



**00664/11/EN
WP 181**

Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Adopted on 5 April 2011

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

The Working Party on the protection of individuals with regards to the processing of personal data

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, having regard to its Rules of Procedure,

has adopted the following opinion.

1. Introduction

On 2 February 2011 the European Commission published its proposal for a Directive on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The Working Party provided an opinion on the previous EU PNR proposal (Proposal for a Council Framework Decision on the use of passenger name records (PNR) for law enforcement purposes), presented by the Commission on 6 November 2007¹. The Working Party has also previously commented extensively in several opinions on the various PNR agreements in place between the EU and third countries, and on the Commission's approach as set out in their communication of 21 September 2010². In addition, the Working Party has reiterated its concerns regarding PNR issues in various letters to Commissioner Barrot, Commissioner Malmström, Director General Faull, and the LIBE Committee of the European Parliament.

This opinion is directed at those involved in the discussion and development of the latest proposal, namely the Commission, the GENVAL Council working group and the European Parliament.

2. Necessity and proportionality

The 2011 proposal is accompanied by an impact assessment which aims to set out in more detail the rationale behind the proposal and its provisions. The Working Party considers that the fight against terrorism and organised crime is necessary and legitimate and personal data, and in particular some passenger data, might be valuable in assessing risks and preventing and combating terrorism and organised crime. However, in the case of a European PNR system the limitation of fundamental rights and freedoms has to be well justified and its necessity clearly demonstrated so as to be able to strike the right balance between demands for the protection of public security and the restriction of privacy rights.

The Working Party has consistently questioned the necessity and proportionality of PNR systems and continues to do so with the 2011 proposal. While we appreciate the extra detail provided in the impact assessment, we consider that it does not provide a proper evaluation of the use of PNR and does not demonstrate the necessity of what is being proposed. The proposal should be clear about whether the aim is to fight serious (transnational) crime, which includes terrorism; or whether the aim is to fight terrorism and terrorism-related crimes only.

¹ WP 145 – joint opinion with the Working Party on Police and Justice.

² Opinions WP 103 (Canada); WP 138 (US); WP 151 (US - information to passengers); and WP 178 (Commission global approach).

Chapter 3.2 of the impact assessment “Respect of fundamental rights” merely states that the Fundamental Rights Check List has been used, but there is no further information about this assessment to justify its conclusions. In addition, this chapter provides circular reasoning for the interference with privacy rights under Article 8 of the European Convention of Human Rights, and Articles 7 and 8 of the Charter on Fundamental Rights of the European Union. The legal precondition for interfering with these rights is that it is “necessary in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others” as well as being “necessary in a democratic society” and “subject to the principle of proportionality”. The fact that the purpose of the proposal is the prevention of terrorism and serious crime does not mean it clearly complies with these requirements; the necessity and proportionality have still to be proven. The Commission’s own overview of information management systems³ states:

“Necessity

Interference by a public authority with individuals’ right to privacy may be necessary in the interest of national security, public safety or the prevention of crime. The jurisprudence of the European Court of Human Rights establishes three conditions under which such restrictions may be justified: if it is lawful, if it pursues a legitimate aim and if it is necessary in a democratic society. Interference with the right to privacy is considered necessary if it answers a pressing social need, if it is proportionate to the aim pursued and if the reasons put forward by the public authority to justify it are relevant and sufficient. In all future policy proposals, the Commission will assess the initiative’s expected impact on individuals’ right to privacy and personal data protection and set out why such an impact is necessary and why the proposed solution is proportionate to the legitimate aim of maintaining internal security within the European Union, preventing crime or managing migration.”

The Working Party does not consider that the Commission has fulfilled the commitments made above in relation to the EU PNR proposal. There are several other aspects to the necessity and proportionality arguments and these are also considered below.

2.1. Enhanced security

The proposal and impact assessment state that an EU PNR system would ensure security and prevent gaps caused by the abolition of internal border controls under the Schengen Convention. This would be a legitimate aim if properly justified, however, the Working Party has yet to see any satisfactory evidence that processing PNR data in all Member States would prevent security gaps arising from processing this data in only a few Member States.

There are systems and tools already in place at EU level to compensate for the abolition of border controls between Schengen countries, building on the so-called Schengen acquis, so if there are still security gaps then the first step should be to analyse the proper functioning of the existing systems.

³ Overview of information management in the area of freedom, security and justice, COM(2010)385 final.

2.2. Existing systems, tools and co-operation

The Commission's overview of information management in the area of freedom, security and justice did not evaluate the effectiveness of the various existing systems, nor did it consider whether taken together they provide the appropriate tools to fight terrorism and organised crime and, if not, where the gaps may be. The Working Party considers that such an evaluation is necessary before imposing further, similar measures, such as an EU PNR system. The PNR proposal will lead to overlapping obligations on carriers, collection of data already available through other systems, and presents a serious risk of function creep. For example, the API Directive obliges carriers to communicate passenger information in advance, and use of the data is not limited to border checks but can also be used for law enforcement activities. Despite raising the issue with the Commission several times, the Working Party has yet to see a proper evaluation of the effectiveness of the API Directive and its national implementation, and questions the continuing need for it if an EU-wide PNR system is introduced.

The Working Party questions whether all the forms of police and judicial co-operation in place in the EU aimed at preventing and prosecuting crime, which include the fight against terrorism and serious crime, do not represent adequate tools for the purpose for which the EU PNR proposal is intended to fulfill. The impact assessment does not carry out this analysis.

The Working Party acknowledges that some non-Schengen Member States cannot benefit from some of the tools and systems in place, which may have an impact on the necessity test for these countries. However, those Member States can and do apply the API Directive and it should be considered whether improved use of existing systems and improved co-operation between these Member States and others might in fact provide the necessary information for the relevant purposes. It should also be noted that the fact that PNR data would be used as an intelligence tool, as mentioned in the impact assessment, also raises the level of requirements with regard to data protection safeguards.

2.3. Proportionality

Under the proposal, a huge amount of personal information on all passengers flying into and out of the EU will be collected, regardless of whether or not they are suspects. Collecting and processing PNR data for the fight against terrorism and serious crime should not enable mass tracking and surveillance of all travellers. The Working Party considers it disproportionate and therefore not in line with Article 8 of the Charter of Fundamental Rights to collect and retain all data on all travellers on all flights. As previously mentioned above, the impact assessment does not include convincing evidence in this respect. EU-level proposals should be specific and targeted to address a particular issue and in this context the focus of any proposal should be on the risks posed by terrorism and serious crime.

The Working Party has serious doubts about the proportionality of the systematic matching of all passengers against some pre-determined criteria and unspecified "relevant databases". It is not clear how these pre-determined criteria and relevant databases are to be defined, whether PNR data will be used to create or update the criteria, and to what extent all matches will automatically become subject to additional investigations. The Working Party would also like to recall that in some Member States similar methods of policing are only constitutional and therefore available to the police on judicial approval and under specific circumstances, such

as a specific threat. The proposed PNR system would render this exceptional method an ordinary instrument for police work.

Measures put in place that cannot provide for the protection of the rights and freedoms of travellers are only proportionate when introduced as a temporary measure for a specific threat, which is not the case for this proposal. The invasion of privacy of travellers must be proportionate to the benefits as regards fighting terrorism and serious crime. The Working Party has yet to see any statistics showing the ratio between the number of innocent travellers whose PNR data was collected to the number of law enforcement outcomes resulting from that PNR data.

In summary, the Working Party still considers that the necessity of the system has not been proven, and that the measures proposed are not in line with the proportionality principle. Despite this, the Working Party considers it constructive to also comment on other aspects of the proposed Directive, as set out below.

3. Purposes

The proposed Directive sets out two general purposes for processing with four specific activities specified. PNR data can only be processed for the purposes of:

- preventing, detecting, investigating and prosecuting terrorist offences and serious crime by assessing passengers before arrival or departure by comparing against relevant databases (purpose 1, activity 1) and by responding to requests from competent authorities in specific cases (purpose 1, activity 2); and
- preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime by assessing passengers before arrival or departure against specified criteria (purpose 2, activity 3) and by analysing PNR data to update or create new criteria (purpose 2, activity 4).

It is not clear what these purposes mean in practice. Purpose 1, activity 1 appears to mean matching against watchlists, SIS or other EU and national level databases. Purpose 1, activity 2 appears to mean sharing information on a case-by-case basis following a specific request. Purpose 2, activity 3 appears to mean comparing PNR data against profiles for specific crimes; and purpose 2, activity 4 appears to mean using PNR data to develop these profiles.

It is a core data protection principle that the purposes and activities are strictly defined. The “relevant databases” should also be more specifically defined, perhaps by also adding these to the list of competent authorities that each Member State would be required to provide to the Commission. In any event, the databases used should be those set up for the same purposes, namely preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Furthermore, the implementing legislation must be clear as regards the restrictions on the use of these databases. The Working Party also recalls the importance of making sure any assessment criteria used by Member States to analyse data are specific, necessary, justified and regularly reviewed.

3.1. Definitions

The proposal defines ‘terrorist offences’ as the offences under national law referred to in articles 1 to 4 of Framework Decision 2002/475/JHA. ‘Serious crime’ and ‘serious transnational crime’ are defined as offences under national law referred to in article 2(2) of Framework Decision 2002/584/JHA. The Working Party highlights the importance of concrete definitions in this field, however, the definition of serious crime is quite wide and we question the necessity and proportionality of using PNR data for some of these crimes.

In relation to this, recital 12 of the proposal states that Member States can exclude minor offences if this would not be proportionate, but it is a choice for each Member State to make. This is likely to lead to a situation where offences are included in one Member State and not in another. It is not clear who makes the decision on proportionality and whether this decision is to be reported to the Commission, who could have a role in ensuring consistency and correct application of the proportionality principle.

The Working Party’s concerns over the potential wide scope of the definition of serious crime are also relevant for the proposed Directive’s provisions on sharing data with other authorities both within and outside the EU.

4. Retention

The retention periods proposed are clearly reduced as compared to the previous proposal and the various EU-level PNR agreements. However, the Working Party still views the proposal to retain data, even if masked, for five years as disproportionate. It has always been a longstanding concern with PNR systems that all data on all travellers are kept for the same period of time; and that this retention period is itself disproportionate. The Working Party has not seen satisfactory evidence that the data on all travellers needs to be retained; and that it needs to be retained for five years.

4.1. Masking of data

While the proposal states that data will be masked after 30 days and, generally, only accessible to certain staff at the PIU whose role is to develop profiles and travel patterns, full access to all data would remain possible for the full retention period. Even though masking is an attempt at data minimisation and access control, which are important data protection principles, the Working Party still questions why all data on all travellers is needed, and considers that the data of non-suspect travellers should be deleted.

Should the legislator decide to retain the data for a limited period of time, the data should be protected in such a way that the identifying particulars are not revealed. This protection should take place at the latest on the arrival of the flight. Access to the protected data to retrieve identifying particulars should be subject to a judicial decision on a case-by-case basis for specific criminal investigations.

The Working Party would also like to strongly stress the need for accurate language that does not confuse and mislead. The proposal mentions both masking and anonymisation. These are not the same and it is clear that masking is what is intended, not anonymisation, as the identifying data of an individual can still be easily retrieved. The proposal should not deliberately or otherwise confuse and mislead, nor promise what it cannot possibly deliver.

5. Individual data protection rights

The proposal contains provisions specifically relating to data protection. The Working Party considers it necessary that any EU-level proposal impacting on the rights and freedoms of individuals contains provisions relating to individual rights of access, correction, compensation and judicial redress. However, the rights in this proposal are those of Framework Decision 2008/977/JHA, not Directive 95/46/EC. As a result, the rights are more limited. It is not clear if the rights only apply to data transferred to another authority, or include the data held by the national authority. In some Member States currently using PNR data, individuals have access, correction and redress rights under national law that implements Directive 95/46; these rights will be reduced if the PNR Directive proposal is brought into force.

There is also the risk of discrimination as a result of the profiling activity as this system targets airline passengers as a group. There is no information given to passengers about the criteria they are being assessed against and this impacts on the exercise of rights for those directly affected by profiling activity.

The Working Party recalls the importance of including appropriate data protection measures and safeguards in EU-level proposals impacting the rights and freedoms of individuals, such as rules on confidentiality and security processing; obligations to inform individuals; prohibitions on transfers of data to private parties; and that decisions should not be made on the basis of automated processing alone. The Working Party also highlights the importance of including national supervisory authorities who have a role at national level as regards the implementation of EU-level legislation.

With regard to sensitive data, the proposal states that the filtering and deletion of this data should be done by the PIU. In its opinions on the various EU PNR agreements with third countries, the Working Party has always supported the prohibition on processing sensitive data in this context, and strongly reiterates its long-held view that the filtering process should be done by the carrier before data is pushed to the receiving authority.

The Working Party highlights the importance of making sure EU-level proposals impacting the rights and freedoms of individuals include monitoring and review requirements, such as logging processing and data requests to allow verification of the lawfulness of processing, self-monitoring, and ensuring proper data integrity and security by national data protection authorities. However, it is important to understand how such systems will work in practice and how effective logging and documentation will comply with the principles of data minimisation as mentioned above.

6. Data elements

Unlike API data, PNR data are not verified and are therefore more unreliable. The data elements listed as an annex in this proposal are the same 19 elements as in the EU-US and EU-Canada PNR agreements. The Working Party reiterates its position that there is no satisfactory evidence to suggest which fields have proved necessary, so such a list is disproportionate. The categories are general and several include further subsets of data. Even with a prohibition on processing sensitive personal data, the list of data elements includes the field 'general remarks' which could contain all kinds of information, such as meal requests, special service requests and so on. The Working Party has not yet seen satisfactory evidence

showing which PNR data elements have proved necessary or been successfully used for law enforcement outcomes. In addition, not all carriers collect PNR data.

7. Competent authorities and onward transfers

The proposal states that Member States have to notify the list of its competent authorities to the Commission within 12 months of the Directive coming into force, and this list will be published in the Official Journal. The Working Party supports transparency measures which give a clear view of who is entitled to receive and process data. However, the roles (controller/processor) of the competent authorities and PIUs are not clear.

The Working Party reiterates its concerns on the wide definition of serious crime in particular in relation to onward transfers, both within and outside the EU.

8. Review and reciprocity

According to the proposal, the Directive will be reviewed within four years of it coming into force. A special review will take place within two years of the Directive coming into force into extending the scope to cover intra-EU flights. The Working Party stresses the need for EU legislative review processes to contain clear criteria against which a review can assess the necessity and effectiveness of a system. The Working Party also reiterates the importance of including national data protection authorities in any review process, especially as this is provided for under other EU-level instruments, such as the EU PNR agreements with third countries.

In developing EU proposals, the Working Party underlines the importance of considering the implications of potential reciprocity requirements. A European PNR model could result in similar requirements being raised reciprocally by non-democratic countries or countries that do not provide an adequate level of protection of fundamental rights and freedoms, including personal data and privacy. It is clear that there could be serious consequences for individuals should such countries receive EU PNR data.

9. Conclusion

The Working Party considers that the necessity of an EU PNR system has not yet been proven and the measures proposed are not in line with proportionality principle, in particular as the system envisages the collection and retention of all data on all travellers on all flights. The Working Party also has serious doubts about the proportionality of systematic matching of all passengers against pre-determined criteria

The Working Party recommends first evaluating the existing systems and methods of co-operation and how they fit together to identify security gaps. If any exist, then the next step should be to analyse the best way to fill these gaps, which does not necessarily mean introducing a whole new system. The existing mechanisms could be further exploited and improved.

If this proposed Directive comes into force it should ensure appropriate and adequate data protection measures and safeguards. The Commission should also consider whether any existing systems could be repealed as a result, such as the API Directive, to avoid overlapping measures.

The Working Party will continue to follow the developments closely and welcomes any opportunity to present and further develop their views to the various parties involved in this proposal. The Working Party will also continue to provide opinions as appropriate and necessary.

Done at Brussels, on 5 April 2011

*For the Working Party
The Chairman
Jacob KOHNSTAMM*