DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei
Guisanplatz 1A
3003 Bern

Per E-Mail an: kd-rechtsabteilung@fedpol.admin.ch

27. Juli 2022

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

Sehr geehrte Damen und Herren

Am 13. April 2022 eröffnete der Bundesrat die Vernehmlassung zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Flugpassagierdatengesetz, FPG). Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur, weitreichende Transparenz sowie Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Gerne nehmen wir zum Entwurf wie folgt Stellung:

1. Grundsätzliches

Mit dem Flugpassagierdatengesetz (FPG) müssen verdachtsunabhängig alle Flugpassagierdaten von den Airlines an eine neu geschaffene Stelle (Passenger Information Unit, PIU), die dem fedpol angegliedert ist, übermittelt werden. Diese bearbeitet die Daten, insbesondere durch Speichern, Abgleichen und Weiterleiten oder kann sogar Risikoprofile daraus erstellen.

Gemäss dem erläuternden Bericht stellt die verdachtsunabhängige Bearbeitung von Personendaten einen «Paradigmenwechsel» für die Schweiz dar. Als Rechtfertigung für diesen Paradigmenwechsel wird mit der Erhöhung der Sicherheit für die ganze Gesellschaft argumentiert. Das FPG soll der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten dienen (vgl. Art. 1 lit. a FPG). Mit dem Übermitteln, Speichern und Abgleichen sämtlicher Flugpassagierdaten wird dabei stark in die Grundrechte der Individuen eingegriffen.

Trotz diesem Paradigmenwechsel und den schwerwiegenden Grundrechtseingriffen bietet das FPG aber keinen genügenden Datenschutz. Die Erhebung sämtlicher, verdachtsunabhängiger Flugpassagierdaten ist nicht verhältnismässig. Zudem ist äusserst fraglich, ob die verdachtsunabhängige Erhebung sämtlicher Flugpassagierdaten tatsächlich der Bekämpfung des Terrorismus dient und zur Erhöhung der Sicherheit führt.

Dass dies nur leere Schlagwörter sind, die das tatsächliche Ziel des Gesetzes, die Massenüberwachung, verschleiern, wird u. a. durch die zu weitgehenden Deliktskataloge deutlich. Unter dem Vorwand des Terrorismus und der Sicherheit werden mit dem FPG digitale Ein- und Ausreisekontrollen geschaffen. Auch das erklärte Ziel, für mehr Transparenz bei den Flugpassagier:innen zu sorgen, wird durch das Unwissen darüber, auf welche Informationssysteme zugegriffen werden kann, die Erstellung von Risikoprofilen und Beobachtungslisten sowie die Streckenbestimmung des Nachrichtendienst des Bundes (NDB) vollkommen unglaubwürdig.

Die Digitale Gesellschaft lehnt die verdachtsunabhängige Erhebung von Personendaten und damit das Flugpassagierdatengesetz ausdrücklich ab.

Wir positionieren uns deutlich gegen Massenüberwachungsmassnahmen, so z. B. auch gegen die Vorratsdatenspeicherung (gemäss Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs, BÜPF), bei der die Telekommunikationsprovider Daten aufbewahren müssen. Das FPG geht aber noch

darüber hinaus, da die Airlines die Daten direkt an die PIU weiterleiten müssen, wie wenn bei der Vorratsdatenspeicherung die Provider die Daten direkt an die Überwachungsbehörde weiterleiten müssten. Das FPG geht damit nicht nur eindeutig zu weit, sondern ist gänzlich abzulehnen.

Von dieser allgemeinen Ablehnung gegenüber dem Flugpassagierdatengesetz und der damit verbundenen Massenüberwachung abgesehen, weist das FPG in vielerlei Hinsicht problematische Ansätze und Formulierungen auf, die folgend im Detail thematisiert werden. Die Kritik und Änderungsforderungen zu den einzelnen Artikeln bedeuten keine grundsätzliche Zustimmung zum FPG. Wir erachten das FPG als nicht revidierbar und lehnen es ausdrücklich ab.

2. Übermittlung der Daten i.S.v. Art. 2 FPG

2.1 Datensicherheit

Gemäss Art. 2 Abs. 1 FPG müssen die Luftverkehrsunternehmen der zuständige Stelle (Passenger Information Unit, PIU) die Flugpassagierdaten für alle Flüge von der Schweiz ins Ausland und vom Ausland in die Schweiz übermitteln. Darunter fallen gemäss Anhang 1 z. B. Name, Adresse, Kreditkarten-Nummer und die Beziehung zu Begleitpersonen. Es handelt sich dabei um Personendaten, welche schützenswert sind. Der erläuternde Bericht erkennt richtig, dass dem Datenschutz ein hohes Gewicht zukommen muss, besonders deshalb, weil auch bzw. vor allem Daten von Personen ohne jeglichen Bezug zu Straftaten bearbeitet werden. Auch die Datensicherheit bei der Übermittlung ist von grösster Bedeutung. Art. 2 Abs. 4 FPG sieht jedoch nur vor, dass die technischen Einzelheiten der Übermittlung durch das Bundesamt für Polizei (fedpol) festgelegt werden. Diese Delegation ist ungenügend. Die Datenübermittlung muss im FPG selbst festgehalten werden. Einzelheiten müssen zumindest in einer Verordnung des Bundesrates geregelt werden, nicht aber durch das fedpol.

Zur technischen Regelung der Datenübermittlung ins Ausland gemäss Art. 3 FPG wird gar nichts geregelt. Auch die Datenübermittlung ins Ausland muss im FPG selbst geregelt werden, damit die Datensicherheit bei der Übermittlung gewährleistet ist.

2.2 Zeitpunkt der Übermittlung i.S.v. Art. 2 Abs. 2 FPG

Gemäss Art. 2 Abs. 2 FPG sind die Daten frühestens 48 bis spätestens 24 Stunden vor der planmässigen Abflugzeit sowie unmittelbar nach Abschluss des Boardings zu übermitteln. Damit müssen die Flugpassagierdaten zu zwei unterschiedlichen

Zeitpunkten von den Fluggesellschaften an die PIU übermittelt werden. Gemäss erläuterndem Bericht sind die Daten zu zwei Zeitpunkten zu übermitteln, um der PIU eine gewisse Vorlaufzeit bis zum Eintreffen des Fluges zu geben, was allerdings nur bei kurzen Flügen von Bedeutung sein dürfte. Dies scheint zudem kein ausreichender Grund zu sein, da erst die zweite Übermittlung die definitive Datenbekanntgabe zu allen sich an Board befindenden Flugpassagieren erlaubt. Wenn eine Person einen Flug erst kurzfristig, weniger als 24 Stunden vor Abflug bucht, wird die erste Datenübermittlung umgangen und somit das Ziel der Vorlaufzeit unterlaufen. Die Vorlaufzeit ist also kein geeignetes Argument, die Übermittlung der Daten zu einem ersten Zeitpunkt zu rechtfertigen.

Gemäss Ziff. 10 Anhang 1 werden auch die Daten von nicht angetretenen Flügen übermittelt. Es werden also nicht nur die Daten aller tatsächlichen Passagiere an Board weitergegeben, sondern auch Daten derjenigen, welche einen Flug buchen, aber dann nicht auf dem Flug sind. Es ist nicht ersichtlich, wie die Daten einer potenziellen Passagierin, welche dann vielleicht ihren Flug verpasst, zur Verhinderung von schweren Straftaten dienen soll, zumal diese Straftaten gemäss dem Europäischen Gerichtshof (EuGH) zumindest einen mittelbar objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen müssen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Die Übermittlung der Daten bis spätestens 24 Stunden vor der Abflugzeit ist nicht mit dem öffentlichen Interesse der Sicherheit zu rechtfertigen.

Es ist unverständlich, weshalb die Übermittlung an zwei verschiedenen Zeitpunkten stattfinden muss. Die zweifache Übermittlung führt einzig dazu, dass eine zweifache Menge an Daten entsteht. Wir fordern, dass die Daten nicht bereits vor dem Abschluss des Boardings übermittelt werden.

3. Informationspflicht i.S.v. Art. 5 FPG

Gemäss Art. 5 FPG müssen die Luftverkehrsunternehmen die Flugpassagier:innen schriftlich informieren, dass die sie betreffenden Flugpassagierdaten bearbeitet werden. Gemäss erläuterndem Bericht kann hierzu in den AGB stehen, dass «auch nach dem Flugpassagierdatengesetz bearbeitet werden». Dies ist ungenügend und zu wenig präzis. Es muss klar geregelt sein, dass vor der Buchung der Tickets verständlich über die Bearbeitung der Daten informiert werden muss. Die Information muss sämtliche Daten aufzählen, die übermittelt werden und darf nicht nur pauschal auf die Übermittlung «nach dem Flugpassagierdatengesetz» hinweisen.

4. Bearbeiten der Daten i.S.v. Art. 6 FPG

Gemäss Art. 6 Abs. 1 FPG dürfen die Flugpassagierdaten nur zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten bearbeitet werden. Als Bearbeiten von Daten gilt gemäss Glossar des erläuternden Berichts aber jeder Umgang mit Personendaten, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten. Damit stellt das Weiterleiten schon das Bearbeiten von Daten dar sowie auch das Speichern der Daten vom PIU. Da die Daten ja gerade verdachtsunabhängig übermittelt werden, kann Art. 6 Abs. 1 FPG gar nicht erfüllt werden.

Zudem steht im Glossar, dass das Flugpassagierdatengesetz die Bearbeitung von Daten für die Bekämpfung von Terrorismus und anderen schweren Straftaten vorsieht und ergänzend zum Datenschutzgesetz ihren Schutz regelt. Das FPG regelt das Bearbeiten von Daten aber nicht ergänzend zum Datenschutz, sondern stellt durch das verdachtsunabhängige Bearbeiten von Flugpassagierdaten vielmehr eine Ausnahme des Datenschutzes dar. Wir fordern, dass das FPG das Datenschutzgesetz tatsächlich ergänzt und damit den Datenschutz weiter stärkt, statt ihn einzuschränken, indem z. B. das Auskunftsrecht bei pseudonymisierten Daten verwehrt wird.

5. Terroristische oder andere schwere Straftaten

Das FPG regelt klar, dass es die Bearbeitung der Flugpassagierdaten nur zur Verhinderung, Aufdeckung, Ermittlung und Verfolgung von terroristischen und anderen schweren Straftaten (Art. 1 lit. a und Art. 6 Abs. 1 FPG) erlaubt. In mehreren Artikeln wird dann jedoch nicht mehr ausdrücklich festgehalten, dass es sich dabei nur um terroristische oder andere schwere Straftaten handeln darf, womit Unsicherheit besteht, ob es sich wirklich nur um terroristische und andere schwere Straftaten handelt.

So regelt Art. 6 Abs. 6 lit. b FPG, dass die PIU besonders schützenswerte Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen bearbeiten darf. Es muss ausdrücklich festgehalten werden, dass sich «strafrechtliche Verfolgungen und Sanktionen» nur auf terroristische und andere schwere Straftaten beziehen darf. Das Bearbeiten von verwaltungsrechtlichen Verfolgungen oder Sanktionen ist aus Art. 6 Abs. 6 lit. b FPG zu streichen.

Auch in Art. 7 Abs. 1 FPG soll nochmals ausdrücklich festgehalten werden, dass sich die Zwecke von lit. a - d nicht auf alle Straftaten beziehen dürfen, sondern nur auf terroristische und andere schwere Straftaten im Sinne dieses Gesetzes. Zudem werden gemäss Art. 7 Abs. 1 lit. d FPG Flugpassagierdaten zum Zweck der Informationen in Zusammenhang mit ungeklärten oder geplanten Straftaten automatisch abgeglichen. Dabei ist unklar, was unter «geplanten Straftaten» zu verstehen ist. Daher ist «oder geplanten» aus Art. 7 Abs. 1 lit. d FPG zu streichen.

Die Deliktskataloge der terroristischen und anderen schweren Straftaten sind umfassender als für den Zweck der Sicherheit der Gesellschaft notwendig. Der Europäische Gerichtshof (EuGH) hat entschieden, dass sich die Straftaten auf diejenigen beschränken müssen, bei welchen zumindest ein mittelbarer objektiver Zusammenhang mit der Beförderung von Fluggästen bestehen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Deshalb sollen sämtliche Deliktskategorien aus dem Anhang 2 ausgenommen werden, welche keinen mittelbaren objektiven Zusammenhang mit der Beförderung von Fluggästen aufweisen, namentlich Nr. 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26.

Als besonders problematisch erachten wir, dass der Landfriedensbruch i.S.v. Art. 260 StGB unter terroristische Straftaten fällt, sofern er «terroristisch motiviert» ist, da die Verwendung und Abgrenzung dieses Begriffs insbesondere seit dem Bundesgesetz über die polizeilichen Massnahmen zur Bekämpfung von Terrorismus (PMT) unklar und zu weitgehend ist. Auch die Delikte der betrügerischen Nachahmung und Produktpiraterie gemäss Anhang 2 werden dem Anspruch an schwere Straftaten i.S.v. Art. 6 Abs. 3 FPG nicht gerecht. Damit wird deutlich, dass es nur vordergründig um die Verhinderung von Terrorismus und schweren Straftaten geht. Vielmehr wird unter dem verschleiernden Schlagwort des Terrorismus und der Sicherheit für die Bevölkerung ein weitgehender Deliktskatalog und eine ausufernde Überwachung geschaffen, die in keinem Verhältnis mit dem Sicherheitsbedürfnis der Gesellschaft stehen.

Wir fordern, dass der Delikt des Landfriedensbruchs gemäss Art. 6 Abs. 2 FPG und die Delikte der betrügerischen Nachahmung und Produktpiraterie aus dem Deliktskatalog (Nr. 17 in Anhang 2) der schweren Straftaten gemäss Art. 6 Abs. 3 lit. a FPG gestrichen werden sowie die Nr. 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26 aus Anhang 2.

6. Weitere Informationssysteme i.S.v. Art. 7 Abs. 3 FPG

Gemäss Art. 7 Abs. 3 FPG sind automatisch erzielte Übereinstimmungen vor ihrer Übermittlung an die zuständige Behörde manuell und nötigenfalls unter Zugriff auf weitere Informationssysteme zur Klärung der Identität einer Person oder der Ausschreibungsgründe auf ihre Plausibilität hin zu überprüfen. Im Gesetz ist nicht geregelt, welche Informationssysteme unter «weitere» fallen. Im erläuternden Bericht sind zwar verschiedene Informationssysteme aufgelistet. Dies ist jedoch ungenügend.

Es ist ausdrücklich zu regeln, auf welche Informationssysteme die PIU Zugriff hat. Ansonsten ist für die Rechtsunterworfenen nicht ersichtlich, wohin ihre Daten gehen. Das widerspricht der Idee des FPG, Rechtssicherheit und Transparenz für die Flugpassagier:innen zu schaffen. Der Zugriff muss ausserdem protokolliert werden, damit nachvollziehbar ist, warum welche Personen auf welche Daten zugreifen. Diese Zugriffsprotokollierung kann auch auf Verordnungsebene geregelt werden.

Wie im erläuternden Bericht erwähnt wird, ist es das Ziel des FPG, ein neues Gesetz zu schaffen, das die Bearbeitung von Flugpassagierdaten umfassend regelt, um grösstmögliche Transparenz und Kohärenz zu schaffen. «Für Flugpassagier:innen soll einfach erkennbar sein, wofür und zu welchen Bedingungen ihre Daten staatlich bearbeitet werden dürfen und welche Rechte ihnen als Betroffene zustehen.» Aus dem Gesetz gehen aber keine Rechte der Flugpassagier:innen hervor. Im Gegenteil, diese werden weiter eingeschränkt, wie das verwehrte Auskunftsrecht zeigt. Dies zeigt deutlich auf, dass das Gesetz nicht für die Überwachten, sondern für die Überwachenden geschrieben wurde. Der Schutz der Betroffenen ist nicht gewährleistet. Umso mehr lehnen wir grundsätzlich die Übermittlung der Daten ab.

Das FPG muss ausdrücklich regeln, auf welche Informationssysteme die PIU Zugriff hat. Zudem muss die Zugriffsprotokollierung auf Verordnungsebene geregelt werden.

7. Vorliegen einer Straftat i.S.v. Art. 8 FPG

Gemäss Art. 8 Abs. 1 FPG übermittelt die PIU die Daten an die zuständige Behörde, soweit die Überprüfung das Vorliegen einer Straftat nach Artikel 6 Absätzen 2-3 bestätigt hat. Hier muss ausdrücklich festgehalten werden, dass nur eine richterliche Behörde das Vorliegen einer Straftat überprüfen und bestätigen kann und die PIU diese Überprüfung nicht selbst vornehmen kann.

8. Risikoprofile und Beobachtungslisten i.S.v. Art. 9 FPG

Gemäss Art. 9 FPG kann die PIU aufgrund eigener Analysen oder auf Antrag der Behörden Risikoprofile und Beobachtungslisten erstellen. Worin diese eigenen Analysen bestehen, wird nicht geregelt. Dies führt zu einer enormen Unsicherheit. Die Rechtsunterworfenen wissen nicht, auf welcher Grundlage ihre Daten zu Risikoprofilen oder Beobachtungslisten erstellt werden. Dies entspricht nicht dem bereits oben erwähnten Ziel, dass für Flugpassagier:innen einfach erkennbar sein soll, wofür und zu welchen Bedingungen ihre Daten bearbeitet werden.

Wir fordern, dass solche Risikoprofile und Beobachtungslisten unterlassen werden und der ganze Artikel ersatzlos gestrichen wird. Es soll keine neue Überwachungsbehörde geschaffen werden, welche Daten selber analysieren kann. Die PIU soll höchstens nach Treffern suchen und das Resultat weitergeben können. Danach hat sie die Daten sofort zu löschen. Wird Art. 9 FPG nicht gestrichen, muss genau geregelt werden, wie diese Analysen gemacht werden, damit Transparenz hinsichtlich der Risikoprofile und Beobachtungslisten geschaffen wird und insbesondere keine diskriminierenden Merkmale Grundlage der Risikoprofile und Beobachtungslisten sind. Zudem müssen die Ergebnisse der Überprüfung gemäss Art. 9 Abs. 5 FPG veröffentlicht werden.

9. Zusammenarbeit mit dem NDB i.S.v. Art. 10 FPG

Gemäss Art. 10 FPG kann der Nachrichtendienst des Bundes (NDB) Strecken bestimmen, für die ihm die PIU im automatisierten Verfahren die Daten übermittelt. Mit Art. 8 Abs. 2 lit. b FPG besteht bereits die Möglichkeit, dass die PIU Daten an den NDB weiterleitet. Es ist nicht ersichtlich, weshalb, und völlig unverhältnismässig, dass der NDB die Flugpassagierdaten für von ihm bestimmten Strecken automatisch erhält.

Es ist anzunehmen, dass dies alle möglichen Strecken sein werden, damit auch «Umwege» ersichtlich werden (und dies nicht zur Umgehung der Überwachung verwendet werden könne). Der NDB wird diese Strecken vermutlich geheim halten und die Rechtsunterworfenen damit nicht erfahren, ob ihre Daten direkt an den NDB weitergeleitet werden. Diese Intransparenz ist inakzeptabel und widerspricht ebenfalls dem bereits erwähnten Ziel, Transparenz für die Flugpassagier:innen zu schaffen. Zudem widerspricht Art. 10 FPG auch dem Zweck der Verhinderung, Aufdeckung, Ermittlung und Verfolgung von Straftaten gemäss Art. 1 lit. a FPG, da der NDB keine Strafverfolgungsbehörde ist.

Wir fordern, dass Art. 10 FPG restlos gestrichen wird. Andernfalls ist sicherzustellen, dass, wenn der NDB solche Strecken bestimmt, diese öffentlich gemacht werden müssen, damit für die Flugpassagier:innen klar ersichtlich ist, welche Daten direkt an den NDB weitergeleitet werden.

Gemäss Art. 10 Abs. 3 FPG sind die Daten innerhalb von 96 Stunden nach Erhalt zu löschen, wenn der Abgleich zu keiner Übereinstimmung geführt hat. Diese Frist ist zu lang. Es ist nicht verständlich, weshalb diese Daten noch 96 Stunden aufbewahrt werden dürfen, wenn sie offensichtlich nicht dem Zweck des FPG entsprechen, zumal sie ja beim PIU noch vorhanden wären, sollte es zu einem Vorfall kommen. Art. 6 Abs. 5 FPG regelt, dass Ergebnisse von Bearbeitungen, die den Zwecken nach Art. 6 Abs. 1 FPG nicht entsprechen, umgehend gelöscht werden. Dies ist auch vom NDB zu verlangen. Wir fordern, dass der Art. 10 Abs. 3 FPG ausdrücklich festhält, dass die Daten umgehend zu löschen sind, wenn der Abgleich zu keiner Übereinstimmung geführt hat.

10. Meldung bei einem Verdacht i.S.v. Art. 12 FPG

Gemäss Art. 12 FPG meldet die PIU der zuständigen Strafverfolgungsbehörde einen konkreten Verdacht. Die StPO kennt den hinreichenden Verdacht, jedoch keinen konkreten. Es sollen keine neuen Verdachtskategorien mit dem FPG eingeführt werden, weshalb die Begriffe an die StPO anzupassen sind. Art. 12 Abs. 1 ist deshalb zu einem «hinreichenden Verdacht» zu ändern. Auch in Art. 22 Abs. 3 FPG wird der «begründete Verdacht» erwähnt, welchen die StPO ebenfalls nicht kennt. Art. 22 Abs. 3 FPG soll im Sinne der Vereinheitlichung zu «kein hinreichender Verdacht» geändert werden.

In Art. 12 Abs. 2 FPG soll ergänzt werden, dass es sich um schützenswerte Personendaten gemäss Art. 6 Abs. 6 FPG handeln muss. Damit soll ausdrücklich festgestellt werden, dass nur jene besonders schützenswerten Personendaten übermittelt werden dürfen, welche auch bearbeitet werden dürfen.

11. Zugriff auf das PNR-Informationssystem i.S.v. Art. 13 FPG

Gemäss Art. 13 Abs. 2 lit. a FPG haben die Mitarbeitenden der PIU zur Erfüllung ihrer Aufgaben Zugriff auf das Informationssystem «Passenger Name Record» (PNR-Informationssystem). Das muss konkretisiert werden. Es muss organisatorisch klar geregelt werden, wer Zugriff auf welche Daten hat. Zudem soll ein Vier-Augen-Prinzip

eingeführt werden, wenn Daten manuell bearbeitet werden müssen.

Gemäss Art. 13 Abs. 2 lit. b FPG haben die für die Wartung und Programmierung des Systems zuständigen Personen Zugriff auf das PNR-Informationssystem, soweit dies zur Erfüllung ihrer Wartungs- und Programmierarbeiten unbedingt erforderlich ist. Da Mitarbeitende mit Zugriff auf die Personendaten Beispiel-Daten erstellen können, mit denen programmiert werden kann, ist es nicht erforderlich, dass Personen, die für die Wartung und Programmierung des Systems Zugriff darauf haben. Es gibt keinen Grund, weshalb dabei der Zugriff auf das PNR-Informationssystem notwendig sein sollte. Art. 13 Abs. 2 lit. b ist zu streichen.

12. Datenschutz, Auskunftsrecht und Pseudonymisierung i.S.v. Art. 14 f. FPG

Der Datenschutz bekommt zwar einen eigenen Abschnitt im FPG, mehr aber auch nicht. Im erläuternden Bericht steht, dass der Datenschutz bei der Datenbearbeitung nach dem Flugpassagierdatengesetz eine zentrale Rolle spielt; alles was dieser Abschnitt «Datenschutz» jedoch vorsieht, ist die Pseudonymisierung der Daten, welche wieder rückgängig gemacht werden kann.

Pseudonymisierte Daten gelten gemäss Glossar des erläuternden Berichts weiterhin als Personendaten im Sinne des Datenschutzes, solange die Konkordanztafel noch verfügbar ist. Es handelt sich dabei um sehr persönliche und damit schützenswerte Daten, welche dies auch nach der Pseudonymisierung bleiben. Somit ist die Pseudonymisierung kein ausreichendes Mittel für einen starken Datenschutz. Im Gegenteil, sie schränkt die Rechte der Betroffenen noch weiter ein, da durch die Pseudonymisierung das Auskunftsrecht verloren geht (Art. 18 Abs. 2 FPG). So lassen sich die Daten noch auf eine Person zurückführen, ohne dass diese aber ein Auskunftsrecht hat, welche Daten das sind. Es ist völlig unverständlich, weshalb man mit der Pseudonymisierung das Auskunftsrecht verlieren sollte, da es sich weiterhin um Personendaten handelt. Dieser Widerspruch ist aufzulösen, indem bei pseudonymisierten Daten das Auskunftsrecht gewährt bleibt, genauso wie bei allen anderen Personendaten auch. Art. 18 Abs. 2 FPG ist zu streichen.

Im erläuternden Bericht werden Elemente eines Datensatzes einer Person aufgezählt, welche pseudonymisiert werden müssen. Diese Aufzählung stimmt nicht vollständig mit den zu übermittelnden Daten gemäss Anhang 1 des FPG überein. Es müssen sämtliche Daten gemäss Anhang 1 des FPG pseudonymisiert werden.

Die Frage bleibt, weshalb die pseudonymisierten Daten überhaupt aufbewahrt werden. Es scheint, als sei die Pseudonymisierung eher eine Sicherstellung, dass die Daten nur zweckmässig verwendet werden. Dann geht es dabei aber nicht um Datenschutz, sondern um die zweckmässige Verwendung dieser Daten. Die Pseudonymisierung als Mittel zur Zweckbindung der Daten ist grundsätzlich nicht falsch, hat aber nichts mit der Verletzung der Grundrechte der Betroffenen zu tun.

Wenn allerdings eine Pseudonymisierung durchgeführt werden soll, so ist unerlässlich, dass die pseudonymisierten Daten und die Konkordanztafel sowohl technisch als auch organisatorisch wirklich voneinander getrennt sind. Die Konkordanztafel muss bei einer anderen Organisation aufbewahrt werden und der Zugriff darauf darf für die zuständige Stelle (Passenger Information Unit, PIU) nicht möglich sein. So müsste die Konkordanztafel z. B. bei einem Treuhänder liegen, damit die Pseudonymisierung wirklich nur durch einen Gerichtsbeschluss rückgängig gemacht werden kann.

13. Aufbewahrungsdauer i.S.v. Art. 16 FPG

Die Aufbewahrungsdauer von fünf Jahren gemäss Art. 16 Abs. 1 FPG ist zu lang. Dies hat auch der Europäische Gerichtshof (EuGH) so entschieden: Eine allgemeine, unterschiedslos für alle Fluggäste geltende Speicherfrist von fünf Jahren überschreitet demnach die Grenzen des absolut Notwendigen (vgl. Urteil C-817/19 des EuGH vom 21. Juni 2022). Auch im erläuternden Bericht wird anerkannt, dass es sich um eine verhältnismässig lange Aufbewahrungsdauer handelt, und auch hier wird von einem «Paradigmenwechsel» gesprochen.

Die Digitale Gesellschaft lehnt die Übermittlung und Speicherung der Flugpassagierdaten ausdrücklich ab. Werden diese dennoch übermittelt, so müssen sie unmittelbar nach der Trefferanalyse gelöscht werden und dürfen nicht aufbewahrt werden. Die Aufbewahrungsdauer stellt einen Grundrechtseingriff dar, egal, wie lange die Daten effektiv aufbewahrt werden. Wir fordern, dass die Daten sofort gelöscht werden, wenn sie beim Abgleich zu keinem wesentlichen Ergebnis im Sinne eines konkreten Verdachts auf eine terroristische oder andere schwere Straftat führen. Dieser Abgleich hat gemäss Art. 7 Abs. 2 unmittelbar nach Erhalt der Daten zu erfolgen. Es ist nicht ersichtlich, weshalb die Daten danach noch weiter aufbewahrt werden sollten, wenn dieser Abgleich zu keinem Ergebnis geführt hat. Die Aufbewahrungsdauer in Art. 16 Abs. 1 FPG ist gänzlich zu streichen.

Wird die Aufbewahrungsdauer nicht gestrichen, so muss zumindest die Pseudonymisierung effektiv durchgeführt werden (s. u. Datenschutz und Pseudonymisierung). Gemäss Art. 14 FPG werden die Flugpassagierdaten sechs Monate nach ihrer Übermittlung automatisch pseudonymisiert. Diese Frist ist zu lang. Die Pseudonymisierung hat unmittelbar und automatisiert nach dem Abgleichen der Daten zu geschehen, wenn dabei kein wesentlicher Verdacht auf eine terroristische oder andere schwere Straftat resultiert.

Gemäss Art. 16 Abs. 2 FPG legt der Bundesrat die maximale Aufbewahrungsdauer der Daten, die aus einem Abgleich nach den Artikeln 7 und 9 resultieren, in einer Verordnung fest. Es ist anzunehmen, dass die Aufbewahrungsdauer länger als fünf Jahre sein wird, wenn gemäss Abs. 1 die Daten auch bei keinem Ergebnis fünf Jahre aufbewahrt werden dürfen. Die Aufbewahrung der Daten stellt einen schweren Eingriff in die Grundrechte dar. Es ist nicht verständlich, weshalb die Aufbewahrungsdauer von Daten, die kein Ergebnis erzielt haben im FPG selbst geregelt wird, die Aufbewahrungsdauer von Daten, welche aus einem Abgleich nach Art. 7 oder 9 resultieren jedoch auf Verordnungsstufe geregelt werden sollte. Ausserdem wird diese Aufbewahrungsdauer nicht einer ständigen Anpassung unterliegen, weshalb nicht klar ist, warum die Verordungsstufe dafür ausgewählt wird. Die Aufbewahrungsdauer für Daten, die aus einem Abgleich nach den Artikeln 7 und 9 resultieren, muss im FPG selbst festgehalten werden. Eine Delegation an eine Verordnung genügt nicht.

14. Völkerrechtlicher Vertrag i.S.v. Art. 21 FPG

Gemäss Art. 3 FPG übermitteln die Luftverkehrsunternehmen die Flugpassagierdaten bei Flügen von der Schweiz ins Ausland an die am Ort der Landung zuständigen Behörde, wenn ein völkerrechtlicher Vertrag mit dem betreffenden Staat die Übermittlung und Bearbeitung der Flugpassagierdaten vorsieht. Dass der Bundesrat solche völkerrechtlichen Verträge nur mit Staaten abschliessen kann, die einen mit der Schweiz «vergleichbaren Schutz der Daten» gewährleisten (Art. 21 FPG), ist alles andere als beruhigend, da der Datenschutz im FPG nicht gewährleistet ist. So haben die Betroffenen weder ein Auskunftsrecht, noch wird die Datensicherheit bei der Übermittlung im FPG selbst geregelt (s. u. 2. und 12.).

Art. 16 Abs. 1 und 2 des neuen Datenschutzgesetzes (nDSG) regeln, dass Personendaten nur ins Ausland bekanntgegeben werden dürfen, wenn der betreffende Staat einen angemessenen oder geeigneten Datenschutz gewährleistet. Dieser

Standard des nDSG soll auch für Flugpassagierdaten gelten. In Art. 3 und Art. 21 FPG muss explizit vorgesehen werden, dass ein völkerrechtlicher Vertrag nur mit Staaten abgeschlossen werden kann, die einen angemessenen oder geeigneten Datenschutz gewährleisten, damit der Standard im nDSG nicht untergraben wird.

Schlussbemerkung

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Artikeln bedeutet keine Zustimmung der Digitalen Gesellschaft.

Freundliche Grüsse

Erik Schönenberger