P6_TA(2008)0561

EU and PNR data

European Parliament resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes

The European Parliament,

– having regard to the statement by the Commission during the debate of 21 October 2008, following the Oral Question B6-0476/2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes (COM(2007)0654),

– having regard to the current debates in the Council at ministerial and working group levels on the above-mentioned proposal,

– having regard to the opinions delivered by the Fundamental Rights Agency, the European Data Protection Supervisor, the Article 29 Working Party and the Working Party on Police and Justice,

– having regard to its previous resolutions[1] on the EU-US PNR agreement[2], the EU-Canada PNR agreement[3] and the EU-Australia PNR agreement[4],

– having regard to Rule 108(5) of its Rules of Procedure,

A. whereas the data protection principles to be respected by the EU institutions and Member States are outlined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Articles 7 and 52 of the Charter of Fundamental Rights of the European Union (the Charter of Fundamental Rights), Article 286 of the EC Treaty, Article 5 of Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and, at secondary level, Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] and the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters),

B. whereas any new EU legislation should comply with the proportionality and subsidiarity principles, as outlined in Article 5 of the EC Treaty and Protocol 30 thereto,

On procedural aspects

---

1 OJ C 61 E, 10.3.2004, p. 381; OJ C 81 E, 31.3.2004, p. 105; OJ C 103 E, 29.4.2004, p. 665; OJ C 157 E, 6.7.2006, p. 464; OJ C 305 E, 14.12.2006, p. 250; OJ C 287 E, 29.11.2007, p. 349; OJ C 175 E, 10.7.2008, p. 564; Texts adopted, 22.10.2008, P6_TA(2008)0512.

2 OJ L 204, 4.8.2007, p. 18.

3 OJ L 82, 21.3.2006, p. 15.

4 OJ L 213, 8.8.2008, p. 49.

5 OJ L 281, 23.11.1995, p. 31.

1. Acknowledges the need for stronger cooperation at European level and internationally in the fight against terrorism and serious crime; recognises that the collection and processing of data can be a valuable tool for law enforcement purposes;

2. Takes the view that law enforcement authorities should be provided with all the tools they need to adequately carry out their tasks, including access to data; emphasises, however, that since such measures have a considerable impact on the personal life of Union citizens, their justification in terms of necessity, proportionality and usefulness in achieving their stated objectives needs to be convincingly substantiated, and stresses that effective safeguards for privacy and legal protection must be put in place; believes that this is a precondition for lending the necessary political legitimacy to a measure which citizens may view as an inappropriate intrusion into their privacy;

3. Regrets that the formulation and justification of the Commission's proposal have left so many legal uncertainties with respect to compatibility with the ECHR and the Charter of Fundamental Rights, as well as its legal basis, which has raised questions as to the appropriate role for Parliament in the legislative procedure; notes that the same concerns regarding the proposal's lack of legal certainty:

   – are raised in the opinions delivered by the Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS) , the Article 29 Working Party and the Working Party on Police and Justice;

   – require the Council to undertake a substantial review of the possible scope and impact of a future EU initiative in this domain, and incorporate significant amounts of additional information, including the above-mentioned opinions;

4. Considers that under these conditions Parliament must reserve its formal opinion under the formal consultation procedure until the concerns raised in this resolution are properly addressed and the minimum information necessary is provided;

5. Maintains its strong reservations as to the necessity for and added value of the proposal for the establishment of an EU PNR scheme and the safeguards which it contains, notwithstanding the explanations and points of clarification given by the Commission and the Council so far, both orally and in writing; observes, furthermore, that many of the questions raised by Parliament, the Article 29 Working Party, the Working Party on Police and Justice, EDPS and the FRA have not been satisfactorily answered;

6. Shares the FRA's view that the mere availability of commercial databases does not automatically justify their use for law enforcement purposes; moreover, the same or even better results could be obtained by improving mutual legal assistance between law enforcement authorities;

7. Invites the Council, if it intends to continue the examination of the Commission text, to take into account the recommendations in this resolution and to duly justify the conditions of pressing social need which could make this new EU intervention 'necessary', as required under Article 8 of the ECHR; considers these to be the minimum conditions of support for the introduction of an EU PNR scheme; is ready to contribute and participate in this work at all levels;

8. Reiterates its calls for clarification of the relationship between the use of PNR and other

measures such as Council Directive 2004/82/EC[1] of 29 April 2004 on the obligation of carriers to communicate passenger data, the proposed Entry-Exit scheme, the Electronic System for Travel Authorisation, biometrics in passports and visas, SIS, VIS, Regulation (EC) No 2320/2002[2] of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security, and national border protection schemes; notes with regret that the implementation of some of these measures has been considerably delayed and considers that a full and systematic evaluation of the current EU and Schengen security cooperation mechanisms and tools aimed at ensuring aviation security, protecting external borders and fighting terrorism could help in assessing the added value of the proposed EU PNR scheme;

9. Recalls that the debate on the appropriate legal basis for the proposal is continuing and reiterates that, according to Article 47 of the EU Treaty, legislative measures within the framework of judicial and police cooperation should be accompanied by the necessary accompanying Community measures to be adopted in codecision with Parliament on all first-pillar aspects, particularly those defining the scope of the obligations to be fulfilled by economic operators[3];

10. Recalls that the Court of Justice of the European Communities has already challenged the EU-US PNR Agreement on the grounds that its legal basis is wrong; calls therefore on the Commission to examine carefully which legal basis is appropriate;

11. Considers that, in connection with the tabling of the new legislation, national parliaments must be fully involved in the legislative process, given the impact of the proposal on both citizens and the national legal orders of the Member States;

12. Stresses that possible future legislation establishing an EU PNR scheme as a new framework for EU police cooperation should contain provisions for periodic evaluation of its implementation, application, usefulness and breaches of safeguards; considers that national parliaments, the EDPS, the Article 29 Working Party and the FRA should be invited to play a role in both review and evaluation; considers, therefore, that the new legislation should include a sunset clause;

13. Emphasises, in this context, that each Member State bears the initial responsibility for the collection of PNR data and their protection; stresses that safeguards are mandatory when PNR data are transmitted, exchanged or transferred to or between other Member States; takes the view, therefore, that access to PNR data exchanged between Member States should be strictly limited only to those authorities that deal with counter-terrorism and organised crime; considers that other law enforcement agencies may be granted access subject to judicial approval;

Subsidiarity

14. Notes with concern that the need for Community action has not yet been sufficiently demonstrated; in this connection, questions the claim by the Commission that the stated aim

---

[1] OJ L 261, 6.8.2004, p. 24.

[2] OJ L 355, 30.12.2002, p. 1.

[3] See, in particular, the Council Legal Service opinion on this subject and the Opinion of the Advocate General delivered on 14 October 2008 on Case C-301/06, Ireland v European Parliament and Council of the European Union on the Data Retention Directive 2006/24/EC.

of the proposal is harmonisation of national schemes, when only a few Member States have a system for the use of PNR data for law enforcement and other purposes, or plans for such a scheme; considers, therefore, that the Commission's proposal does not harmonise national systems (as they are non-existent), but merely creates the obligation for all Member States to set up such a system;

15. Notes that the Commission is proposing a 'decentralised' scheme, which means that the European added value is even less clear;

Proportionality

16. Recalls that Article 8 of the ECHR and Article 52 of the Charter of Fundamental Rights require that such a massive infringement of the right to the protection of personal data be legitimate and justified by a pressing social need, provided for by law and proportionate to the end pursued, which must be necessary and legitimate in a democratic society; in this connection, deplores the fact that the purpose of this envisaged police cooperation measure is not limited to issues such as combating terrorism and organised crime;

17. Is concerned that, in essence, the proposal gives law enforcement authorities access to all data without a warrant; points out that the Commission has not demonstrated the need for new law enforcement powers, or that this goal cannot be achieved with less far reaching measures; criticises the fact that there is no information as to how existing law enforcement powers fall short of what is needed, and where and when the authorities have demonstrably lacked the powers they needed for the stated purpose; requests that a review of the existing measures mentioned below take place before an EU PNR system is further developed;

18. Notes the Commission's claim that 'the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes', but stresses that to date there is no evidence to substantiate this claim, given that:

– any information so far provided by the US is anecdotal and the US have never conclusively proven that the massive and systematic use of PNR data is necessary in the fight against terrorism and serious crime,

– there has only been one joint review of the US-EU PNR Agreement, which assessed only the implementation, not the results,

– the preliminary conclusions from the UK system for the use of PNR data refer to law enforcement purposes other than counterterrorism, which fall outside the scope of the Commission’s proposal, and to the use of PNR on a case-by-case basis in the context of ongoing investigations, on the basis of a warrant and with due cause; so far they provide no evidence of the usefulness of the mass collection and use of PNR data for counterterrorism purposes;

Purpose limitation

19. Stresses that the principle of purpose limitation is one of the basic principles of data protection; points out, in particular, that Convention 108 states that personal data shall be ‘stored for specified and legitimate purposes and not used in a way incompatible with those purposes’ (Article 5(b)); notes also that derogations from this principle are allowed only insofar as they are provided for by law and constitute a necessary measure in a democratic

society in the interests of, inter alia, the ‘suppression of criminal offences’ (Article 9); points out that the case-law of the European Court of Human Rights has made clear that these derogations must be proportionate, precise and foreseeable, pursuant to Article 8(2) of the ECHR;

20. Deplores the lack of precise purpose limitation which is an essential safeguard in the imposition of restrictive measures, and considers that such protection is even more important as regards secret surveillance measures, given the heightened risk of arbitrariness in such circumstances; considers that, as the stated purposes and definitions are imprecise and open-ended, they should be strictly specified to avoid exposing the EU PNR scheme to legal challenge;

21. Reiterates that PNR data may be very useful as supportive, additional evidence in a specific investigation into known terrorism suspects and associates; points out, however, that there is no evidence that PNR data are useful for massive automated searches and analyses on the basis of risk criteria or patterns (i.e. profiling or data mining) in seeking potential terrorists[1];

22. Stresses, furthermore, that EU data protection rules place restrictions on the use of profiling on the basis of personal data (Article 8 of the Charter of Fundamental Rights and the ECHR); concurs, therefore, with the FRA's opinion that profiling based on PNR data should only be intelligence-led, based on individual cases and factual parameters;

23. Reiterates its concerns regarding the measures outlining an indiscriminate use of PNR data for profiling and for the definition of risk assessment parameters; recalls that any kind of profiling based on ethnicity, nationality, religion, sexual orientation, gender, age or medical condition should be expressly banned as incompatible with the prohibition of any discrimination as defined in the Treaties and in the Charter of Fundamental Rights;

24. Recalls that, in the event of any extension of the proposal's scope, the Commission and the Council should clarify in detail for each stated purpose what use will be made of the PNR data and why existing law enforcement powers are not sufficient; considers that, for each specific purpose, the appropriate legal basis must be established;

Protection of personal data

25. Stresses that the adoption of an adequate data protection framework under the third pillar is an absolute precondition for any EU PNR scheme, as are specific rules for the transfer and use of PNR data that are not covered by the EU data protection framework under the first and third pillars; stresses the need to clarify which data protection rules apply to Passenger Information Units (PIUs) and to ensure the traceability of all access, transfer and use of PNR data;

26. Emphasises that sensitive data may be used only on a case-by-case basis in the context of a regular investigation or prosecution, obtained under a warrant; notes the concern of airlines that sensitive data cannot be filtered from general remarks; calls, therefore, for the

---

[1] CRS report for the American Congress 'Data Mining and Homeland Security: An Overview' by Jeffrey Seifert; 'Effective counter-terrorism and the limited role of predicative data mining' by CATO Institute; 'Protecting individual privacy in the struggle against terrorists: a framework for program assessment'; 'No dream ticket to security' by Frank Kuipers, Clingendael Institute, August 2008.

definition of strict conditions for the processing of these data by PIUs, as defined by the FRA in its opinion;

Details of implementation

27. Stresses that, as regards storage periods, the Commission fails to justify the proposed retention period; considers, however, that for the purpose of developing risk indicators and establishing patterns of travel and behaviour, anonymised data should be sufficient; considers also that, if the scope of the PNR scheme is extended, retention periods must be justified for each separate purpose;

28. Reiterates that data transfers should be made using the PUSH method alone and that third countries should not have direct access to PNR data in EU reservation systems;

29. Welcomes the fact that, as regards access to PNR data, the proposal states that all entities having access to PNR data should be named in an exhaustive list;

30. Stresses, as regards transfers to third countries, that data may not be transferred to third countries unless an adequate level of protection (as specified in Directive 95/46/EC and the legal instruments establishing Europol and Eurojust) or appropriate safeguards are provided by the third countries concerned (in accordance with Convention 108), and that transfers should be made only on a case-by-case basis;

31. Reiterates that passengers must be informed in full and in an accessible manner of the details of the scheme and of their rights, and that Member State authorities are responsible for providing this information; suggests that the example of the 'denied boarding' information in airports should be used; considers it essential to define a right of access, rectification and appeal for passengers;

32. Requests that detailed and harmonised rules be laid down on the security of PNR data, in terms of both IT solutions and authorisation and access rules;

Consequences for carriers

33 Notes that air carriers collect PNR data for commercial purposes and that data are not systematically collected to complete all PNR fields; insists that airlines should not be required to collect any data additional to those which they are collecting for their commercial purposes; considers that air carriers should not be made responsible for verifying whether records are complete and accurate, nor should any sanctions be applied in respect of incomplete or incorrect data; calls for a clear evaluation of the costs involved in an EU PNR scheme; considers that any additional costs should be borne by the requesting parties;

Intermediaries/ Passenger Information Units (PIUs)

34. Calls for a clear definition of the role and powers of the PIUs, in particular in terms of transparency and democratic accountability and in order to lay down appropriate data protection rules; requests that the role of PIUs be limited to the transfer of data to competent authorities, in order to ensure that risk assessments may only be carried out by competent authorities and in the context of an inquiry; asks for clarification of the law which will govern the risk assessment conducted by the PIUs, and the responsibility of data protection

authorities in cases where Member States cooperate to set up a joint PIU;

°

° °

35. Instructs its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States, the European Data Protection Supervisor, the Fundamental Rights Agency, the Article 29 Working Party and the Working Party on Police and Justice.