EU Directive

PASSENGER NAME RECORD DATA

Status: 21 March 2011

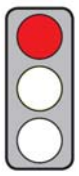
Centrum für Europäische Politik

MAIN ISSUES

Objective of the Directive: Air carriers are under obligation to transfer passenger name record data to "Passenger Information Units" in Member States, who can use this data to combat serious crime and terrorism.

Parties Affected: Air passengers, air carriers.

Pros: –



Cons: (1) The Directive is disproportionate and therefore infringes the European fundamental right to data protection (Art. 8 Charter of Fundamental Rights). It further infringes the German basic right to privacy of personal data as it constitutes a random dragnet investigation without given suspicion (Art. 2 (1) in conjunction with Art. 1 (1) German Basic Law).

(2) The benefits are negligible, as experience gained in the USA has shown.

(3) Intriguingly, according to the Commission the costs for setting up the "Passenger Information Units" are suddenly supposed to represent only a third of their own original cost estimate.

CONTENT

Title

Proposal COM(2011) 32 of 2 February 2011 for a **Directive** of the European Parliament and the Council on the **use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime**

Brief Summary

- **Background and targets**
  - The proposed collection and processing of Passenger Name Record data (PNR) serves to support criminal investigations of persons that may have committed a terrorist offence or serious crime.
  - "PNR data" of passengers travelling from or to third countries are to be collected by air carriers during the passengers' flight booking procedure and must be transferred to Member States' authorities.
  - The PNR data includes up to 19 different pieces of information which until now air carriers have collected for their own purposes, such as travel dates, billing information and addresses as well as the number and names of fellow passengers (see Annex to the Directive).
  - The Directive regulates data processing (collection, retention and analysis) through national authorities (Art. 4), the data exchange between Member States (Art. 7) and the data transfer to third countries (Art. 8).
- **Transfer of PNR data by air carriers to Passenger Information Units**
  - Member States are to set up national "Passenger Information Units" for the collection, retention and analysis of PNR data (Art. 3 (1)).
  - Air carriers must enter PNR data electronically into the database of the Passenger Information Units of those Member States in which the flight concerned will land or depart ("push" method"; Art. 6 (1)).
    - The transfer must be carried out within 24 to 48 hours before the scheduled time for departure and again immediately after boarding time (Art. 6 (2)).
    - In the case of a specific and actual threat emanating from a terrorist offence or serious crime, Passenger Information Units may request PNR data from air carriers ("pull" method", Art. 6 (4)).
  - Member States must provide for "dissuasive" penalties (incl. financial penalties) against air carriers which infringe any of their obligations regarding data transfer (Art. 10).
- **Competent authorities**
  - "Competent authorities" means all national authorities engaged in preventing, detecting, investigating and prosecuting terrorist offences and serious crimes.
  - They are entitled to request or obtain PNR data or the results of PNR data processing from Passenger Information Units in order to further assess them or take appropriate action (Art. 5 (1)).
- **Data retention, "anonymisation" and deletion**
  - Passenger Information Units retain the transmitted PNR data
    - first for a period of 30 days (Art. 9 (1)),
    - then for a further five years (Art. 9 (2)).
      - For this, they must always "anonymise" the data by separating it from any identification features. Moreover, only a "limited" number of staff may have access to the data.
      - In exceptional circumstances, the Passenger Information Unit staff may reverse the said separation in order to access the non-anonymised PNR data in full form if requested by an authority to do so in

Authors: Marcus Schwenke and Benedikt Langner | schwenke@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-105 | www.cep.eu

order to avert a specific danger or an acute threat or if this is necessary to carry out a specific investigation or prosecution.
  - Upon expiry of the period of five years and 30 days, PNR data must be deleted. Data which has been transmitted to the competent authorities is excluded from this rule (Art. 9 (3)).

- **Processing PNR data by Passenger Information Units**
  - The Passenger Information Units may use PNR data to prevent, detect, investigate and prosecute terrorist offences and serious crime as follows:
    - It may compare PNR data of passengers prior to their scheduled arrival and/or their departure against "relevant" international or national databases in order to identify suspicious persons. This must be carried out in a "non-discriminatory manner" and without using "sensitive data", e.g. race, ethnic origin or religious belief (Art. 4 (2) lit. b).
    - It may, in the case of "duly reasoned" requests, provide PNR data to competent authorities and, in specific cases also "process" data and transmit the results of such processing (Art. 4 (2) lit. c).
  - Moreover, in the case of terrorist offences and "serious transnational crime" the Passenger Information Units may use PNR data as follows:
    - They may process PNR data against "pre-determined criteria" in order to assess passengers prior to their scheduled arrival or departure (Art. 4 (2) lit. a).
    - They may analyse PNR data for the purpose of updating or creating "new criteria" to assess passengers (Art. 4 (2) lit. d).
  - The Passenger Information Units are to transfer the PNR data of the persons identified to the competent authorities for further examination on a case-by-case basis (Art. 4 (4)).
  - Member States are to ensure that each positive match resulting from such automated processing of PNR data against databases or "pre-defined criteria" is reviewed by a staff member (cp. Art. 4 (2) lit. a, b).

- **Protection of personal data**
  Member States must ensure the protection of personal data in compliance with the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2008/977/JHA). This includes, in particular, the right to rectification, erasure and blocking, the right to compensation and the right to judicial remedy.

- **Exchange of PNR data**
  - The Passenger Information Unit of a Member State may request, if necessary, "anonymised" PNR data and also the results of the processed data from Passenger Information Units of any other Member State (Art. 7 (2)).
  - In the case of a specific threat or a specific investigation, the Passenger Information Unit of any other Member State may also request the identification features in addition to "anonymised" PNR data, so that the identity of a passenger can be determined (Art. 7 (3)).
  - Member States may transfer PNR data and the results of the processing of these data to a third country on a case-by-case basis. However, in so doing the purpose of the transfer must be in line with the purpose of the Directive and the third country must ensure an "appropriate level of data security" (Art. 8).

- **Review and analysis of the Directive**
  The Commission will draw up:
  - a report on the integration of intra-European flights within 4 years following the Directive's entry into force (Art. 17 lit. a);
  - a report on the functionality of the Directive within 6 years following the Directive's entry into force (Art.17 lit. b).

Changes Compared to the Status Quo

- To date, air carriers have been obliged by international agreements to deliver PNR data to authorities in the US, Canada and Australia if passengers entered these states via the EU. In future, the Member States' authorities will also be entitled to access PNR data.
- The existing provision on the use of "advance passenger information (API)" – in particular, biographic information from the machine-readable part of passports (Directive 2004/82/EC) – remains unaffected by this proposal for a directive.

Statement on Subsidiarity by the Commission

The Commission assumes that the effective combating of terrorism and serious crime is a cross-border task. It further assumes that the different security systems of Member States constitute an obstacle for effective cooperation. Besides, strong differences in national rules might lead to unequal levels in protection as well as to safety gaps, higher costs and legal uncertainty.

Policy Context

In November 2007, the Commission submitted a Proposal for a Council Framework Decision on PNR data for law enforcement purposes in the EU [COM(2007) 654]. Although the Council working groups reached

consensus on the Proposal in 2008, the Council failed to adopt it in time before the treaty of Lisbon entered into force on 1 December 2009. Since then, the European Parliament also has a voice in this matter; the current Directive Proposal takes this into account.
Since the abolition of border controls, the EU has taken various actions to facilitate the cross-border exchange of personal data between prosecution authorities and other authorities, e.g. the Schengen Information System (SIS and SIS II).

Legislative Procedure

02 February 2011	Adoption by Commission
Open	Adoption by the European Parliament and Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Leading Directorate General:	DG Internal Affairs
Committees of the EP:	Not yet known
Committees of the German Bundestag:	Not yet known
Decision mode in the Council:	Qualified majority (approval by a majority of Member States and at least 255 out of 345 votes; Germany: 29 votes)

Formalities

Legal competence:	Art. 82 (1) lit. d and Art. 87 (2) lit. a TFEU
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Legislative procedure:	Art. 294 TFEU (ordinary legislative procedure; ex-Art. 251 TEC)

ASSESSMENT

Economic Impact Assessment

Ordoliberal Assessment

With the intended use of PNR data to combat serious crime and terrorism, the data of many respectable passengers will be subjected systematically to police investigation and retained by public authorities for more than five years. Such a massive intrusion upon the basic right to privacy of personal data therefore requires very sound substantiation.

The Commission itself, however, **admits that "detailed statistics on the extent to which such data help prevent, detect, investigate and prosecute serious crime and terrorism are not available"** [COM(2011) 32, p. 6]. According to the Commission, this is due to the fact that the EU has little experience in using PNR data. However, it – consciously (?) – ignores the existing experience gained from PNR agreements with third countries. This could be explained by the fact that this experience indicates that the impact of PNR data on successful counter-crime and counter-terrorism is insignificant: for instance, **the report of the US-Department of Homeland Security** of 5 February 2010, p. 7, **states that** under the PNR data agreement between the EU and US, **PNR data were "used" only once for a lawsuit**. The essential question of whether or not the data were decisive in the lawsuit and what its outcome was is not mentioned in the report. **Therefore, it is not justified to propose the retention and use of PNR data in the EU**.

Equally problematic is the fact that the Commission wishes to examine the extension of the Directive to intra-European flights, two years before any experience of the functionality of the Directive can even be gained. Just as incomprehensible is the fact that the Commission is considering extending the scope of the Directive to include sea and rail transport, "once we will have learned from the experiences with PNR [data]collection from air travel" [see SEC (2011) 132, p. 36]. On the one hand, this is consistent, as using PNR data exclusively for air transport might tempt potential criminals to transfer their attention to other transport modes.

However, **extending the measures to include rail transport,** as is currently under consideration, **is not practicable** due to the different utilisation characteristics: passengers tend to use trains more spontaneously and, apart from a few exceptions (Eurostar and online bookings), **railway undertakings have** normally **so far not collected PNR data**. Moreover, actual train usage is not checked compared with actual aeroplane usage. Consequently, using PNR data in rail transport would be even less significant.

The Commission must accept that there is no comprehensive protection against serious crime and terrorism. At most, this would be only possible at the price of an all-embracing police state.

Impact on Efficiency and Individual Freedom of Choice

In 2007, when the Commission presented its Framework Decision Proposal, it estimated the costs for the establishment of Passenger Information Units and communication infrastructures of all Member States at 615 million Euros [see SEC(2007) 1453, p. 28]. Within the current presentation of the latest Directive Proposal it projects costs to the amount of 221 million Euros only [see SEK(2011) 132, p. 39]. **However, the Commission fails to give any explanation as to why the costs** that Member States have to bear for **setting up these units**

have suddenly dropped to only one third of the original cost estimate. The Commission's remark that the actual costs lie "somewhere between these two assessments" is not acceptable [see SEC(2011) 132, p. 40]. Comprehensible estimates were also demanded by the Commission's internal Impact Assessment Board, IAB, when assessing an earlier version of the Impact Assessment [see IAB Statement of 10 September 2010].

Legal Assessment

Legislative Competence

The relevant legal basis is laid down in Art. 82 (1) lit. d and Art. 87 (2) lit. a TFEU.

Subsidiarity

It is not evident that action taken at EU level would generate any added value. The Commission's claim that a harmonization of national rules is necessary is unsustainable, as the United Kingdom is the only Member State with a fully established system for the processing of PNR data for prosecution or counter-terrorism and only a few further Member States are planning to introduce such a system. Therefore, the planned Directive infringes the principle of subsidiarity.

Proportionality

The Commission fails to provide any explanation as to why the proposed collection and processing of personal data is considered necessary. In particular, it **fails to give evidence** as to **why further data beyond the already raised API data must be collected** in order to combat terrorism and serious crime. The use of API data constitutes a significantly lower intrusion into the fundamental right to data protection (Art. 8 Charter of Fundamental Rights).

The proposed **retention of five years and 30 days is both too long and arbitrary**: the Commission fails to explain this duration period and, in particular, why and according to which "criteria" – justifying such a long period – the assessment of passengers in Member States is to be carried out. Besides, the retention periods for API data are only 24 hours (Directive 2004/82/EC, Art. 6 (1)), two years for data retention in telecommunications (Directive 2006/24/EC, Art. 6) and three and a half years for PNR data to be transferred to Canada.
The disproportionality of the retention periods is not redressed by the proposed separation of identity features from the remaining data, as this can be reversed during the proposed five years without any major obstacles.

Compatibility with EU Law

Any random retention and processing of PNR data without given suspicion infringes the fundamental right to data protection (Art. 8 Charter of Fundamental Rights), as the interference is disproportionate. Collecting and retaining the personal data of unsuspicious persons also infringes the principle of this fundamental right according to which data must be processed only for specified purposes (Art. 8 (2) Charter of Fundamental Rights), as most of the PNR data is retained for non-foreseeable future use.

Compatibility with German Law

The German Federal Constitutional Court (*Bundesverfassungsgericht – BverfG*) waives the exercise of its competence as long as the European Court of Justice (ECJ) guarantees the protection of fundamental rights which essentially correspond to German Basic Law ("Solange II", 2 BvR 197/83; "Lissabon", 2 BvE 2/08, 337). Therefore, in implementing the Directive, German Basic Law must be implicitly taken into account.
The data retention proposed in the Directive interferes with the basic right to privacy of personal data (Art. 2 (1) in conjunction with Art. 1 (1) German Basic Law). With regard to a random retention of personal telecommunications data without given suspicion, as prescribed by an EU Directive, the BVerfG has already determined a maximum ceiling of six months of what is deemed justifiable (1 BvR 256/08). Relevant to the court's judgement in favour of the data retention was the fact that the data is retained by service providers and not by the states itself, as proposed for PNR data.
What is also problematic is the comparison of PNR data against "criteria" still to be defined by the Passenger Information Units, which in effect constitutes a sort of "dragnet investigation". A preventative police dragnet investigation complies with the basic right to privacy of personal data only if there is at least a concrete danger for high-ranking legal interests. **As a random preventative measure without given suspicion, the dragnet investigation proposed by the Commission does not comply with the requirements of Basic Law** (BVerfG, 1 BvR 518/02).

Alternative Action

The Directive Proposal should be withdrawn. Instead, police and judicial cooperation in the EU, e.g. through the Schengen Information Systems, should be improved.

Conclusion

The Directive Proposal should not be adopted. The random retention and processing of PNR data without given suspicion infringes the fundamental right to data protection due to its inappropriateness (Art. 8 Charter of Fundamental Rights), and in the form of a random dragnet investigation it also infringes the basic right to privacy of personal data (Art. 2 (1) in conjunction with Art. 1 (1) German Basic Law). Moreover, the actual benefit for counter-crime and counter-terrorism is insignificant, as US experience has proven. Furthermore, it is not comprehensible why the costs for the new system have dropped to only a third of the original cost estimate.