



**11070/03/EN  
WP 78**

**Opinion 4/2003 on the Level of Protection ensured in the US  
for the Transfer of Passengers' Data**

**Adopted on 13 June 2003**

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 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.  
Website: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)

*Opinion 4/2003 on the Level of Protection ensured in the US  
for the Transfer of Passengers' Data*

**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<sup>1</sup>,

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 a previous opinion issued in October 2002<sup>2</sup>, the Working Party reached the conclusion that compliance with the US requirements by the Airlines creates problems in respect of Directive 95/46/EC on data protection<sup>3</sup> and called for a common approach at the European Union level to be found. A specific recommendation was made for the European Commission to enter into negotiations with the United States of America to resolve this matter.

The Working Party has been updated by the Commission on the progress of the talks, which were conducted by the Commission in order to establish the conditions that would allow the Commission to adopt a decision recognising the "adequate protection" on the basis of Article 25 (6) of Directive 95/46/EC and has also gained further insight from the opportunity to discuss the US requirements with high-level officials of the Department of Homeland Security at its meeting of 5 May.

In particular, the Working Party has received from the Commission a document dated 22 May 2003 of "undertakings" issued by the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration<sup>4</sup>. It understands that these undertakings are the result so far of the on-going negotiation between the US

---

<sup>1</sup> 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](http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm)  
Opinion 6/2002 of the Working Party on "transmission of Passenger Manifest Information and other data from Airlines to the United States", WP 66 of the Working Party, issued 24 October 2002.

<sup>3</sup> Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>4</sup> Referred to as "undertakings" in this document.

administration and the Commission and that the Commission is still pressing the US side to make further progress on a number of issues.

The present Opinion is issued with reference to the level of protection ensured by the United States of America after the requested transmission by airlines of personal data concerning their passengers and crewmembers on the basis of their law and international commitments, as described in the undertakings and as laid down in relevant law. The Working Party has been guided by the general criteria set forth to assess adequacy of protection in previous documents<sup>5</sup> and by its previous opinion on the subject of PNR/APIS data required by the US<sup>6</sup>.

This opinion is given at a time when US are requesting from EU or directly from Member States numerous flows of personal data (e.g. visa, etc. ).

In addition, the Working Party is fully aware that similar flows from airlines have already been requested and/or proposed by several other third countries. This raises the issue of non-discrimination between third States and the necessity for a global evaluation, which might be a model solution for other countries that may receive similar requests. The Working Party underlines the necessity to provide a framework for personal information circulating throughout the world for purposes related to security in connection with air travel.

## **1. Action against terrorism and the protection of fundamental rights and freedoms**

The issue at stake regarding the transfer of data by airlines 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 freedoms of the individuals including the right to privacy and data protection must be ensured<sup>7</sup>.

Such rights are protected in particular by Directive 95/46/EC, Article 8 of the European Convention on Human Rights<sup>8</sup> and are enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union<sup>9</sup>. Moreover data protection is further recognised and expanded in the draft European Constitution discussed by the Convention on the future of Europe.

The legitimate requirements of internal security in the United States of America may not interfere with these fundamental principles. Limitations to fundamental rights and freedoms regarding the processing of personal data in the European Union should only

---

<sup>5</sup> Working Document on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", WP 12 of the Working Party, issued 24 July 1998.

<sup>6</sup> Opinion 6/2002 on "transmission of Passenger Manifest Information and other data from Airlines to the United States".  
See Opinion 10/2001 « on the need for a balanced approach in the fight against terrorism », adopted 14 December 2001.

<sup>8</sup> See also the relevant case-law of the European Court on Human Rights.

<sup>9</sup> The European Commission has committed itself to respect the Charter. See Commission Communication on the Charter of Fundamental Rights of the European Union (COM(2000) 559 final).

take place if necessary in a democratic society and for the protection of public interests exhaustively listed in those instruments<sup>10</sup>.

---

<sup>10</sup> See the interests listed in Article 13 of Directive 95/46/EC.

## **2. General remarks**

The scope of the present opinion concerns the protection of fundamental rights and freedoms regarding the processing of personal data.

This opinion is given by the Working Party with a view to assessing the adequacy of protection provided by the US in connection with envisaged Commission decisions or other legal instruments dealing with this issue. The Working Party reserves the right to supplement the present opinion by a further opinion should this opinion not be adequately taken into account or if substantial changes are made in the course of future negotiations, such as to warrant specific consideration.

The Working Party observes that the circumstances referred to in the “undertakings” require accurate analysis with a view to assessing the adequacy of the level of protection they provide for personal data.

The choice between different mechanisms for the transfer of data (direct access by the US authorities into the databases of the airlines versus proactive disclosure of the data by airlines) raises not only technical problems but also, more importantly, questions of proportionality.

It also means that US authorities have requests that exceed the powers currently granted to European judicial and police authorities and/or authorities in charge of immigration matters or even of intelligence and security services when carrying out similar activities in the European Union.

Furthermore, the issues at stake affect judicial and police co-operation and should be assessed in the light of the safeguards laid down in recent EU-US agreements and draft agreements concerning co-operation, mutual assistance and extradition.

The collection of the data included in the databases of airlines as requested by the US covers a large number of passengers (estimated to amount to at least 10-11 million per annum) which underlines the need for a cautious approach bearing in mind the possibilities this opens up for data mining affecting, in particular, European citizens and entailing the risk of generalised surveillance and controls by a third State. Therefore, the requests coming from the US administration should be addressed with the utmost attention.

## **3. Transitional Nature of an Adequacy finding**

The scope of the data flows is related to recent serious circumstances at the international level. The Working Party recommends that periodical short-term re-evaluations of the situation shall be made to assess if the necessity for such flows remains. Should the international circumstances alter, it would be necessary to review the situation. The Working Party recommends the Commission to include clauses in its decision providing for ‘sunset’ limitation and review the situation after 3 years in any event.

Additionally, if the guarantees provided by the US administration are not correctly implemented, re-evaluation of the situation will be necessary. For this reason, it is essential that a regular report on the actual use of the data in the US be submitted by the Commission on the implementation of the protection in the US. This should allow for the

verification of the conditions of processing in the US, to ensure that the underlying assumptions, which justified the Commission's decision, still hold good.

#### **4. The US Regulatory Framework**

The Working Party considers that any Commission Decision recognising the provided protection as adequate as well as any other instrument(s) providing a legal framework for the data flows should be based on a clear-cut picture of primary and secondary US legislation regulating purposes, mechanisms and rationale of data utilisation in the US and the entities entitled to access such data.

A full picture of the relevant US regulatory framework, to meet openness and transparency requirements in respect of European citizens, should be included as an annex to any Commission Decision. In addition, provision should be made for a mechanism that ensures that any relevant legislative innovation is communicated to the Commission. It is necessary to avoid other legislation, including legislation passed prior to the Commission Decision (the "undertakings" create a very broad mandate for use and disclosure of the data "as otherwise required by law"), or conflicting interpretations or implementing instruments passed in the US with regard to, in particular, CAPPS II and the collection of biometric data<sup>11</sup>, resulting in substantial unilateral changes to the conditions in the US which are the agreed basis for an adequacy finding.

Moreover, it is essential that the decision should not rest only on mere "undertakings" of administrative agencies aimed at supporting certain interpretations at national level (see point 11).

An evaluation of the adequacy of the level of protection cannot be made with respect to areas of the US administration whose regulatory framework concerning processing of PNR data may not be regarded as stable or adequately clarified in terms of data access rules and entitlement to process such data. The Working Party makes particular reference to the points in the "undertakings" concerning the Transportation Security Administration and its CAPPS II programme. Nor should the evaluation of the adequacy of the level of protection apply to those systems capable of performing mass data processing operations, whose actual functioning and features involve wide-ranging issues yet to be clarified in particular, the Terrorism Information Awareness Initiative.

In this context, the Working Party highlights the need to avoid a situation where TSA or other agencies operating mass data processing systems would receive data indirectly. In case data are to be transmitted to such systems, an additional and specific assessment of the level of protection would be required.

#### **5. Method of transfer and legal concerns**

As for the legal basis, which was especially stressed in the European Parliament's Resolution of 13 March 2003, the Working Party is of the opinion that, given the complexity of the legal issues surrounding the lawfulness of communicating the data to third parties and transferring such data to third countries, it may be necessary – having regard to Directive 95/46/EC as a whole – that a positive finding by the EC Commission

---

<sup>11</sup> The issue related to collection of biometric data as envisaged starting from October 2004 for issuing entry documents should be assessed separately and only at a later stage.

pursuant to Article 25(6) of the Directive should be accompanied by a formal commitment made by the US Administration upon conclusion of the negotiations.

The legal basis is referred to by the Working Party on the assumption that, considering possible technical differences between various systems, 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 online access to airline and reservation systems databases.

In addition to ensuring a greater measure of compliance with the principle by which personal data should be adequate, relevant and not excessive (Article 6 of the Directive), entailing fewer data security problems and making certain US access filtering mechanisms superfluous, the “push-system” would make it unnecessary to apply the national measures adopted in transposing the Directive to the US authorities – which would otherwise be necessary if a pull-system were implemented. Indeed, in the latter case, the entire Directive including Article 4, 6 and 13 could be considered as being directly and completely applicable to the US authorities. Moreover, a “push” system is the only solution to ensure that liability rules provided for by Directive 95/46/EC can be correctly applied to European controllers of data.

The Working Party is therefore pleased to note that the US sees no objection to the “push” system. This solution should be substituted for the present mechanism as soon as possible.

## **6. Purposes**

The purposes for which the data will be used should be limited to fighting acts of terrorism without expanding their scope to other unspecified “serious criminal offences”. A clear and limited list of serious offences directly related to terrorism should be provided by the US side, without prejudice to the possibility of performing additional specific and individual data exchanges within the framework of judicial and police co-operation.

The need for clarification also relates to the other public bodies entitled to receive the data, as they are currently not identified. The precise identification of such public bodies and their missions or alternatively, for the precisely identifiable authorities such as the judicial bodies, a functional description of them should be detailed. It is in any case necessary to make it absolutely clear that the data might only be communicated to other authorities where necessary in specific cases for the fight against serious offences directly related to terrorism and that subsequent use of such data continues to be limited in the same way.

Clarification is also needed as to the public bodies and the procedures of the said bodies operating the “no fly” and “watch” lists, against which the PNR is processed.

The Working Party questions the justification of disclosure on the ground of the protection of the vital interests of the data subject or of other persons, since this would significantly increase the possibility for additional transmission of the data. Other ways of meeting this requirement would appear to be available.

As for authorities from other third countries, without prejudice to the possibility of performing additional specific and individual data exchanges within the framework of judicial and police co-operation, 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 in connection with protecting the transferred data.

## **7. Proportionality**

Proportionality should be ensured not only with regard to purposes and the type of offence to be monitored, but also in respect of other issues concerning:

### *Transferable Personal Data*

The Working Party considers that the amount of data to be transferred<sup>12</sup> goes well beyond what could be considered adequate, relevant and not excessive (Article 6 (1) (c) of the Directive)<sup>13</sup>. Access to the full set of PNR data is excessive. Data should be limited to the following information : PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items.

The US primary legislation requiring airlines to provide PNR on request does not make it obligatory for the US authorities concerned to request the data, still less to require that it be transmitted on a systematic basis. Moreover, the US authorities concerned could limit the PNR data elements they request airlines to send. The US authorities are thus interpreting their legal mandate very broadly.

The Working Party finds it necessary to take into account the other sources of information which the US authorities have available to them or try to obtain in their efforts to acquire information on foreigners, such as the data provided via immigration formalities, APIS etc. Additional data exchanges within the framework of judicial and police co-operation channels should also be taken into account in this context.

Transfer of what can be regarded, broadly speaking, as sensitive data - protected by Article 8 of the Directive – should be ruled out. Furthermore, transfer of SSR data – which are actually processed on an optional basis by certain reservation systems – would not appear to be proportionate, in particular in the light of the initiatives undertaken by IATA to update the relevant Manual, which has reached its 20<sup>th</sup> edition. This also applies to OSI (Other Service-Related Information) data, open or free-text fields (such as the “General Remarks” where data of a delicate nature can appear), and to the information concerning frequent-flyers and “behavioural data”.

A clear, exhaustive list of the data transferred on the basis of the Commission Decision should be attached as an annex alongside the table referred to under point 4).

---

<sup>12</sup> See Annex B of the « undertakings ».



### *Time of Data Transfer*

The Working Party is of the opinion that US CBP should receive the data concerning a specific flight no earlier than 48 hours prior to departure. Thereafter, the data should only be updated once.

### *Data Retention Time*

The Working Party is doubtful whether an excessively long data retention time with regard to millions of individuals can be effective for investigative purposes. Personal data should be kept for no longer than is necessary for the purposes for which they were collected. Thus, only retention of the transferred data in line with the announced purpose of controlling the entry to the US territory with a view to the detection of terrorist acts may be accepted. Data should only be retained for a short period that should not exceed some weeks or even months following the entry to the US. A period of 7-8 years cannot be considered as justified. A short period would seem better adjusted to discharging the highly difficult tasks in question, as well as being considerably less expensive. This is obviously without prejudice to the possible need for the processing to continue on a transitional basis in individual cases where there are well-established, specific grounds to examine certain persons more closely, in view of taking measures related to their actual and/or potential involvement in terrorist activities.

## **8. Subcontractors**

The Working Party underlines the necessity to provide for the same level of liability of subcontractors and their employees as for US officials, to ensure that the provided guarantees are upheld.

## **9. Guarantees - rights of the data subjects**

One of the most basic principles of an adequate data protection regime is for the data subject to be provided with information and to be able to exercise his/her rights, in an easy, quick and effective manner.

### *Information*

Data subjects should be clearly and precisely informed about their rights in particular about the right of access and rectification in addition to the available redress effective mechanisms.

### *Access*

The Working Party underlines the necessity of effectively enforceable safeguards, in respect of the general freedom of information rules (FOIA), in order to ensure that the latter are not used by third parties to access PNR data held by the US administration. In this context, it is important to prevent possible discrimination between citizens and to ensure that the data subjects' right of access to their own data is enforced generally and unambiguously.

The “undertakings” provided by the US authorities create 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.

The Working Party is of the opinion that the data subjects’ right of access should extend 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...).

### *Rectification*

Since the scope of the US Privacy Act is limited to US residents, the Working Party underlines the importance to provide the data subject with an efficient mechanism to have his/her data corrected.

## **10. Enforcement and Dispute Settlement**

### *Timely support and help for the individual and independent redress and supervision*

The ensured protection should provide rapid support and help to individual data subjects in exercising their rights and provide in their favour independent and appropriate redress.

The Working Party sees major flaws concerning enforcement and independent third-party supervision of the application of the undertakings. The available mechanisms at this moment are limited to audits and the internal Chief Privacy Officer. Moreover, it is not clear how the “undertakings” may produce binding legal effects and be the source of obligations that can give rise to claims before a court (see below point 11).

Moreover, the Working Party notes the need to be provided with more information on the supervisory independent body that has control on the “no fly”, “watch” lists and on the logic of the profile mechanism.

### *Audits*

A guarantee of a good level of compliance with the data protection safeguards should exist. In this context, the Working Party underlines the importance of the public availability of certain audits results. The public reports should contain the number and volume of PNR requests from other US public bodies and the number, volume and the motivating reason for those requests for which authorisation has been granted by the first recipients.

## **11. Level of commitments**

The Working Party underlines the necessity to have commitments from the US side 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. This raises the point of which authority precisely will commit the US side. Directive 95/46/EC indeed provides that a decision recognising as adequate the protection ensured by a third country to transferred data must be based on its domestic law and/or the international commitments into which it has entered.

## **Conclusion**

This opinion sets out the concerns of the Working Party from a data protection perspective in assessing the level of protection ensured in the US with a view of a possible Commission Decision. The overall objective is to establish as quickly as possible a clear legal framework for any transfer of airline data to the US in a way which is compatible with data protection principles. While recognising that ultimately political judgements will be needed, the Working Party urges the Commission to take its views fully into account in its negotiations with the US authorities.

The Working Party is aware that a more global approach concerning the conditions of the use of air transport data for security purposes in a multilateral context might be necessary.

Done at Brussels, on 13 June 2003  
For the Working Party  
*The Chairman*  
Stefano RODOTÀ