ARTICLE 29 DATA PROTECTION WORKING PARTY

622/10/EN
WP 178

Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries

Adopted on 12 November 2010

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD 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 21 September 2010 the European Commission presented its Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries. The Commission considers that the use of PNR data for law enforcement purposes is growing and is increasingly seen as a mainstream and necessary aspect of law enforcement work. Therefore, the Commission has decided to establish a set of general criteria which should be applied to all future PNR agreements with third countries. The Communication furthermore contains an analysis of the current use of PNR and gives an indication of the Commission's plans on which agreements with third countries are to be concluded in the following years.

As more and more countries are requesting PNR, the number of agreements is likely to rise as well. The Commission has decided it is therefore desirable to define a framework which will be applicable to all future PNR agreements, in order to avoid legal uncertainty for both airlines and member states as well as unnecessary administrative burdens caused by the need to comply with different sets of rules for the various third countries. The Article 29 Working Party welcomes the global approach taken by the Commission to deal with requests at an EU level and to ensure strong data protection standards in full respect of fundamental rights.

The Working Party wishes to stress that the exchange of PNR data should not be considered in isolation. Therefore, the global approach should be extended to third country requests for all passenger data, including API data, watchlist matching and other prescreening activities. This should also mean that the Commission should decide upon receipt of a request for passenger data whether and which kind of data, for example API data, would be sufficient and conclude an agreement to that effect.

As far as PNR data are concerned, the Working Party closely followed the negotiations that led to PNR agreements with the US, Canada and Australia, and it has issued a number of opinions identifying privacy issues related to these PNR systems. Up to now, many of the objections raised by the Working Party have not been met. The current Communication, however, is a step in the right direction, although several concerns remain.

II. NECESSITY OF THE USE OF PNR DATA

The Working Party has always supported the fight against international terrorism and serious transnational crime. It considers this fight necessary and legitimate. It acknowledges that personal data can be valuable under certain circumstances, but is of the view that the collection and processing of all passenger data may not be able to defeat this phenomenon and that all other available means, preferably with a less intrusive effect on innocent travellers, should be exploited as well to increase security and ensure safe and efficient air travel. It should be stressed that airlines collect and use passenger data for their own business purposes. To enable the use of these data for another purpose, i.e. the use for law enforcement purposes, calls for a balanced approach between demands for the protection of public safety and other public interests, such as the fundamental rights of individuals.

In the current Communication, the European Commission merely states that PNR are an *increasingly accepted tool*, necessary in the fight against terrorism and serious crime, without substantiating this statement. The Commission does not seem to make a distinction between the increasing use of PNR data and the increasing acceptance of the use of these data. It may be the case that the law enforcement authorities have indeed become used to having PNR data at their disposal, but that fact alone does not prove political or public acceptance of the collection and use of PNR data, nor does it justify its necessity.

The three arguments given in paragraph 2.2 of the Communication seem to indicate that: "it is nice for the law enforcement authorities to have PNR data" rather than "the law enforcement authorities need to have PNR data to combat terrorism and serious crime". The Working Party also regrets the Commission has not felt the need to further elaborate on the effectiveness of the use of PNR data, which is an essential element when judging necessity.

In its previous opinions, the Working Party has time and again stressed the importance of striking the right balance. So far, this has not been the case. Most importantly, there are no objective statistics or evidence which clearly show the value of PNR data in the international fight against terrorism and serious transnational crime. This makes it impossible to clearly assess the necessity or the proportionality of the use of PNR for law enforcement purposes.

According to the Working Party, any PNR system should be:

- demonstrably necessary to address the problem;
- demonstrably likely to address the problem;
- proportionate to the security benefit;
- demonstrably less invasive than alternative measures; and
- regularly reviewed to ensure the measures are still proportionate[1].

These requirements can be elaborated as follows. The necessity of the analysis of passengers' travel patterns must be established, considering the concrete and specific purpose envisaged. As an illustration: Fighting terrorism will not necessarily require the same data and will not result in the same balance of rights and interests as, for example, the fight against drug smuggling. It shall be recalled that PNR data were originally collected after the events of 11 September 2001, in view of an extraordinary threat. The context is now shifting to general processing for various purposes sometimes with no link with the original justification.

[1] Opinion of 5 December 2007 of the Working Party on a European PNR system.
See also the Resolution of the 29th International Conference of Data Protection and Privacy Commissioners, Montreal, 28 September 2007.

A detailed analysis of the efficiency of existing databases and exchanges of information already taking place[2] should be conducted before any new PNR agreements are considered or new PNR systems are developed.

The Working Party reiterates that to meet the requirement of necessity API data could in many cases be sufficient to meet the request of a third country for passenger data. Being based on exact identification information rather than on travel intentions, the adequacy and proportionality of data processed would be easier to establish. The Working Party furthermore calls for clearly defined purposes for the use of API and PNR systems by law enforcement authorities, to make the effectiveness of these systems truly measurable.

There are currently many systems and mechanisms in place for requesting or requiring passenger data, including the bilateral agreements between member states and the US. The Commission should evaluate whether the request for passenger data from third countries could be satisfied through these existing systems and mechanisms, before entering into new agreements.

The proportionality of the system must be evaluated taking into account the impact of the means used (for example analysis of patterns and risk assessment) on the fundamental rights of individuals. Alternative options must be carefully considered before establishing such a system, in view of the intrusive character of decisions taken, at least for a large part, in an automated way on the basis of standard patterns, and in light of the difficulties for individuals to object to such decisions. The Working Party therefore would welcome a proper fundamental rights impact assessment to be carried out for all future PNR-related legislative proposals of the European Commission.

The usefulness of large-scale profiling on the basis of passenger data must be questioned thoroughly, based on both scientific elements and recent studies. Up to now the Working Party has not seen any information confirming the usefulness of such profiling. On the contrary, recent studies tend to establish the counter-productive character of such screening, especially in relation to the fight against terrorism.[3]

---

2 For example multilateral or bilateral agreements between member states and third countries. Also, see within the EU the regulations on VIS and on SIS and on external exchanges the agreements with third countries, especially the Agreement on mutual legal assistance between the European Union and the United States of America, the Agreement between the USA and the European Police Office of 6 December 2001 and the Agreement Eurojust-USA of 6 November 2006.

3 Harvard Civil Rights- Civil Liberties Review, “Government Data Mining, the Need for a Legal Framework”, by Fred H. Cate, page 468: “Mounting evidence suggests that data mining is not likely to be effective for many of the purposes for which the government seeks to use it, especially in the national security and law enforcement arenas. Not only have government officials failed to identify any successful efforts to detect or even top prevent terrorist activity based on the analysis of databases, there are significant obstacles to such efforts succeeding. These include the impediments presented by data quality issues, difficulties with data matching and limits in data mining tools, especially when data mining in the national security setting is contrasted with data mining for commercial target marketing”.
And page 475: “If a data mining system intended to keep potential terrorists off of airplanes yielded a positive rate of only one percent – a far better rate than that achieved by publicly disclosed government or commercial data mining – that would still mean that 7.4 million travellers (one percent of the 739 million passengers that the US TSA screened in 2005) would have wrongly been identified as terrorist suspects”.
See also Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining", Policy Analysis, 11 December 2006, pp. 8 and 9: "Unlike consumers’ shopping habits and financial fraud, terrorism does not occur with enough frequency to enable the creation of valid predictive models. (...) Without well-constructed algorithms based on extensive historical patterns, predictive data mining for terrorism will fail. The result would be to flood the national security system with false positives—suspects who are truly innocent".

Finally, with regard to the technical network of airlines or of computer reservation systems, the adaptation of the infrastructure to comply more easily with law enforcement requests raises serious privacy issues: no redefinition of the system should take place at a preliminary stage for purposes that have in principle no link with the primary commercial activities. On the contrary, such infrastructure should be designed to meet the industry's needs, and not law enforcement purposes. In line with industry needs, the system design should incorporate privacy enhancing technologies, in particular to prevent unauthorised access and to protect the integrity of the personal data.

III. STANDARDS, CONTENT AND CRITERIA

The Working Party welcomes the general standards set out in paragraph 3.3 of the Communication. These standards should, however, be seen as the essentials which should be met by every future PNR agreement, and not as a wish list to be negotiated. Many of the standards and criteria meet the concerns raised in the past, both by the Working Party and by the European Parliament. Their application through binding agreements should in principle lead to a much better level of data protection for the European citizen and would ensure legal certainty. The Working Party does, however, see room for further improvement and would like to urge the EU legislator to include the following items in the framework of general standards and criteria for future PNR agreements as well as the subsequent negotiating mandates.

Compliance with EU legal framework on privacy and data protection

It should speak for itself that any future PNR agreement should fully meet the conditions set out in the EU's legal framework on privacy and data protection, both in the former first and the former third pillars. This means, among others, that the rights given to data subjects in both Directive 95/46/EC, Decision 2008/977/JHA and their national implementation should at least be ensured in all future PNR agreements. It should speak for itself that all rights attributed to the data subject should be exercisable in practice as well. Coherence should also be assured with both the future comprehensive EU framework on data protection and the future general EU-US agreement on the exchange of data in police and criminal justice cooperation. Furthermore, the agreements should respect the right of the protection of one's personal data as is laid down in the EU's Charter of Fundamental Rights, which has a binding legal status as of the entry into force of the Treaty of Lisbon.

The Working Party stresses the need for appropriate legislation in the receiving third country that allows for the collection and processing of PNR data for law enforcement purposes by competent authorities. The relevant national law needs to reference in any future PNR agreement. Also, since all conditions in the agreement should be bilaterally agreed upon and respected by all parties, no conditions should be imposed, modified or interpreted unilaterally.

Data quality

In its analysis of the international trends of PNR, the Commission observes that PNR data is unverified information, mostly provided by the passengers themselves or their tour operators or travel agencies and collected for business purposes, not law enforcement purposes. As there is no (easy) way to objectively verify these data, PNR data cannot be considered as exact information. Their collection for law enforcement and immigration purposes therefore raises adequacy and accuracy issues. Should the necessity of the exchange of PNR data be

proven, the exchange needs to be assessed on a case-by-case basis, including a strict necessity and proportionality test.

Retention periods by law enforcement authorities in the receiving third country

As is rightly stated in the Communication, retention periods should not be longer than necessary for the performance of the defined purpose. In other words, they should be adequate and proportionate. Retention of data of non-suspected individuals raises the question of their necessity and might conflict with constitutional principles in some Member States. The Working Party has not yet seen any evidence that particular retention periods are adequate and proportionate. Data should be deleted immediately after analysis, except in specific cases where they have triggered an investigation in relation to a specific passenger. In such cases they may be kept in the relevant files as long as necessary for the ongoing investigation, in compliance with an existing legal procedural framework which includes adequate safeguards with regard to the security and integrity of the personal data, and deleted from the original database. In view of the desired harmonising effect of the general standards, the Working Party considers it is desirable for the inclusion of the same retention period in all future PNR agreements, while reiterating that the retention period should be no longer than necessary.

Conditions of transfer

The Working Party is satisfied the Commission proposes using exclusively the so-called "push" method of transfer – whereby the data are selected and transferred directly by airlines to the authorities – rather than a "pull" system. Pull systems will thus belong to the past. While the Working Party agrees that a "push" system is more privacy friendly than a "pull" system, for future agreements, the Working Party suggests that other systems of transfer, developed with privacy friendly features, could also be considered. This could, for example, be a system where there is no storage or retention of data unless it is used for an alert or investigation so that only data identified as being necessary are effectively transferred to law enforcement authorities. Such a system should be designed with state of the art security, including access logs.

The Working Party furthermore thinks it is preferable that air carriers (as data controllers) filter out sensitive data before transmitting PNR data to law enforcement bodies. If this is not feasible for technical reasons, a filtering mechanism should be put in place so that law enforcement authorities only access the filtered data. Finally, the Working Party reiterates its objections against so-called bulk transfers of PNR data. From the proportionality perspective, transfers of PNR data would only be acceptable if strictly lead-based and on a case-by-case basis. The requesting competent authority then needs to substantiate that the PNR data are needed in that specific case.

Access and storage

In compliance with the proportionality test, access to data should happen on a case-by-case basis. The criteria used to screen the list of passengers should function on a "hit/no hit" basis, with access to identifiable information only in case of a "hit". There should be access controls in place so that the personal data is only accessed by authorised personnel in competent authorities on a need-to-know basis. As previously mentioned, personal data should only be stored where it relates to an investigation into a specific passenger.

Onward transfers

The Communication is not very clear on onward transfer of PNR data, both to other government authorities in the receiving country and to other third countries. The Working Party agrees with the criteria stated, but wishes to limit the possibilities for onward transfer even more. Most importantly, the principle of purpose limitation should apply, which means that the collected data may not be used by other government authorities in the receiving country for purposes other than the combating of transnational serious crime and terrorism. In general, it should be pointed out that the authority that has originally requested the PNR data is to be seen as the data controller, who remains responsible for the data even after a transfer to third parties. In case of doubt, the authority concerned should be obliged to withhold its consent to the disclosure of the data to a third party. Also, should misuse be made of the PNR data by such a third party, the data subject should be able to hold the original recipient of the data to account. More specifically, where the transfer of data to other government authorities is concerned, the Working Party calls for a limited list of clearly defined authorities permitted to receive PNR data to be included as an annex to each future agreement. Furthermore, when considering onward transfer provisions in the negotiations, the Commission is requested to take account of existing bilateral agreements on the exchange of PNR data the third country may have. The Working Party would prefer for the EU agreement to prevail over bilateral agreements at all times.

Joint review

The Working Party agrees with the Commission that it is essential to monitor and review the PNR agreements on a regular basis. Such joint reviews should also include representatives of the European data protection authorities. Matters to be included in the joint review are the possibility to evaluate the functioning of the agreement, including the results of the exercise of the right of access and other relevant data subject rights and cooperation between supervisory authorities. Furthermore, the Working Party deems it important that any future agreements foresee penalties if a scheduled joint review is not carried out in time or not carried out at all. Ultimately, this should lead to the termination of the agreement.

Sunset clause
It is necessary to periodically reassess and evaluate the necessity of a PNR system. Such a comprehensive in-depth assessment cannot be done during a review as described above. Therefore a sunset clause which mandates a thorough and independent assessment and evaluation of the provisions of the PNR system should be introduced in every future agreement. After the date mentioned in the sunset clause is reached, no data can be exchanged unless the parties to the agreement specifically decide to extend the agreement.

IV. CONCLUSION

Overall, the Working Party is satisfied with the fact the European Commission is showing clear understanding of the need to pay more attention to data protection in future PNR agreements and is willing to conclude binding agreements to ensure legal certainty and equal treatment. The Communication presented on 21 September 2010 is a step in the right direction. However, the usefulness of large-scale profiling on the basis of passengers' data must be questioned thoroughly, based on scientific elements and recent studies.

The Working Party emphasises once again the need for a global approach for all passenger data and not only PNR data. Coherence is needed in light of current developments, including the review of the EU data protection legal framework and the proposed negotiations with the US on a general data protection agreement.

The Working Party emphasises that the general standards and criteria included in the Communication should be seen as the minimum level of data protection to be achieved in future PNR agreements. However, on several points the standards could and should be further developed.

The Working Party therefore urges the Commission, the European Parliament and the Council to take this opinion into account when discussing negotiating mandates for and draft versions of future PNR agreements and to keep it informed on the follow up. Naturally, the Working Party is available to work with any of the EU institutions when clarification or elaboration of its position is required.

Finally, the Working Party would like to request once more to be consulted or asked for advice on the data protection elements of any future agreement, especially given its role as an official EU data protection advisory body and the fact that the members of the Working Party are the national supervisory authorities for the carriers that will be obliged to comply with any future agreements. It also requests to be regularly updated on the state of play during the negotiations on these future agreements.

Done at Brussels, on 12 November 2010

For the Working Party,
The Chairman
Jacob KOHNSTAMM