischen Kommission über die Überprüfung der PNR-Richtlinie deutlich zum Ausdruck bringt, erstrecken sich Ermittlungen bei terroristischen und anderen schweren Straftaten über mehrere Jahre. Dies bestätigen auch die Erfahrungen aus der Schweiz. Abfragen im PNR-Datenbestand müssen deshalb auch dann möglich sein, wenn die Daten älter als sechs Monate und damit pseudonymisiert sind. Solche historischen Suchanfragen setzen voraus, dass die Pseudonymisierung rückgängig gemacht werden kann.

Ein Antrag um Aufhebung der Pseudonymisierung ist bei der PIU einzureichen, die ihn bei hinreichender Begründung mit der eigenen Empfehlung ans

56 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 7031
57 BBl **2017** 7019
58 SR **780.1**

Bundesverwaltungsgericht weiterleitet (Abs. 2). Hinreichend begründet ist ein Antrag dann, wenn

- die Daten, deren Pseudonymisierung aufgehoben werden soll, bestimmt sind. Dies ist namentlich dann erfüllt, wenn sich die anbegehrte Aufhebung der Datenpseudonymisierung beispielsweise auf eine bestimmte Person oder einen bestimmten Flug bezieht.
- glaubhaft gemacht wird, dass die Aufhebung der Pseudonymisierung massgebliche Informationen zur erfolgreichen Verhinderung, Aufdecken, Ermitteln oder Verfolgen einer terroristischen oder anderen schweren Straftat liefert. Die erwarteten massgeblichen Informationen sind dabei möglichst genau zu umschreiben.

Fehlt im Antrag eine solche Begründung oder ist diese unzureichend, teilt die PIU dies der antragstellenden Behörde mit, die damit die Möglichkeit einer Nachbesserung hat.

Über eine allfällige Aufhebung der Pseudonymisierung soll das Bundesverwaltungsgericht innerhalb von fünf Arbeitstagen entscheiden (Abs. 4). Die Zuständigkeit eines Gerichts sehen grundsätzlich auch das deutsche[59] wie das österreichische[60] Recht in Umsetzung von Artikel 12 Absatz 3 der PNR-Richtlinie der EU vor.

Die dem Bundesverwaltungsgericht eingeräumte Frist beläuft sich auf maximal fünf Arbeitstage (Abs. 4). Diese Maximalfrist entbindet das Gericht jedoch nicht davon, bei Dringlichkeit umgehend zu entscheiden. Dringlichkeit ist namentlich dann gegeben, wenn beispielsweise ein terroristischer Anschlag droht.

Der technische Schlüssel zur Aufhebung der Pseudonymisierung befindet sich zugriffsgeschützt bei der PIU. Sie darf ihn nur einsetzen, wenn und soweit das Bundesverwaltungsgericht einen Antrag um Aufhebung der Pseudonymisierung gutheisst.

Die Bekanntgabe von Daten, die jünger als sechs Monate sind, richtet sich nach Artikel 11 und bedingt keine Mitwirkung des Bundesverwaltungsgerichts.

Art. 16 Aufbewahrungsdauer und Löschung

Die Flugpassagierdaten im PNR-Informationssystem werden fünf Jahre nach ihrem Eingang automatisch gelöscht (Abs.1).

Die fünfjährige Aufbewahrungsdauer gemäss Artikel 16 orientiert sich an der PNR-Richtlinie und gewährleistet damit die Kompatibilität des PNR-Systems der Schweiz mit den PNR-Systemen der EU-Mitgliedstaaten. Die Kompatibilität ist eine wichtige Voraussetzung für das Abkommen, das die Schweiz mit der EU über den gegenseitigen Austausch von Flugpassagierdaten abschliessen möchte.

59 Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG), § 5 Abs. 2, BGBl I 17s1484

60 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

Die verhältnismässig lange Aufbewahrungsdauer leitet sich primär aus der Nutzung der Flugpassagierdaten als Instrument zur Bekämpfung von terroristischen und anderen schweren Straftaten ab. Die Ermittlungen vieler dieser Straftaten ziehen sich oft über Jahre hin. Zeitaufwändig erweisen sich dabei insbesondere Ermittlungen, mit denen internationale Netzwerke aufgedeckt werden sollen. Anlässlich der Evaluation der PNR-Richtlinie durch die Europäische Kommission bestätigten die EU-Mitgliedstaaten, dass die in der PNR-Richtlinie vorgesehene Aufbewahrungsdauer der Daten aus operativer Sicht nötig sei. Darüber hinaus hätten sich die Regelungen des Zugangs von Behörden zu den bei der PNR-Zentralstelle gespeicherten Daten und deren Depersonalisierung (entspricht Pseudonymisierung nach Art. 14 des Vorentwurfs) als ausreichend erwiesen, um Missbräuche zu verhindern.[61]

Für die Schweiz stellt die lange Aufbewahrungsdauer von Daten, die in ihrer überwiegenden Zahl ohne Bezug zu einem Verdacht sind, einen Paradigmenwechsel dar. Dieser lässt sich nur mit dem übergeordneten Ziel rechtfertigen, dass der Schwerstkriminalität mit PNR national und international wirkungsvoll begegnet wird.

Wie lange Übereinstimmungen von Abgleichen nach den Artikeln 7 und 9 aufbewahrt werden dürfen, soll der Bundesrat in einer Verordnung regeln (Abs. 2). Damit lässt sich den verschiedenen Verfahren gerecht werden, in denen Behörden die mit einem bestätigten Verdacht behafteten Daten benötigen, so namentlich bei Ermittlungen oder in Strafverfahren.

Art. 17 Aufsicht

Amtsintern überwacht die Datenschutzstelle von fedpol, ob die datenschutzrelevanten Bestimmungen dieses Gesetzes sowie jene des Datenschutzgesetzes des Bundes eingehalten werden.

Von der Aufsicht erfasst ist sowohl die Datenbearbeitung durch die PIU wie auch die technische Seite des Datenschutzes, die durch das PNR-Informationssystem gewährleistet wird. Dazu gehören die automatische Pseudonymisierung der Daten nach sechs Monaten sowie die automatische Löschung nach Ablauf von fünf Jahren.

Trotz der Aufsichtsfunktion, welche die Datenschutzstelle von fedpol wahrnimmt, bleibt die Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemäss Artikel 4 des nDSG vorbehalten.

Art. 18 Auskunftsrecht

Eine Flugpassagierin oder ein Flugpassagier erhält durch die Information des Luftverkehrsunternehmens nach Artikel 5 Kenntnis davon, dass ihre/seine Passagierdaten nach diesem Gesetz bearbeitet werden. Ersuchen um Auskunftserteilung nach Artikel 18 des Flugpassagiergesetzes beziehungsweise nach den Artikeln 25-28 des nDSG sind an fedpol zu richten.

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

Mit Blick auf den Zweck der Datenbearbeitung versteht es sich, dass die Auskunft nicht immer oder nicht immer vollständig erteilt werden kann. Von diesem Recht wird fedpol gestützt auf Artikel 26 Absatz 2 Buchstabe b des nDSG Gebrauch machen müssen, wenn

- die Verweigerung der Auskunftserteilung im überwiegenden öffentlichen Interesse, insbesondere der inneren oder der äusseren Sicherheit der Schweiz, erfolgt oder
- die Auskunftserteilung eine Ermittlung, eine Untersuchung oder ein behördliches oder gerichtliches Verfahren gefährden kann.

Ausgeschlossen ist eine Auskunftserteilung auch dann, wenn die Daten bereits älter als sechs Monate und deshalb pseudonymisiert sind. Der Antrag auf Aufhebung der Pseudonymisierung steht gemäss Artikel 15 Absatz 1 nur den Strafverfolgungsbehörden und dem NDB zu.

Hat die PIU Daten der betroffenen Person an eine andere Behörde übermittelt, spricht sich fedpol mit dieser vor der Auskunftserteilung ab. Damit lässt sich sicherstellen, dass allfällige Gründe für eine Einschränkung des Auskunftsrechts nach Artikel 26 des nDSG zeitgerecht berücksichtigt werden können.

6. Abschnitt: Organisation und Personal der PIU

Art. 19 Organisation

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

Angesichts der Besonderheit der Flugpassagierdaten, deren Schutz es zu gewährleisten gilt, rechtfertigt es sich, dass die PIU organisatorisch von den Einheiten getrennt ist, die bei fedpol Ermittlungsaufgaben wahrnehmen. Für diese Einheiten gelten damit die gleichen Voraussetzungen, um Daten von der PIU zu erhalten, wie für die anderen Strafverfolgungsbehörden des Bundes sowie jene der Kantone.

Die PIU soll hinsichtlich PNR der Single Point of Contact (SPOC) für die Luftverkehrsunternehmen und ausländische Behörden sein. Ob ein 24/7-Dienst der PIU gewährleistet sein soll, ist noch offen. In der Schweiz gilt zwar ein Nachtflugverbot, Flugpassagierdaten werden aber auch in der Nacht von den Luftverkehrsunternehmen an die PIU übermittelt.

Art. 20 Personal

Die Bearbeitung von Flugpassagierdaten bietet sowohl für die Strafverfolgungsbehörden des Bundes, als auch für jene der Kantone einen grossen Mehrwert.

Die Strafverfolgung liegt aufgrund des föderalistischen Systems der Schweiz in mehrheitlich originärer 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[62]-, im Markenschutz[63]-, im Transplantations[64]- oder im Waffengesetz[65] gehören.

Insofern versteht sich die Bekämpfung von terroristischen und anderen schweren Straftaten als eine gemeinsame Aufgabe von Bund und Kantonen mit je spezifischen Schwerpunkten. Die PIU unterstützt die zuständigen Behörden dabei.

Für eine organisatorische Ansiedelung der PIU beim Bund spricht insbesondere der internationale Bezug der Aufgabenerfüllung, was aber nicht heissen darf, dass der Bund allein für die mit dieser neuen Aufgabe verbundenen Kosten aufzukommen hat. Bund und Kantone sollen je hälftig für die bei der PIU eingesetzten Mitarbeitenden aufkommen.

Vorgesehen ist ein Modell, wonach sowohl der Bund wie auch die Kantone Mitarbeitende für eine befristete Zeit in die PIU entsenden. Besondere Zusammenarbeitsmodelle wie hier vorgeschlagen finden sich heute bei den Polizei- und Kooperationszentren in Genf und Chiasso[66] sowie bei der Zeugenschutzstelle.

Die Grundlage für die Zusammenarbeit nach diesem Gesetz bilden einerseits dieses Gesetz und die dazugehörige Verordnung und anderseits eine Vereinbarung zwischen dem Bund und den Kantonen. Ob die Kantone ihre jeweilige Beteiligung im Rahmen eines Konkordats regeln, ist derzeit noch offen.

Der Basler-Kommentar zur Bundesverfassung[67] hält dazu 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 Rechtsgrundlage (…) kann der Vertrag mit den Kantonen abgeschlossen werden. »

Gegenstand des Vertrages zwischen Bund und Kantonen ist die Entsendung von Mitarbeitenden in den Dienst der PIU.

Aus dem Gesetz muss sich deshalb ergeben,

- zu welchem Zweck die Kantone Mitarbeitende entsenden
- in welchem Verhältnis sich Bund und Kantone an der personellen Ressourcierung der PIU beteiligen.

62 SR **732.1**
63 SR **232.11**
64 SR **810.21**
65 SR **514.54**
66 Siehe dazu: Vereinbarung vom 2. April 2014 über den nationalen Betrieb gemeinsamer Polizei- und Zollkooperationszentren (CCPD) in Genf und Chiasso, SR **360.4**
67 Schweizerisches Verfassungsrecht, 3.A., Basel 2016; Waldmann Bernhard /Belser Eva Maria / Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015, Art. 48 N 37

Die PIU setzt sich je hälftig aus Mitarbeitenden des Bundes und der Kantone zusammen (Absatz 1). Ihre Kosten trägt die entsendende Behörde (Absatz 4).

Ebenfalls aus dem Gesetz muss sich herleiten lassen, dass die Mitarbeitenden trotz ihres Einsatzes bei der PIU weiterhin bei der entsendenden Behörde angestellt sind, die vertraglich somit ihre Arbeitgeberin bleibt. Dies ergibt sich einerseits aus Absatz 2 (geteiltes Weisungsrecht) und anderseits aus dem bereits erwähnten Absatz 4.

Einer gesetzlichen Grundlage bedürfen auch die wichtigsten Abweichungen vom bisherigen Arbeitsverhältnis. Es sind dies

- das fachliche Weisungsrecht von fedpol (Abs. 2), welches dasjenige des vertraglichen Arbeitgebers für die Dauer des Einsatzes bei der PIU ablöst;
- die Pflicht der Mitarbeitenden zur Verschwiegenheit (Abs. 3), die auch gegenüber ihrem vertraglichen Arbeitgeber zu wahren ist.

Beim vertraglichen Arbeitgeber verbleiben das disziplinarische Weisungsrecht (Abs. 2) und die Pflicht zur Übernahme der Lohnkosten sowie allfälliger Spesen, Überzeitentschädigungen und Prämien. Für die Mitarbeitenden aus den Kantonen bestimmt sich die Höhe dieser Entschädigungen nach den für sie geltenden kantonalen Bestimmungen.

Ergänzend zu diesen gesetzlichen Bestimmungen kann der Bundesrat weitere Regelungen auf Verordnungsebene vorsehen (Abs. 5).

Unabhängig von diesem Gesetz gilt für die kantonalen Mitarbeitenden, die bei der PIU im Einsatz stehen, im Übrigen das Verantwortlichkeitsgesetz vom 14. März 1958 (VG)[68]. Dies folgt aus Artikel 1 Absatz 1 Buchstabe f des VG.

In der Vereinbarung mit den Kantonen ist namentlich festzuhalten, welche Qualifikationen von Mitarbeitenden erwartet werden, die zum Einsatz in die PIU zu entsenden sind. In Betracht fallen insbesondere Mitarbeitende, die über ausgewiesene Erfahrung in der Strafverfolgung verfügen.

Zudem wird zu vereinbaren sein, wie zu verfahren ist, wenn sich eine Mitarbeiterin oder ein Mitarbeiter

- als ungeeignet erweist;
- eines Verhaltens schuldig macht, das disziplinarrechtliche Massnahmen nach sich ziehen könnte.

Auch zu regeln ist das Verfahren bei Uneinigkeit zwischen fedpol und einem Kanton.

Gemäss Absatz 3 dürfen Mitarbeitende über Sachverhalte, von denen sie während ihres Einsatzes bei der PIU Kenntnis erhalten, ausserhalb der PIU nicht verfügen. Dies gilt auch nach Beendigung ihres Einsatzes. Damit wird der informelle Austausch von Inhalten, die dem Datenschutz unterstehen, 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

68 SR **170.32**

beispielsweise die Erfahrungen, wie Risikoprofile und Beobachtungslisten möglichst wirksam konzipiert und eingesetzt werden. Damit gewährleistet das Entsendemodell einen Kompetenztransfer von der PIU in die entsendenden Behörden.

7. Abschnitt: Abschluss von Verträgen und Vereinbarungen sowie Amtshilfe

Art. 21 Abschluss von Verträgen und Vereinbarungen

Das Flugpassagierdatengesetz sowie das Datenschutzgesetz entfalten nur für die Schweiz bindende Wirkung.

Soll die Übermittlung von Flugpassagierdaten aus der Schweiz an einen anderen Staat erfolgen, ist sicherzustellen, dass dessen nationales Recht einen mit der Schweiz vergleichbaren Schutz der bekanntgegebenen Daten gewährleistet. Aufschluss darüber, ob ein Staat diesen Schutz bietet, gibt die Staatenliste, die elektronisch abrufbar ist. [69]

Wird der Datenschutz als vergleichbar beurteilt, dürften Daten aus der Schweiz dem entsprechenden Staat auch ohne einen völkerrechtlichen Vertrag bekanntgegeben werden (Art. 16 Abs. 1 nDSG). Dennoch verlangt Artikel 21 in Absatz 1 des Flugpassagierdatengesetzes auch in diesen Fällen den Abschluss eines völkerrechtlichen Vertrages. Der Grund liegt darin, dass sich die Schweiz nur auf diesem Weg die Gegenseitigkeit der Datenübermittlung zur Bekämpfung von Terrorismus und anderen schweren Straftaten sichern kann und die Flugpassagierdaten jener Flüge erhält, die von diesem Staat in die Schweiz fliegen.

Mit Absatz 2 erhält das fedpol die Kompetenz, selbständig Vereinbarungen mit Behörden anderer Staaten abzuschliessen. Diese Kompetenz ist begrenzt auf operative, technische oder administrative Inhalte. Grundsätzliche Belange des Datenschutzes oder Rechte und Pflichten der Behörden sind dagegen immer in einem völkerrechtlichen Vertrag nach Absatz 1 durch den Bundesrat zu vereinbaren.

Art. 22 Amtshilfe

Die Amtshilfe, welche die PIU einer ausländischen PIU leistet, ohne dass ein völkerrechtlicher Vertrag die Datenbekanntgabe zwischen der Schweiz und diesem Staat näher regelt, ist auf begründete Ausnahmesituationen beschränkt. Unzulässig ist die Übermittlung von Flugpassagierdaten, wenn gegen die betreffende Person kein begründeter Verdacht vorliegt, eine terroristische oder andere schwere Straftat zu planen oder begangen zu haben.

Die Bekanntgabe ist auf die im Antrag der nachsuchenden PIU hinreichend zu konkretisierenden Daten beschränkt. Zudem müssen diese Daten unerlässlich zur Abwendung einer unmittelbaren Bedrohungssituation sein. Eine ähnliche Ausnahmeregelung sieht auch die PNR-Richtlinie (Art. 9 Abs. 1 und 2) vor.

Eine Aufhebung der Pseudonymisierung ist für die Amtshilfe nach dieser Bestimmung nicht zulässig.

69 https://www.edoeb.admin.ch>edoeb>2017/04

8. Abschnitt: Administrative Sanktionen

Art. 23 Pflichtverletzung durch Luftverkehrsunternehmen

Eine Verletzung der Sorgfalts- und der Informationspflicht nach den Artikeln 4 und 5 soll unabhängig von einem Verschuldensnachweis geahndet werden, wie dies seit dem 1. Oktober 2015 in Artikel 122b des AIG vorgesehen ist. Der Bundesrat begründete die Abkehr vom Verschuldensnachweis damals mit den umfangreichen Abklärungen, die auch im Ausland durchgeführt werden mussten. Faktisch hätte sich dieser Nachweis in der Praxis als unmöglich erwiesen.[70]

Pflichtverletzungen durch ein Luftverkehrsunternehmen werden beispielsweise vermutet, wenn dieses der PIU die Flugpassagierdaten

- nicht oder zu spät
- unter Nichtbeachtung technischer Vorgaben von fedpol oder
- nicht von allen Flugpassagierinnen und –passagieren

übermittelt.

Gleiches gilt, wenn

- sich übermittelte Daten als offenkundig falsch erweisen oder
- Flugpassagiere nicht oder nicht schriftlich über die Datenbearbeitung nach diesem Gesetz informiert werden (vgl. Art. 5).

Als schwer gilt eine Verletzung der Sorgfaltspflicht namentlich dann, wenn sie wiederholt festgestellt wird oder wenn die gesamten Datensätze eines Fluges nicht geliefert werden. Einer Nichtlieferung gleichzusetzen ist eine Datenübermittlung, wenn sich die übermittelten Daten in ihrer Mehrzahl als falsch erweisen.

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

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

Die Flugpassagierdaten dürften in der Hälfte der Fälle von einem Abflugort im Ausland geliefert werden. Absatz 5 stellt deshalb sicher, dass auch Sorgfaltspflichtverletzungen im Ausland geahndet werden können.

Art. 24 Verfahren

Wird eine Verletzung der Meldepflicht nach Artikel 122b des AIG mit einer Sanktion belegt, soll sie dafür nicht zusätzlich nach dem Flugpassagierdatengesetz sanktioniert werden. Verletzungen der Informationspflicht nach Art. 5 sind dagegen unabhängig

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

vom AIG sanktionierbar, da nur das Flugpassagierdatengesetz ihre Sanktionierung vorsieht, nicht aber das AIG.

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 jene Flugpassagierinnen und Flugpassagiere 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 werden. Die ursprünglich erhobenen Daten werden gesplittet.

Ein *Sharing* (Ziff. 15) liegt vor, wenn eine andere Fluggesellschaft als die durch die Flugnummer angeführte den Flug ausführt.

Anhang 2 Deliktkategorien nach Anhang II der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016

Als schwer im Sinne von Artikel 6 Absatz 3 Buchstabe a dieses Gesetzes gelten nur jene Straftaten nach Anhang 1 des Schengen-Informationsaustausch-Gesetzes (SIaG), die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind und sich einer PNR-Deliktkategorie nach Anhang 2 dieses Gesetzes zuordnen lassen.

In Anhang 2 sind die PNR-Deliktkategorien den entsprechenden Kategorien des Deliktkatalogs nach Anhang 1 des SIaG gegenübergestellt. Damit lässt sich nachvollziehen, welche Verbrechen nach dem SIaG-Deliktkatalog als schwere Straftaten gemäss Artikel 6 Abs. 3 Buchstabe a zu gelten haben.

Anhang 3 Änderung anderer Erlasse

1. Bundesgesetz vom 20. Juni 2003[71] über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA)

Art. 9 Abs. 1 Bst. c^{bis} Abrufverfahren

Weil der automatische Abgleich der Flugpassagierdaten mit verschiedenen Informationssystemen des Bundes in Artikel 7 des Vorentwurfs technologieneutral geregelt ist, ist die Berechtigung der PIU zum manuellen Zugriff auf ZEMIS vorliegend vorzusehen.

2. Ausländer- und Integrationsgesetz vom 16. Dezember 2005 (AIG)[72]

Art. 109c Bst. f Ziff. 1 Abfrage des nationalen Visumsystems

Weil der automatische Abgleich der Flugpassagierdaten mit verschiedenen Informationssystemen des Bundes in Artikel 7 des Vorentwurfs technologieneutral geregelt ist, ist die Berechtigung der PIU zum manuellen Zugriff auf ORBIS in Artikel 109c AIG vorzusehen.

71 SR **142.51**
72 SR **142.20**

3. Verwaltungsgerichtsgesetz vom 17. Juni 2005[73]

Art. *36c* *Einzelrichter oder Einzelrichterin*

Das Bundesverwaltungsgericht prüft als unabhängige Instanz, ob die Aufhebung der Pseudonymisierung nach Artikel 15 des Flugpassagierdatengesetzes erfolgen darf. Neben der Prüfung, ob der Antrag hinreichend begründet ist, gilt es die mit der Aufhebung der Pseudonymisierung verfolgten Sicherheitsinteressen gegenüber den Interessen am Schutz der Daten abzuwägen.

4. Bundesgesetz vom 13. Juni 2008[74] über die polizeilichen Informationssysteme des Bundes (BPI)

Art. 10 Abs. 4 bst. d System zur Unterstützung gerichtspolizeilicher Ermittlungen des Bundes

Art. 11 Abs. 2 Bst. b System Bundesdelikt

Weil der automatische Abgleich der Flugpassagierdaten mit verschiedenen Informationssystemen des Bundes in Artikel 7 des Vorentwurfs technologieneutral geregelt ist, ist die Berechtigung der PIU zum automatischen Abgleich und zum manuellen Zugriff auf JANUS in den Artikeln 10 und 11 BPI vorzusehen.

Art. 15 Abs. 6 Bst. a^{bis} Automatisiertes Polizeifahndungssystem

Weil der automatische Abgleich der Flugpassagierdaten mit verschiedenen Informationssystemen des Bundes in Artikel 7 des Vorentwurfs technologieneutral geregelt ist, ist die Berechtigung der PIU zum automatischen Abgleich und zum manuellen Zugriff auf RIPOL in Artikel 15 BPI vorzusehen.

Art. 17 Abs. Abs. 4 Bst. m Nationaler Polizeiindex

Weil der Zugriff auf verschiedene Informationssystemen des Bundes in Artikel 7 Absatz 3 des Vorentwurfs technologieneutral geregelt ist, ist die Berechtigung der PIU vorliegend einzufügen.

5. Luftfahrtgesetz vom 21. Dezember 1948[75]

Art. 29 Abs. 5

Luftverkehrsunternehmen sollen nicht weiterhin unbehelligt in der Schweiz starten und landen können, wenn sie wiederholt erfolglos aufgefordert worden sind, Sanktionen nach Artikel 26 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[76] über Schuldbetreibung und Konkurs [SchKG]).

Voraussetzungen für den Entzug der Betriebsbewilligung sind in diesem Falle:

73 SR **173.32**
74 SR **361**
75 SR **748.0**
76 SR **281.1**

- eine Sanktion nach Artikel 26 des Flugpassagierdatengesetzes ist in Rechtskraft erwachsen;
- ihre Bezahlung wurde wiederholt gefordert, 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.

5 Auswirkungen

5.1 Finanzielle und personelle Auswirkungen auf den Bund

Die Einführung eines nationalen PNR-Systems ist mit der Entwicklung und dem Betrieb eines technischen Informationssystems sowie dem Aufbau und der Organisation einer PIU ein komplexes Unterfangen, dessen Kosten in Projekt-, Betriebs- und Personalkosten gefasst werden können.

Projektkosten

Die Konzipierung, Entwicklung und Einführung eines PNR-Systems sowie der Aufbau einer PIU verursachen Projektkosten. Die Höhe dieser Kosten hängt davon ab, ob das PNR-System der UNO «goTravel» verwendet werden kann (Option 1) oder ein PNR-System gekauft oder selber entwickelt werden soll (Option 2). Die beiden Optionen haben einen Einfluss auf die Finanzierung des Projekts, nicht aber auf den Inhalt des Gesetzes.

- Option 1 – «UNO-Lösung goTravel» – ist das bestehende PNR-System der UNO. Es kann ohne grosse Anpassungen übernommen und sofort eingesetzt werden und ist bereits in verschiedenen Ländern in Gebrauch. Diese Option wird derzeit vom EJPD favorisiert. Zurzeit wird neben den technischen Möglichkeiten im sogenannten «Proof of Concept» (PoC) evaluiert, welche Anforderungen an ein Schweizer PNR-System erfüllt sind. Fehlende Funktionalitäten könnten zu einem späteren Zeitpunkt ergänzt werden. Die Projektkosten 2020-2025 für diese Option belaufen sich auf ca.11.6 Mio. Franken (davon 6.82 Mio. Franken finanzierungswirksame Ausgaben).
- Option 2 – «Kauf oder Eigenentwicklung PNR-Lösung» – deckt finanziell sowohl die (WTO)-Beschaffung und Anpassung eines bestehenden Systems auf dem Markt als auch die Eigenentwicklung eines Systems durch den Bund ab. Weil derzeit Option 1 favorisiert und eingehend geprüft wird, soll erst im Falle eines Verzichts darauf eingehender geprüft werden, welche käuflichen PNR-Systeme in Frage kommen oder ob ein System vom Bund selber gebaut werden soll. Die Projektkosten von 2020-2026 für diese Option belaufen sich auf ca. 22.5 Mio. Franken (davon 16.82 Mio. Franken finanzierungswirksame Ausgaben). Es müsste gemäss Artikel 21 des Finanzhaushaltgesetzes vom 7. Oktober 2005 (FHG) ein Verpflichtungskredit anbegehrt werden.

Im Mai 2022 wird die Evaluation des UNO-Systems abgeschlossen sein. Danach ist klar, ob das UNO-System in die IT-Umgebung des Bundes integriert werden kann. Ist

die Systemprüfung erfolgreich, wird entschieden, ob die favorisierte Option 1 oder Option 2 zum Tragen kommt. Ist die Evaluation nicht erfolgreich, muss von Option 1 abgesehen und Option 2 konkreter erarbeitet werden.

In der Botschaft wird der Kostenrahmen des Projekts PNR Schweiz detaillierter ausgewiesen werden können.

In jedem Fall wird mit der System-Entwicklung oder -Adaption erst begonnen, wenn die Inkraftsetzung der gesetzlichen Grundlage definitiv erwartet werden kann.

Betriebskosten PNR-Informationssystem und PIU ab 2025

Für den Betrieb des PNR-Informationssystems und der PIU-Infrastruktur fallen Kosten unter anderem für die Miete der Räumlichkeiten, für die Instandhaltung der IKT-Struktur (Hardware, Software, Netzwerk etc.), für das Mobiliar und allenfalls notwendige technische Geräte an sowie Abschreibungskosten und Kosten für Ersatzbeschaffungen.

Die konkreten Infrastruktur- und Betriebskosten werden im Verlauf des Projektes weiter ausgearbeitet werden.

Personalkosten

Der Personalbedarf der PIU hängt von der Betriebsform und der voraussichtlich etappenweise angebundenen Flugstrecken resp. der zu analysierenden Datenmenge ab. Derzeit wird von einem Personalbestand von 20 und nach vollem PIU-Ausbau 30 Vollzeitäquivalenten (FTE) ausgegangen.

5.2 Auswirkungen auf die Kantone

Viele Straftatbestände, die künftig mittels PNR bekämpft werden sollen, liegen in der Strafverfolgungskompetenz der Kantone. Der Bund stellt ihnen mit dem PNR-Informationssystem nötige Instrumente zur Verfügung, damit die kantonalen Strafverfolgungsbehörden einfacher und schneller an Informationen gelangen, welche die Prävention und Bekämpfung von Schwerstkriminalität erleichtern.

An den Kosten der PIU beteiligen sich die Kantone durch die Entsendung von Mitarbeitenden, für deren Entschädigung sie auch während des Einsatzes in der PIU aufkommen.

Mit PNR erhalten die kantonalen Strafverfolgungsbehörden Informationen über national oder international gesuchte Personen, die sich im Anflug auf die Schweiz oder unmittelbar vor der Ausreise aus der Schweiz befinden. Damit können die Kantone – allenfalls im Verbund mit anderen Behörden – zeitgerecht die nötigen Massnahmen treffen. Die PIU entspricht auch mit ihren gezielten Analysen einem grossen Anliegen der Strafverfolgungsbehörden. Zudem erspart PNR den Kantonen zeitaufwändige Nachfragen bei Luftverkehrsunternehmen, wenn es darum geht, zu kriminellen Zwecken genutzte Reisewege nachzuverfolgen. Auch nützliche Hinweise auf bisher ungeklärte Straftaten sind mit PNR zu erwarten.

Insgesamt leistet das Flugpassagierdatengesetz einen wichtigen Beitrag zur Steigerung von Effizienz und Effektivität in der Verbrechensprävention und Strafverfolgung. Davon werden die Kantone massgeblich profitieren.

Finanzielle Auswirkungen auf die Kantone

Ein schweizerisches PNR-System kann nur effektiv funktionieren, wenn sich auch die Kantone personell am Betrieb beteiligen. Deshalb ist vorgesehen, dass Bund und Kantone je die Hälfte der Mitarbeitenden stellen und finanzieren. Die restlichen Kosten einschliesslich der Investitions- und Betriebskosten des PNR-Informationssystems sowie die übrigen Betriebskosten der PIU gehen zu Lasten des Bundes. Die weiteren Modalitäten sind Gegenstand einer Vereinbarung des Bundes mit den Kantonen. Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) sowie die Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS) befürworten den Aufbau eines nationalen PNR-Systems und zeigen Bereitschaft, sich personell an der PIU zu beteiligen. Eine entsprechende Vereinbarung wird in der Phase Konzept des Projekts ab Anfang 2022 mit den Kantonen erarbeitet.

Operativer Aufwand

Die Kantone werden sich ausserdem Überlegungen machen müssen, inwiefern sie die Bearbeitung von PNR-Daten in ihren Korps integrieren und welche Auswirkungen das auf die Organisation und die Ressourcen haben wird. So müssen sie zum einen in ihren Korps Spezialisten ausbilden, welche erfolgsversprechende Profile, Beobachtungslisten und Rechercheanfragen an die PIU übermitteln und mit dieser fallbezogen eng zusammenarbeiten können.

Zum anderen obliegen der Entscheid über und die Durchführung von Folgemassnahmen, die sich aus den Erkenntnissen der PNR-Datenanalyse ergeben, immer den zuständigen Behörden.

Weil ein Grossteil der Erstmassnahmen bei der Einreise von Personen am Flughafen erfolgt, ist davon auszugehen, dass die Nutzung 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.

5.3 Auswirkungen auf die Volkswirtschaft und die Gesellschaft

Mit dem Flugpassagierdatengesetz 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 wird PNR aufgrund internationaler Verpflichtungen heute bereits von mehr als 60 Staaten angewandt. Für die Luftverkehrsunternehmen stellt somit auch die Übermittlung der PNR-Daten kein Novum mehr dar.

Die Vorlage bezweckt in der Hauptsache eine Erhöhung der Sicherheit. Ein sicheres gesellschaftliches Umfeld ist eine wichtige Rahmenbedingung für den Erhalt und die Stärkung des Wirtschaftsstandorts Schweiz. Dabei gilt es mit zu berücksichtigen, dass die Lieferung der PNR-Daten mehr und mehr zu einer Bedingung für den Anflug gewisser Destinationen gemacht wird. Die weitere Anbindung der Schweiz an den internationalen Luftverkehr ist volkswirtschaftlich von grosser Bedeutung.

Terrorismus und Schwerstkriminalität destabilisieren eine Gesellschaft und untergraben das Vertrauen in den Rechtsstaat. Instrumente, die zur Bekämpfung

solcher Verbrechen eingesetzt werden können, sind eine wichtige Grundlage für eine positive gesellschaftliche Entwicklung.

Die USA, welche PNR zur Bedingung für einen Verbleib in ihrem Visa Waiver Program erklären, erwarten von der Schweiz konkrete Fortschritte bei der Einführung eines nationalen PNR-Systems. Das Visa Waiver Program ermöglicht es Staatsangehörigen bestimmter Staaten, unter anderem der Schweiz, zu touristischen oder geschäftlichen Zwecken ohne Visum in die USA zu reisen und sich dort während höchsten 90 Tagen aufzuhalten. Ein Ausschluss aus dem Visa Waiver Program würde für die Schweiz erhebliche Nachteile bringen, weil Geschäftsreisende nicht mehr einfach in die USA reisen könnten und somit die Handelsbeziehungen zwischen der Schweiz und den USA schwer beeinträchtigt würden.

Die verdachtsunabhängige Bearbeitung von Personendaten stellt für die Schweiz einen Paradigmenwechsel dar. Allerdings ist der Eingriff in die Privatsphäre der Flugpassagiere in der Hauptsache auf den Abgleich mit den polizeilichen Informationssystemen gemäss Artikel 7 Absatz 1 begrenzt. Dies lässt sich mit dem Ziel von PNR, der Erhöhung der Sicherheit für die ganze Gesellschaft, rechtfertigen.

6 Rechtliche Aspekte

6.1 Verfassungsmässigkeit

Das Flugpassagiergesetz bildet eine neue Aufgabe mit einer sicherheitspolitischen Dimension sowie einem Bezug zum Luftverkehr ab.

Die Bearbeitung von Flugpassagierdaten als neue Aufgabe des Bundes ist primär sicherheitspolitisch motiviert. Die Wahrung der inneren Sicherheit steht im Vordergrund und ist eine gemeinsame Aufgabe von Bund und Kantonen ist (Art. 57 Abs. 1 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 unterstützen. Die Kompetenzaufteilung zwischen Bund und Kantonen wird dabei nicht tangiert. Auch vor diesem Hintergrund lässt sich die Verfassungsmässigkeit des Flugpassagierdatengesetzes bejahen.

Schliesslich weist das Flugpassagierdatengesetz einen engen Bezug zum Luftverkehr auf, indem Luftverkehrsunternehmen zur Datenübermittlung verpflichtet werden und für allfällige Pflichtverletzungen mit Sanktionen zu rechnen haben. Artikel 87 der Bundesverfassung weist die Kompetenz zur gesetzlichen Regelung des Luftverkehrs ausschliesslich dem Bund zu.

6.2 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. Gleichzeitig setzt die Schweiz auch die Standards der ICAO für die Schweizer Luftfahrt um und gewährleistet den Verbleib der Schweiz im Visa Waiver Program der USA. Dieser wichtige Status ist zurzeit nur provisorischer Natur.

Der Vorentwurf des Flugpassagierdatengesetzes lehnt sich weitgehend an die PNR-Richtlinie der EU an, was für den Abschluss eines PNR-Abkommens mit der EU

zuträglich sein dürfte. Nicht davon betroffen ist das Abkommen vom 21. Juni 1999[77] zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über den Luftverkehr.

6.3 Erlassform

Der vorliegende Entwurf eines Bundesgesetzes regelt die Bearbeitung von Flugpassagierdaten, die auch Personendaten umfassen. Aus dem automatischen Abgleich der Flugpassagierdaten mit verschiedenen Informationssystemen des Bundes können schützenswerte Personendaten in die weitere Datenbearbeitung einfliessen.

Die Datenbearbeitung kann das verfassungsmässige Recht auf Schutz der Privatsphäre von Flugpassagieren tangieren, was nur auf der Grundlage eines formellen Gesetzes zulässig ist (Art. 164 Abs. 1 Bst. b BV).

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

6.4 Einhaltung des Subsidiaritätsprinzips und des Prinzips der fiskalischen Äquivalenz

Nach dem Prinzip der Subsidiarität soll in einem Bundesstaat die übergeordnete Gebietskörperschaft eine Aufgabe oder Teilbereiche davon nur dann übernehmen, wenn sie diese nachweislich besser erfüllen kann als die untergeordneten Gebietskörperschaften (Art. 5*a* BV). Das Subsidiaritätsprinzip geht implizit davon aus, dass die Aufgabenerfüllung so nahe wie möglich bei den Bürgerinnen und Bürgern erfolgen soll und diese so auf den politischen Prozess eher Einfluss nehmen können.

Vorliegend macht es kaum Sinn, dass sich die Kantone zuerst für eine gemeinsame Bearbeitung von Flugpassagierdaten organisieren. Mit diesem Gesetz kommt der Bund drei verbindlichen UNO-Resolutionen nach, indem er ein zentrales Informationssystem für die Bearbeitung von Flugpassagierdaten beschafft und betreibt. Das Informationssystem steht insbesondere im Dienste der Strafverfolgungsbehörden von Bund und Kantonen, die wertvolle Informationen für ihre jeweiligen Aufgaben proaktiv oder auf Antrag hin erhalten. Eine Nähe zur Bevölkerung ist für diese Art der Aufgabenerfüllung kaum angezeigt. Gefragt ist eine einheitliche Lösung, was ein weiterer Grund für eine bundesrechtliche Zuständigkeit darstellt (vgl. Art. 43a Abs. 1 BV).

Nach dem Prinzip der fiskalischen Äquivalenz trägt das Gemeinwesen die Kosten einer staatlichen Leistung, in dem der Nutzen daraus anfällt (Art. 43*a* Abs. 2 BV).

Die Bearbeitung von Flugpassagierdaten entfaltet sowohl einen landesweiten Nutzen als auch einen konkreten Nutzen für Behörden von Bund und Kantonen. Eine spezifische Rechnungsstellung an die einzelnen Kantone würde einen nicht unbeachtlichen Aufwand nach sich ziehen. Vor diesem Hintergrund überzeugt die pragmatische Lösung, wonach die Kantone auf eigene Kosten die Hälfte der Mitarbeitenden stellen, die für die Bearbeitung der Flugpassagierdaten nötig sind.

77 SR **0.748.127.192.68**

6.5 Delegation von Rechtsetzungsbefugnissen

Mit *Artikel 2 Absatz 4* erhält fedpol die Kompetenz, auf Verordnungsebene die internationalen Industriestandards der ICAO, WZO und IATA nötigenfalls zu konkretisieren.

Artikel 6 Absatz 4 des Vorentwurfs sieht vor, dass der Bundesrat die schweren Straftaten nach Artikel 6 Absatz 3 Buchstabe b in einer Verordnung ausweist. Wie bereits in den Erläuterungen zu dieser Bestimmung ausgeführt, handelt es sich hierbei nicht um eine Delegation von Rechtsetzungsbefugnissen. Was als schwere Straftat zu verstehen ist, wird in Art. 6 Absatz 3 Buchstabe b bereits klar umschrieben. Der Ausweis der konkreten Straftatbestände auf Verordnungsebene dient einzig der Transparenz und der Rechtssicherheit.

Gemäss *Artikel 9 Absatz 6* soll der Bundesrat auch die massgeblichen Straftatbestände auf Verordnungsstufe festlegen, die zu einer weiteren Bearbeitung von Flugpassagierdaten nach einem positiven Abgleich mit Beobachtungslisten berechtigen. Der Fokus liegt auf terroristischen Straftaten und solchen des organisierten Verbrechens.

Gemäss *Artikel 16 Abs. 2* legt der Bundesrat die maximale Aufbewahrungsdauer der Daten, die aus einem Abgleich resultieren, in einer Verordnung fest. Hinsichtlich der Aufbewahrungsdauer von Übereinstimmungen von Flugpassagierdaten aus dem Abgleich mit den polizeilichen Informationssystemen oder mit Risikoprofilen und Beobachtungslisten ist im Unterschied zu den Flugpassagierdaten (Artikel 16 Abs. 1) auf eine generelle zeitliche Einschränkung zu verzichten. Andernfalls besteht die Gefahr, dass je nach Fallkonstellation Daten bereits vor Abschluss eines laufenden Verfahrens gelöscht werden müssen. Die Verfügbarkeit dieser Daten während laufender Verfahren muss gewährleistet werden können. Die Festlegung der Aufbewahrungsdauer auf Verordnungsstufe schafft diesen notwendigen Spielraum.

Die Bundesverfassung sieht die rechtsetzenden Verträge zwischen Bund und Kantonen nicht als eigenständige Erlassform (vgl. Art. 163 BV) vor. Folglich müssen zumindest die Rahmenbedingungen des Vertrags durch ein Bundesgesetz oder bei Bestimmungen von untergeordneter Bedeutung durch eine Verordnung festgelegt werden. Erst auf der Basis dieser Rechtsgrundlage kann der Vertrag mit den Kantonen abgeschlossen werden[78]. Aus diesem Grund soll der Bundesrat gemäss *Art. 20 Abs. 5* die Rahmenbedingungen für eine Vereinbarung mit den Kantonen über die Entsendung von Mitarbeitenden und deren Einsatz bei der PIU in einer Verordnung festhalten können.

Mit *Artikel 21 Absatz 1* erhält der Bundesrat die Kompetenz, selbständig völkerrechtliche Verträge über die Bearbeitung von Flugpassagierdaten abzuschliessen. Als mögliche Vertragspartner kommen nur Staaten in Frage, die einen mit der Schweiz vergleichbaren Schutz der übermittelten Daten gewährleisten. Fedpol kann Vereinbarungen abschliessen, die diese völkerrechtlichen Verträge in operativer, technischer oder administrativer Hinsicht ergänzen (Art. 21 Abs. 2).

[78] BSK BV-Waldmann/Schnyder von Wartensee, Art. 48 N 37

6.6 Datenschutz

Das Flugpassagierdatengesetz orientiert sich vollständig am neuen Bundesgesetz vom 25. September 2020[79] über den Datenschutz (nDSG), das voraussichtlich 2023 in Kraft treten wird. In der Botschaft vom 15. September 2017[80] führte der Bundesrat aus, dass mit dem nDSG namentlich die Schwächen des aktuellen Datenschutzgesetzes behoben werden sollen, die aufgrund der rasanten technologischen Entwicklung entstanden sind. Das Flugpassagierdatengesetz entspricht dieser Aktualisierung des Datenschutzrechts des Bundes. Dies ist umso wichtiger, als der Datenschutz bei der Datenbearbeitung nach dem Flugpassagierdatengesetz eine zentrale Rolle spielt.

Der Flugpassagierdatensatz setzt sich aus verschiedenen Kategorien von Daten zusammen. Für den Datenschutz relevant sind vor allem die Personendaten. Es sind dies alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 Bst. a nDSG). Dazu gehören der Name, die Telefonnummer, die Wohn- und die E-Mailadresse. Nach dem Abgleich mit verschiedenen Informationssystemen des Bundes (vgl. Art. 7 Abs. 1) können zusätzlich besonders schützenswerte Personendaten dazukommen. Nach dem Flugpassagierdatengesetz dürfen diese nur bearbeitet werden, wenn es sich um biometrische Daten oder allenfalls um Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen handelt. Alle anderen besonders schützenswerten Daten, die allenfalls bei der Bearbeitung von Flugpassagierdaten nach diesem Gesetz anfallen, sind umgehend zu löschen (Art. 6 Abs. 5).

Die Flugpassagierdaten dürfen nur zum gesetzlich vorgesehenen Zweck, bearbeitet werden (Art. 6 Abs. 4 nDSG). Flugpassagierdaten dürfen nach dem Flugpassagierdatengesetz nur bearbeitet werden, wenn dies der Bekämpfung von terroristischen und anderen schweren Straftaten dient (Art. 6 Abs. 1). Ergebnisse, die diesem Zweck widersprechen, sind umgehend zu löschen (Art. 6 Abs. 5).

Werden Personendaten bearbeitet, ist ihre Richtigkeit sicherzustellen (Art. 6 Abs. 5 nDSG). Die PIU ist verpflichtet, die bei einem Abgleich der Flugpassagierdaten mit den Informationssystemen des Bundes erzielten Übereinstimmungen einzeln manuell zu überprüfen und zu plausibilisieren (Art. 7 Abs. 3).

Die Flugpassagierdaten werden in zwei Schritten mit Informationssystemen des Bundes abgeglichen (Art. 7 Abs. 1 und 3). In einem ersten Schritt werden alle verfügbaren Daten abgeglichen. Nur jene Daten, die mit Inhalten der Informationssysteme übereinstimmen und somit mit einem ersten Verdacht behaftet sind, werden weiterbearbeitet. Sie werden manuell und allenfalls unter gezieltem Zugriff auf weitere Informationssysteme des Bundes plausibilisiert. Im Vordergrund dieses zweiten Bearbeitungsschrittes geht es darum, die Richtigkeit der Übereinstimmung sowie ihre Vereinbarkeit mit dem gesetzlichen Zweck der Bearbeitung sicherzustellen. Übereinstimmungen, die keinen Zusammenhang mit terroristischen oder anderen schweren Straftaten gemäss Artikel 6 Absätze 2 und 3

79 BBl **2020** 7639
80 BBl **2017** 6941

aufweisen, sind umgehend zu löschen. Die Zweistufigkeit dieses Verfahrens trägt dazu bei, dass die Flugpassagierdaten nur insoweit bearbeitet werden, als dies für den Zweck des Gesetzes sowie die Gewährleistung der Datenrichtigkeit nötig ist.

Die Sicherheit der Flugpassagierdaten wird sechs Monate nach ihrem Eingang im PNR-Informationssystem durch die Pseudonymisierung (Art. 14) erhöht. Gemäss Botschaft zum neuen Datenschutzgesetz gilt die Pseudonymisierung als eine geeignete technische Massnahme, um die Datensicherheit (Art. 8 nDSG) zu gewährleisten.[81] In besagter Botschaft hält der Bundesrat zudem fest, 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 kein Interessent auf sich nehmen würde. Das gilt ebenfalls für pseudonymisierte Daten.»[82]

81 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl **2017** 7031

82 BBl **2017** 7019

Anhang 1

A. Terroristische Straftaten gemäss Art. 6 Abs. 2

Terroristische Straftaten iS der Artikel 1 bis 4 des Rahmenbeschlusses 2002/475/JI	**Anwendbar, soweit terroristisch motiviert:** Schreckung der Bevölkerung, Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit, Landfriedensbruch, Strafbare Vorbereitungshandlungen, Kriminelle und terroristische Organisationen, Gefährdung der öffentlichen Sicherheit mit Waffen, Finanzierung des Terrorismus, Anwerbung, Ausbildung und Reisen im Hinblick auf eine terroristische Straftat, Rechtswidrige Vereinigung (Art. 258, 259, 260 Abs. 1, 260bis, 260ter, 260quater, 260quinquies, 260sexies, 275ter) Organisationsverbot (Art. 74 Nachrichtendienstgesetz[83]) Strafbestimmungen gemäss Bundesgesetz vom 12. Dezember 2014[84] über das Verbot der Gruppierungen «Al-Qaïda» und «Islamischer Staat» sowie verwandter Organisationen (Art. 2)

B. Schwere Straftaten gemäss Art. 6 Abs. 3 Bst. a

Anhang II der PNR-RL EU	Straftaten nach schweizerischem Recht[85]
Beteiligung an einer kriminellen Vereinigung	Kriminelle und terroristische Organisation (Art. 260ter)
Menschenhandel	Zwangsheirat, erzwungene eingetragene Partnerschaft, Menschenhandel (Art. 181a, 182 Abs. 1, 2 und 4 StGB)
Sexuelle Ausbeutung von Kindern und Kinderpornografie	Gefährdung der Entwicklung von Minderjährigen: sexuelle Handlungen mit Kindern, Förderung der Prostitution, Pornografie (Art. 187 Ziff. 1, 195 Bst. a und Art. 197 Abs. 4 StGB)

83 SR **121**
84 SR **122**
85 Straftaten nach Anhang 1 des Schengen-Informationsaustausch-Gesetzes (SR **362.2**), die mit einer Freiheitsstrafe von mehr als drei Jahren bedroht sind

Anhang II der PNR-RL EU	Straftaten nach schweizerischem Recht[85]
Illegaler Handel mit Drogen und psychotropen Stoffen	Strafbestimmungen des Betäubungsmittelgesetzes[86] (Art. 19 Abs. 2 und 20 Abs. 2 BetmG)
Illegaler Handel mit Waffen, Munition und Sprengstoffen	Gefährdung der öffentlichen Sicherheit mit Waffen (Art. 260quater StGB)
	Vergehen und Verbrechen gemäss Waffengesetz[87] (Art. 33 Abs. 3 WG)
Korruption	Bestechen, Sich bestechen lassen, Bestechung fremder Amtsträger (Art. 322ter, Art. 322quater, Art. 322septies StGB)
Betrugsdelikte	Betrug, Betrügerischer Missbrauch einer Datenverarbeitungsanlage, Check- und Kreditkartenmissbrauch, Warenfälschung, betrügerischer Konkurs und Pfändungsbetrug (Art. 146 Abs. 1 und 2, 147 Abs. 1 und 2, 148, 155 Ziffer 2, 163 Ziff. 1 StGB)
	Leistungs- und Abgabebetrug (Art. 14 Abs. 4 des Bundesgesetzes über das Verwaltungsstrafrecht[88])
Wäsche von Erträgen aus Straftaten und Geldfälschung	Geldfälschung, Geldverfälschung, Einführen, Erwerben, Lagern falschen Geldes, Geldwäscherei (Art. 240 Abs. 1, 241 Abs. 1, 244 Abs. 2, 305bis Ziff. 2 StGB)
Computerstraftaten /Cyberkriminalität	Unbefugte Datenbeschaffung, Datenbeschädigung, Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 143, 144bis Abs. 3, 147 Abs. 1 und 2 StGB)
Umweltkriminalität (einschliesslich illegaler Handel mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten)	Ungerechtfertigte Bestrahlung von Personen (Art. 43 Abs. 2 Strahlenschutzgesetz[89])
Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt	Förderung der rechtswidrigen Ein- und Ausreise sowie des rechtswidrigen Aufenthalts (Art. 116 Abs. 1 Bst. a, abis und c i.V.m. Abs. 3 Ausländer- und Integrationsgesetz[90])

86 SR **812.121**
87 SR **514.54**
88 SR **313.0**
89 SR **814.50**
90 SR **142.20**

Anhang II der PNR-RL EU	Straftaten nach schweizerischem Recht[85]
Vorsätzliche Tötung, schwere Körperverletzung	Vorsätzliche Tötung, Mord, Totschlag, schwere Körperverletzung, Verstümmelung weiblicher Genitalien (Art. 111, 112, 113, 122, 124 StGB)
Illegaler Handel mit menschlichen Organen und menschlichem Gewebe	Verbrechen gemäss Transplantationsgesetz[91] (Art. 69 Abs. 2) Verbrechen gemäss Stammzellenforschungsgesetz[92] (Art. 24 Abs. 3 StFG)
Entführung, Freiheitsberaubung und Geiselnahme	Erpressung, Freiheitsberaubung und Entführung, Erschwerende Umstände einer Freiheitsberaubung und Entführung, Geiselnahme, Verbotene Handlungen für einen fremden Staat (Art. 156, 183, 184, 185, 271 Ziff. 2 und 3 StGB)
Diebstahl in organisierter Form oder mit Waffen	Diebstahl, Raub (Art. 139 Ziff. 3, 140 StGB)
Illegaler Handel mit Kulturgütern (einschliesslich Antiquitäten und Kunstgegenstände)	---
Betrügerische Nachahmung und Produktpiraterie	Warenfälschung (Art. 155 Ziff. 2 StGB) Markenrechtsverletzung, betrügerischer Markengebrauch, reglementswidriger Gebrauch einer Garantie- oder Kollektivmarke, Gebrauch unzutreffender Herkunftsangaben (Art. 61 Abs. 3, 62 Abs. 2, 63 Abs. 4, 64 Abs. 2 Markenschutzgesetz[93]) Designrechtsverletzung (Art. 41 Abs. 2 Designgesetz[94]) Urheberrechtsverletzung, Verletzung von verwandten Schutzrechten (Art. 67 Abs. 2, 69 Abs. 2 Urheberrechtsgesetz[95]) Patentverletzung (Art. 81 Abs. 3 Patentgesetz[96])

91 SR **810.21**
92 SR **810.31**
93 SR **232.11**
94 SR **232.12**
95 SR **231.1**
96 SR **232.14**

Anhang II der PNR-RL EU	Straftaten nach schweizerischem Recht[85]
Fälschung von amtlichen Dokumenten und Handel damit	Fälschung von Mass und Gewicht, Geld und Wertzeichen des Auslands, Urkundenfälschung, Erschleichung einer falschen Beurkundung, Urkunden des Auslandes, Urkundenfälschung im Amt (Art. 248, 250. 251 Ziff. 1, 253, 255, 317 Ziff. 1 StGB)
Illegaler Handel mit Hormonen und Wachstumsförderern	Strafbestimmung gemäss Sportförderungsgesetz[97] (Art. 22 Abs. 2 SpoFöG)
	Verbrechen gemäss Heilmittelgesetz[98] (Art. 86 Abs. 2 und 3 HMG)
Illegaler Handel mit nuklearen und radioaktiven Substanzen	Gefährdung durch Kernenergie, Radioaktivität und ionisierende Strahlen, strafbare Vorbereitungshandlungen (Art. 226bis, 226ter StGB)
	Missachtung von Sicherheits- und Sicherungsmassnahmen, Widerhandlungen bei nuklearen Gütern und Abfällen (Art. 88 Abs. 2 und 89 Abs. 2 Kernenergiegesetz[99])
Vergewaltigung	Vergewaltigung (Art. 190 StGB)
Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen	Völkermord, Verbrechen gegen die Menschlichkeit, Schwere Verletzungen der Genfer Konventionen, Angriffe gegen zivile Personen und Objekte, Ungerechtfertigte medizinische Behandlung, Verletzung der sexuellen Selbstbestimmung und der Menschenwürde, Rekrutierung und Verwendung von Kindersoldaten, Verbotene Methoden der Kriegführung, Einsatz verbotener Waffen (Art. 264, 264a, 264c–h StGB)
Flugzeug- und Schiffsentführung	Erpressung, Freiheitsberaubung und Entführung, Geiselnahme (Art. 156, 183, 185 StGB)
Sabotage	Sachbeschädigung, Brandstiftung, Verursachung einer Explosion, Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht, Herstellen, Verbergen, Weiterschaffen von Sprengstoffen und giftigen Gasen, Verursachen einer Überschwemmung oder eines Einsturzes, Beschädigung von elektrischen Anlagen,

97 SR **415.0**
98 SR **812.21**
99 SR **732.1**

Anhang II der PNR-RL EU	Straftaten nach schweizerischem Recht[85]
	Wasserbauten und Schutzvorrichtungen (Art. 144 Abs. 3, 221 Abs. 1 und 2, 223 Ziff. 1, 224 Abs. 1, 226, 227 Ziff. 1,228 Ziff. 1 StGB)
Handel mit gestohlenen Kraftfahrzeugen	Hehlerei (Art. 160 StGB)
Wirtschaftsspionage	---

C. Schwere Straftaten gemäss Art. 6 Abs. 3 Bst. b

Straftaten in der Strafverfolgungskompetenz des Bundesamtes für Zoll und Grenzsicherheit (BAZG) mit einer maximalen Strafandrohung von mindestens 3 Jahren Freiheitsstrafe

1. Leistungs- und Abgabebetrug, Urkundenfälschung; Erschleichen einer falschen Beurkundung; Unterdrückung von Urkunden; Begünstigung (Art. 14 Abs. 4, Art. 15, Art. 16 Abs. 1 und Art. 17 Ziff. 1 des Bundesgesetzes über das Verwaltungsstrafrecht (VStrR)[100] .
2. Die folgenden Delikte, soweit sie in der Strafverfolgungskompetenz des BAZG liegen und in Verbindung mit einer Vortat stehen, für die eine maximale Freiheitsstrafe von mindestens drei Jahren angedroht ist:
   Art. 37 Automobilsteuergesetz (AStG)[101]; Art. 39 Mineralölsteuergesetz (MinöstG)[102].
3. Die folgenden weiteren Delikte:

   Art. 36 Abs. 2 i.V.m. Art. 40 AStG;

   Art. 38 Abs. 2 i.V.m. Art. 42 MinöstG;

   Art. 86 Abs. 1, 2, 3 i.V.m. Art. 90 Abs. 1 des Bundesgesetz über Arzneimittel und Medizinalprodukte vom 15.12.2000 (HMG)[103]

   Art. 26 Abs. 2 mit i.V. m. Art. 27 des Bundesgesetzes über den Verkehr mit Tieren und Pflanzen geschützter Arten (BGCITES)[104];

   Art. 63 Abs. 1 und 2 i.V.m. Art. 65 des Bundesgesetzes über Lebensmittel und Gebrauchsgegenstände (LMG)[105];

   Art. 26 Abs. 1 i.V.m. Art. 31 Abs. 3 Tierschutzgesetz (TSchG)[106].

100 SR **313.0**
101 SR **641.51**
102 SR **641.61**
103 SR **812.21**
104 SR **453**
105 SR **817.0**
106 SR **455**

Glossar

API-Daten	API ist die Abkürzung von Advance Passenger Information. Dabei handelt es sich um Daten, welche die Luftverkehrsunternehmen dem Staat vor bestimmten Abflügen zustellen müssen. In der Schweiz findet sich die Regelung der API-Daten in den Artikeln 104 und 104*a* des Ausländer- und Integrationsgesetzes (SR 142.20). *Relevanz PNR: API-Daten stellen eine Datenkategorie im PNR-Datensatz dar.*
Bearbeiten von Daten	Als Bearbeiten gilt jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. *Relevanz PNR: Das Flugpassagierdatengesetz sieht die Bearbeitung von Daten für die Bekämpfung von Terrorismus und anderen schweren Straftaten vor und regelt, ergänzend zum Datenschutzgesetz, ihren Schutz.*
Besonders schützenswerte Personendaten	Besonders schützenswerte Personendaten sind → Personendaten, die nur unter besonderen Voraussetzungen bearbeitet werden dürfen. Als besonders schützenswert gelten: 1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, 2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie, 3. genetische Daten, 4. → biometrische Daten, 5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,

	6. Daten über Massnahmen der sozialen Hilfe. *Relevanz PNR: Besonders schützenswerte Personendaten können anfallen, wenn die Flugpassagierdaten mit anderen Informationssystemen des Bundes abgeglichen oder mittels Zugriffs auf solche plausibilisiert werden. Der Vorentwurf des Flugpassagiergesetzes erlaubt ihre Bearbeitung jedoch nur, wenn es sich dabei um → biometrische Daten oder um Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen handelt (vgl. Art. 9 Abs. 4). Alle anderen besonders schützenswerten Daten sind umgehend zu löschen.*
Biometrische Daten	Unter biometrischen Daten sind Personendaten zu verstehen, die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Biometrische Daten gelten als → besonders schützenswerte Personendaten, die nur unter besonderen Voraussetzungen bearbeitet werden dürfen. *Relevanz PNR: Bei der Bearbeitung von Flugpassagierdaten können biometrische Daten bei einem Abgleich oder bei einem Zugriff auf Informationssysteme anfallen. Die zuständige Stelle darf sie für den gesetzlich definierten Zweck bearbeiten.*
Datensatz	Mehrere logisch zusammenhängende, aufeinanderfolgende Daten mit fester oder variabler Länge. *Relevanz PNR: Der Flugpassagierdatensatz setzt sich aus 19 Kategorien von Daten zusammen, die in*

	Zusammenhang mit der Buchung von Flugtickets anfallen. In der Regel entfällt auf einen Flugpassagier ein Datensatz. Immer mehr Staaten nutzen diese Datensätze zur Bekämpfung von Terrorismus und weiteren schweren Straftaten. Die Schweiz sieht die Bearbeitung dieser Datensätze im Vorentwurf des Flugpassagierdaten-gesetzes vor, der in der ersten Hälfte 2022 in die Vernehmlassung geht.
depersonalisieren	Ein anderer Begriff für → pseudonymisieren. *Relevanz PNR: Sowohl die PNR-Richtlinie der EU wie auch die entsprechenden Gesetze von Deutschland und Österreich verwenden den Begriff der Depersonalisierung.*
pseudonymisieren	Daten gelten als pseudonymisiert, wenn sie mit einem Pseudonym versehen werden und sich dadurch nicht mehr einer bestimmten Person zuordnen lassen. Die Pseudonymisierung lässt sich rückgängig machen, indem eine dazu berechtigte Stelle das Pseudonym wieder durch den zugehörigen Namen ersetzt. Ab diesem Zeitpunkt sind die Daten wieder der ursprünglichen Person zuordenbar. Aufschluss darüber, welches Pseudonym zu welchem Namen gehört, gibt die Konkordanztafel. Daten, die pseudonymisiert sind, gelten weiterhin als Personendaten im Sinne des Datenschutzes, solange die Konkordanztafel noch verfügbar ist. *PNR-Relevanz: Flugpassagierdaten, die in der Schweiz nach dem Flugpassagierdatengesetz bearbeitet werden, werden automatisch nach sechs Monaten pseudonymisiert. Über eine allfällige Rückgängigmachung der Pseudonymisierung entscheidet das Bundesverwaltungsgericht.*

Personendaten	Bei Personendaten handelt es sich um alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Eine natürliche Person ist bestimmbar, wenn sie direkt oder indirekt identifiziert werden kann, beispielsweise über den Hinweis auf Informationen, die sich aus den Umständen oder dem Kontext ableiten lassen (Identifikationsnummer, Standortdaten, spezifische Aspekte, die ihre physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder gesellschaftliche Identität betreffen). Die Identifizierung kann über eine einzige Information möglich sein (Telefonnummer, Hausnummer, AHV-Nummer, Fingerabdrücke) oder über den Abgleich verschiedener Informationen (Adresse, Geburtsdatum, Zivilstand). Die rein theoretische Möglichkeit, dass jemand identifiziert werden kann, reicht nicht aus, um anzunehmen, eine Person sei bestimmbar. Zu den Personendaten gehören auch die → besonders schützenswerten Personendaten, für die das Datenschutzrecht einen höheren Schutz vorschreibt. *PNR-Relevanz: Der Flugpassagierdaten-satz, den die Luftverkehrsunternehmen der PIU übermitteln müssen, enthält auch Personendaten, nicht jedoch besonders schützenswerte. Sollten dennoch solche übermittelt werden, ist die PIU gesetzlich verpflichtet, diese zu löschen.*
Visa Waiver Program	Das Programm für visumfreies Reisen (Visa Waiver Program) erlaubt es Staatsangehörigen bestimmter Länder, zu geschäftlichen oder touristischen Zwecken (Reisezweck « Besucher ») für bis zu 90 Tage ohne Visum in die Vereinigten Staaten zu reisen. *PNR-Relevanz: Die USA macht den Verbleib der Schweiz im Visa Waiver Program abhängig von ihrer Einführung von PNR.*