Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bern, 8. Oktober 2025

Entwurf zur Flugpassagierdatenverordnung und Änderung weiterer Verordnungen

Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens

Erläuterungen

1 Ausgangslage

Das Passagieraufkommen im Luftverkehr ist in den letzten Jahrzehnten international massiv angestiegen. Das BAZL verzeichnete für das Jahr 2024 rund 58 Millionen Passagierinnen und Passagiere, die mit Linien- und Charterflügen in die Schweiz einreisten oder die Schweiz auf diesem Weg verliessen. Damit hat das Passagieraufkommen wieder den Stand vor Ausbruch der Corona-Pandemie erreicht.

Zu der Vielzahl von Personen, die grenzüberschreitend mit Linien- oder Charterflügen unterwegs sind, gehören auch solche, die sich der Schwerstkriminalität schuldig gemacht haben und rechtskräftig verurteilt, aber flüchtig sind, der Begehung einer solchen Straftat verdächtigt werden oder eine solche zu begehen beabsichtigen. Deshalb nutzen bereits 70 Staaten die Daten der Flugpassagierinnen und -passagiere als Instrument zur Bekämpfung von Schwerstkriminalität.

Die Flugpassagierdaten fallen bei der Buchung eines Flugtickets an. Sie werden von den Luftverkehrsunternehmen für die Reservation und Abfertigung des Fluges benötigt. Die Daten jeder Passagierin oder jedes Passagiers sind im Flugpassagierdatensatz zusammengefasst, international als «Passenger Name Record» (PNR) bezeichnet. Der Datensatz setzt sich aus 19 Datenkategorien zusammen und umfasst unter anderem den Namen und die Adresse der Flugpassagierin oder des Flugpassagiers, Angaben zum mitgeführten Gepäck und zu den Zahlungsmodalitäten.

Künftig wird auch die Schweiz diese Daten zur Bekämpfung von Schwerstkriminalität nutzen können. Die Grundlage dazu bildet das Flugpassagierdatengesetz (FPG), welches die eidgenössischen Räte am 21. März 2025 verabschiedet haben.[1] Voraussichtlich Ende 2026 wird das FPG in Kraft treten.

Zeitgleich mit dem FPG soll auch die vorliegende Flugpassagierdatenverordnung (VFPG) in Kraft treten. Sie beinhaltet die für die Umsetzung des FPG nötigen Ausführungsbestimmungen.

Damit die für die Bearbeitung der Flugpassagierdaten zuständige Stelle beim Bundesamt für Polizei (fedpol), die Passenger Information Unit (PIU), über die nötigen Zugriffsrechte auf Informationssysteme des Bundes verfügt, müssen zusätzlich acht Verordnungen angepasst werden.

[1] BBl **2025** 1097

Es sind dies:

a. Visa-Informationssystem-Verordnung vom 18. Dezember 2013[2];
b. ZEMIS-Verordnung vom 12. April 2006[3];
c. Ausweisverordnung vom 20. September 2002[4];
d. NES-Verordnung vom 15. Oktober 2008[5];
e. RIPOL-Verordnung vom 26. Oktober 2016[6];
f. IPAS-Verordnung vom 15. Oktober 2008[7];
g. Polizeiindex-Verordnung vom 15. Oktober 2008[8];
h. N-SIS-Verordnung vom 8. März 2013[9].

Diese Änderungen, die zur Umsetzung des FPG nötig sind, werden aus gesetzestechnischen Gründen bzw. aus Gründen der Lesbarkeit in separaten Änderungserlassen ausgewiesen.

2 Grundzüge der Vorlagen

2.1 VFPG

Die Artikel 1−5 widmen sich den Rechten und Pflichten der Luftverkehrsunternehmen und umfassen vor allem technische und organisatorische Aspekte, die von den Luftverkehrsunternehmen bei der Bekanntgabe der Flugpassagierdaten an die PIU zu beachten sind. Der Bundesrat orientiert sich dabei an den Standards und Empfehlungen, die Anhang 9 des Übereinkommens vom 7. Dezember 1944[10] über die internationale Zivilluftfahrt in Zusammenhang mit PNR aufstellt.

Daneben finden sich auch Ausführungsbestimmungen zur Informationspflicht, welche die Luftverkehrsunternehmen gegenüber ihren Passagierinnen und Passagieren bei der Buchung wahrzunehmen haben (Art. 5). Die buchende Person soll die Kenntnisnahme dieser Information vor Abschluss der Buchung bestätigen.

---

2 SR **142.512**
3 SR **142.513**
4 SR **143.11**
5 SR **360.2**
6 SR **361.0**
7 SR **361.2**
8 SR **361.4**
9 SR **362.0**
10 SR **0.748.0**

Die Artikel 6−8 beinhalten Ausführungsbestimmungen zu den Rechten und Pflichten der PIU. So verweist Artikel 6 auf die Zugriffsrechte, über welche die PIU zum automatischen Datenabgleich und zur manuellen Überprüfung der dabei erzielten Übereinstimmungen (vgl. Art. 6 FPG) verfügen muss. Datenspezifisch festgelegt werden die Zugriffsrechte in den acht anzupassenden Verordnungen (siehe Beilage). Artikel 8 bestimmt das in der Botschaft zum FPG in Aussicht gestellte Vorgehen, wonach die zuständigen Behörden von Bund und Kantonen an ihre Pflicht erinnert werden, die PIU über bekanntgegebene Daten zu informieren, die sie nicht mehr benötigen (vgl. Art. 10 FPG).

Artikel 9 regelt die Einzelheiten zur Umsetzung von Artikel 2 Absatz 2 FPG. Eine von fedpol geführte und veröffentlichte Liste soll alle Staaten ausweisen, welche die Voraussetzung nach Artikel 2 Absatz 2 FPG erfüllen und damit von den in der Schweiz ansässigen Luftverkehrsunternehmen Daten nach dem FPG erhalten dürfen.

In der Liste aufgenommen werden die Staaten, die mit der Schweiz zu PNR einen völkerrechtlichen Vertrag abgeschlossen haben. Zusätzlich sind all jene Staaten in der Liste ausgewiesen, welche das Übereinkommen über die internationale Zivilluftfahrt vom 7 Dezember 1944 unterzeichnet und als Vertragsstaat die für die Flugpassagierdaten geltenden Standards (vgl. Ziff. 9.24−9.39 des Anhangs 9) vorbehaltlos als verbindlich anerkennen.

Abhängig vom Nachweis, Gewähr für die Einhaltung der Standards und Empfehlungen nach Anhang 9 zu bieten, ist dagegen die Aufnahme in die Liste für jene Staaten, die

- zu PNR keinen völkerrechtlichen Vertrag mit der Schweiz abgeschlossen haben; und
- das Übereinkommen nicht unterzeichnet haben; oder
- dieses zwar unterzeichnet haben, jedoch gemäss Artikel 38 des Übereinkommens Vorbehalte gegen einzelne, für die Flugpassagierdaten nach dem FPG geltende Standards angebracht haben.

Diese Staaten haben aufgrund eines Fragebogens von fedpol darzulegen, wie sie die Flugpassagierdaten bearbeiten und schützen. Fedpol prüft sodann, ob dies mit den Standards und Empfehlungen nach Anhang 9 vereinbar ist.

Datenschutzrechtlich relevant sind insbesondere die Standards

- zur Zweckgebundenheit der Datenbearbeitung (Ziff. 9.25 Bst. b und c).
- zu den Rechten der Passagierinnen und Passagiere (Ziff. 9.26f.)
- zu den Löschfristen (Ziff. 9.31f.),
- zur Unabhängigkeit der Aufsichtsbehörde (Ziff. 9.29).

Weichen Staaten hiervon ab, wird auf dem Verhandlungsweg eine Lösung anzustreben sein, die den in der Schweiz ansässigen Luftverkehrsunternehmen eine Datenbekanntgabe gemäss Artikel 2 Absatz 2 FPG ermöglicht.

Artikel 10 legt die Mindestinhalte fest, die dem Bundesrat im Hinblick auf seine Überprüfung der Risikoprofile und Beobachtungslisten nach Artikel 15 FPG jährlich zur Kenntnis zu bringen sind. Grundlage der Überprüfung ist ein Bericht des EJPD, der sich zur Zahl und den Schwerpunkten der eingesetzten Risikoprofile und Beobachtungslisten sowie zu deren Erforderlichkeit und Eignung zur Bekämpfung von Terrorismus und anderer Schwerstkriminalität äussert.

Die Artikel 11–13 regeln Einzelheiten zum Schutz der bearbeiteten Personendaten.

Artikel 14–15 umfassen Ausführungsbestimmungen zu den Artikeln 31 und 32 FPG, welche die Sanktionierung von Luftverkehrsunternehmen regeln, die ihre Pflichten nach den Artikeln 3 und 4 FPG verletzen.

2.2 Anzupassende Verordnungen

Zusammen mit der VFPG müssen insgesamt acht Verordnungen angepasst werden, die Informationssysteme des Bundes regeln. Mit diesen Anpassungen werden die Zugriffsrechte der PIU in jedem Informationssystem datenspezifisch festgelegt**.**

3 Erläuterungen

3.1 Flugpassagierdatenverordnung (VFPG)

1. Abschnitt: Rechte und Pflichten der Luftverkehrsunternehmen

Zu den gesetzlichen Pflichten der Luftverkehrsunternehmen gehören die Bekanntgabe der Flugpassagierdaten an die PIU (vgl. Art. 2 FPG) sowie die Information der Flugpassagierinnen und -passagiere über die Bearbeitung ihrer Daten und ihr Recht auf Auskunft (vgl. Art. 4 FPG). Die Verordnung legt in der Hauptsache Einzelheiten fest, die bei der Umsetzung dieser Pflichten zu beachten sind. Zudem gilt es auf Verordnungsebene auch Rechte der Luftverkehrsunternehmen festzuhalten, so in Artikel 1 Absatz 2 (Freistellung von den vorgegebenen Datenformaten) und in Artikel 4 (Eingangsbestätigung für bekanntgegebene Daten).

Artikel 1 Formate der Datenübermittlung

Das Übereinkommen über die internationale Zivilluftfahrt vom 7. Dezember 1944 unterscheidet zwei Arten, nach denen die Luftverkehrsunternehmen ihre Daten an die PIU bekanntgeben können:

- Bei der «Push-Methode» übermittelt ein Luftverkehrsunternehmen die verlangten Flugpassagierdaten an die PIU.
- Bei der «Pull-Methode» greift die PIU direkt auf das Buchungssystem eines Luftverkehrsunternehmens zu und extrahiert eine Kopie der benötigten Flugpassagierdaten.

Die Luftverkehrsunternehmen sollen die Daten mittels Push-Methode an die PIU übermitteln. Damit entspricht die Verordnung dem Standard gemäss Ziffer 9.34 Buchstabe a von Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt vom 7. Dezember 1944. Der Verordnungstext bringt dies zum Ausdruck, indem er für die Datenbekanntgabe durch die Luftverkehrsunternehmen den Begriff «Übermittlung» verwendet.

Das PNR-Informationssystem (Art. 16 FPG) ist auf die Bearbeitung bestimmter Formate der Flugpassagierdaten ausgelegt. Daher schreibt die Verordnung die unterstützten Formate verbindlich vor, welche die Luftverkehrsunternehmen für die Übermittlung der Flugpassagierdaten zu verwenden haben. Artikel 16 orientiert sich an den für die

Zivilluftfahrt geltenden Standards und Empfehlungen (vgl. Ziff. 9.24 von Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt).

Absatz 1

Das für die PNR-Daten geltende Format PNRGOV wurde unter der Federführung der Internationalen Flug-Transport-Vereinigung (IATA) zusammen mit der Internationalen Zivilluftfahrtorganisation (ICAO) und der Weltzollorganisation (WZO) sowie Behörden und Luftverkehrsunternehmen entwickelt.

Ziffer 9.24 Buchstabe c von Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt verpflichtet die Vertragsstaaten und damit auch die Schweiz, dieses Datenformat für die Bekanntgabe der PNR-Daten zu verwenden. Als technische Standards zulässig sind entweder EDIFACT oder XML.

Absatz 2

Ein spezifisches Format ist für die Advance Passenger Information (kurz API-Daten; vgl. Anhang 1 FPG, Datenkategorie 18) vorgesehen, wenn Luftverkehrsunternehmen sie nicht als Teil eines PNR-Datensatzes, sondern separat bekanntgegeben werden. EDIFACT PAXLST ist das Datenformat für die strukturierte Bekanntgabe der API-Daten. Auch dieses Format entspricht Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt (Standard 9.10).

Absatz 3

Luftverkehrsunternehmen können mit der PIU separate Formate zur elektronischen Datenbekanntgabe vereinbaren, wenn sie nicht über die für eine Bekanntgabe nach den Absätzen 1 und 2 nötige Infrastruktur verfügen. Das Hauptaugenmerk liegt dabei vor allem auf den Formaten XML, Excel oder CSV.

Diese Möglichkeit steht jedoch nur jenen Luftverkehrsunternehmen offen, die nicht nach dem öffentlichen Flugplan verkehren. Von allen übrigen Luftverkehrsunternehmen wird erwartet, dass sie über die nötige Infrastruktur verfügen, um ihre Daten in jenen Formaten bekanntzugeben, die nach den Absätzen 1 und 2 vorgegeben sind.

Artikel 2 Übermittlung im Fall einer technischen Störung

Als technische Störung gilt eine zeitlich begrenzte Beeinträchtigung des ordentlichen Datenverkehrs zwischen einem Luftverkehrsunternehmen und der PIU. Die Gründe, welche die technische Störung ausgelöst haben, sind hier nicht relevant. Denn jede technische Störung, welche eine ordentliche Bekanntgabe verunmöglicht, verpflichtet ein Luftverkehrsunternehmen, sich an die PIU zu wenden, um eine Alternativzustellung der Daten zu vereinbaren.

Die Gründe, die zur technischen Störung geführt haben, sind jedoch bei der Prüfung allfälliger Sanktionen relevant, wobei nur dann Sanktionen nach Artikel 31 FPG ausgesprochen werden können, wenn das betreffende Luftverkehrsunternehmen seine Sorgfaltspflicht nach Artikel 3 FPG verletzt hat.

Artikel 3 Zeitpunkt der Übermittlung

Artikel 3 konkretisiert mit der Festlegung der Zeitpunkte, an denen die Übermittlung an die PIU zu erfolgen hat, die in Artikel 2 Absatz 3 FPG festgelegten Zeitfenster.

Absatz 1

Die Luftverkehrsunternehmen haben der PIU die Flugpassagierdaten normalerweise zu drei Zeitpunkten zu übermitteln: 48 und 24 Stunden vor dem geplanten Abflug sowie unmittelbar nach Abschluss des Boarding.

Absatz 2

Die API-Daten sind der PIU *spätestens* mit der dem dritten Push unmittelbar nach Abschluss des Boarding zu übermitteln.

Ein früherer Push ist jedoch insbesondere für all jene Luftverkehrsunternehmen angezeigt, welche die API-Daten nicht erst beim Boarding, sondern früher erheben. Denn die API-Daten sind der PIU als Kategorie 18 des Flugpassagierdatensatzes nach Anhang 1 FPG bekanntzugeben, «soweit verfügbar». Sind sie also früher als beim Boarding verfügbar, sind sie auch früher an die PIU zu übermitteln.

Absatz 3

Absatz 3 orientiert sich an Ziffer 2.8.3 der ICAO-Leitlinien zu PNR[11]. Die Leitlinien sind für die Vertragsstaaten gemäss Ziffer 9.24 von Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt ebenfalls verbindlich.

Ad hoc und damit abweichend von Absatz 1 soll die PIU im Falle einer konkreten Bedrohung eine zusätzliche Übermittlung der PNR-Daten verlangen dürfen. Damit werden grundsätzlich nicht zusätzliche Daten verlangt und übermittelt, sondern eine aktualisierte Fassung der Daten aller Personen, die sich zum Zeitpunkt der Übermittlung auf der Passagierliste befinden. Ein Bedarf nach dieser zusätzlichen Übermittlung dürfte zeitlich insbesondere kurz vor dem Boarding gegeben sein. Mit diesem zusätzlichen Push werden insbesondere Passagierinnen und Passagiere erfasst, die spät einchecken oder den Flug spät buchen.

Eine Begründungspflicht der PIU gegenüber dem betroffenen Luftverkehrsunternehmen besteht nicht. Sie hat die Rechtmässigkeit dieses zusätzlichen Push jedoch bei Bedarf gegenüber jenen Personen zu begründen, die mit der Überwachung oder Aufsicht nach Artikel 25 FPG betraut sind.

Artikel 4 Bestätigung des Erhalts der Daten

Sobald die Daten bei der PIU eingetroffen sind, erhalten die Luftverkehrsunternehmen eine automatisch ausgelöste Eingangsbestätigung.

Mit dieser Mitteilung wird lediglich der Eingang der Daten bestätigt, nicht jedoch die Rechtzeitigkeit des Eingangs oder die Vollständigkeit der Daten. Die Bestätigung schliesst somit Sanktionen nach Artikel 31 FPG nicht aus. Denn die Rechtzeitigkeit und Vollständigkeit der Datenübermittlung lässt sich erst beurteilen, wenn die PIU die eingegangenen Daten geprüft hat.

[11] Abrufbar unter https://www.icao.int > Security and Facilitation >Facilitation > ANNEX 9 > Publications > Document 9944 – Guidelines on Passenger Name Record

Artikel 5 Information der Flugpassagierinnen und Flugpassagiere

Zu den Pflichten der Luftverkehrsunternehmen gehört − neben der Pflicht zur Datenbekanntgabe − auch jene zur Information der Passagierinnen und Passagiere über die Datenbearbeitung (vgl. Art. 4 FPG). Die Verordnung legt dazu die Einzelheiten fest.

Absatz 1

Gemäss Absatz 1 muss die buchende Person ihre Kenntnisnahme der Information vor Abschluss der Buchung bestätigen können. Dadurch ist diese Information unübersehbar in den Buchungsprozess eingepflegt.

Jedes Luftverkehrsunternehmen hat der Informationspflicht nach Artikel 4 FPG nachzukommen, das Buchungen auf einen bestimmten Flug ab der und in die Schweiz vornimmt. Damit unterliegt auch jenes Luftverkehrsunternehmen der Informationspflicht, das den Flug nicht selber durchführt, sondern lediglich Plätze gekauft hat (Code Sharing).

Beispiel: Eine Person bucht ihren Flug beim Luftverkehrsunternehmen x; durchgeführt wird der Flug jedoch durch das Luftverkehrsunternehmen y.

Aus Absatz 1 ergibt sich, dass nicht nur Luftverkehrsunternehmen y, sondern auch das Luftverkehrsunternehmen x der Informationspflicht nach Artikel 4 des FPG nachkommen muss, selbst wenn letzteres den Flug nicht selber durchführt. Denn nur so erhält eine bei x buchende Person *vor* Abschluss der Buchung Kenntnis von der staatlichen Datenbearbeitung und dem Auskunftsrecht nach Artikel 26 FPG.

Von allfälligen Sanktionen nach Artikel 31 FPG betroffen sein können somit sowohl Luftverkehrsunternehmen x und y. Demgegenüber haftet lediglich Luftverkehrsunternehmen y für fehlende Sorgfalt in Zusammenhang mit der Datenbekanntgabe (Art. 3 FPG).

Absatz 2

Artikel 4 Absatz 1 FPG verlangt, dass die Information angemessen sein muss.

Wann eine Information als angemessen beurteilt werden kann, legt dieser Absatz in Einklang mit Artikel 13 der Datenschutzverordnung vom 31. August 2022[12] fest.

Absatz 3

Die Information hat in der für die Buchung gewählten Sprache und mindestens in Englisch zu erfolgen. Bei Buchungen in englischer Sprache reicht damit die englischsprachige Information.

2. Abschnitt: Rechte und Pflichten der PIU

Artikel 6 Zugriffsberechtigungen der PIU

Die PIU nimmt einerseits mittels automatischen Abgleichs (vgl. Art. 6 Abs. 1 FPG) und anderseits mittels Einzelabfragen (vgl. Art. 6 Abs. 2 und 3 FPG) Zugriff auf Daten verschiedener Informationssysteme des Bundes. Auf welche Datenfelder dabei zugegrif-

[12] SR **235.11**

fen werden darf, bestimmt sich nach den Regelungen in den Verordnungen der jeweiligen Informationssysteme. Die Erläuterungen zu den Anpassungen, die in diesen Verordnungen zeitgleich mit Erlass der VFPG vorgenommen werden, finden sich nachstehend unter Ziffer 3.2.

Artikel 7 Modalität der Datenbekanntgabe

Diese Bestimmung legt nicht nur fest, wie die PIU Daten an eine zuständige Behörde nach Artikel 1 Abs. 2 FPG im Inland bekanntzugeben hat.

Nach Artikel 7 hat sich die PIU auch bei der Bekanntgabe von Daten an eine ausländische PIU zu richten, soweit nicht ein völkerrechtlicher Vertrag mit dem Staat, dem Daten bekanntgegeben werden sollen, Abweichendes vorsieht.

Absatz 1

Grundsätzlich sind die Daten schriftlich über einen gesicherten oder verschlüsselten Kanal bekanntzugeben. Als gesicherter Kanal gilt die geschützte Direktverbindung zwischen dem IT-System der PIU und der empfangenden Behörde. Verschlüsselt ist dagegen ein Kanal, in dem die bekanntgegebenen Daten nur für Personen lesbar sind, die über den hierzu nötigen Schlüssel verfügen.

Absatz 2

Absatz 2 regelt die Voraussetzungen, unter denen die PIU ausnahmsweise mündlich Daten bekanntgeben kann. Dies ist allerdings nur zulässig, wenn Gefahr im Verzug ist.

Gefahr im Verzug liegt insbesondere vor, wenn die ordentliche Datenbekanntgabe zu langsam wäre, um

- eine unmittelbar drohende Straftat nach Anhang 2 FPG zu verhindern oder
- eine Person an der Ausreise zu hindern, die sich mit grosser Wahrscheinlichkeit einer solchen Straftat schuldig gemacht hat.

Absatz 3

Auch über eine mündliche Datenbekanntgabe nach Absatz 2 muss im Nachgang ein Protokoll erstellt werden. Es gibt nicht nur Aufschluss über die bekanntgegebenen Daten, das Datum des Gesprächs und die Identität der daran beteiligten Personen, sondern auch über die besonderen Umstände, die diese Art der Datenbekanntgabe rechtfertigten.

Artikel 8 Erinnerung der zuständigen Behörden an ihre Meldepflicht

Das FPG sieht vor, dass Flugpassagierdaten, die einer zuständigen Behörde (vgl. Art. 1 Abs. 2 FPG) aufgrund des automatischen Abgleichs oder auf deren Antrag bekanntgegeben werden, von der PIU elektronisch zu markieren sind (vgl. Art. 7 Abs. 3 FPG). Die markierten Daten unterstehen fortan der fünfjährigen Speicherfrist.

Allerdings kann eine zuständige Behörde zum Schluss gelangen, dass der ursprüngliche Verdacht gegen eine Person unbegründet ist.

Beispiel: *Der Verdacht, dass Passagier x Person y ermordet hat, wird anlässlich der ersten Einvernahme durch ein stichhaltiges Alibi entkräftet.*

In einem solchen Fall muss die Behörde der PIU mitteilen, dass sich der Verdacht als unbegründet erwiesen hat und sie die Daten nicht mehr benötigt. Die PIU hebt sodann unverzüglich die Markierung der betroffenen Daten auf (vgl. Art. 10 FPG).

Mit der Aufhebung der Markierung gelten diese Daten wieder als unmarkiert und unterstehen den für diese Daten geltenden Regelungen, so insbesondere der auf sechs Monate verkürzten Speicherfrist (vgl. Art. 21 Abs. 1 FPG).

Artikel 8 sieht vor, dass die zuständigen Behörden zumindest im ersten Monat nach der Datenbekanntgabe an ihre Mitteilungspflicht erinnert werden. Denn in diesem Zeitabschnitt ist am ehesten damit zu rechnen, dass sich ein Verdacht als unbegründet erweist.

Mit dieser Erinnerung soll erwirkt werden, dass bekanntgegebene Daten

- zügig durch die zuständige Behörde geprüft werden und
- nicht länger markiert bleiben, als sich dies rechtfertigen lässt.

Absatz 1

Die zuständige Behörde wird 20 Tage nach Erhalt von Flugpassagierdaten an ihre Mitteilungspflicht nach Artikel 10 FPG erinnert.

Absatz 2

Erhält die PIU innert 10 Tagen nach der Erinnerung keine oder keine den Bedarf nach diesen Daten bestätigende Antwort, wird die Markierung aufgehoben. Die Daten gelten fortan als unmarkiert. Danach sind sie, je nach dem Datum ihres ursprünglichen Eingangs bei der PIU, unverzüglich zu pseudonymisieren oder zu löschen.

Absatz 3

Sowohl die Erinnerung, welche die PIU den zuständigen Behörden zukommen lässt, als auch die Aufhebung der Markierung der betroffenen Daten können automatisch ausgelöst werden.

Nicht zulässig ist dagegen eine automatische Antwort, mit der eine zuständige Behörde den Bedarf dieser Daten bestätigt. Denn damit würde der Zweck des Erinnerungsmanagements untergraben: Nur Daten, die tatsächlich zur Bekämpfung von Straftaten nach Anhang 2 des Gesetzes benötigt werden, sollen länger als sechs Monate gespeichert werden dürfen.

3. Abschnitt: Datenbekanntgabe ins Ausland durch die Luftverkehrsunternehmen

Artikel 9

Artikel 9 legt fest, wie Artikel 2 Absatz 2 FPG umzusetzen ist.

Artikel 2 Absatz 2 FPG legt die Voraussetzung fest, die ein Staat zu erfüllen hat, an den die in der Schweiz ansässigen Luftverkehrsunternehmen die Flugpassagierdaten bekanntgeben dürfen.

Artikel 2 Absatz 2 FPG erfuhr im Rahmen der parlamentarischen Beratung eine Änderung. Zwar hielten die eidgenössischen Räte am Grundsatz fest, dass Flugpassagierdaten ins Ausland bekanntgegeben werden dürfen, wenn ein völkerrechtlicher Vertrag

mit der Schweiz dies vorsieht. Gemäss Artikel 2 Absatz 2 FPG bedarf es neu keines völkerrechtlichen Vertrages mit einem Staat, der Gewähr für die Einhaltung der für PNR geltenden Standards und Empfehlungen nach Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt bietet.

Anhang 9 ist im Übrigen gemäss Artikel 122*p* der Luftfahrtverordnung vom 14. November 1973[13] (LFV) für die Schweiz seit dem 1. Januar 2019 zur Durchführung von Massnahmen für Erleichterungen in der Luftfahrt (Facilitation) «unmittelbar anwendbar».

Die für die Bearbeitung von Flugpassagierdaten nach dem FPG geltenden Standards und Empfehlungen sind solche Massnahmen. Sie bezwecken, dass die rechtlichen Rahmenbedingungen in den Vertragsstaaten

- im Interesse der Luftverkehrsunternehmen möglichst einheitlich sind
- und im Interesse der Passagierinnen und Passagiere eine datenschutzrechtlich vertretbare Bearbeitung der bekanntgegebenen Daten vorsehen.

Die für die Flugpassagierdaten nach dem FPG geltenden Standards und Empfehlungen finden sich im Kapitel D des Anhangs 9 (Ziffern 9.24 – 9.39).

Absatz 1

Durch Absatz 1 wird fedpol verpflichtet, eine Liste der Staaten zu führen, welche die Voraussetzungen nach Artikel 2 Absatz 2 FPG erfüllen.

Absatz 2

Die Liste umfasst all jene Staaten, die

a) mit der Schweiz einen völkerrechtlichen Vertrag über die Bekanntgabe der Flugpassagierdaten abgeschlossen haben; oder

b) das Übereinkommen über die internationale Zivilluftfahrt unterzeichnet und sich als Vertragsstaat vorbehaltlos den Standards in Anhang 9 verpflichtet haben; oder

c) aufgrund einer Prüfung durch fedpol insbesondere die datenschutzrechtlichen Standards und Empfehlungen gemäss Anhang 9 umsetzen und zusichern, die Schweiz über wichtige Änderungen in der Umsetzung dieser Standards und Empfehlungen zu informieren.

Erfüllt ein Staat eine dieser drei Voraussetzungen, und hat der Bundesrat davon Kenntnis genommen, veröffentlicht fedpol die um diesen Staat ergänzte Liste.

Die in der Schweiz ansässigen Luftverkehrsunternehmen dürfen ihre Flugpassagierdaten an all diese, in der veröffentlichten Liste ausgewiesenen Staaten bekanntgeben.

Absatz 3

Absatz 3 regelt den ersten Schritt des Prüfverfahrens, das ein Staat zu durchlaufen hat, der die Bekanntgabe der Flugpassagierdaten aus der Schweiz wünscht, aber mit ihr keinen völkerrechtlichen Vertrag abgeschlossen und auch das Übereinkommen nicht oder nicht vorbehaltlos unterzeichnet hat.

[13] SR **748.01**

Ziffer 1

In einem ersten Schritt eröffnet fedpol einem solchen Staat die Möglichkeit, anhand eines Fragebogens darzulegen, *wie* er die Flugpassagierdaten bearbeitet. Bei Staaten, die zwar das Übereinkommen unterzeichnet haben, aber Vorbehalte gegen einzelne, für die Flugpassagierdaten nach dem FPG geltenden Standards angebracht haben, kann fedpol diese Prüfung auf jene Regelungen beschränken, welche die Standards mit Vorbehalten betreffen.

Aus Sicht der Schweiz von Interesse sind in Zusammenhang mit den Flugpassagierdaten insbesondere die datenschutzrechtlich relevanten Standards, so jene zu den Löschfristen (Ziff. 9.31f.), die Rechte der Passagierinnen und Passagiere (Ziff. 9.26f.) und die Unabhängigkeit der Aufsichtsbehörde (Ziff. 9.29). Zudem soll der Zweck, der eine Bearbeitung der Daten erlaubt, begrenzt sein. Dies soll auch für Behörden gelten, an welche die Daten aus der Schweiz weitergegeben werden (Ziff. 9.25 Bst. b und c).

Die Ausführungen des befragten Staates müssen nachvollziehbar und damit plausibel sein. Denn fedpol wird sodann gemäss Absatz 4 prüfen, ob er mit seiner Bearbeitung der Flugpassagierdaten insbesondere den datenschutzrechtlich relevanten Standards nach Anhang 9 entspricht.

Die Empfehlungen äussern sich dazu, welche der möglichen Umsetzungen von Standards wünschbar wäre. Auch aus Sicht der Schweiz wäre es wünschbar, dass ein Staat bei der Bearbeitung der Flugpassagierdaten die Empfehlungen gemäss Anhang 9 berücksichtigt. Denn diese orientieren sich materiell am europäischen Datenschutzrecht und weichen damit kaum von den Regelungen im FPG und DSG ab. Verbindlich sind die Empfehlungen jedoch selbst für Staaten nicht, welche das Übereinkommen über die internationale Zivilluftfahrt unterzeichnet haben.

Ziffer 2

Zudem muss sich der Staat bereit erklären, die Schweiz zeitgerecht über wesentliche Änderungen in der Bearbeitung der Flugpassagierdaten zu informieren.

Wesentlich ist eine Änderung insbesondere dann, wenn sie die Bandbreite eines bisher eingehaltenen Standards sprengt.

Absatz 4

Fedpol muss sodann die Angaben des befragten Staates prüfen. Primär wird es sich dabei um eine Prüfung der Plausibilität handeln, denkbar ist aber auch ein Besuch vor Ort.

Die Prüfung durch fedpol ist positiv abgeschlossen, wenn die dargelegten Regelungen des befragten Staates insbesondere den datenschutzrechtlich relevanten Standards nach Anhang 9 oder einzelnen Empfehlungen dazu entsprechen. Positiv abschliessen kann diese Prüfung selbst ein Staat, der Vorbehalte gegen datenschutzrelevante Standards angebracht hat, so namentlich dann, wenn er über eine innerstaatliche Regelung verfügt, die diesen Standards entspricht, ohne die Vorbehalte offiziell zurückgezogen zu haben.

Absatz 5

Weicht ein Staat indes von einem oder mehreren der datenschutzrechtlich relevanten Standards ab, wird auf dem Verhandlungsweg eine Lösung anzustreben sein, die den

in der Schweiz ansässigen Luftverkehrsunternehmen eine Datenbekanntgabe gemäss Artikel 2 Absatz 2 FPG ermöglicht.

Die Lösung kann in einem völkerrechtlichen Vertrag oder in einem Austausch diplomatischer Noten − oder kurz Notenaustausch – bestehen.

4. Abschnitt: Risikoprofile und Beobachtungslisten

Artikel 10

Gemäss Artikel 15 FPG hat der Bundesrat den Einsatz der Risikoprofile und der Beobachtungslisten zu überprüfen.

Absatz 1

Die Überprüfung durch den Bundesrat soll jährlich und auf der Basis eines Berichts des Eidgenössischen Justiz- und Polizeidepartements (EJPD) erfolgen.

Der Bericht soll dem Bundesrat ein möglichst aufschlussreiches Bild über den Einsatz der Risikoprofile und der Beobachtungslisten ermöglichen. Deshalb ist die Aufzählung der Berichtsinhalte nicht abschliessend.

Buchstabe a

Der Bericht äussert sich namentlich zur Zahl der eingesetzten Risikoprofile und Beobachtungslisten sowie zu deren durchschnittlicher Laufzeit und Schwerpunkte.

Zum heutigen Zeitpunkt ist davon auszugehen, dass Risikoprofile schwerpunktmässig im Kampf gegen die organisierte Kriminalität und gegen Menschenhandel zum Einsatz gelangen. Dieser Schwerpunkt kann sich indes mit der Zeit ändern. Beobachtungslisten dürften dagegen insbesondere dann zum Einsatz kommen, wenn flüchtige Verurteilte direkt oder indirekt gesucht werden oder wenn von Tatverdächtigen nur einzelne Angaben wie beispielsweise Telefon- oder Kreditkartennummer verfügbar sind.

Buchstabe b

Zusätzlich soll sich der Bericht zur Erforderlichkeit und Eignung der Risikoprofile und Beobachtungslisten äussern (Bst. b).

Der Einsatz von Risikoprofilen ist aufgrund ihrer Abstraktheit anspruchsvoll. Denn Gegenstand eines Risikoprofils können nur Daten sein, die nicht einer bestimmten natürlichen Person zuordenbar sind. Damit besteht die Gefahr, dass Risikoprofile zu wenig konkret ist und damit zu viele Treffer generiert.

Risikoprofile sollen nur eingesetzt werden, wenn stichhaltige Hinweise auf eine wiederholte Schwerstkriminalität vorliegen, die einem gleichen Muster folgt. Nur in diesem Fall lässt sich der Einsatz eines Risikoprofils, das eine Form der Rasterfahndung darstellt, rechtfertigen und ist damit erforderlich.

Geeignet ist ein Risikoprofil, wenn es sich aus hinreichenden Kriterien zusammensetzt, welche die Zahl der Treffer und damit den Kreis der betroffenen Passagierinnen und Passagiere eingrenzt. Um dies sicherzustellen, führt die PIU vor der Aufschaltung eines Risikoprofils Tests durch (vgl. Art. 12 Abs. 3 FPG).

Demgegenüber setzen sich Beobachtungslisten aus Daten natürlicher und allenfalls juristischer Personen zusammen: Namen, Kontaktdaten, eine Kreditkartennummer,

das Geburtsdatum usw. Beobachtungslisten sind dadurch konkreter und damit einfacher in ihrem Einsatz als Risikoprofile. Dennoch gilt auch hier: Geeignet ist eine Beobachtungsliste nur, wenn sie sich aus den nötigen Daten zusammensetzt, welche möglichst eindeutig zur gesuchten Person führen. Je weniger solche Daten verfügbar sind, desto mehr kann es zu Fehl-Treffern kommen.

Absatz 2

Der Bericht des EJPD bildet die Grundlage für die jährliche Überprüfung der von der PIU eingesetzten Risikoprofile und Beobachtungslisten durch den Bundesrat.

Dieser informiert das Parlament im Anhang zum Geschäftsbericht über die Ergebnisse seiner Überprüfung.

Vertiefte Informationen an parlamentarische Kommissionen, die dies wünschen, sind mit dieser Regelung nicht ausgeschlossen.

Absatz 3

Nicht Gegenstand der bundesrätlichen Überprüfung sind Beobachtungslisten nach Artikel 14 FPG. Denn das zuständige Zwangsmassnahmengericht entscheidet über ihren Einsatz, was eine bundesrätliche Überprüfung ausschliesst.

Gegenstand der bundesrätlichen Überprüfung sind somit die Risikoprofile nach Artikel 12 und die Beobachtungslisten nach Artikel 13 FPG.

5. Abschnitt: Datenschutz

Artikel 11 Anträge um Aufhebung der Pseudonymisierung

Das Bundesverwaltungsgericht entscheidet über die Aufhebung der Pseudonymisierung, wenn dies von einer zuständigen Behörde beantragt wird. Dabei kann es sich um eine ordentliche Aufhebung der Pseudonymisierung (vgl. Art. 19 FPG) handeln oder um eine solche bei Dringlichkeit (vgl. Art. 20 FPG). Der gerichtliche Entscheid ist gemäss Artikel 83 Buchstabe a des Bundesgerichtsgesetzes vom 17. Juni 2005[14] in beiden Fällen endgültig.

Artikel 11 legt fest, wie die PIU die Anträge der zuständigen Behörden um Aufhebung der Pseudonymisierung vorzuprüfen hat.

Artikel 12 Aufhebung und Wiederherstellung der Pseudonymisierung

Mit Artikel 12 wird die Zuständigkeit, die Pseudonymisierung aufzuheben (Bst. a) und je nachdem unverzüglich wiederherzustellen (Bst. b), auf wenige Personen innerhalb der PIU zu beschränken. Diese Besonderheit rechtfertigt sich, weil beide Bearbeitungsschritte datenschutzrechtlich einschneidend sind und sich aufgrund ihrer Spezifität nicht automatisch durchführen lassen. Zudem muss die zuständige Person sicherstellen, dass das Protokoll auf das diesen Bearbeitungsschritt legitimierende Dokument verweist (vgl. Art. 13 Abs. 2).

[14] SR **173.110**

Buchstabe a

Auslöser für die Aufhebung der Pseudonymisierung ist entweder der Antrag einer zuständigen Behörde (vgl. Art. 19 und 20 FPG) oder aber das Gesuch einer Person um Auskunft über ihre Daten (Art. 26 FPG). Wie bereits ausgeführt, entscheidet das Bundesverwaltungsgericht über die Aufhebung der Pseudonymisierung auf Antrag einer zuständigen Behörde. Keines Gerichtsentscheids bedarf es dagegen, wenn ein Auskunftsbegehren der betroffenen Person vorliegt und ihre Daten pseudonymisiert sind. Denn aus Artikel 25 Absatz 2 des Datenschutzgesetzes vom 25. September 2020[15] ergibt sich, dass der betroffenen Person in der erteilten Auskunft auch «die bearbeiteten Personendaten» mitzuteilen sind. Sind diese pseudonymisiert, muss die Pseudonymisierung aufgehoben werden – quasi auf Begehren der um Auskunft ersuchenden Person.

Buchstabe b

In den zwei Fällen, die in Buchstabe b explizit genannt werden, muss die Pseudonymisierung unverzüglich nach ihrer Aufhebung wiederhergestellt werden.

Dabei handelt es sich immer um Daten, die vorher pseudonymisiert waren. Zudem stellt Buchstabe b eine Rechtfolge klar, die sich nur implizit aus dem Gesetz ergibt.

Nicht erwähnt wird unter Buchstabe b die Wiederherstellung der Pseudonymisierung von Daten, deren Markierung gemäss Artikel 10 Absatz 2 FPG aufgehoben wird. Dass diese Daten zu pseudonymisieren sind, sofern sie nicht aufgrund ihres Alters zu löschen sind, ergibt sich aus Artikel 18 Absatz 2 FPG. Namentlich aus diesem Grund erübrigt sich hier eine Regelung auf Verordnungsebene.

Artikel 13 Protokolle

Alle automatisierten Bearbeitungen von Flugpassagierdaten durch die PIU sind elektronisch zu protokollieren (vgl. Art. 24 FPG). So insbesondere:

a) die Bekanntgaben nach den Artikeln 7−11 und 30 FPG;
b) die Pseudonymisierung nach Artikel 18 sowie deren Aufhebung nach den Artikeln 19 und 20 FPG;
c) die Aufhebung der Pseudonymisierung nach Artikel 26 Absatz 1 FPG;
d) die unverzügliche Wiederherstellung der Pseudonymisierung in den Fällen von Artikel 20 Absatz 4 und 26 Absatz 1 FPG;
e) die Löschungen nach den Artikeln 21 und 22 FPG;
f) die Anonymisierung nach Artikel 23 FPG.

Die Protokolle dürfen nur zur Überprüfung der Einhaltung des Datenschutzes sowie zur Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten genutzt werden.

[15] SR **235.1**

Gespeichert werden die Protokolle ausserhalb des PNR-Informationssystems, aber innerhalb des Bundes in der IT-Umgebung des ISC-EJPD.[16]

Die Zugriffe der PIU auf die Informationssysteme des Bundes im Rahmen von Artikel 6 FPG sind nicht Gegenstand von Artikel 13, sondern werden in den von diesen Informationssystemen zu erstellenden Protokollen erfasst.

Absatz 1

Diese Bestimmung nennt die zwingenden Inhalte der Protokolle und entspricht Artikel 4 Absatz 4 der Datenschutzverordnung vom 31. August 2022[17].

Absatz 2

Zusätzlich zu den Angaben nach Absatz 2 ist im Protokoll über eine Aufhebung der Pseudonymisierung und ihre allfällige Wiederherstellung auf das Dokument zu verweisen, das zu diesem Bearbeitungsschritt legitimiert. Dadurch wird die Nachvollziehbarkeit dieser Bearbeitungsschritte für jene Personen vereinfacht, die gemäss Artikel 25 FPG Überwachungs- und Aufsichtsaufgaben wahrnehmen.

6. Abschnitt: Administrative Sanktionen

Artikel 14 Zeitpunkt

Luftverkehrsunternehmen müssen ihren Pflichten nach den Artikeln 3 und 4 FPG erst nachkommen, wenn die PIU ihnen die Einzelheiten ihrer technischen Anbindung an das PNR-Informationssystem mitgeteilt hat. Die Mitteilung erfolgt in Form einer Verfügung.

Erst ab diesem Zeitpunkt müssen die Luftverkehrsunternehmen mit Sanktionen rechnen, wenn sie ihren Pflichten nach den Artikeln 3 und 4 FPG nicht nachgekommen sind. Weisen sie indes nach, dass sie alle zumutbaren technischen und organisatorische Massnahmen getroffen haben, entfällt die Sanktion (vgl. Art. 31 FPG).

Artikel 15 Prüfung

Mit Artikel 32 Absatz 2 FPG wird die PIU verpflichtet, von einer Sanktion abzusehen, wenn ein Luftverkehrsunternehmen für den gleichen Flug bereits gestützt auf Artikel 122*b* des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005[18] (AIG) durch das Staatssekretariat für Migration (SEM) sanktioniert wird.

Da es sich hierbei um eine objektive Strafbarkeitsbedingung handelt, hat die PIU vor jeder Sanktion von Amtes wegen abzuklären, ob das SEM hinsichtlich des gleichen Fluges bereits ein Verfahren im Sinne von Art. 122*b* AIG führt.[19]

---

[16] Botschaft vom 15. Mai 2025 zum FPG, Erläuterungen zu Artikel 24 Absatz 4 FPG; BBl **2024** 1485

[17] SR **235.11**

[18] SR **142.20**

[19] Urteil des Bundesverwaltungsgerichts A-1679/2016 vom 31. Januar 2017

3.2 Änderung anderer Erlasse

Artikel 6 FPG sieht vor, dass alle Flugpassagierdaten nach ihrem Eintreffen bei der PIU mit zwei polizeilichen Informationssystemen (RIPOL, N-SIS) automatisch abgeglichen werden (Abs. 1). Die dabei erzielten Übereinstimmungen hat die PIU manuell und unter Zugriff auf diese und sechs weitere Informationssysteme des Bundes zu überprüfen Abs. 2 und 3). Nur positiv überprüfte Übereinstimmungen dürfen an eine zuständige Behörde des Bundes oder der Kantone bekanntgegeben werden.

Um die Zugriffsrechte der PIU im verlangten Detaillierungsgrad zu regeln, müssen acht Verordnungen über diese Informationssysteme angepasst werden.

3.2.1 Visa-Informationssystem-Verordnung vom 18. Dezember 2013[20]

Art. 10 Abs. 1 Bst. f Ziff. 8

Artikel 10 Absatz 1 Buchstabe f dieser Verordnung nennt die Einheiten von fedpol, die berechtigt sind, Abfragen im nationalen Visumsystem (Orbis) vorzunehmen. Mit der neuen Ziff. 8 wird in dieser Aufzählung künftig auch die PIU aufgeführt, die den Zugriff für die Abklärung der Identität einer Person benötigt, deren Daten beim automatischen Abgleich nach Artikel 6 FPG eine Übereinstimmung erzielt haben (vgl. Art. 6 Abs. 3 Bst. b Ziff. 2 FPG).

Anhang 2

Datenspezifisch umgesetzt werden die Zugriffsrechte der PIU auf Orbis mit der Anpassung von Anhang 2 dieser Verordnung. Der Zugriff beschränkt sich auf Daten, die es der PIU ermöglichen, die Identität einer Person zu überprüfen.

Zu diesen Daten gehören nicht nur Angaben zur Person, sondern auch zum mitgeführten Visum. Denn die Nummer, der Ausstellerstaat, Art und Ablaufdatum des mitgeführten Visums oder Aufenthaltstitels sind Daten, die von den Luftverkehrsunternehmen in Kategorie 18 des PNR-Datensatzes (vgl. Anhang 1 FPG) zu übermitteln sind, soweit die Daten verfügbar sind (vgl. Art. 92a Abs. 3 Bst. c AIG). Die hinterlegten Angaben zu den Dokumenten ermöglichen der PIU, Rückschlüsse auf die Verlässlichkeit der Angaben in den mitgeführten Dokumenten (Kategorie 18 des Flugpassagierdatensatzes gemäss Anhang 1 FPG) zu ziehen.

3.2.2 ZEMIS-Verordnung vom 12. April 2006[21]

Art. 9 Bst. b Ziff. 9

Artikel 9 dieser Verordnung nennt die Einheiten, denen das Staatssekretariat für Migration den Zugang zu Daten im Zentralen Migrationsinformationssystem (ZEMIS) einräumen kann. Mit der neuen Ziff. 9 wird die Aufzählung in Buchstabe b mit der PIU ergänzt, die künftig den Zugriff im Abrufverfahren für die Abklärung der Identität einer Person benötigt, deren Daten beim automatischen Abgleich nach Artikel 6 FPG eine Übereinstimmung erzielt haben (vgl. Art. 6 Abs. 3 Bst. b Ziff. 2 FPG).

[20] SR **142.512**

[21] SR **142.513**

Anhang 1

Datenspezifisch umgesetzt werden die Zugriffsrechte der PIU auf das ZEMIS mit der Neufassung von Anhang 1 dieser Verordnung.

Der Zugriff auf ZEMIS ermöglicht es der PIU, Personendaten von Ausländerinnen und Ausländern in der Schweiz und Daten zur Ausstellung von schweizerischen Reisedokumenten und Bewilligungen zur Wiedereinreise von Ausländerinnen und Ausländer zu überprüfen. Die hinterlegten Angaben zu den Dokumenten ermöglichen der PIU, Rückschlüsse auf die Verlässlichkeit der Angaben in den mitgeführten Dokumenten (Kategorie 18 des Flugpassagierdatensatzes gemäss Anhang 1 FPG) zu ziehen.

3.2.3 Ausweisverordnung vom 20. September 2002[22]

Anhang 1

Mit der Neufassung von Anhang 1 werden der PIU datenspezifisch die nötigen Zugriffe auf das Informationssystem Ausweisschriften (ISA) eingeräumt. Die PIU benötigt diese Informationen, damit sie die Identität einer Person überprüfen kann, deren Daten beim automatischen Abgleich nach Artikel 6 FPG eine Übereinstimmung erzielt haben (vgl. Art. 6 Abs. 3 Bst. b Ziff. 2 FPG).

Für die Identitätsüberprüfung kann die PIU auf Daten zugreifen, die im Pass oder in der Identitätskarte von Schweizer Staatsangehörigen hinterlegt sind. Auf die Angaben zu den Dokumenten darf die PIU ebenfalls zugreifen. Dies ermöglicht ihr Rückschlüsse auf die Verlässlichkeit der Angaben in den mitgeführten Dokumenten (Kategorie 18 des Flugpassagierdatensatzes gemäss Anhang 1 FPG).

3.2.4 NES-Verordnung vom 15. Oktober 2008[23]

Ingress

Da der Ingress dieser Verordnung alle gesetzlichen Grundlagen der Verordnung nennt, muss neu auch Artikel 6 Absatz 3 Buchstabe a Ziffer 1 FPG als gesetzliche Grundlage für die vorliegende Änderung aufgeführt werden.

Art. 11 Abs. 1 Bst. m.

Mit der Ergänzung von Artikel 11 Absatz 1 wird die PIU berechtigt, Zugriff auf Daten des Nationalen Ermittlungssystems (NES) zu nehmen und damit nach Artikel 6 Absatz 3 Buchstabe a Ziffer 1 FPG zu überprüfen, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG aufgeführten Tatbestand erfüllt.

Anhang 2, Ziff. 1.1 und 1.2

Anhang 2 weist datenspezifisch die Zugriffsberechtigungen der PIU auf das System zur Unterstützung gerichtspolizeilicher Ermittlungen des Bundes (Ziff. 1.1; vgl. Art. 2 Abs. 3 NES-Verordnung) sowie auf das System Bundesdelikte (Ziff. 1.2; vgl. Art. 2 Abs. 2 NES-Verordnung) aus.

---

[22] SR **143.11**

[23] SR **360.2**

Diese Zugriffe benötigt die PIU namentlich zur Abklärung, ob die qualifizierenden Elemente einer Straftat vorliegen. Denn verschiedene Straftatbestände, die im Deliktskatalog in Anhang 2 FPG aufgeführt sind, berechtigen nur dann zur Bearbeitung der Flugpassagierdaten, wenn diese Elemente vorliegen.

Beispiel: Diebstahl allein reicht gemäss Ziffer 2.1.12.1 von Anhang 2 FPG nicht aus, Flugpassagierdaten zu bearbeiten. Vielmehr muss es im konkreten Fall um eine qualifizierte Form dieser Straftat gehen. Dies ist unteranderem gegeben, wenn Gewerbsmässigkeit vorliegt oder wenn dabei eine Waffe mitgeführt worden ist (vgl. Art. 139 Abs, 3 StGB). Nur dann liegt Schwerstkriminalität vor, die den Einsatz von PNR datenschutzrechtlich zu rechtfertigen vermag.

3.2.5 RIPOL-Verordnung vom 26. Oktober 2016[24]

Art. 6 Abs. 1 Bst. a^{bis} Ziff. 3

Mit der Ergänzung von Art. 6 Abs. 1 Bst. a^{bis} wird die PIU berechtigt,

- den automatischen Abgleich mit dem automatisierten Polizeifahndungssystem (RIPOL) nach Artikel 6 Absatz 1 FPG durchzuführen und
- nach Artikel 6 Absatz 2 FPG die im Rahmen des automatischen Abgleichs erzielte Übereinstimmungen zu überprüfen.

Anhang 1

Die Neufassung von Anhang 1 dieser Verordnung sieht auch die datenspezifische Festlegung der Zugriffsrechte vor, über welche die PIU («fedpol II») künftig zu verfügen muss.

Die ausgewiesenen Zugriffe sind sowohl für den automatischen Abgleich wie für die manuelle Überprüfung massgebend.

Aufgrund des automatischen Abgleichs können lediglich jene Daten Übereinstimmungen auslösen, die sowohl in RIPOL wie auch im Flugpassagierdatensatz gemäss Anhang 1 FPG aufgeführt sind, so insbesondere Namen, Kontaktdaten, Angaben aus und zu den Reisedokumenten.

Gegenstand der manuellen Überprüfung ist einerseits die Frage, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG enthaltenen Tatbestand erfüllt. Dazu benötigt die PIU Hintergrundinformationen, woraus sich qualifizierende Elemente der begangenen Straftat eruieren lassen. Anderseits muss die Identität der betroffenen Person abgeklärt werden. Unter Ziffer 1 (Personen-Datenbank) finden sich Angaben zu polizeilich bekannten Personen. Handelt es sich um eine unbekannte Täterschaft, ist auf Daten unter Ziffer 2 (Ungeklärte Straftaten) zuzugreifen.

3.2.6 IPAS-Verordnung vom 15. Oktober 2008[25];

Anhang 2

[24] SR **361.0**

[25] SR **361.2**

Die Tabelle «Internationale Polizeikooperation» legt datenspezifisch neu auch die Zugriffsberechtigungen auf das Informatisierte Personennachweis-, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (IPAS) fest. Diese Informationen benötigt die PIU für die Prüfung, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG aufgeführten Tatbestand erfüllt (Art. 6 Abs. 3 Bst. a Ziffer 1 FPG). Siehe dazu die Erläuterungen unter Ziff. 3.2.4 betreffend Anhang 2.

3.2.7 Polizeiindex-Verordnung vom 15. Oktober 2008[26];

Art. 5 Abs. 1 Bst. e^{bis}

Mit der Ergänzung von Artikel 5 Absatz 1 der Verordnung wird die PIU berechtigt, Zugriff auf Daten des Nationalen Polizeiindex zu nehmen, um abzuklären, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG aufgeführten Tatbestand erfüllt (Art. 6 Abs. 3 Bst. a Ziffer 1 FPG).

Anhang

Die Tabelle «Internationale Polizeikooperation (IPK)» im Anhang zur Verordnung weist die Zugriffsberechtigungen datenspezifisch aus und neu auch jene der PIU.

3.2.8 N-SIS-Verordnung vom 8. März 2013[27]

Art. 7 Abs. 1 Bst. a. Ziff. 10

Mit der Ergänzung von Artikel 7 Absatz 1 Buchstabe a der Verordnung wird die PIU berechtigt

- den automatischen Abgleich mit den im Schengener Informationssystem (SIS) gespeicherten Daten nach Artikel 6 Absatz 1 FPG durchzuführen und
- nach Artikel 6 Absatz 2 FPG die im Rahmen des automatischen Abgleichs erzielte Übereinstimmungen zu überprüfen.

Gegenstand der manuellen Überprüfung ist nicht nur Frage, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG aufgeführten Tatbestand erfüllt, sondern auch die Abklärung der Identität jener Person, deren Daten beim automatischen Abgleich eine Übereinstimmung erzielt haben.

Anhang 2, Ziffer 1 und Anhang 3 Ziffer 1

Mit der Neufassung der beiden Anhänge werden die Zugriffsrechte der PIU (Anhang 2: fedpol V; Anhang 3: fedpol XI) datenspezifisch festgelegt.

Die ausgewiesenen Zugriffe sind sowohl für den automatischen Abgleich wie für die manuelle Überprüfung massgebend.

Aufgrund des automatischen Abgleichs können lediglich jene Daten Übereinstimmungen auslösen, die sowohl in N-SIS wie auch im Flugpassagierdatensatz gemäss Anhang 1 FPG aufgeführt sind, so insbesondere Namen, Kontaktdaten, Angaben zu und aus den Reisedokumenten.

[26] SR **361.4**

[27] SR **362.0**

Gegenstand der manuellen Überprüfung ist einerseits die Frage, ob die im Raum stehende Straftat einen im Deliktskatalog nach Anhang 2 FPG aufgeführten Tatbestand erfüllt. Dazu benötigt die PIU Hintergrundinformationen zur Straftat, woraus sich qualifizierende Elemente einer Straftat eruieren lassen. Die nötigen Angaben finden sich im N-SIS unter der Rubrik Personenausschreibungen.

Anderseits muss für die Abklärung der Identität der Person, deren Daten beim automatischen Abgleich eine Übereinstimmung erzielt haben, je nachdem nicht nur auf Personen-, sondern allenfalls auch auf einzelne Sachdaten zugegriffen werden können. Zu letzterer Datenkategorie zählen die Angaben zu und aus Reisedokumenten, nach denen gefahndet wird (Sachausschreibungen, Bst. I). Denn daraus lassen sich allfällige Rückschlüsse auf eine falsche Identität ziehen.

4 Auswirkungen

Die Auswirkungen entsprechen jenen, die unter Ziffer 6 der Botschaft des Bundesrates vom 15. Mai 2024[28] zum Flugpassagierdatengesetz ausgewiesen worden sind.

5 Rechtliche Aspekte

Die nachfolgenden Ausführungen beschränken sich auf jene Inhalte, zu denen sich nicht schon die Botschaft vom 15. Mai 2024 zum Flugpassagierdatengesetz geäussert hat.

5.1 Verfassungsmässigkeit

Die VFPG umfasst rechtsetzende sowie Ausführungsbestimmungen.

Auf die Delegationsnorm

- in Artikel 2 Absatz 4 FPG (Bekanntgabe der Flugpassagierdaten) stützen sich die Artikel 1−5 der Verordnung;
- in Artikel 7 Absatz 4 FPG (Bekanntgabe im Falle einer überprüften Übereinstimmung) stützt sich Artikel 7 der Verordnung;
- in Artikel 15 Absatz 2 FPG (Überprüfung der Risikoprofile und Beobachtungslisten) stützt sich Artikel 10 der Verordnung.

Die restlichen Verordnungsbestimmungen weisen Vollzugscharakter auf und stützen sich auf Artikel 33 FPG.

Die Anpassungen der acht Verordnungen weisen ebenfalls Vollzugscharakter auf und basieren auf den folgenden gesetzlichen Grundlagen, die bei Erlass des FPG geschaffen worden sind (vgl. Anhang 3 des FPG):

[28] BBl **2024** 1485

- *Visa-Informationssystem-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich im gemäss Anhang 3 Ziffer 2 FPG ergänzten Artikel 109*c* Buchstabe j des Ausländer- und Integrationsgesetzes vom 16. Dezember 2005[29];
- *ZEMIS-Verordnung:* Die gesetzliche Grundlage für die Änderung findet sich im gemäss Anhang 3 Ziffer 3 FPG ergänzten Artikel 9 Absatz 1 Buchstabe q des Bundesgesetzes vom 20. Juni 2003[30] über das Informationssystem für den Ausländer- und Asylbereich.
- *Ausweisverordnung:* Artikel 6 Absatz 3 Buchstabe b Ziffer 4 FPG bildet unmittelbar die gesetzliche Grundlage für die Revision von Anhang 1 der Ausweisverordnung. Denn das Ausweisgesetz vom 22. Juni 2001[31] sieht die Berechtigung von fedpol und damit der PIU zum Zugriff auf Daten von ISA bereits vor und musste deshalb nicht im Zuge des FPG angepasst werden.
- *NES-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich in den gemäss Anhang 3 Ziffer 6 FPG ergänzten Artikeln 10 und 11 des Bundesgesetzes vom 13. Juni 2008[32] über die polizeilichen Informationssysteme (BPI).
- *RIPOL-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich im gemäss Anhang 3 Ziffer 6 FPG ergänzten Artikel 15 BPI.
- *IPAS-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich im gemäss Anhang 3 Ziffer 6 FPG ergänzten Artikel 12 BPI.
- *Polizeiindex-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich im gemäss Anhang 3 Ziffer 6 FPG ergänzten Artikel 17 BPI.
- *N-SIS-Verordnung:* Die gesetzliche Grundlage dieser Änderung findet sich im gemäss Anhang 3 Ziffer 6 FPG ergänzten Artikel 16 BPI.

Mit Erlass der VFPG sowie der Anpassung der acht Verordnungen entspricht der Bundesrat seiner Kompetenz gemäss Artikel 182 der Bundesverfassung vom 18. April 1999[33].

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Insbesondere die Pflichten der Luftverkehrsunternehmen in den Artikeln 1−5 der Verordnung bewegen sich im Rahmen, der sich aus den für PNR geltenden Standards und Empfehlungen gemäss Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt ergibt, und entsprechen damit den massgeblichen internationalen Verpflichtungen der Schweiz.

[29] SR **142.20**
[30] SR **142.51**
[31] SR **143.1**
[32] SR **361**
[33] SR **101**

5.3 Datenschutz

Mit Artikel 9 setzt die VFPG den im Rahmen der parlamentarischen Beratung ergänzten Artikel 2 Absatz 2 FPG um. Diese Bestimmung regelt, unter welchen Voraussetzungen ein in der Schweiz ansässiges Luftverkehrsunternehmen Daten ins Ausland bekanntgeben darf.

Zulässig soll die Datenbekanntgabe neu auch an einen Staat sein, der Gewähr für die Einhaltung der für PNR geltenden Standards und Empfehlungen gemäss Anhang 9 des Übereinkommens über die internationale Zivilluftfahrt bieten. Die Standards und Empfehlungen tragen dazu bei, dass bei der Bearbeitung der Flugpassagierdaten weltweit ein Mindestmass an Datenschutz zu gewährleisten ist. Bezogen auf die Schweiz erklärt zusätzlich Artikel 122p LFV die Standards und Empfehlungen nach Anhang 9 in der Schweiz als «unmittelbar anwendbar».

In seiner Stellungnahme vom 28. Mai 2025 weist der EDÖB darauf hin, dass Artikel 2 Absatz 2 FPG teilweise von Artikel 16 f. DSG abweicht. Den Angemessenheitsbeschluss, den die EU gegenüber der Schweiz gefällt hat, gilt es deshalb im Auge zu behalten.

Beilagen (Erlassentwürfe)

- Flugpassagierdatenverordnung
- Anpassung der Visa-Informationssystem-Verordnung vom 18. Dezember 2013[34];
- Anpassung der ZEMIS-Verordnung vom 12. April 2006[35];
- Anpassung der Ausweisverordnung vom 20. September 2002[36];
- Anpassung der NES-Verordnung vom 15. Oktober 2008[37];
- Anpassung der RIPOL-Verordnung vom 26. Oktober 2016[38];
- Anpassung der IPAS-Verordnung vom 15. Oktober 2008[39];
- Anpassung der Polizeiindex-Verordnung vom 15. Oktober 2008[40];
- Anpassung der N-SIS-Verordnung vom 8. März 2013[41].

[34] SR **142.512**
[35] SR **142.513**
[36] SR **143.11**
[37] SR **360.2**
[38] SR **361.0**
[39] SR **361.2**
[40] SR **361.4**
[41] SR **362.0**