EU-Richtlinie

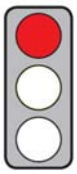
FLUGGASTDATEN

Stand: 21.03.2011

KERNPUNKTE

Ziel der Richtlinie: Die Fluggesellschaften werden verpflichtet, Fluggastdaten an mitgliedstaatliche „Zentralstellen" zu leiten, die diese Daten zur Bekämpfung von schwerer Kriminalität und Terrorismus nutzen können.

Betroffene: Flugreisende, Fluggesellschaften.



Pro: –

Contra: (1) Die Richtlinie verstößt, da unverhältnismäßig, gegen das europäische Grundrecht auf Datenschutz (Art. 8 ChGR) und als verdachtsunabhängige Rasterfahndung gegen das deutsche Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

(2) Der Nutzen ist vernachlässigbar, wie die Erfahrungen der USA zeigen.

(3) Verblüffend ist, dass die Kosten für die Einrichtung von „Zentralstellen" laut Kommission plötzlich nur noch bei etwa einem Drittel des von ihr selbst errechneten Betrags liegen sollen.

INHALT

Titel

Vorschlag KOM(2011) 32 vom 2. Februar 2011 für eine **Richtlinie** des Europäischen Parlaments und des Rates über die **Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität.**

Kurzdarstellung

- **Hintergrund und Ziel**
  - Durch die Erhebung und Verarbeitung von Fluggastdaten sollen strafrechtliche Ermittlungen gegen Personen unterstützt werden, die an einer terroristischen oder schweren Straftat beteiligt sein könnten.
  - Fluggesellschaften müssen die von Ihnen bei jeder Flugbuchung erfassten „PNR-Daten" zu all jenen Fluggästen an Behörden der Mitgliedstaaten weiterleiten, die aus Drittstaaten in die EU einreisen oder in Drittstaaten aus der EU ausreisen.
  - Die PNR-Daten (Passenger Name Record) umfassen bis zu 19 verschiedene Angaben, die die Fluggesellschaften bislang für eigene Zwecke erheben, u. a. Reisedaten, Rechnungsdaten und Anschrift sowie die Zahl und die Namen von Mitreisenden (s. Anhang der Richtlinie).
  - Die Richtlinie regelt die Datenverarbeitung (Sammlung, Speicherung und Auswertung) durch nationale Behörden (Art. 4), den Datenaustausch zwischen den Mitgliedstaaten (Art. 7) und die Datenweitergabe an Drittstaaten (Art. 8).
- **Übermittlung der PNR-Daten von Fluggesellschaften an PNR-Zentralstellen**
  - Für die Sammlung, Speicherung und Auswertung der PNR-Daten errichten oder benennen die Mitgliedstaaten jeweils eine nationale „PNR-Zentralstelle" (Art. 3 Abs. 1).
  - Die Fluggesellschaften müssen die PNR-Daten auf elektronischem Wege in die Datenbank der Zentralstelle des Mitgliedstaats einspeisen, in dem ein Flug startet oder landet („Push-Methode"; Art. 6 Abs. 1).
    - Die Übermittlung hat 24 bis 48 Stunden vor der flugplanmäßigen Abflugzeit sowie ein weiteres Mal sofort nach Abfertigungsschluss zu erfolgen (Art. 6 Abs. 2).
    - Zentralstellen dürfen bei konkreten und akuten Bedrohungen durch terroristische Straftaten oder schwere Kriminalität PNR-Daten von Fluggesellschaften anfordern („Pull-Methode", Art. 6 Abs. 4).
  - Die Mitgliedstaaten müssen gegen Fluggesellschaften, die gegen ihre Pflichten bei der Datenübermittlung verstoßen, „abschreckende" Sanktionen (inkl. Geldbußen) festlegen (Art. 10).
- **Zuständige Behörden**
  - „Zuständige Behörden" sind alle nationalen Behörden, die für die Verhütung, Aufdeckung, Aufklärung oder strafrechtliche Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständig sind.
  - Sie sind berechtigt, PNR-Daten oder die Ergebnisse der Verarbeitung von PNR-Daten von den PNR-Zentralstellen anzufordern oder entgegenzunehmen, um sie einer weiteren Prüfung zu unterziehen oder geeignete Maßnahmen zu veranlassen (Art. 5 Abs. 1).
- **Speicherung, „Anonymisierung" und Löschung**
  - Die Zentralstelle speichert die übermittelten PNR-Daten
    - zunächst für 30 Tage (Art. 9 Abs. 1),
    - danach für weitere fünf Jahre (Art. 9 Abs. 2).
      - Hierfür muss sie grundsätzlich die Daten durch Trennung von Daten und Identifikationsmerkmalen „anonymisieren". Auch darf sie sie nur einer „begrenzten" Zahl ihrer Mitarbeiter zugänglich machen.
      - Ausnahmsweise dürfen diese Mitarbeiter die Trennung rückgängig machen und auf die vollständigen nicht-anonymisierte PNR-Daten zugreifen, wenn dies auf Anfrage einer Behörde für Ermittlungen zur

Autoren: Marcus Schwenke und Benedikt Langner | schwenke@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-105 | www.cep.eu

Abwehr einer konkreten Gefahr, akuten Bedrohungen oder für eine konkrete Ermittlung oder Strafverfolgungsmaßnahme erforderlich ist.
  - Nach Ablauf der fünf Jahre und 30 Tage müssen die PNR-Daten gelöscht werden. Ausgenommen sind die Daten, die an die zuständigen Behörden übermittelt wurden (Art. 9 Abs.3).

- **Verwendung der PNR-Daten durch die PNR-Zentralstelle**
  - Die Zentralstelle darf die PNR-Daten zur Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität wie folgt verwenden:
    - Sie darf die PNR-Daten von Fluggästen vor ihrer planmäßigen Ankunft bzw. ihrem Abflug mit „relevanten" internationalen oder nationalen Datenbanken abgleichen, um verdächtige Personen zu ermitteln. Dies hat „in nichtdiskriminierender Weise" und ohne Verwendung „sensibler Daten", z. B. zu Rasse, ethnischer Herkunft oder religiöser Überzeugung, zu erfolgen (Art. 4 Abs. 2 lit. b).
    - Sie darf die PNR-Daten bei „begründeten" Anfragen an die zuständigen Behörden weiterleiten, in besonderen Fällen auch Anfragen nach „spezieller Verarbeitung" dieser Daten entsprechen und die Ergebnisse dieser Verarbeitung weiterleiten (Art. 4 Abs. 2 lit. c).
  - Zudem darf die Zentralstelle die PNR-Daten bei terroristischen Straftaten und „schwerer grenzüberschreitender" Kriminalität wie folgt verwenden:
    - Sie darf die PNR-Daten anhand „im Voraus festgelegter Kriterien" abgleichen, um Fluggäste vor ihrer planmäßigen Ankunft bzw. ihrem Abflug zu überprüfen (Art. 4 Abs. 2 lit. a).
    - Sie darf die PNR-Daten auswerten, um sie zu aktualisieren oder „neue Kriterien" für die Überprüfungen der Fluggäste aufzustellen (Art. 4 Abs. 2 lit. d).
  - Die Zentralstelle leitet die PNR-Daten der ermittelten Personen auf Einzelfallbasis zur weiteren Überprüfung an die jeweilig zuständigen Behörden weiter (Art. 4 Abs. 4).
  - Die Mitgliedstaaten stellen sicher, dass jeder einzelne Treffer bei einem automatisierten Abgleich von PNR-Daten mit Datenbanken oder mit „im Voraus festgelegten Kriterien" von einem Mitarbeiter überprüft wird (Art. 4 Abs. 2 lit. a, b).

- **Schutz personenbezogener Daten**
  Die Mitgliedstaaten haben den Schutz personenbezogener Daten gemäß dem Rahmenbeschluss des Rates über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit (2008/977/JI) zu gewährleisten. Dies umfasst insbesondere die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung, Schadenersatz und Rechtsbehelfe.

- **Weitergabe von PNR-Daten**
  - Die PNR-Zentralstelle eines Mitgliedstaats kann im Bedarfsfall die „anonymisierten" PNR-Daten und gegebenenfalls auch die Ergebnisse der Verarbeitung dieser Daten bei der Zentralstelle jedes anderen Mitgliedstaats anfordern (Art. 7 Abs. 2).
  - Im Fall konkreter Bedrohungen oder konkreter Ermittlungen kann die Zentralstelle eines anderen Mitgliedstaat neben den „anonymisierten" PNR-Daten auch die Identifikationsmerkmale anfordern, so dass sie die Identität des Fluggastes ermitteln kann (Art. 7 Abs. 3).
  - Die Mitgliedstaaten dürfen PNR-Daten und die Ergebnisse der Verarbeitung dieser Daten in konkreten Einzelfällen an einen Drittstaat weitergeben. Dabei muss allerdings die Übermittlung dem Zweck der Richtlinie dienen und der Drittstaat insbesondere ein „angemessenes Schutzniveau" für die beabsichtigte Datenverarbeitung gewährleisten (Art. 8).

- **Überprüfung und Auswertung der Richtlinie**
  Die Kommission erstellt
  - 4 Jahre nach Inkrafttreten der Richtlinie einen Bericht über die Einbeziehung von innereuropäischen Flügen (Art. 17 lit. a);
  - 6 Jahre nach Inkrafttreten der Richtlinie einen Bericht über die Funktionsweise der Richtlinie (Art.17 lit. b).

Änderung zum Status quo

- Bislang müssen die Fluggesellschaften ihre PNR-Daten, aufgrund völkerrechtlicher Abkommen, nur an die Behörden der USA, Kanadas und Australiens weiterleiten, sofern Passagiere über die EU in diese Staaten einreisen. Künftig sollen auch die Behörden der Mitgliedstaaten über PNR-Daten verfügen können.
- Die bestehende Regelung zur Nutzung von „erweiterten Fluggastdaten" – insbesondere die biografischen Informationen aus dem maschinenlesbaren Teil des Reisepasses – („API-Daten", Richtlinie 2004/82/EG) bleibt von dem Richtlinienvorschlag unberührt.

Subsidiaritätsbegründung der Kommission

Die Kommission geht davon aus, dass die wirksame Bekämpfung von Terrorismus und schwerer Kriminalität eine grenzüberschreitende Aufgabe ist. Die verschiedenen Sicherheitssysteme der Mitgliedstaaten sind einer wirksamen Zusammenarbeit abträglich. Außerdem können die starken Unterschiede der nationalen Regelungen zu einem ungleichen Schutzniveau, Sicherheitslücken, höheren Kosten und Rechtsunsicherheit führen.

Politischer Kontext

Im November 2007 legte die Kommission einen Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von PNR-Daten zur Strafverfolgung in der EU vor [KOM(2007) 654]. Obwohl die Ratsarbeitsgruppen

2008 Einigkeit über den Vorschlag erzielten, versäumte es der Rat, diesen vor Inkrafttreten des Vertrages von Lissabon am 1. Dezember 2009 anzunehmen. Seitdem verfügt das Europäische Parlament über ein Mitspracherecht. Der vorliegende Richtlinienvorschlag trägt dem nun Rechnung.
Die EU hat seit Aufhebung der Kontrollen an den Binnengrenzen Maßnahmen ergriffen, um den grenzüberschreitenden Austausch personenbezogener Daten zwischen Strafverfolgungs- und anderen Behörden zu erleichtern, z.B. die Schengener Informationssysteme (SIS und SIS II).

Stand der Gesetzgebung

02.02.11	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Federführende Generaldirektion:	GD Inneres
Ausschüsse des EP:	N.N
Ausschüsse des Bundestags:	N.N
Entscheidungsmodus im Rat:	qualifizierte Mehrheit (Ablehnung mit 91 von 345 Stimmen; Deutschland: 29 Stimmen)

Formalien

Kompetenznorm:	Art. 82 Abs.1 lit. d und Art. 87 Abs. 2 lit. a AEUV
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren; ex-Art. 251 EGV)

BEWERTUNG

Ökonomische Folgenabschätzung

Ordnungspolitische Beurteilung

Durch die beabsichtigte Verwendung von PNR-Daten zur Bekämpfung von schweren Straftaten und Terrorismus werden die Daten vieler unbescholtener Fluggäste systematisch Gegenstand polizeilicher Untersuchungen und über mehr als fünf Jahre bei staatlichen Behörden gespeichert. Ein solch massiver Eingriff in das Grundrecht auf informationelle Selbstbestimmung bedarf daher einer fundierten Rechtfertigung.
Die Kommission selbst **räumt** jedoch **ein, dass ihr „keine detaillierten Statistiken dazu vor[liegen], inwieweit** solche **[PNR-]Daten dazu beitragen, schwere Kriminalität oder Terrorismus zu verhüten, aufzudecken, aufzuklären oder strafrechtlich zu verfolgen."** [KOM(2011) 32, S. 6]. Sie führt dies darauf zurück, dass es in der EU kaum Erfahrungen über die Verwendung von PNR-Daten gibt. Sie ignoriert allerdings – bewusst (?) – die vorhandenen Erfahrungen aus den PNR-Abkommen mit Drittstaaten. Dies lässt sich damit erklären, dass diese Erfahrungen indizieren, dass der Beitrag von PNR-Daten zur erfolgreichen Verbrechens- und Terrorismusbekämpfung vernachlässigbar ist: **Der Bericht des US-Department of Homeland Security** vom 5. Februar 2010, S. 7, etwa **stellt** über das PNR-Daten-Abkommen der EU mit den USA **fest, dass PNR-Daten nur ein einziges Mal für einen Gerichtsprozess „verwendet" wurden.** Zu den zentralen Fragen, ob die Daten für den Prozess wesentlich waren und wie der Prozess ausging, schweigt sich der Bericht aus. **Es ist daher nicht gerechtfertigt, in der EU die Speicherung und Verwertung von PNR-Daten vorzuschreiben.**
Genauso problematisch ist, dass die Kommission die Ausweitung auf innereuropäische Flüge prüfen will, zwei Jahre bevor überhaupt Erfahrungen über die Funktionsweise der Richtlinie vorliegen. Ebenso wenig nachvollziehbar ist, dass sie eine Ausweitung auf den Eisenbahn- und Seeverkehr in Erwägung zieht, „sobald erste Erfahrungen über die Verwendung von PNR-Daten im Luftverkehr vorliegen." [s. SEK (2011) 132, S. 36]. Dies ist zwar insofern folgerichtig, als eine Verwendung von PNR-Daten nur des Flugverkehrs potentielle Straftäter in der Tat dazu verleiten könnte, auf andere Verkehrsträger auszuweichen.
Die erwogene **Ausweitung der Maßnahmen auf den Eisenbahnverkehr ist** aber bereits wegen der unterschiedlichen Nutzungscharakteristika **nicht praktikabel:** Reisende nutzen Züge oftmals spontan, und **Eisenbahnverkehrsunternehmen erfassen** bis auf wenige Ausnahmen (Eurostar und Online-Buchungen) **bislang keine PNR-Daten.** Auch die tatsächliche Nutzung eines Zuges wird im Gegensatz zur tatsächlichen Nutzung eines Flugzeugs nicht überprüft. Die Aussagekraft der PNR-Daten wäre somit deutlich geringer.
Die Kommission muss akzeptieren, dass es keinen umfassenden Schutz vor schwerer Kriminalität und Terrorismus gibt. Dieser wäre bestenfalls zum Preis eines allumfassenden Überwachungsstaats zu haben.

Folgen für Effizienz und individuelle Wahlmöglichkeiten

2007 schätzte die Kommission bei der Präsentation des damaligen Rahmenbeschluss-Vorschlags die Kosten für die Einrichtung von PNR-Zentralstellen und der Kommunikationsinfrastrukturen für alle Mitgliedstaaten auf 615 Millionen Euro [s. SEK(2007) 1453, S. 28]. Bei der Präsentation des jetzigen Richtlinien-Vorschlags rechnet sie nur noch mit 221 Millionen Euro [s. SEK(2011) 132, S. 39]. **Die Kommission bleibt jede Erklärung schuldig, warum die** von den Mitgliedstaaten zu tragenden **Kosten für die Einrichtung plötzlich nur noch bei etwa einem Drittel des ursprünglich errechneten Betrags liegen sollen.** Ihr Hinweis darauf, dass die wahren Kosten „irgendwo zwischen diesen beiden Schätzungen" liegen, ist nicht hinnehmbar [s. SEK(2011) 132, S. 40].

Nachvollziehbare Schätzungen forderte auch das kommissionsinterne Impact Assessment Board, IAB, bei der Bewertung einer früheren Version der Folgenabschätzung [s. IAB-Stellungnahme vom 10. September 2010].

Juristische Bewertung

Kompetenz

Die einschlägige Ermächtigungsgrundlage ist Art. 82 Abs.1 lit. d und Art. 87 Abs. 2 lit. a AEUV.

Subsidiarität

Es ist nicht ersichtlich, dass ein Handeln auf EU-Ebene einen Mehrwert verspricht. Die Begründung der Kommission, eine Harmonisierung nationaler Regelungen sei nötig, ist unhaltbar, da mit dem Vereinigten Königreich nur ein Mitgliedstaat ein fertiges System zur Verarbeitung von PNR-Daten für Strafverfolgungszwecke oder Terrorismusbekämpfung eingerichtet hat und nur wenige weitere Mitgliedstaaten die Einführung eines solchen Systems planen. Die geplante Richtlinie verstößt deshalb gegen das Subsidiaritätsprinzip.

Verhältnismäßigkeit

Die Kommission verzichtet auf jegliche Begründung, warum die vorgesehene Erfassung und Verarbeitung personenbezogener Daten notwendig sein sollte. Insbesondere **bleibt** sie **den Nachweis schuldig, warum** zur Bekämpfung von Terrorismus und schwerer Kriminalität **über die** bereits erhobenen **API-Daten hinaus weitere Daten erfasst werden müssen.** Die Verwendung von API-Daten stellt einen deutlich geringeren Eingriff in das Grundrecht auf Datenschutz (Art. 8 ChGR) dar.

Die vorgeschlagene **Speicherzeit von fünf Jahren und 30 Tagen ist sowohl zu lang als auch willkürlich**: Die Kommission verzichtet auf jede Begründung für diese Dauer, äußert sich insbesondere auch nicht dazu, wie genau und nach welchen – eine derart lange Zeit evtl. rechtfertigenden – „Kriterien" die Überprüfung der Fluggäste in den Mitgliedstaaten erfolgen soll. Im Übrigen betragen die Speicherfristen für API-Daten lediglich 24 Stunden (Richtlinie 2004/82/EG, Art 6 Abs. 1), für Vorratsdatenspeicherung in der Telekommunikation zwei Jahre (Richtlinie 2006/24/EG, Art. 6) und für an Kanada zu übermittelnde PNR-Daten dreieinhalb Jahre.
Die Unverhältnismäßigkeit der Speicherdauer wird auch nicht durch die vorgeschlagene Trennung der persönlichen Identitätsmerkmale von den übrigen Daten geheilt, da dies innerhalb der vorgesehenen fünf Jahre ohne größere Hürden rückgängig gemacht werden kann.

Vereinbarkeit mit EU-Recht

Die verdachtslose Speicherung und Verarbeitung der PNR-Daten verstößt gegen das Grundrecht auf Datenschutz (Art. 8 ChGR), da der Eingriff, wie oben dargelegt, **unverhältnismäßig ist**. Das Sammeln und Aufbewahren von Daten unverdächtiger Personen verstößt auch gegen das für dieses Grundrecht festgelegte Erfordernis der Zweckbindung der Datenverarbeitung (Art. 8 Abs. 2 ChGR), da die Masse der PNR-Daten zum Zweck einer im Voraus nicht absehbaren Datennutzung auf Vorrat gespeichert wird.

Vereinbarkeit mit deutschem Recht

Das Bundesverfassungsgericht (BVerfG) verzichtet auf die Ausübung seiner Zuständigkeit, solange der Europäischer Gerichtshof (EuGH) einen Grundrechtsschutz gewährleistet, der dem des Grundgesetzes im Wesentlichen entspricht („Solange II", 2 BvR 197/83; „Lissabon", 2 BvE 2/08, 337). Das Grundgesetz bleibt daher bei der Umsetzung der Richtlinie implizit zu berücksichtigen.
Die in der Richtlinie vorgesehene verdachtslose Vorratsdatenspeicherung greift in das informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Für die (von einer EU-Richtlinie vorgegebene) verdachtslose Speicherung individueller Telekommunikationsdaten erachtete das BVerfG bereits eine Speicherungsdauer von sechs Monaten als Obergrenze dessen, was zu rechtfertigen sei (1 BvR 256/08). Maßgeblich zugunsten der Vorratsdatenspeicherung wertete das Gericht zudem den Umstand, dass die Daten bei den Diensteanbietern gespeichert werden und nicht direkt beim Staat, wie es der Vorschlag für PNR-Daten vorsieht.
Problematisch ist auch der Abgleich der PNR-Daten mit noch festzulegenden „Kriterien" durch die Zentralstellen, bei dem es sich um eine Art „Rasterfahndung" handelt. Eine präventive polizeiliche Rasterfahndung ist mit dem grundgesetzlichen Grundrecht auf informationelle Selbstbestimmung nur vereinbar, wenn zumindest eine konkrete Gefahr für hochrangige Rechtsgüter gegeben ist. **Als verdachtsunabhängige Vorfeldmaßnahme entspricht die von der Kommission vorgesehene Rasterfahndung nicht den Anforderungen des Grundgesetzes** (BVerfG, 1 BvR 518/02).

Alternatives Vorgehen

Der Richtlinienvorschlag sollte zurückgenommen werden. Stattdessen sollte die polizeiliche und justizielle Zusammenarbeit in der EU, z.B. über die Schengener Informationssysteme, verbessert werden.

Zusammenfassung der Bewertung

Der Richtlinienvorschlag sollte nicht verabschiedet werden. Die verdachtslose Speicherung und Verarbeitung der PNR-Daten verstößt, da unverhältnismäßig, gegen das Grundrecht auf Datenschutz (Art. 8 ChGR) und als verdachtsunabhängige Rasterfahndung gegen das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Überdies ist der Nutzen für die Verbrechens- und Terrorismusbekämpfung vernachlässigbar, wie die Erfahrungen der USA zeigen. Nicht nachvollziehbar ist, warum die Kosten für das neue System bei etwa einem Drittel des ursprünglich errechneten Betrags liegen sollen.