



**piratenpartei**

www.piratenpartei.ch

Piratenpartei Schweiz, 3000 Bern

Sehr geehrter Frau Bundesrätin Keller-Sutter

Sehr geehrte Damen und Herren

## **Stellungnahme der Piratenpartei Schweiz zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten (Vernehmlassung 2021/80)**

Bezugnehmend auf Ihre Vernehmlassungseröffnung zum Entwurf zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 13.04.2022 nehmen wir gerne Stellung und würden es zukünftig sehr begrüßen, wenn wir in Ihre Adressatenliste aufgenommen werden.

Im Weiteren finden wir Piraten es sehr bedenklich, dass Sie für die Stellungnahme auf eine proprietäre Software verweisen (Word der Firma Microsoft), wo es doch heute zahlreiche offene und freie Dateiformate gibt. Wir entsprechen Ihrem Wunsch mit einer docx-Datei, welche auch in neueren Word Versionen geöffnet werden kann.

### **Vorbemerkungen**

Die Piratenpartei Schweiz setzt sich seit Jahren für eine humanistische, liberale und progressive Gesellschaft ein. Dazu gehören die Privatsphäre der Bürger, die Transparenz des Staatswesens, inklusive dem Abbau der Bürokratie, Open Government Data, den Diskurs zwischen Bürgern und Behörden, aber auch die Abwicklung alltäglicher Geschäfte im Rahmen eines E-Governments. Jede neue digitale Schnittstelle und Applikation bedingt aber eine umfassende Risikoanalyse und Folgeabschätzung.

Im Speziellen erachten wir eine anlasslose Vorratsdatenspeicherung, wie sie im vorliegenden Gesetzesentwurf der Fall ist ab. Solche massenhafte Überwachung der Bevölkerung ist vor allem auch in der Abwägung Nutzen - Grundrechtseingriff nie positiv. "Ein Zeichen setzen", Zitat aus dem Einladungsschreiben, ist offensichtlich genau das Gegenteil von einer sorgfältigen Abwägung beim Eingriff in Grundrechte, nur weil man etwas kann, weil Daten vorhanden sind, heisst das noch lange



nicht, dass dies notwendig, wirksam oder verhältnismässig ist. Ein Zeichen setzen bedeutet, dass genau diese Abwägung offensichtlich nicht gemacht wurde.

## **Stellungnahme zum Bundesgesetz über die Bearbeitung von Flugpassagierdaten zur Bekämpfung von terroristischen und anderen schweren Straftaten**

Gerne nehmen wir zu den einzelnen Artikeln wie folgt Stellung:

### Artikel 2

Abs. 1 sieht eine Übermittlung von Daten bei allen Flügen von und in die Schweiz vor. Der EuGH hat hingegen das Datensammeln für Flüge innerhalb der EU deutlich auf besondere Fälle eingeschränkt [1]. Es sollte entsprechend, um der Datensparsamkeit zu genügen, ebenfalls auf die Daten der meisten Flüge im Schengenraum verzichtet werden.

In Abs. 2 wird eine Übermittlung der Flugpassagierdaten 48-24 Stunden vor Abflug festgelegt. Indes ist keine Löschung der Daten von Passagieren, die den Flug nicht antreten, festgeschrieben. Diese fehlende Regelung ist nicht nachvollziehbar.

Für die in Abs. 3 angedachte Löschung von besonders schützenswerten Daten fehlt eine Instanz, welche eine allfällige Löschung kontrolliert. Ferner stellt sich die Frage, was nach der in Art. 14 geplanten Pseudonymisierung geschieht, da hier Betroffene ihr Auskunftsrecht verlieren.

### Art. 2 Abs. 4

Im FPG werden in grossem Masse schützenswerte Daten gespeichert und übermittelt. Deshalb ist es unabdingbar dem Datenschutz eine sehr grosse Rolle beizumessen. Es ist unzureichend die technischen Einzelheiten der Datenübermittlung dem Fedpol zu überlassen. Das Fedpol muss diese zwingend gemeinsam mit dem EDÖB festlegen, wobei dem EDÖB die finale Entscheidung obliegt.

### Artikel 5

Die Übermittlung der persönlichen Daten der Flugpassagiere stellt einen schwerwiegenden Eingriff in die Grundrechte dar, der klar kommuniziert werden muss. Die aktuelle Formulierung lässt jedoch offen, wie und in welcher Form dies geschehen soll. Hier ist eine Präzisierung erforderlich, dass Passagiere klar, verständlich mit expliziter Nennung aller Daten, und auch



gesondert, und nicht verklausuliert und versteckt, vor der Buchung auf diesen Vorgang hingewiesen werden und einwilligen müssen. Diese Einwilligung muss eine bewusste Entscheidung darstellen.

## Artikel 6

Die Piratenpartei hält es weiterhin für rechtsstaatlich äusserst fragwürdig den Begriff der "schweren Straftat" wie in Absatz 1 zu verwenden, welcher bekanntermassen nicht genauer definiert ist und auch in der Lehre die Meinungen weit auseinandergehen. Bevor dieser Begriff in neuen Gesetzen (oder in Gesetzesanpassungen) genutzt wird muss diese Definitionslücke geschlossen werden. Siehe auch Urteil 6B\_1468/2019 des Bundesgerichtes [2]:

"1.4.2. Der Gesetzgeber verzichtete darauf, schwere Straftaten im Sinne von Art. 141 Abs. 2 StPO zu definieren. Das Bundesgericht klärte bisher nicht abschliessend, was generell unter diesem Begriff zu verstehen ist (vgl. Urteil 6B\_287/2016 vom 13. Februar 2017 E. 2.4.4). Auch in der Lehre finden sich keine Vorschläge für eine Definition und die Ansichten gehen auseinander."

Absatz 3 zeigt, wie so häufig bei Überwachungsgesetzen, dass es bei diesem Gesetz entgegen den grossen Versprechungen nicht um Terrorismus oder besonders schwere Straftaten geht, sondern abermals um einen nicht zu rechtfertigenden möglichst breiten Deliktskatalog. Dass der tiefe Grundrechtseingriff beispielsweise mit "Handel mit Hormonen" oder "Produktpiraterie" begründet wird, steht in keinem Verhältnis. Spannend wird es sicher bei Computerstraftaten. Hier stellt sich die Frage, ob hierunter dann auch die Mitarbeiter der (ausländischen) Geheimdienste, welche weithin auch für Wirtschaftsspionage bekannt sind, fallen und beispielsweise auch die Führungsriege des CIA betroffen sind, oder ob hier grosszügige Ausnahmen gelten sollen.

Wir fordern, dass die PNR-Daten ausschliesslich für terroristische Straftaten oder für Straftaten, für die der Gesetzgeber eine Mindeststrafe von 3 Jahren Haft vorsieht, bearbeitet werden dürfen. Darüber hinaus ist unbedingt eine explizite Terrorismusdefinition festzulegen, damit nicht wie im PMT ein Grossteil der Bevölkerung als potentielle Terroristen verfolgt werden können [3]

Absatz 6 widerspricht Art. 2 Abs. 3, welcher den Luftverkehrsunternehmen verbietet besonders schützenswerte Personendaten zu übermitteln, was biometrische Daten einschliesst, und eine sofortige Löschung bei der PIU vorsieht. Ausserdem sind biometrische Daten im Anhang 1 "Flugpassagierdaten" (inkl. dem Verweis in Punkt 18) nicht vorgesehen und sollten somit per se nicht Teil der Daten sein.



Weiter ist bekannt, dass das US-Department for homeland-security diese Daten vollumfänglich abrufen will, was zu verhindern ist und mit Datensparsamkeit zusätzlich erschwert werden sollte [4].

Darüber hinaus hat auch der der EuGH vor wenigen Wochen geurteilt, dass das durch die PNR-Richtlinie eingeführte System sich nur auf die in den Rubriken ihres Anhangs I aufgeführten, klar identifizierbaren und umschriebenen Informationen erstrecken darf [1].

Deshalb fordern wir die ersatzlose Streichung dieses Absatzes.

#### Artikel 9

Die unklare Definition von Analysen, Risikoprofilen und Beobachtungslisten führt zu Unsicherheiten. Hier muss eine entsprechende Präzisierung ergänzt werden.

Auch zu Risikoprofilen und Beobachtungslisten äusserte sich der EuGH insoweit, dass: "keine Technologien der künstlichen Intelligenz im Rahmen selbstlernender Systeme („machine learning“)" herangezogen werden dürfen, da diese in fünf von sechs Fällen zu Falschbeschuldigungen führen [1,5] + ).

"Schon jetzt definieren Algorithmen - unter anderem auf Basis der „flight history“ einer Person - die Vorauswahl jener Personen, deren Datensätze rund um den Grenzübertritt genau analysiert werden. Auch das ist nicht statthaft. Der EuGH merkt dazu an, dass eine Überprüfung dieser Methode durch die Kommission aus den Jahren 2018 und 2019 ergeben habe, dass fünf von sechs so generierten „Treffern“ völlig Unbeteiligte trafen. In Folge wurden diese Personen bei jedem neuen Flug beobachtet und nach ihrer Landung oft eingehend „befragt“. Nach diesem Urteil ist ein solcher Automatismus unzulässig, wenn diese Vorabselektion nicht durch Beamte überprüft wird." [6]

Oben genannte Einschränkung sollte in Art. 9 ebenfalls explizit festgehalten werden. Sofern die oben genannte Präzisierung der Definitionen von Analyse, Risikoprofilen und Beobachtungslisten nicht möglich ist, sollte der Artikel 9 ersatzlos gestrichen werden.

#### Artikel 10

Die aktuelle Formulierung lässt dem NDB die Möglichkeit offen, sämtliche Flugstrecken zu erhalten. Diese offene Formulierung ist unhaltbar und benötigt dringend eine stark einschränkende Präzisierung. Wir schlagen vor, dass die vom NDB erbetenen Strecken von den



GPK des Bundesparlamentes genehmigt werden müssen. Des Weiteren muss eine Löschung der übermittelten Daten direkt nach negativem Abgleich erfolgen.

#### Artikel 11

Die aktuelle Formulierung lässt ebenfalls eine massenhafte Übermittlung von Daten zu. Diese Einzelfälle müssen die Ausnahme bleiben und gut begründet sein. Über einen solchen Antrag müsste zwingend eine richterliche Behörde entscheiden. Wobei sich hier die Frage stellt, weshalb dieser Artikel überhaupt existiert. An die Behörden in Art. 11 Abs. 2 Bst. a und b können und werden mit der Vorlage schon alle nach Art. 6 Abs. 1 relevanten Daten übermittelt. Es drängt sich der Verdacht auf, dass hier auf Zuruf und ausserhalb des Geltungsbereiches von Art. 6 Daten übermittelt werden sollen. Wir fordern eine Streichung des Artikels.

#### Artikel 13

Personen, die für die Programmierung des Systems zuständig sind, können für diese Aufgabe Dummy-Daten verwenden.

Personen, die für die Wartung des Systems zuständig sind, benötigen ebenfalls nie Zugriff auf die Daten des Systems.

Abs. 2 Bst. b ist daher ersatzlos zu streichen.

#### Artikel 14

Diese Pseudonymisierung ist per se umkehrbar und damit keine Verbesserung bezüglich der Grundrechtseingriffe. Es wäre dringend angebracht die Speicherzeit an sich drastisch zu senken (siehe Art. 16).

#### Artikel 16

Der EuGH hat auf der europäischen Ebene den Normalfall der Speicherfrist von 5 Jahren auf 6 Monate gekürzt [1]. Dies wäre die von der Schweiz mindeste, notwendige Anpassung. Es erschliesst sich der Piratenpartei aber nicht, weshalb eine Abwägung zwischen der massenhaften Speicherung von persönlichen Daten unzähliger Unschuldiger und den äusserst seltenen Fällen der zu erwartenden positiven Treffer bezüglich Terrorismus zu einem positiven Ergebnis kommen



sollte. Deshalb schlagen wir vor, dass die Daten innerhalb von 24 Stunden nach Landung gelöscht werden müssen - inklusive eines funktionierenden Kontroll- und Sanktionsmechanismus.

#### Artikel 18

Absatz 2 ist besonders bedenklich bezüglich der Gewichtung der Grund- und Menschenrechte der Bürgerinnen und Bürgern seitens des Gesetzgebers.

Die Daten können weiterhin problemlos jederzeit von Behörden abgerufen werden (siehe Art. 15), während Betroffene gleichzeitig jegliches Auskunftsrecht durch die Pseudonymisierung verlieren.

Die Pseudonymisierung der Daten ist damit de facto eine massive Schlechterstellung aller Betroffenen - ohne Grund. Es handelt sich immer noch um besonders schützenswerte Personendaten und damit muss man weiterhin vom Auskunftsrecht Gebrauch machen können, alles andere ist eine Farce. Falls die Daten nicht wie von uns vorgeschlagen innert 24 Stunden nach Landung gelöscht werden, müssen Betroffene auf jeden Fall über den gesamten Zeitraum der Speicherung der Daten (mit oder ohne Pseudonymisierung) von ihrem Auskunftsrecht Gebrauch machen können.

#### Artikel 20

Aus dem Gesetzestext und dem erläuternden Bericht geht kein ausreichender Grund hervor weshalb ein solch kompliziertes Konstrukt zwingend notwendig sein sollte. Für die Piraten stellt sich die Frage, weshalb nicht die Kantone einfach die Kosten übernehmen anstatt, die Hälfte der Mitarbeitenden zu stellen?

#### Artikel 21

In diesem Artikel wird festgehalten, dass der Bundesrat mit anderen Staaten völkerrechtliche Verträge zur Bearbeitung der Daten abschliessen kann, "soweit ihr nationales Recht einen mit der Schweiz vergleichbaren Schutz dieser Daten gewährleistet." Wir halten hier eine Präzisierung von "vergleichbar" für notwendig, da unklar ist, ob dies auch "etwas schlechter" beinhalten kann. Und der einzige "Datenschutz" im Schweizer Gesetz ist ja auch nur eine Pseudonymisierung, welche auch noch rückgängig gemacht werden kann, und entspricht somit eigentlich gar keinem Datenschutz.



## Artikel 22

In Absatz 3 ist die Präzisierung erforderlich, wer entscheidet, ob ein begründeter Verdacht vorliegt? Wir schlagen ein Gremium aus Bundesrichtern in 5er-Besetzung vor.

## Schlussbemerkungen

Wir beschränken uns in dieser Stellungnahme auf unsere Kernanliegen. Bei Verzicht unsererseits auf umfassende allgemeine Anmerkungen oder auf Anmerkungen zu einzelnen Regelungen, ist damit keine Zustimmung durch die Piraten zu solchen Regelungen verbunden.

Kontakt details für Rückfragen finden Sie in der Begleit-E-Mail.

## Quellen:

[1] <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105de.pdf>

[2]

[https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?highlight\\_docid=aza%3A%2F%2F01-09-2020-6B\\_1468-2019&lang=fr&type=show\\_document&zoom=YES&](https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F01-09-2020-6B_1468-2019&lang=fr&type=show_document&zoom=YES&)

[3] <https://www.piratenpartei.ch/2021/05/20/abstimmungsbeschwerde-der-piratenpartei-gegen-pmt/>

[4] <https://www.patrick-breyer.de/internes-libe-treffen-mit-homeland-security-plaene-fuer-biometrie-datenbanken-bringen-daten-von-eu-buergerinnen-in-gefahr/>

[5] <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:62019CJ0817&from=EN>

[6] [https://home-affairs.ec.europa.eu/system/files/2020-07/20200724\\_swd-2020-128\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_swd-2020-128_en.pdf)—

—

Piratenpartei Schweiz, Arbeitsgruppe Vernehmlassungen, 28. Juli 2022

