Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Polizei fedpol

Factsheet Passenger Name Record (PNR) – Datenschutzfolgeabschätzung (DSFA)

Hintergrund

Der Bundesrat hat an seiner Sitzung vom 15. Mai 2024 die Botschaft zum Flugpassagierdatengesetz verabschiedet und ans Parlament überwiesen. Dank dieser Gesetzesgrundlage wird die Schweiz ein nationales PNR-System (Passenger Name Records) einrichten können. Das neue Gesetz wird dazu beitragen, Terrorismus und andere Schwerstkriminalität zu bekämpfen und den Wirtschaftsstandort Schweiz zu schützen.

Datenschutz und Wahrung der Persönlichkeitsrechte

Das Gesetz garantiert den Schutz der Daten und der Persönlichkeitsrechte der Flugpassagierinnen und Flugpassagiere. Der Zugriff auf die PNR-Daten und ihr Verwendungszweck sind streng geregelt.

Gegenüber der Vernehmlassungsvorlage hat der Bundesrat den Datenschutz verstärkt. Die Aufbewahrungsdauer der Daten wurde verkürzt. So dürfen Daten, die keine objektiven Anhaltspunkte für Terrorismus oder andere Schwerstkriminalität aufweisen, nicht länger als sechs Monate gespeichert werden. Diese Daten werden zudem bereits nach einem Monat pseudonymisiert. Das heisst, dass identifizierende persönliche Informationen wie zum Beispiel Name, Kontaktdaten und Geburtsdatum nicht mehr direkt im System sichtbar sind. Weisen die Daten hingegen objektive Anhaltspunkte für Terrorismus oder andere Schwerstkriminalität auf, dürfen sie maximal fünf Jahre gespeichert werden.

Nach Inkrafttreten des Gesetzes wird die Einhaltung des Datenschutzes vom Eidgenössischen Datenschutzbeauftragten – EDÖB – beaufsichtigt. Bei der Erarbeitung der Gesetzesvorlage wurde erstmals eine Datenschutz-Folgenabschätzung (DSFA) gemäss dem neuen Datenschutzgesetz durchgeführt. Die Anliegen des EDÖB wurden bei der Erarbeitung der Vorlage berücksichtigt.

Zusammenfassung der Datenschutz-Folgenabschätzung (DSFA) für das Projekt PNR Schweiz

Das Projekt PNR (Passenger Name Record) Schweiz befasst sich mit der Sammlung und Bearbeitung von Flugpassagierdaten durch das Bundesamt für Polizei (fedpol), um Terrorismus und schwere Kriminalität zu bekämpfen. Die Datenschutz-Folgenabschätzung (DSFA) dient dazu, potenzielle Datenschutzrisiken frühzeitig zu erkennen und zu bewerten. Der Zweck der DSFA erschöpft sich dabei nicht in der Voraussehbarkeit und Bewertung «hoher» Projektrisiken. Der praktische Nutzen des Arbeitsinstruments liegt viel-mehr auch darin, die Herleitung und Analyse systemischer und sicherheitstechnischer Risiken nachvollziehbar zu dokumentieren und durch geeignete Massnahmen auf ein datenschutzrechtlich vertretbares Niveau zu senken.

Nachfolgend werden die wesentlichen Inhalte der DSFA zusammengefasst:

Beschreibung der Datenbearbeitung

Flugpassagierdaten, die von Fluggesellschaften gesammelt werden, umfassen Namen, Kontaktinformationen und Reisedetails der Passagiere. Diese Daten werden von den Luftverkehrsgesellschaften an die Passenger Information Unit (PIU) weitergegeben und umfassen 19 Datenkategorien gemäss Anhang 1 des Flugpassagierdatengesetzes (FPG).

Beschreibung betroffener besonders schutzbedürftiger Personen

In diesem Abschnitt der DSFA werden Personen beschrieben, die aufgrund ihrer speziellen Situation als besonders schutzbedürftig gelten. Dazu zählen:

- **Kinder:** Kinder, die alleine reisen oder von einer nicht-elterlichen Begleitperson begleitet werden, sind besonders schutzbedürftig. Dies schliesst unbegleitete Minderjährige unter 18 Jahren ein, für die detaillierte Informationen wie Name, Alter, Sprache und Kontaktdaten der Begleitpersonen am Abflug- und Zielflughafen erfasst werden.
- **Personen mit Behinderungen:** Obwohl das Vorhandensein einer Behinderung normalerweise nicht direkt aus den PNR-Daten hervorgeht, könnte der Umstand, dass beispielsweise ein Rollstuhl transportiert wird, darauf hinweisen. Diese Information bleibt jedoch spekulativ und wird nicht systematisch erfasst.

Bearbeitung der Personendaten

Die DSFA beschreibt in diesem Kapitel, wie die Personendaten im Rahmen von PNR behandelt werden, inklusive Bearbeitung und Aufbewahrung innerhalb der vorgegebenen Fristen:

PNR Daten werden von den Fluggesellschaften während des Buchungsprozesses erhoben, um die Flugabwicklung zu unterstützen. Die staatliche Nutzung der Daten ist nachgelagert, indem sie als sogenannte «Passenger Name Records (PNR)» zur «Passenger Information Unit (PIU)» weitergeleitet werden. Der Hauptnutzen dieser Datenbearbeitung liegt in der Möglichkeit für die zuständigen Behörden, frühzeitig präventive und repressive Massnahmen zur Verhinderung oder Verfolgung von Terrorismus und schweren Straftaten ergreifen zu können. Sie umfasst den Datenabgleich mit polizeilichen Informationssystemen und Beobachtungslisten sowie mit Risikoprofilen zur Identifizierung potenzieller Bedrohungen. Die Bearbeitungsvorgänge schliessen den Empfang, die Aufbewahrung, die Änderung und bei verifizierten Übereinstimmungen (Treffern) die Bekanntgabe der Daten an zuständige Behörden ein, wobei Daten, die keinen Treffer erzeugen, nach einem Monat pseudonymisiert und nach weiteren fünf Monaten gelöscht werden.

Die an der Bearbeitung beteiligten Personen sind Mitarbeiterinnen und Mitarbeiter der PIU und anderer zuständiger Behörden. Da jährlich die Daten von Millionen Passagieren bearbeitet werden könnten, ist die Zahl der Bearbeitungsvorgänge sehr hoch (umfangreich). Für die Datenbearbeitung werden fortschrittliche Technologien und ein erprobtes PNR-System der UNO eingesetzt. Es ist kein Einsatz künstlicher Intelligenz in diesem Bereich vorgesehen, und alle Massnahmen werden strikt nach gesetzlichen Vorgaben und Datenschutzstandards durchgeführt.

Erkannte Risiken

Die DSFA identifiziert insgesamt 14 systemische Risiken für die Grundrechte Betroffener. Mögliche Risiken sind insbesondere:

- der unbefugte Zugriff auf PNR-Daten
- die Fehlklassifikation von Personen und fälschliche Markierung derer Daten aufgrund unvollständiger Informationen oder mangelnder Datenqualität.
- Bearbeitung unerlaubter, besonders schützenswerter Personendaten

Massnahmen zur Risikominderung

Die DSFA weist insgesamt 26 Massnahmen aus, mit denen sich die identifizierten Risiken wirksam auf ein vertretbares Restrisiko minimieren lassen.

Die Massnahmen sind rechtlicher, organisatorischer, technischer Natur und zielen darauf ab, die Eintrittswahrscheinlichkeit und das Schadensausmass der Risiken zu reduzieren.

Hier einige Beispiele, wie die Massnahmen das Restrisiko beeinflussen:

- **Verschärfte Zugangskontrollen und technische Sicherheitsmassnahmen** wie verbesserte Überprüfungsverfahren und Protokollierung helfen, unbefugten Zugriff auf die PNR-Daten zu verhindern und reduzieren damit das Risiko von Datenschutzverletzungen.
- **Regelmässige Schulungen der Mitarbeiterinnen und Mitarbeiter erhöhen das Bewusstsein und die Kompetenz im Umgang mit sensiblen Daten**, was dazu beiträgt, menschliche Fehler zu minimieren, die zu Datenschutzverletzungen führen könnten.
- **Technologische Verbesserungen und regelmässige Systemüberprüfungen**, einschliesslich Penetrationstests und Überprüfungen der Datenintegrität, stellen sicher, dass die Systeme sicher sind und korrekt funktionieren, was das Risiko von technischen Pannen verringert.
- **Klare rechtliche und organisatorische Richtlinien** sorgen für eine bessere Compliance und stärkere Rechenschaftspflicht innerhalb der Organisation. Dies trägt zur Reduzierung von rechtlichen und operationellen Risiken bei.
- **Datenminimierung und verbesserte Datenschutzpraktiken** wie das automatisierte Löschen oder Pseudonymisieren von Daten nach festgelegten Fristen helfen, das Risiko des Missbrauchs alter oder nicht mehr benötigter Daten zu verringern.

Die Umsetzung dieser Massnahmen ist entscheidend, um die Sicherheit und den Schutz der bearbeiteten personenbezogenen Daten zu gewährleisten.

Einschätzung des EDÖB

Der EDÖB hat die vorliegende DSFA geprüft und stellt in seiner Stellungnahme vom April 2024 fest, dass:

- die DSFA sorgfältig erarbeitet wurde;
- die für die Beurteilung benötigen Informationen vorliegen;
- die aufgeführten Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen den gesamten, durch das FPG neu einzuführenden Datenbearbeitungsprozess abdecken;
- bei mehreren festgestellten hohen Risiken zweckmässige Massnahmen vorgesehen sind.

Weiterführende Informationen

Das vollständige Dokument «Datenschutzfolgeabschätzung PNR Schweiz» ist auf Nachfrage unter folgender Mailadresse erhältlich: pnr@fedpol.admin.ch