

PNR

<<TableOfContents>>

Passenger Name Records sind umfangreiche Datensätze über Flugpassagiere, die bei den Fluggesellschaften anfallen und von zahlreichen staatlichen Stellen in großen Mengen und für lange Zeiten gespeichert werden.

Diese Seite beschäftigt sich vor allem mit bilateralen Abkommen der EU mit Drittstaaten zum Austausch dieser Daten. Zur eigenen PNR-System der EU vgl. [[EU-PNR]], das neue (ab 2018) deutsche System wird unter [[DE-PNR]] beschrieben. Auch „Erkenntnisse“, die aus den hier behandelten Systemen kommen, können aber durchaus an Europol oder nationale Polizeien zurückfließen.

Von PNR zu unterscheiden sind die [[API]]-Daten. Dies sind typischerweise die Daten, die maschinenlesbar auf Identitätsdokumenten stehen (Name, Geburtsdatum, Staatsangehörigkeit) plus Daten zum Verkehrsmittel (etwa Flugnummer und -gesellschaft, Abflug- und Zielort). Im Vergleich zu den manuell erfassten PNR-Daten haben sie typischerweise höhere Qualität, weil sie frei von Tippfehlern und ähnlichem sind; sie sind aber auch weit weniger umfangreich und stehen erst deutlich später zur Verfügung.

= Allgemeines zu PNR mit Drittstaaten =

Der Begriff PNR kam auf im Zusammenhang mit Übertragungen umfangreicher Datensätze von Fluggesellschaften an das Department of Homeland Security in den USA. Die Zielstaaten gleichen die Daten mit nationalen Datenbanken ab und versuchen ansonsten, mit Data Mining oder einfachem Raten, unerwünschte Menschen rauszufiltern.

Für Flüge, die eine Schengengrenze überschreiten, fühlte sich die EU-Kommission berufen (vgl. [[#Geschichte]]), den Datenaustausch zu regulieren. Das Ergebnis war ein Satz von Abkommen und „Understandings“, die eher beschreiben als beschränken, was da gemacht wird. Im „Gegenzug“ sollte v.a. [[Europol]] Informationen aus den „Erkenntnissen“ zurück erhalten, welche die USA aus den PNR-Daten erhalten wollten.

Dieses Grundprinzip ist inzwischen etwas verrechtlicht und wird zumindest auch für Australien und Kanada ähnlich angewandt.

Die PNR-Daten werden von den Empfängerländern über viele Jahre gespeichert, in den USA etwa für Jahrzehnte beim Department of Homeland Security.

Es gibt Zusagen der Empfängerländer zu den Zwecken – Terror ist immer dabei, dann natürlich die unvermeidbare „Organisierte Kriminalität“ oder auch „serious crime“, ohne dass dieses im Einzelnen konkretisiert würde; im Fall von Australien fand sich zeitweise sogar ein „significant

public health risk“ unter den Fahndungszielen, der es so allerdings nicht in die EU-Vereinbarung geschafft hat.

== Datensatz ==

Im Brief an die EU-Kommission (<<BtDS(16/6750)>>, S. 11) beschreibt das US-DHS den PNR-Datensatz wie folgt (vgl. unten für den Australischen Datensatz):

- PNR-Buchungscode (Record Locator)
- Datum von Reservierung bzw. Ausgabe des Flugtickets
- Die vorgesehenen Reisedaten
- Passagiernamen
- Verfügbare Informationen über Vielflieger- und andere Bonusprogramme sowie weitere Rabatte
- Andere Namen innerhalb des PNR, einschließlich der Anzahl der Reisenden, die der PNR betrifft
- Alle verfügbaren Kontaktinformationen
- Alle verfügbaren Rechnungs- und Zahlungsinformationen, mit Ausnahme anderer Transaktionsdetails, die eine Kreditkarte betreffen und nicht mit den Reisetransaktionen zu tun haben
- Reiseablauf für den jeweiligen PNR
- Reisebüro, bei dem die Reise für den jeweiligen PNR gebucht wurde
- Informationen zu eventuellem Code-Sharing
- Informationen über die Splittung/Teilung einer Buchung
- Reisestatus des Passagiers, einschließlich von Buchungsbestätigungen und Informationen über den Check-in
- Ticket-Informationen einschließlich Flugscheinnummer, Infos über One-Way-Tickets und zur automatischen Tarifabfrage
- Alle Informationen über das aufgegebene Gepäck
- Informationen zum Sitzplatz einschließlich Sitzplatznummer
- Allgemeine Informationen, einschließlich aller Angaben zu Service-Anforderungen wie OSI, SSI, SSR (Other Service Request, Special Service Information, Special Service Request); diese können alles mögliche sein, etwa "Fahrrad dabei", "Säugling dabei", "Koscheres Essen", "Rollstuhl" usf. Wie Gus Hosein [\[\[http://www.publications.parliament.uk/pa/ld200607/ldselect/lddeucom/108/7022803.html| vor dem UK House of Lords ausführt\]\]](http://www.publications.parliament.uk/pa/ld200607/ldselect/lddeucom/108/7022803.html), ist Terminologie und Inhalt dieser Felder weitgehend abhängig von der Fluggesellschaft. Saftige Stückchen sind in jedem Fall dabei.
- Sofern erfasst und verkünpft, [\[\[API\]\]](#)-Daten (die überschneiden sich zwar in der Regel, sind aber weniger anfällig gegen Tippfehler, Schreibvarianten etc).
- Änderungsgeschichte des kompletten Datensatzes

Der zitierte Brief enthält auch folgenden Datenschutzbarock:

{ { { #!blockquote Soweit sensible EU-PNR-Daten (d.h. personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche

Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben einer Person) [...] in den oben genannten Arten von EU-PNR-Daten enthalten sind, verwendet das DHS ein automatisiertes System, das diese sensiblen PNR-Codes und -Bezeichnungen herausfiltert, und nutzt derartige Informationen nicht. Das DHS löscht die sensiblen EU-PNR-Daten unverzüglich, sofern nicht in einem Ausnahmefall (siehe folgenden Absatz) auf sie zugegriffen wird. }}}

Die Ausnahmeklausel ist „Leben [...] gefährdet oder ernsthaft beeinträchtigt werden“ – was natürlich immer konstruierbar ist; dann ist auch der Zugriff auf weitere verfügbare Daten erlaubt. Immerhin soll das DHS, wenn es zusätzliche Daten dieser Art verwendet, etwas ernsthafter protokollieren und der EU-Kommission berichten, wenn es so etwas tut. Ob es einen solchen Bericht je gab, ist unbekannt; da allerdings die EU-Kommission als Wahrerin von Menschenrechten ohnehin kaum glaubwürdig ist, kommt es darauf vielleicht auch nicht an.

Daten dieser Art werden über viele Jahre gespeichert, zur Beruhigung naiver EU-Parlamentarier_innen auch mal „ruhend“ (was heißt, dass der Personenbezug etwas schwerer herzustellen ist). Die ersten Verträge sagten noch nichts zu Datensatz und Speicherfristen aus, Entsprechendes wurde in relativ informellen Selbstverpflichtungen der Vertragspartner geregelt, die damit ihr „ausreichendes Datenschutzniveau“ dokumentieren sollen. Am Beispiel Kanadas, dessen erster Vertrag 2010 noch angewandt wurde, obwohl die Datenschutzregelungen verletzt waren (vgl. unten), lässt sich illustrieren, dass darauf nicht viel zu geben ist.

== Zahlen ==

Jedenfalls anfangs wurden bei weitem nicht sämtliche PNRs auch wirklich übertragen; im Groben waren die PNR-Systeme anfänglich wohl einfach nur Zugriffsmöglichkeiten der Repressionsbehörden auf die Passagierinformationssysteme der Fluggesellschaften (edel als „Pull-Zugriff“ bezeichnet). Welcher Anteil der möglichen PNRs von den jeweiligen Staaten wirklich verarbeitet wird und wie viele Menschen deswegen Ärger bekommen, ist nicht bekannt.

In einem [[<http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf>][Untersuchungsbericht des britischen House of Lords von 2008]] (PDF-Seite 37) beschreibt Meg Hillier vom UK-Innenministerium die großen Erfolge des UK-PNR-Systems; so wurden im Untersuchungszeitraum 38 Millionen PNR-Datensätze verarbeitet. Dies ist sicher nur ein überschaubarer Teil der Daten, die im UK insgesamt verarbeitet werden sollen. Eine 95%-Abdeckung der Flugbewegungen erwartete Hillier für Ende 2010.

Die 38 Millionen PNRs haben demnach zu 17000 „Alerts“ geführt. Diese wiederum hätten zu 1400 Festnahmen geführt, womit die Effizienz des Verfahrens erwiesen sei, weil immerhin einer von zwölf Belästigten zu Recht belästigt worden sei. Dass bereits eine polizeiliche Verhaftung als Schuldnachweis gilt, illustriert recht schön das Rechtsverständnis dieser Leute.

Für das US-PNR-System berichtet [[<http://euobserver.com/9/31731>]|ein Artikel auf euobserver.com von 2011]] über Aussagen eines anonymen US-Beamten, der angab, von den 80 Millionen Menschen, die 2008 in die USA einreisten, seien 1800 aufgrund von PNR-Daten abgewiesen worden. Wiederum gibt es keine Erwähnung möglicher gerichtlicher Prüfungen.

In einer [[<http://www.heise.de/newsticker/meldung/EU-Parlament-segnet-Fluggastdaten-Transfer-in-die-USA-ab-1542874.html>]|heise-Meldung vom 19.4.2012]] wird die Berichterstatte(r)in zum PNR-Abkommen mit den USA, Sophie in't Veld, mit der Angabe zitiert, schon „derzeit zögen US-Behörden täglich bis zu 82.000-mal am Tag Daten aus den Reservierungssystemen der Fluglinien ab.“ Was das bedeutet, ist völlig unklar, zumal ja zu diesem Zeitpunkt die Fluggesellschaften ihre Daten in aller Regel schon an die Repressionsbehörden „pushen“ sollten und nicht diese „pullen“.

Kanadische Behörden berichten in einem [[http://www.oag-bvg.gc.ca/internet/English/parl_oag_200710_05_e_23829.html]|Papier von 2012]] (Abschnitt 5.47), 37% der API und PNR-Records hätten sich bei einem Test im Jahr 2006 als so schlecht erwiesen, dass für Repressionszwecke nicht getaugt hätten.

= PNR EU-US =

Das PNR-Abkommen zwischen den USA und der EU war das erste, und die USA waren führend in der Nutzung von PNR-Daten zu Repressionszwecken. Wie in [[#Geschichte]] dargestellt, war zunächst alles geheim, die USA versuchten, Regelungen möglichst zu vermeiden. Nach viel Grummeln von europäischer Seite ist ab 2009 ein halbwegs öffentliches Verfahren zur Aushandlung eines immerhin offiziell bekannten Vertrags im Gange; auch hier versuchten die Regierungen noch rumzuspooken, etwa, indem ein [[<http://papersplease.org/wp/wp-content/uploads/2011/11/eu-us-pnr-2011-de.pdf>]|Vertragsentwurf]] laut [[<http://www.heise.de/newsticker/meldung/Entwurf-fuer-transatlantisches-Abkommen-zum-Fluggastdaten-Transfer-steht-1386435.html>]|heise.de-Meldung vom 28.11.11]] den Parlamentsabgeordneten zunächst nur in einem „Leseraum“ hätte zugänglich sein sollen.

== Speicherdauer ==

Die US-Behörden versprechen in einem Brief an die EU-Kommission (<<BtDS(16/6750)>>, S. 13, Artikel VII) folgendes Verfahren: Die Daten werden in den USA generell 15 Jahre gespeichert, wobei nach sieben Jahre nur durch einen „hochrangigen, vom US-Heimatschutzminister benannten DHS-Beamten zugegriffen werden“ können soll (der DHS-Jargon ist „ruhend“). Daten, die zu einer Ermittlung gehören, dürfen die US-Behörden weitgehend beliebig speichern und verarbeiten.

== Rechtsgrundlage ==

Rechtsgrundlage für die Übermittlung von PNR-Daten aus der BRD an die USA ist <<Ratsdokument(17434/11)>> sowie umsetzende BRD-Gesetze, für die Übertragungen in die USA derzeit das "Gesetz zu dem Abkommen vom 26. Juli 2007 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS)", abgedruckt in <<BtDS(16/6750)>>.

Auf EU-Ebene ist das Analogon der (ausgerechnet vom schillernden Tom Ridge mitunterschriebenen) [[<http://eur-lex.europa.eu/Notice.do?val=340489:cs&lang=en&list=340546:cs,340545:cs,340489:cs,340544:cs,402655:cs,340690:cs,340689:cs,340688:cs,340687:cs,340686:cs,&pos=3&page=1&nbl=24&pgs=10>]|Vertrag mit den USA]] und entsprechende Dokumente für Kanada und Australien. Diese

Verträge definieren allerdings kaum wirksam Rechte, Pflichten und Prozesse.

Die datenschutzrechtlich interessanten Vereinbarungen sind in begleitenden Briefwechseln enthalten; für die USA ist dieser in <<BtDS(16/6750)>>, S. 10ff zu finden. Dass diese quasi in Seitenprotokollen abgehandelt werden, lässt schon ahnen, dass sie eher Vorschlagscharakter haben, und das DHS ist kaum bekannt für behutsamen Umgang mit Menschenrechten.

= PNR EU-Kanada =

Besonders pikant an der Vereinbarung mit Kanada ist, dass der <<Doclink(2010-eu-overview.pdf,EU-Überblick von 2010)>> (S. 17) zwar einräumt, auch nach Ansicht der Kommission sei spätestens seit September 2009 nicht mehr von einem ausreichenden Datenschutzniveau in Kanada auszugehen, das PNR-Abkommen aber weiterhin als gültig ansieht.

Nach Darstellung des <<Doclink(2010-eu-overview.pdf,EU-Überblicks von 2010)>> (S. 18) werden in Kanada die Daten 72 Stunden aktiv und 3.5 Jahre ruhend.

= PNR EU-Australien =

Zur PNR in Australien hat die Kommission 2011 <<Ratsdokument(10093/11)>> vorgelegt, den Vertrag mit Australien, das, nach Maßstäben dieses Geheimdienstgeschäfts, relativ umfangreich spezifiziert, was gemacht werden soll; diese relativ große Offenheit ist vermutlich recht heftigen Interventionen des Parlaments geschuldet, das sich gerade im Fall Australien besonders geschnitten gefühlt hat.

""Zweck"": Australien darf die Daten für Terror und „schwerwiegende transnationale“ Verbrechen, in Ausnahmefällen auch bei Gesundheitsgefahren für Einzelpersonen verwenden. Der Vertrag bemüht sich, ie Begriffe in Art. 3 (2) und (3) genauer zu bestimmen.

""Terrordefinition"": Dabei umfasst Terror auch Geldbeschaffung oder Rechtshilfe für Organisationen, die eine Regierung oder internationale Organisation einschüchtern oder zu Handlungen zwingen wollen und dabei Schaden an Eigentum riskieren – mithin ist eigentlich jede politische Aktivität bei Bedarf erfassbar. Schwere Kriminalität wird über Australisches Recht definiert (Höchststrafe mindestens vier Jahre), transnational heißt ein Verbrechen, das entweder grenzüberschreitend geplant oder durchgeführt wird, grenzüberschreitende Wirkungen hat oder von einer grenzüberschreitenden Gruppe begangen wird. Auch hier ist also nicht viel ausgeschlossen.

""Rückflussgebot"": Art. 6 sieht vor, dass aus EU-PNR-Daten gewonnene Informationen an die EU-Behörden (der Länder oder Europol oder Eurojust) zurückfließen sollen, wenn diese zuständig sind, und dass Datenwünsche für jeweils bestimmte Fälle aus dem Bereich Schwere Kriminalität und „Terrorismus“ erfüllt werden.

""Weitergabe"": Die PNR-Daten können nach Art. 18 und 19 recht frei übertragen werden, insbesondere an eine durch Regierungsdekret erweiterbare Liste von australischen Behörden. Speziell für maskierte Daten gibt es keine nennenswerte Beschränkung (z.B. auf Einzelfälle), zumal im üblichen Bock-Gärtner-Paradigma die Grenzbehörden selbst die Recht- und Verhältnismäßigkeit

von Anfragen prüfen soll. An Drittstaaten soll aber grundsätzlich nur fallbezogen übertragen werden. Weiter im Bock-Gärtner-Paradigma sollen die zuständigen Behörden von EU-Ländern informiert werden, wenn Daten eines Bürgers ihrer Staaten übertragen werden (Art 19 (1f)).

""Auskunftsrecht"": Artikel 12 regelt das Auskunftsrecht unter Verweis auf australisches Fol-Recht, zuständige Stelle sind die australischen Grenzbehörden; insbesondere soll „without undue constraint or delay“ auch Auskunft über Übertragungen der Daten gegeben werden. Wie üblich kann die Auskunft aus vielen Gründen verweigert werden („safeguard the prevention, detection, investigation, or prosecution...“); immerhin sollen die Grenzbehörden (anders als Europol) nicht lügen dürfen, der Umstand, "dass" gespeichert wird und eine Auskunft unterbleibt, muss also mitgeteilt werden, und Opfer können sich an den Information Commissioner in Australien wenden. In Artikel 14 wird sogar Schadenersatz angeboten, wenn dabei rauskommen sollte, dass Daten missbräuchlich verarbeitet wurden. Wir alle warten auf die erste Anwendung "dieser" Regel.

""Speicherfrist"" (Art. 16): 5.5 Jahre, wobei in den letzten 2.5 Jahren der volle Datensatz „maskiert“ werden soll (Art 16 (a): Namen, Kontaktinfo, Teile von OSI, SSI, SSR, Teile von API-Daten werden zwar weiter gespeichert, aber normalerweise nicht genutzt). Konfus dabei: Die Daten sollen grundsätzlich zur Identifikation von „potential persons of interest“ dienen können. Dies scheint sich eben nicht nur auf Terror und Schwerverbrechen zu beziehen, denn das wird speziell nochmal für die demaskierten Daten in 16 (1b) gefordert. Letztlich wird aber ohnehin niemand die Australier daran hindern, mit einmal übertragenen Daten zu tun, was immer sie wollen.

""Datensatz"" für Australien

- PNR-Identifizier
- Datum der Reservierung, Reisetermine, geplante Strecke
- Namen (auch etwa von Begleitpersonen), augenblicklicher Status (Rückbestätigung, Check-In usf)
- Infos zu Bonusprogrammen
- Alle Kontaktinformationen
- Alle Informationen zur Bezahlung
- Alle Informationen zum Gepäck
- Informationen zum Ticket (Nummer, One-way, ...), Sitznummer
- Reisebüro
- Infos zu Codesharing (evtl, weil bei Codeshare-Flügen zwei PNRs anfallen?)
- Split/divided information (?)
- OSI, SSI, SSR, weitere "allgemeine Bemerkungen"
- Informationen aus APIS
- Changelog

Wie auch bei den PNR-Daten für die USA sollen „sensible Daten“ (s.o.) rausgefiltert und „nicht verwendet“ werden. Angesichts eines Mangels an Details in dieser Hinsicht ist nicht damit zu rechnen, dass aus dieser Vorschrift irgendeine praktische Einschränkung für den Datensatz ergibt.

= Geschichte =

"In chronologischer Reihenfolge, neuer Kram kommt unten hin"

Kurz nach 9/11 wollen die USA PNR-Daten für Flüge in die USA und bekommen sei wohl auch. Es beginnen Verhandlungen, um diese Datenübertragungen und -speicherungen zu legalisieren. Auch UK, Kanada und Australien fangen an, mit PNR-Systemen zu experimentieren.

Wenig später beginnt in der EU die Diskussion über eigene europäische PNR-Systeme; Streitfragen sind die Architektur -- ein zentrales vs. ein PNR-System pro Mitgliedsstaat --, Umfang -- nur Flüge, die die Schengengrenzen überschreiten, auch solche, die Staatengrenzen überschreiten, überhaupt alle Flüge oder auch noch gleich Schiffe und Züge --, Zweck -- reiner Terror oder auch verschiedene Sorten von Verbrechen oder Ordnungswidrigkeiten -- sowie nachrangig Datenschutzfragen wie Speicherfristen und Bestandteile des Datensatzes.

2003 legt die britische Regierung einen

[[<http://www.statewatch.org/news/2003/nov/10952.en03.pdf> Forderungskatalog]], der humanitäre Einsätze rechtfertigt hätte, im Jahr darauf gibt es dann einen

[[<http://www.statewatch.org/news/2004/jan/spain-pnr-7161-03.pdf>]]ersten Richtlinienentwurf der spanischen Regierung]]. Die Monstrosität der Pläne sorgt für nachhaltige Ablehnung, wann immer funktionierende Gremien beschäftigt werden.

Die daraus entstehende Situation wird in einem [[<http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf>]]2008er Bericht des UK House of Lords]] (PDF-Seite 20) wie folgt umrissen:

{{{#!blockquote Of the six largest Member States, Germany shared the view of the United Kingdom that flights between Member States should be covered, France was doubtful, while Italy, Spain and Poland (and nearly all the smaller States) wanted the Framework Decision restricted to flights to and from third countries. Spain and France wanted, like the United Kingdom, to include both sea and rail transport, while Germany, Italy and nine smaller Member States wanted in due course to include sea transport but not rail. Poland and the remaining Member States which replied wanted the Framework Decision restricted to air travel}}}}

2007 steht die Association of European Airlines (mit Mitgliedern wie Lufthansa, BA, Air France oder KLM) auf und spricht sich [[<http://www.statewatch.org/news/2007/nov/eu-pnr-airlines-reactions.pdf>]]in einer Erklärung]] (bei statewatch gespiegelt) gegen die dann aktuellen Pläne aus. Ihre Skepsis bezieht sich aber nicht auf die bürgerrechtliche Implikationen, sondern nur darauf, dass sie in einem Modell mit PNR-Systemen der Einzelstaaten fürchterliche Bürokratie hätten.

Das EU-Parlament äußert sich immer mal wieder eher menschenrechtsfreundlich. In einer

[[[http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:015E:0046:0050:EN:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:015E:0046:0050:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:015E:0046:0050:EN:PDF)]]Stellungnahme zum Vertrag mit Australien (OJ C15E/46ff))] etwa äußert es sich u.a. folgendermaßen:

- Die vertrauensvolle Zusammenarbeit mit dem Parlament sei missachtet worden, weil das Parlament von den Geheimverhandlungen nichts gewusst habe, und so fehle dem Vertrag demokratische Legitimation, abgesehen davon, dass unklar sei, warum die Kommission eigentlich mit einer Sache beschäftigt sei, die exklusiv die innere Sicherheit eines Drittstaates angeht

- PNR ist sehr wohl grundrechtsrelevant
- Das Abkommen hat uneinheitliche Terminologie und nennt an verschiedenen Stellen verschiedene Zwecke (Einführung vs. Art. 5(1)(iii) vs. Art 5(2) vs. Art. 5(3)), so dass die Zweckbestimmung "totally inadequate" sei
- Während immerhin erfreulich ist, dass EU-Bürger_innen keine schlechteren Datenschutzrechte haben als Australier_innen, sollte doch EU-Recht die Verarbeitung der Daten von EU-Bürger_innen bestimmen
- Die Beteiligung von Datenschutzorganen ist so schwammig spezifiziert, dass unklar ist, ob überhaupt so etwas stattfindet
- 5.5 Jahre Speicherfrist ist nicht verhältnismäßig
- Die im PNR-Geschäft übliche Praxis, in diplomatischen Briefe die Details der Verarbeitung festzulegen, ist nicht geeignet, den Datenschutz zu gewährleisten
- Das breite Spektrum der übertragenen Datentypen ist nicht verhältnismäßig

Schließlich lehnt das EU-Parlament im November 2008 die Abstimmung über [\[\[http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf|](http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf)einen letzten Entwurf]] ab, was Hoffnungen nährte, der Spuk könnte vorüber sein.

Leider sterben Pläne zum Bürgerrechtsabbau nicht, und im Stockholm-Programm (vgl. [\[\[Datenbanken EU#Fünfjahrespläne\]\]](#)) kam ein eigenes EU-PNR-System als Wiedergänger.

Die Kommission hat daraufhin am 2.2.2011 [\[\[http://www.statewatch.org/news/2011/feb/eu-com-eu-pnr-com-32-11.pdf|](http://www.statewatch.org/news/2011/feb/eu-com-eu-pnr-com-32-11.pdf)Kommissionsdokument 2011/0023]] vorgelegt, in dem vorgeschlagen wird, zur Bekämpfung aller möglichen Sorten von Kriminalität (neben politischer auch Drogen u.ä.) PNR-Daten von Flügen, die über eine Schengen-Außengrenze führen.

Nicht faul, hat die UK-Delegation [\[\[http://www.statewatch.org/news/2011/feb/eu-pnr-uk-proposals-6359-11.pdf|](http://www.statewatch.org/news/2011/feb/eu-pnr-uk-proposals-6359-11.pdf)Ratsdokument 6359/11]] nachgelegt, in dem PNR-Daten "for the prevention, detection, investigation and prosecution of terrorist offences and serious crime" auch dann verwendet werden sollen, wenn die Flüge innerhalb der EU stattfinden.

Im April 2011 stocken die Verhandlungen über die PNR-Übertragung in die USA laut einer Mitteilung auf dem Webportal der Datenschutzbeauftragten

[\[\[http://www.datenschutz.de/news/detail/?nid=4886|](http://www.datenschutz.de/news/detail/?nid=4886)datenschutz.de]], weil diese sich die Nutzung der PNR-Daten im Zusammenhang mit fast allen Verbrechen genehmigen wollen (statt bisher nur für TerroristInnen) und dazu eine Speicherfrist von 22 Jahren vorsehen (statt bisher 15). Im Wissen, dass solche Maßnahmen in der [\[\[EU\]\]](#) kaum durchsetzbar sein werden, verweigert selbst die kaum als datenschutzfreundlich bekannte EU-Innenkommissarin "Zensilia" Malmström die Zustimmung.

2011 berichtet

[\[\[http://www.unwatched.org/20110524_Flugastdaten_EU_Plaene_verfassungswidrig|](http://www.unwatched.org/20110524_Flugastdaten_EU_Plaene_verfassungswidrig)ein Artikel auf unwatched.org vom 24.5.]] von einem geheimen Gutachten des juristischen Dienstes des Rates der Mitgliedsstaaten zur PNR-Verarbeitung der EU selbst. Das Gutachten wurde offenbar an die Financial Times Deutschland geleakt, die am [\[\[http://www.ftd.de/politik/europa/:juristisches-gutachten-eu-plaene-fuer-fluggastdaten-nicht-verfassungsgemaess/60056184.html|](http://www.ftd.de/politik/europa/:juristisches-gutachten-eu-plaene-fuer-fluggastdaten-nicht-verfassungsgemaess/60056184.html)24.5.2011 berichtet]] (kostenpflichtiger Artikel), die Gutachter seien zur "Auffassung [gelangt], dass die

Richtlinie in der vorgeschlagenen Form das Recht auf Achtung des Privatlebens und das Recht auf Schutz der personenbezogenen Daten dermaßen einschränkt, dass sie (...) vor Gericht angefochten werden könnte."

Im Ende 2011 kommt viel Bewegung in die Vertragsprozesse mit Australien und den USA. Zunächst winkt der EU-Rat den Vertragsentwurf mit Australien durch

(<http://www.heise.de/newsticker/meldung/EU-Rat-verabschiedet-Abkommen-zum-Fluggastdaten-Transfer-nach-Australien-1348739.html>|heise.de vom 22.9.2011)). Dann wird der von deutlich mehr Geheimhaltungswahn umschwebte (<http://papersplease.org/wp/wp-content/uploads/2011/11/eu-us-pnr-2011-de.pdf>|Vertragsentwurf für US-EU-PNR) geleakt, den die EU-Parlamentarier_innen eigentlich nur in einem "Leseraum" hätten studieren dürfen (<http://www.heise.de/newsticker/meldung/Entwurf-fuer-transatlantisches-Abkommen-zum-Fluggastdaten-Transfer-steht-1386435.html>|heise.de vom 28.11.2011)). Dieser Entwurf wurde dann wenig überraschend im Dezember vom EU-Rat abgesegnet (<http://www.heise.de/newsticker/meldung/EU-Rat-winkt-Passagierdaten-Abkommen-durch-1394801.html>|heise.de vom 13.12.2011)).

Ende 2011 stehen damit die Verträge mit Australien und den USA kurz vor der parlamentarischen Beratung.

Im März 2012 winkt der Innenausschuss des EU-Parlaments das US-PNR-Abkommen mit immerhin relativ knappen 31:23 durch, bemerkenswerterweise gegen die Empfehlung der Berichterstatterin Sophie in't Veld (ALDE), die danach von einem "schweren Schlag für die bürgerlichen Freiheiten" sprach (<http://www.heise.de/newsticker/meldung/EU-Parlament-Innenausschuss-billigt-Fluggastdaten-Abkommen-1484415.html>|heise.de vom 27.3.2012)):

Im April 2012 nickt das EU-Parlament einen neuen Vertrag mit den USA ab (<http://www.heise.de/newsticker/meldung/EU-Parlament-segnet-Fluggastdaten-Transfer-in-die-USA-ab-1542874.html>|heise-Meldung 19.4.2012]), der für oberflächlich pseudonymisierte Daten unendliche Speicherfrist vorsieht; im Effekt werden die USA nie irgendwelche im Rahmen des PNR-Programms erhobene Daten löschen müssen. Vor der Entscheidung hatte die Parlamentsberichterstatterin Sophie in't Veld aufgrund der monströsen Grundrechtseingriffe Ablehnung gefordert, selbst die für

Nach längerem Widerstand gegen die EU-Pläne, ein eigenes PNR-System zu installieren (vgl. unten), kippt das EU-Parlament unter dem Eindruck des Angriffs auf die Charlie-Hebdo-Redaktion 2015 um. Zuvor hatte die Kommission bereits die Entwicklung nationalstaatlicher PNR-Systeme mit eigenen Mitteln gefördert (vgl. <<Doclink(2015-bfdi-tb.pdf,25. TB BfDI (2015))>>, S. 70).

Im Juli 2015 bewegt heftiger Druck verschiedener Regierungen das LIBE (Menschenrechte und Freiheiten)-Kommittee des EU-Parlaments, seinen Widerstand gegen ein eigenes EU-PNR-System aufzugeben. "[R]espect for the law appears not to be a concern when adopting law enforcement measures," (<https://edri.org/ep-pushes-for-more-surveillance-and-profiling-of-eu-citizens/>|kommentiert Joe McNamee von EDRI]) das Umfallen des Menschenrechtskommittees.

Schließlich verabschiedet das EU-Parlament am 14.4.2016 ein eigenes EU-PNR-System.

<<Ratsdokument(2017/29)>> ist ein Bericht der EU-Kommission zum US-PNR und ist beeindruckend zahnlos. Der offenbar weitgehend unkontrollierte Zugang zur PNR-Sammlung auf US-Seite wird kritisiert als:

{{{#!blockquote In relation to Article 5, the number of personnel with access rights to PNR data has increased since the previous review in 2013. Whilst the EU team is satisfied with the oversight mechanisms in place, DHS is invited to continue to monitor the number of staff with access rights to PNR data to ensure that only those with an operational need to use and view the data can do so. }}}}

Es wird auch berichtet, dass es offenbar Artikel 2-overrides gibt, ohne dass das DHS darüber vernünftig Rechenschaft ablegen könnte („DHS need to record detailed reasons of why overrides have been used“).

Nach unseren Erfahrungen schlicht falsch ist die Behauptung der Kommission, das DHS erteile PNR-Auskünfte:

{{{#!blockquote DHS continues to implement its commitments in relation to passenger rights, in particular as regards providing appropriate information to passengers and implementing the right to access without any exemptions as provided for under Articles 11, 12 and 13. }}}}

Soweit uns bekannt (wir wissen von einer runden Handvoll Anfragen), hat das DHS noch keine diesbezügliche Anfrage aus Europa je beantwortet.

An harter Information kommt aber immerhin heraus, dass die USA am 25.9.2015 Vollzug gemeldet haben fürs Pushen aller Fluggesellschaften.

Im Juli 2017 befindet der EuGH, dass der [[#PNR EU-Kanada|Vertrag mit Kanada]] die Bürgerrechte recht massiv verletzt. Zwar sei, so der EuGH in einer [[<https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084de.pdf>|Erklärung zum Urteil]], die Bekämpfung des Terrorismus ein eminent wichtiger Zweck und die PNR-Daten dazu auch geeignet [TODO: Mal nachsehen, ob es im Urteil irgendein Argument für diese eigenartige Behauptung gibt], doch hapere es bei vielen Regelungen an der Erforderlichkeit. Das betrifft insbesondere die Nutzung nach der Einreise, die der EuGH mit einem Gerichtsvorbehalt versehen will, sowie die fünfjährige Weiterspeicherung nach der Ausreise (und in der Tat muss mensch sich fragen, wie das auch nur einer der Parlamentarier_innen, die dafür die Hand gehoben hat, ernsthaft für grundrechtskonform halten können).

Außerdem fordert der EuGH klarere Bestimmungen über Natur und Nutzungen der PNR-Daten, ihrer Weitergabe durch Kanada sowie einer Pflicht zur Benachrichtung der Opfer für den Fall der Nutzung der Daten nach der Einreise.

Nach Verkündung des Urteils erhob sich der erwartbare Bocksgesang von autoritärer Seite, die klar machte, dass sie an PNR-Systemen, insbesondere auch [[EU-PNR|denen der EU]], strikt festhalte.

(Geschichte ab 2016 für EU unter [[EU-PNR#Geschichte]]).

== Weiteres ==

- [[http://wiki.vorratsdatenspeicherung.de/Passenger_Name_Record|PNR-Kampagne des AK Vorrat]]
- [[<http://www.heise.de/newsticker/meldung/Heikle-Hilfestellung-zur-Weitergabe-von-Fluggastdaten-158879.html>|Heise-Newsticker:]] Heikle Hilfestellung zur Weitergabe von Fluggastdaten
- [[<http://www.heise.de/newsticker/meldung/EU-Staaten-sollen-Flugpassagierdaten-13-Jahre-lang-speichern-192244.html>|Heise-Newsticker:]] EU-Staaten sollen Flugpassagierdaten 13 Jahre lang speichern
- [[<http://www.zeit.de/reisen/2010-09/edward-hasbrouck>|Zeit-Artikel:]] „In dieser Datenbank steht, wer mit wem schläft“

Version #1

Erstellt: 2025-10-27 22:28:15 UTC von Datenschmutz Migration Bot

Zuletzt aktualisiert: 2025-10-27 22:28:15 UTC von Datenschmutz Migration Bot