ARTICLE 29 Data Protection Working Party

10019/04/EN
WP 87

Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)

Adopted on 29 January 2004

Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)

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[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Opinion:

INTRODUCTION

In the aftermath of the events of 11 September 2001, the United States adopted a number of laws and regulations requiring airlines flying into their territory to transfer to the US administration personal data relating to passengers and crew members flying to or from this country. In particular, US authorities imposed on airlines the obligation to provide the US Bureau of Customs and Border Protection (CBP) electronic access to passenger data contained in the Passenger Name Record (PNR) for flights to, from, or through the US. Airlines not complying with these requests may face heavy fines and even loss of landing rights, as well as seeing their passengers subject to delays on arrival in the US.

The Working Party delivered a first opinion in October 2002 and a second one on 13 June 2003. The latter took into consideration the US Undertakings of 22 May 2003 ("Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration"), reflecting the latest state of the dialogue as regards commitments from the US side on the conditions for processing of passenger PNR data by US authorities.

In its opinion of 13 June, the Working Party drew attention to several data protection concerns arising from the transfer to US authorities of passenger PNR data. The main outstanding points concerned the purpose of the transfers; the principle of proportionality as regards the personal data to be transferred as well as the moment of transfers and the retention period; the processing of sensitive data; the importance of adopting a "push" method of transfer; the strict control on further transfers to other Government or Foreign Authorities; the guarantees for and rights of data subjects; the mechanism for enforcement and dispute settlement; and the level of commitments.

---

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

More recently, the Working Party received the Commission's communication to the Council and the Parliament, "Transfer of Air Passenger Name Record (PNR) Data: the Need for a Global Approach"[2] and an updated version of the US "undertakings" dated 12 January 2004 (Annex I).

As stated in the opinion 4/2003, the Working Party deems it appropriate to issue a new opinion in the light of the more recent developments concerning the transfer of passenger PNR data of passengers, and in particular of the results of the negotiations between the European Commission and the US authorities.

1. ACTION AGAINST TERRORISM AND THE PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS.

As already stated in Opinions 6/2002 and 4/2003, the transfer of data to US authorities raises public concern and has broad and sensitive implications in political and institutional terms, as well as having an international dimension.

The fight against terrorism is both a necessary and valuable element of democratic societies. Whilst combating terrorism, respect for fundamental rights and freedom of the individuals including the right to privacy and data protection must be ensured.

Such rights are protected in particular by Directive 95/46/EC, Article 8 of the European Convention on Human Rights as well as being enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union. Data protection is further recognised and expanded in the draft European Constitution discussed by the Convention on the future of Europe.

Therefore, limitations on fundamental rights and freedoms regarding the data protection principles governing the processing of personal data in the European Union should only take place if necessary in a democratic society and for the protection of public interests as exhaustively listed in those instruments.

The case of private data collected for commercial purposes and contained in the databases of airlines offering flight from the EU to or through USA and the associated reservations systems, to be communicated to a public authority by providing access to such systems is without precedent in the relationships between the EU and the USA, as well as an exception to the data protection fundamental principle of purpose specification, taking into account the number and sensitivity of data involved and the number of passengers affected by the US request - amounting to at least 10-11 million individuals per annum. This underlines the need for a cautious approach bearing in mind also the possibilities this opens up for data mining affecting, in particular, European residents and entailing the risk of generalised surveillance and controls by a third State.

Furthermore, similar flows from airlines have already been requested and/or proposed by several other third countries. This raises the issue of equal treatment of third States and the necessity for a global approach concerning the use of air transport data for security purposes in a multilateral context.

---

[2] COM(2003)826 final

It is not proved that not taking into account properly the principles of proportionality and data minimization results into more efficiencies in combating terrorism and maintaining internal security, whilst respecting those principles constitutes an essential guarantee for safeguarding citizens' rights as well as being better suited for commercial development purposes.

In this respect, the Working Party notes that passenger PNR data transfer has become relevant also for other countries, thus requiring a global and uniform approach on a worldwide scale, by ensuring harmonization of the solutions envisaged for different countries.

The Working Party also notes that the recent experience of certain countries, such as Australia, shows that the legitimate requirements of internal security and fight to terrorism can be pursued in a proportionate and reasonable way through systems which are in line with the fundamental principles of privacy and data protection.

2. LEGAL ACTS TO BE ADOPTED

The Working Party understands from the Communication that the Commission considers that the definition of a sound legal basis for the transfer of passenger PNR data to US authorities should take the form of a decision by the Commission under Article 25, paragraph 6 Directive 95/46/EC combined with an international agreement authorising the airlines to treat the US requirements as legal requirements in the EU and binding the US to grant reciprocity and ensure "due process" for EU residents. Therefore, the Commission envisages to enter into a "light bilateral agreement" with the US.

Given the lack of relevant documents, the Working Party is not in a position to adopt an opinion with regard to the content and the possible legal basis and value of such an agreement, also in consideration of Member States' competences for the implementation of Article 6 and 7 of the Directive 95/46.

The Working Party would like to point out, however, that decisions by the Commission under Article 25, paragraph 6 of the Directive, by their nature refer to the adequacy of the protection of personal data after they have been transferred to a third country, and that, so far, they have typically dealt with transfers to private sector organisations in third countries. This is the first occasion in which the transfer takes place because of a legal obligation from a third country which requires operators in the EU to transfer data to a public authority in that third country in a way which is not in conformity with the Directive.

In order to provide a sound legal basis for these transfers, a package is envisaged which consists of an adequacy decision and an international agreement, which is to accomplish a number of legal effects. The Working Party takes the view that, to the extent in which the International Agreement serves to legitimate a limitation of the right to private life, or a restriction of the purpose limitation principle in Article 6 of the Directive, it should in any case respect the limits of both Article 8 of the European Convention on Human Rights and Article 13 of the Directive.

3. SCOPE OF THE ADEQUACY FINDING AND OF A POSSIBLE AGREEMENT: CAPPS II AND TSA

The Working Party expressly excluded the CAPPS II programme and any other system capable of performing mass data processing operations from the scope of its Opinion 4/2003.

In fact, these systems are qualitatively different from the mere transfer of passenger PNR data and involve wide-ranging issues which should be clarified and specifically addressed by the Working Party, in consideration of the more pervasive effects that would affect the fundamental rights of the data subjects concerned.

In particular, the CAPPS II system raises a number of peculiar issues that require not only specific consideration by the Working Party, but also different, higher safeguards. Any possible future decisions on CAPPS II would need specific consideration by the Working Party and should not automatically flow from an extension of the applicable scope of the Commission's first adequacy decision on the transfer of passenger PNR data to the US.

Therefore, also in light of the circumstance that the Working Party has not been informed and consulted about the ultimate CAPSS II legal framework, any use of personal data by TSA with regard to the proposed CAPPS II system or its testing should be considered excluded now and in future from the applicable scope of the Commission's decision. In other words, the considerations made in this Opinion are based on the assumption that the Commission's decision will not be extended in future to CAPPS II, including indirect extension via the reference to internal US legislation; otherwise, far more critical remarks would have to be made already at this stage.

As a result, the Working Party recommends the Commission to make clear, through a specific clause in the decision, that US authorities shall refrain from using passenger PNR data transmitted from the EU not only to implement the CAPPS II system but also to test it.

It is the Working Party's opinion that this should also apply to any other further use of European passengers' data transmitted by airlines in relation with other programmes such as Terrorism Information Awareness and US VISIT, or entailing the processing of biometric data.

4. LEVEL OF COMMITMENTS

The Working Party recalls that any Commission decision should not rest on mere "undertakings" of administrative agencies, but on commitments that are officially published at least at the level of the Federal register and fully binding on the US side. In particular, there should be no ambiguity about the capability to create rights in favour of third parties.

As far as this point is concerned, it is clear that the US undertakings will not be legally binding on the US side. Moreover, the newly added paragraph 47 at the end of the undertakings explicitly clarifies the legal enforceability of the US undertakings, stating that they "do not create or confer any right or benefit on any person or party, private or public".

The Working Party therefore underlines that the level of commitments on the US side cannot be considered as meeting the requirements laid down in its Opinion 4/2003 and considers that this matter is an essential condition which should in any case be addressed before any arrangements are formalised.

5. SPECIFIC ASPECTS

Having regard to the global context described above, the US requests, as reflected in the Undertakings (updated version of 12 January 2004), should be assessed in the light of the Working Party's opinions in this field, and in particular Opinion 4/2003 of 13 June 2003.

A. TRANSITIONAL NATURE OF AN ADEQUACY FINDING

A duration of three and a half years has been suggested for the package including undertakings, adequacy finding and related international agreement.

The Working Party welcomes the introduction of a "sunset clause" in the arrangement and hopes that the three year period proposed in its Opinion 4/2003 will be taken into consideration.

B. PURPOSE LIMITATION.

DHS will use passenger PNR data for CBP purposes for preventing and combating:

1) Terrorism and related crimes;

2) Other serious crimes, including organized crime, that are transnational in nature;

3) Flight from warrants or custody for crimes described above.

The Working Party notes that the description of the purposes for which PNR is used is narrower and more precise than before. However, category 2 remains vague, in particular as for the scope of the "other serious crimes" mentioned in the US Undertakings. Moreover, the purposes remain far broader than the focus on fighting acts of terrorism that the Working Party regarded as necessary in its opinion 4/2003.

C. LIST OF DATA ELEMENTS TO BE TRANSFERRED

US Customs and Border Protection now propose and the Commission has agreed that transfers of passenger PNR data should include a list of 34 data elements. This list results from the exclusion of 4 data fields (identifiers for free tickets, number of bags, number of

bags on each segment, voluntary/involuntary upgrades) from the list of 38 PNR elements contained in Annex B of the Undertakings of 22 May 2003[3].

The Working Party notes that very little progress has been made as to the list of data elements to be transmitted. Indeed, the revised US list still contains all of the 20 elements that the Working Party considered as disproportionate and problematic in its opinion 4/2003.

It should be noted moreover that US authorities have only reduced the requested data elements from 38 to 34, by deleting four elements which had been accepted by the Working Party in its opinion of 13 June. As for the remaining 20 elements which, though not accepted by the Working Party, are still requested by the US authorities, no evidence or explanation has been provided about how their processing could be deemed to be necessary , proportionate and not excessive in a democratic society for combating terrorism.

The Working Party recalls the list of 19 data elements accepted in its opinion of 13 June 2003, any addition to that list being subject to a strict test in the light of proportionality and data minimisation principles.

D. SENSITIVE DATA

As a result of the dialogue, US authorities will not “use” and will delete “certain” PNR codes and terms considered sensitive, bearing in mind that in this regard, Article 8, paragraph 1 of the Directive refers to personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

The list of fields and code data to be eliminated is as yet unavailable. Nevertheless, the Working Party would like to stress that while certain codes such as those referring to meal preferences, special health requirements and Passenger Type Codes relating to religious belonging, such as 'Pilgrim Fare', 'Missionary' or 'Clergy' and others are clearly to be deleted, others need more in-depth assessment - in particular 'free text' fields, such as "General Remarks", which may contain identified sensitive data. The US Undertakings dated January 12th indicated that those would be eliminated by using a list of “trigger” words. This approach would not guarantee the deletion of all sensitive data contained in those fields. Therefore, the only certain solution would be the exclusion of these fields, in line with Opinion 4/2003.

In this connection, the Working Party recalls its Opinion of 13 June 2003, according to which transfer of sensitive data should be ruled out. It therefore would not be practicable that deletion would be performed only after sensitive data have been transmitted to the US authorities. The Working Party invites the Commission to find the appropriate

---

[3] Although Annex B of the Undertakings of 22 May 2003 lists 39 data element, only 38 of them may actually be present in any given PNR, since the field OSI (other service information) should only be used if a SSR (special service request) code is not available, according to the IATA Reservation Services .-Manual, 20th edition, effective 1 June 2003-31 May 2003, point 10.3, pg. 127.

technical solutions (such as filters) in order to avoid any transmission of sensitive data to the US authorities.

E. USE OF DATA DERIVED FROM PASSENGER PNR DATA

In additional wording for the Undertakings, the US authorities describe the limitations that exist to their accessing data "derived" from PNR elements that may reveal features of a passenger's life and pose the risk of serious interference in the data subject's right to private and family life, under the terms of Article 8 of the European Convention on Human Rights. The new wording is as follows:

"Additional personal information sought as a direct result of passenger PNR data will be obtained from sources outside the government only through lawful channels, and only for legitimate counter-terrorism or law enforcement purposes. For example, if a credit card number is listed in a PNR, transaction information linked to that account will be sought pursuant to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorized by law. In addition, access to records related to e-mail accounts derived from a PNR will follow U.S. statutory requirements for subpoenas, court orders, warrants, and other processes as authorized by law, depending on the type of information being sought."

These clarifications are welcome. They do not, however, on their own fully allay the Working Party's concerns. In particular, the scope of the purposes for which PNR may be used should not allow for further unspecified "law enforcement purposes". Moreover, access to e-mail accounts and other personal information derived from a PNR should only take place in accordance with procedural requirements laid down in international instruments related to judicial and law enforcement cooperation. It must also be clear that in case of abuse, individuals can seek redress from an independent authority.

F. DATA RETENTION PERIOD

CBP will retain collected passenger PNR data for the agreed CBP purposes for 3 and a half years. Data that has been manually accessed during that period will be retained in a deleted data file for an additional 8 years.

The Working Party notes that this represents an improvement over the 7 year initial storage period proposed in the Undertakings of 22 May. Three years and a half remains nevertheless a considerably longer period than the "weeks or months" called for by the WP in its Opinion 4/2003. The Working Party doubts that the undifferentiated storage of all PNR elements for such long periods can be regarded as corresponding to what is "proportionate and necessary in a democratic society".

Furthermore, the additional 8 year retention period, as resulting from the mere circumstance that the data have been accessed, is disproportionate insofar as it is not related to a concrete investigation or warrant on the data subject and makes it possible to *de facto* override the three and a half year term.

In this regard, it should be noted that different solutions can be envisaged which are more respectful of data protection principles but still efficient in fighting crime. For example,

according to the system developed by Australia, Australian customs will not retain or store any passenger information unless the passenger has been identified undertaking an illegal activity or the information is needed as intelligence to assist in investigation of a suspected offence.

G. METHOD OF TRANSFER

As regards the method of transfer, the Working Party recalls its opinion 4/2003, where it considered that the sole data transfer mechanism whose implementation does not raise major problems is the "push" one – whereby the data are selected and transferred by airline companies to US authorities – rather than the "pull" one – whereby US authorities have direct access to airline and reservation systems databases.

The Working Party is seriously concerned that, even though US authorities have seen no objection for several months to the "push" system, the appropriate technical mechanisms to implement a "push" system operated directly by the European airlines are not yet in place. The Working Party considers that concrete measures should be adopted by April 2004 at the latest and urges the Commission to take immediate action with that aim. Furthermore, the Working Party underlines that no adequacy of the level of protection provided for by the US can be assumed without the establishment of a "push" system.

H. TIME OF DATA TRANSFER

In its opinion 4/2003 the Working Party recommended that US CBP should receive the data concerning a specific flight no earlier than 48 hours prior to departure and that thereafter the data should only be updated once.

As far as this point is concerned, the latest version of the Undertakings exactly reflects the previous one, granting US authorities access 72 hours prior to departure and a maximum of three updates.

The Working Party regrets that no improvement has been achieved on this point during the negotiations.

I. TRANSFER OF PASSENGER PNR DATA TO OTHER GOVERNMENT OR FOREIGN AUTHORITIES.

In its opinion 4/2003, the Working Party asked for the precise identification of the other public bodies entitled to receive the data, stating that any direct or indirect onward transfers should be made on a case by case basis and made conditional upon acceptance of specific "undertakings" no less favourable than those provided to the Commission by the US authorities. Moreover, the number of authorities to which data could be transferred should be restricted.

The Working Party notes that a comprehensive list of the relevant government authorities to which data might be transferred has not yet been provided. The Working Party is also still concerned about such provisions allowing CBP to disclose data "as otherwise

required by law", especially if those provisions are considered in the light of existing or proposed laws and Memorandums of understanding requiring US to share their data with other countries in some specific cases.

In particular, the mechanism referred to in points 29 and 35 of the Undertakings deviate considerably from the purpose limitation principle as stated by the Working Party (i.e. fight against terrorism and directly related crimes) and even from the wider purposes as defined in points 1 and 3 of the Undertakings.

J. GUARANTEES – RIGHTS OF THE DATA SUBJECT

1) CLEAR INFORMATION TO THE DATA SUBJECT

According to opinion 4/2003, and in accordance with Article 10 of the Directive, clear and precise information should be provided to data subjects about the identity of the controller, the purpose of the processing, and any further information, such as the existence of a right of access and rectification in addition to the available redress effective mechanisms.

The Working Party notes that the CBP will provide information to the travelling public. In this respect, the Working Party notes that it will be possible to expeditiously finalize a standard information notice after setting out the legal framework more precisely, by having also regard to the draft made available to the Working Party. It should be considered, however, that a comprehensive information notice can complement but in no case surrogate the legal requirements needed for the transfer of passenger PNR data to the US to be lawful.

2) ACCESS

The Working Party, in its opinion 4/2003, underlined the necessity of effectively enforceable safeguards, in respect of the general freedom of information rules (FOIA), in order to ensure both that the latter are not used by third parties to access passenger PNR data held by the US administration and that the data subjects' right of access to their own data is enforced generally and unambiguously.

As far as the access by third parties is concerned, the Working Party welcomes the clarifications provided by CBP in the document "Exemptions Under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data".

Nevertheless, with regard to the access by the passenger to his/her own data, there are still some concerns regarding the way exemptions may be opposed to the data subject in order to allow the administration to refuse access to him or her.

Moreover, the Working Party notes that the data subjects' right of access has not been explicitly extended, as called for in opinion 4/2003, to any new data which may be generated as a result of the processing to which the data transmitted from Europe are submitted (risk profile, exclusionary lists, etc.).

3) RECTIFICATION

The Working Party in its opinion 4/2003 underlined the importance of providing the data subject with an effective mechanism to have his/her data corrected. The Working Party notes that the scope of the Privacy Act 1974 is still limited to US nationals or residents. Therefore, the issue of non-discrimination between US and European residents is not yet solved and it has to be established whether the rectification mechanism laid down in the Undertakings is to be considered as effective and legally binding as the right to rectification granted by the FOIA to US nationals and residents.

4) REDRESS

The DHS Privacy Office has agreed to address expeditiously complaints referred to it by DPAs in the Member States on behalf of an EU resident who considers that his/her complaint has not been dealt with satisfactorily by DHS, including its Privacy Office.

The Working Party welcomes this development. It is important that individuals can obtain qualified help in particular cases; however, the issue concerning the Chief Privacy Officer's actual independence, as raised in WP's opinion 4/2003, is yet unsolved. The members of the Working Party consider that the internal arrangements they made as regards the "panel" functions referred to in FAQ 5 of the Safe Harbor Agreement may be useful in this context. They will consider what adjustment they may need for application in the PNR context.

The Working Party regrets, on the other hand, that there is no guarantee that passengers will in all cases have access to a truly independent redress mechanism in cases of dispute with the DHS. Furthermore, it is now apparent that the "Undertakings" may not produce binding legal effects and may not be the source of obligations that can be enforced before a court (see above point 9). This remains an important gap compared with the rights enjoyed in the EU by any individual whose data are processed there, regardless of his/her origin.

K. AUDITS

The following new wording has been included in the Undertakings (paragraph 43):

"CBP, in conjunction with DHS, undertakes to participate once a year, or more often if agreed by the parties, in a joint review with the Commission assisted as appropriate by experts from Member States of the European Union,[4] on the implementation of these Undertakings, with a view to mutually contributing to the effective operation of the processes described in these Undertakings. Such joint review may cover the results of the

[4] The composition of the teams on both sides will be notified to each other in advance and may include appropriate authorities concerned with privacy/data protection, customs control and other forms of law enforcement, border security and/or aviation security. Participating authorities will be required to respect the confidentiality of the discussions and be covered by any necessary security clearances. Confidentiality will not however be an obstacle to each side making an appropriate report on the results of the joint review to their respective competent authorities, including the US Congress and the European Parliament. The two sides will mutually determine the detailed modalities of the joint review.

DHS Chief Privacy Officer's annual report to Congress (as described in paragraph 42 of these Undertakings) and, to the extent authorized by the Chief Privacy Officer, any audits that have been carried out in the reporting period, or other findings regarding, in particular, data security, sharing of PNR with Designated Authorities and personnel access to PNR in relevant databases, as well as the handling of complaints. To the extent authorized by the DHS Chief Privacy Officer, the joint review may include consideration of the application of the Undertakings and may also address issues which can help to enhance the performance of the uses of passenger PNR data for the purposes set out in paragraph 3 these Undertakings."

This is another welcome development and the Working Party expects the reviews to be conducted with the necessary openness and transparency to be truly effective. In any case, the Working Party's members undertake to co-operate to the extent that they are asked to participate in any such review and to observe the rules regarding confidentiality agreed by the two sides. The Working Party reserves of course the right to reconsider this subject, if it deems it appropriate, regardless of the timing of reviews.

L. MATCHING

Recent experience showed that a new element has to be taken into consideration in addition to the concerns raised above. The passenger PNR data collected by CBP are matched in US with lists of persons searched for. These processing operations led to the fact that several flights from EU had to be cancelled at the last minute. Information given publicly thereafter revealed that they where mistakes or cases of unclear or homonymy problems affecting data related to suspects of terrorism.

These circumstances are related to the data protection principle of data quality. The Working Party considers that further initiatives should take place in order to prevent such consequences for passengers, crew members as well as airline companies.

CONCLUSION

The Working Party reiterates that the overall objective of its assessment is to establish a clear legal framework for transferring airline data to US in a way which is compatible with data protection principles, as pointed out in its Opinion 4/2003. The Working Party has taken duly note of the progress made in the US-EU dialogue concerning passenger PNR data, in particular as regards the latest Undertakings of 12 January 2004 recently made available by the US Administration, and is pleased to record some improvements over the previous version of such Undertakings.

However, in the Working Party's view the progress made does not allow a favourable adequacy finding to be achieved. The Working Party believes that any solution should at least respect the following data protection principles:

- **Data quality**:
    - the purposes of the data transfer should be limited to fighting acts of terrorism and specific terrorism-related crimes to be defined;
    - the list of data elements to be transferred should be proportionate and not excessive;
    - data matching against suspects should be performed according to high quality standards with a view to certainty of the results;
    - the data retention periods should be short and proportionate;
    - passengers' data should not be used for implementing and/or testing CAPPS II or similar systems.
- **Sensitive data** should not be transmitted.
- **Data subjects' rights**:
    - Clear, timely and comprehensive information should be provided to the passengers;
    - rights of access and rectification should be guaranteed on a non discriminatory basis;
    - there should be sufficient guarantee that passengers would have access to a truly independent redress mechanism.
- **Level of commitments by US authorities**:
    - the US commitments should be fully legally binding on the US side;
    - the scope and legal basis and value of a possible "light international agreement" should be clarified.
- **Onward transfers** of passenger PNR data to other government or foreign authorities should be strictly limited.
- **Method of transfer**: a "push" method of transfer – whereby the data are selected and transferred directly by airlines to US authorities – should be put in place.

Done at Brussels, on 29th January 2004

For the Working Party
The Chairman
Stefano RODOTA