11647/02/EN
WP 66

Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States

Adopted on 24 October 2002

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 following opinion:

1. ISSUE UNDER DISCUSSION

1.1 Background and purpose

In the aftermath of the events of 11 September 2001[2], the United States adopted on 19 November 2001, the Aviation and Transportation Security Act [3] requiring airlines flying into their territory to transfer to them data relating to passengers and cabin crew (Passenger Manifest Information)[4]. Such transfers must be made electronically and completed before the plane takes off, at the latest 15 minutes after departure for passengers. Although the "Commissioner of Customs" is the recipient of the data forwarded to the United States, the data will be shared by the US federal authorities. The purpose of data transmission is not solely concerned with aviation security but is also an issue of public order in the United States.

On May 14th 2002, the United States adopted another law to enhance border security that requires airlines arriving and departing from the United States to transmit data relating to passengers and crew to U.S. Immigration and Naturalization Service[5]. For passengers and crew arriving in the United States, the data and transmission requirement is the same as for the U.S. Customs. For passengers and crew departing from the United States, the transfers must be made electronically and completed 15 minutes before the plane takes off, allowing for manifest update or correction within, at the latest, 15 minutes after aircraft has become airborne. U.S. Immigration and Naturalization Service reserves the right to

---

1 Official Journal L 281 of 23.11.1995, p. 31, may be consulted at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 Prior to 11 September 2001, airlines were already transferring certain data to the US on a voluntary basis.

3 Aviation and Transportation Security Act of 19 November 2001 (107-71), Interim Rules of Dep. of The Treasury (Customs) – Passenger and Crew Manifests Required for Passenger Flights in Foreign Air Transportation to the United States (Federal Register, 31 December 2001) and Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States (Federal Register, 25 June 2002).

4 The same obligations have been introduced for maritime transport.

5 Enhanced Border Security and Visa Entry Reform Act of 2002, see also the Immigration and Nationality Act.

require the aircraft to return to U.S. port within one hour after departure should it find necessary.

All the data must be transmitted to a centralised database[6] that is jointly operated by the US Customs and Immigration and Naturalization Service. Once transmitted, the data will be shared with other federal agencies and no longer specifically protected.[7]

1.2 Categories of data transmitted

APIS (an acronym for Advanced Passenger Information System) has seen a number of significant developments, in particular the extension of its list of data. At the outset, the data required were intrinsically linked to the flight taken, visa or residence permit for the United States, and identification information such as that included in passports.

In particular, the recent US law on border security requires the following data to be transferred to the US Immigration for flights departing to and from the United States : name, date of birth, nationality, sex, passport number and place of issue, country of residence, US visa number, date and place of issue (if applicable), foreign registration number (if applicable), address in the United States during the stay and any other data deemed necessary to identify the persons travelling, implement regulations on immigration or protect national security and safety[8].

In addition, the transfer on request of data processed by reservation and departure control systems (DCS), particularly Passenger Name Records (PNR), is currently required[9]. The data in question are not restricted to passengers flying into the United States and may vary from one airline to another. They may involve identification data[10] (name, first name, date of birth, telephone number), the PNR reservation number, the date of the reservation, the travel agent where appropriate, the information displayed on the ticket, financial data (credit card number, expiry date, invoicing address etc.), the itinerary, information from the carrier concerning the flight (flight number etc.), the seat number and earlier PNR. The latter may include not only journeys completed in the past but also religious or ethnic information (choice of meal etc.), affiliation to any particular group, data relating to the place of residence or means of contacting an individual (e-mail address, details of a friend, place of work etc.), medical data (any medical assistance required, oxygen, problems relating to sight, hearing or mobility or any other problem which must be made known to

---

6 The Interagency Border Inspection System (IBIS).

7 Some of these data, might, where appropriate, be made public in accordance with legislation governing access to information held by the public sector.

8 Decision of the Attorney General, in consultation with the Secretary of State and the Secretary of Treasury.

9 Interim Rule (Federal Register, 25 June 2002), Passenger Name Record Information required for Passengers on Flights in Foreign Air Transportation to or from the United States.

10 It is expressly stated that the list is "intended merely to be illustrative of those data elements to which Customs may request access".

ensure a satisfactory flight) and other data linked, for example, with frequent flyer programmes (Frequent Fliers number) [11].

In addition, for countries participating in the "Visa Waiver Program", the transfer of biometric data is due to become compulsory by October 2004[12].

1.3 Sanctions

Failure to forward information required or forwarding incorrect or incomplete information is punishable by severe penalties in particular loss of landing rights and the payment of substantial fines[13].

The Working Party wonders, in this regard, as to whether such unilaterally adopted measures may be compatible with the international agreements and conventions concerning air traffic and transportation as well as with the applicable national law in respect of those countries where air companies operate on a permanent basis.

1.4 Extension to other countries

Other countries as Canada, Mexico[14], Australia, New Zealand, South Africa and the United Kingdom have already implemented or are planning to implement similar systems to meet their own needs.

2. COMPATIBILITY WITH DIRECTIVE 95/46/EC

2.1 Application of the Directive

The data forwarded by airlines relate to identified physical persons. They are processed by airlines within the EU (collected, recorded, modified, stored, modified again, called up, used, forwarded etc.). As such, they are protected by the provisions of Directive 95/46/EC.

Furthermore, the evolution of the APIS system raises specific concerns that are presented below. Most of them are beyond the competence of airlines. Airlines find themselves caught in a dilemma in that although, on the one hand, they are obliged to observe the legislation on data protection transposing Directive 95/46/EC, on the other hand US legislation obliges airlines to forward data and is backed up by severe penalties.

---

[11] These data, contained in the "interim rules" published by the Department of Customs, are nevertheless absent as such from the 107-71 law.

[12] Section 203 of the Enhanced Border Security and Visa Entry Reform Act of 2002.

[13] Around $ 5000 per error for the US Customs (e.g. passenger name or other criteria below the accepted weekly average) and $ 1000 for the US Immigration and Naturalization Service per incorrect name.

[14] Mexico is also going to forward all data obtained on flights flying into Mexico from the United States.

2.2 Information on data subjects

Data subjects should receive the information necessary to ensure fair processing of data. This information should include the specific purposes of processing in the United States and the recipients of the data.

Article 13 of Directive 95/46/EC cannot justifiably be invoked to restrict this obligation where the transfer is systematic and where the required categories of information have already partially been made public in the United States through the publication of legislation. In specific terms, this information should be supplied to the individual at the time when the data are actually collected and covers inter alia the specific purposes of processing in the United States and the recipients of the data [15].

2.3 Safety measures

In accordance with Directive 95/46/EC, airlines are required to implement appropriate security measures to protect personal data. This obligation is without exception. It appears that the technical requirements imposed on airlines by the United States leave data exposed to non-authorised access by third parties.

2.4 Observing the purpose principle

Given the developments made to the system, the transmission of personal data as described in paragraph 1.2 above, which go beyond the limited set of data that are usually provided by passengers in connection with the organisation of the travel, cannot be considered as compatible with the original purpose of collecting personal data by airlines or travel agencies in particular the fulfilment of their contractual obligations vis-à-vis the passengers. Article 6(1)(b) of Directive 95/46/EC prohibits further processing of data collected for specified, explicit and legitimate purposes in a way incompatible with those purposes.

In view of the large, multifarious amount of data involved, the data cannot be considered as adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, as stipulated in Article 6(1)(c) of Directive 95/46/EC.

The possibility therefore remains of having recourse to Article 13 of Directive 95/46/EC, which authorises Member States to adopt legislative measures aiming to restrict the scope of these two obligations insofar as this restriction is necessary to safeguard the interests listed under the same provision (the prevention and investigation of criminal offences, public security etc.). It would, of course, be preferable for Member States to come up with a common approach to this matter.

2.5 Transborder data flows

Directive 95/46/EC stipulates that the transfer of personal data to a third country may only take place if the third country ensures an adequate level of protection. The development of APIS raises concern in this perspective. The processing of data that are transmitted by airlines by US federal authorities falls short of this condition[16]. The limited

---

[15] This does not apply if the persons concerned are suspects under investigation.

[16] The law on privacy applicable to US federal authorities protects only the data of US citizens.

scope of the “Safe Harbor” means that it cannot enter into play for the protection of data transfers to government authorities.

The derogations set out in Article 26 of Directive 95/46/EC also appear not to apply.

– At the present time, the unambiguous consent requirement would not offer a proper solution, as much concern would remain in many respects. In any event it does not appear that the passenger’s consent is asked for, in compliance with the legislation in force. Directive 95/46/EC defines consent as meaning any freely given specific and informed indication of a person's wishes by which data subjects signify their agreement to their personal data being processed. The consent may be complicated to obtain, not least for the practical problems related to clearly conveying all the necessary information to the passengers when buying a flight ticket as we are dealing with global reservation systems which allow one to book a flight from the European Union to the United States from almost every country in the world through very different channels (different airlines, travel agents, etc.). The information provided to the data subject must include the items set out in Articles 10 and 11 of the directive including, where appropriate, the inadequacy of protection in third countries.

– The necessity of the transfer to fulfil a contract between the data subject and the person responsible for processing the data is difficult to invoke, given the scope of the data transmitted. Indeed, transmitting a large amount of data cannot be considered as "necessary" to the performance of a contract. The physical impossibility for airlines to fulfil their contractual obligations, owing to a loss of rights, is an insufficient ground in this case. Moreover, it is impossible to apply this exception to cover the transfer of data relating to persons not travelling to the United States.

– By the same token, neither does it appear possible to rely on the possibility of transferring data where the transfer is necessary to safeguarding important public interests. Firstly, the need for the transfer is not proven and secondly it does not seem acceptable that a unilateral decision taken by a third country for reasons of its own public interest should lead to the routine and wholesale transfer of data protected under the directive.

– Lastly, it appears to be difficult to consider the transfer as necessary in order to protect the vital interests of the data subject.

Directive 95/46/EC does, however, authorise the transfer of personal data by derogation of the condition of adequate level of protection provided by the third country where the controller (recipient) offers sufficient guarantees for protection of the data.

A dialogue could therefore be usefully entered into between European Member States and the US authorities with a view to finding a solution that guarantees adequate protection for the data transmitted. A common approach at EU level would be appropriate.

2.6 Specific issues on the communication and access to PNR data processed in automated reservation systems or departure control systems

The remarks made on this point supplement the remarks made above.

2.6.1 Direct electronic connections between US Customs and reservation and departure control systems

In cases where it is envisaged that US Customs would be able to directly access information systems on the European territory and call up or collect data, rather than be the recipients of conventional transborder data flow, the entire directive could be considered as being directly and completely applicable to them. Article 4(1)(c) defines the application of the directive where the controller is not established on Community territory and, for the purpose of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of a Member State[17]. However the application of the directive as a whole raises numerous questions.

2.6.2 Data relating to persons not travelling to the United States

Data concerning passengers not travelling to the United States are not relevant and may therefore not be transmitted except in the framework of specific justice and home affairs agreements (mutual assistance).

2.6.3 Sensitive data

PNR may contain data that may reveal racial or ethnic origin, religious beliefs, or other sensitive data in the meaning of article 8 of Directive 95/46/EC. Directive 95/46/EC in principle prohibits any processing of sensitive data, save with specific authorisations (explicit consent to processing for a given purpose, data of an obvious public nature etc.). Recourse to consent creates many problems as described above, which should be considered with even greater attention given the highly sensitive nature of these data[18].

Article 8(4) of the directive authorises Member States or supervisory authorities to lay down other exemptions, for reasons of substantial public interest and subject to the provision of suitable safeguards. Provided that these conditions are adhered to, Member States could consequently authorise the transfer of sensitive data contained in the PNR[19].

2.6.4 Processing of data by reservation and departure control systems (DCS)

In addition, the issue of access to PNR at the request of the US authorities raises, from the outset, the issue of the legitimacy of data processing carried out in reservation and

---

17 The 20th recital of Directive 95/46/EC stipulates that the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive and that, in such cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in the directive are respected in practice. In an opinion recently expressed, focusing on the interpretation of the scope of Article 4(1)(c) of the directive (Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites - 30 May 2002), the Article 29 Working Party pointed out that it is not necessary that the controller exercise full control over the equipment, but he should determine which data are collected, stored, transferred, altered etc. and for which purpose.

18 According to Article 8, 2a of the directive, the laws of the Member State may provide that the prohibition to processing data mentioned in article 8, 1 of the directive may not be lifted by the data subject giving his consent.

19 Article 13 of the directive continues to apply.

departure control systems[20]. In particular, the data can only be processed if they are adequate, relevant and not excessive in relation to the purposes for which they are processed. Personal data should no longer be processed in reservation systems since they are no longer being used for the journey for which they were recorded.

2.7 Transfers of biometric data

The transfer of biometric data is submitted to the provisions of Directive 95/46/EC. It should be noted that this directive requires Member States to determine the conditions under which any identifier of general application may be processed. Biometric identifiers permit identification solely of individuals and could be targeted by this provision[21].

Conclusions

1. The Working Party is aware that sovereign States do have discretion over the information that they can require from persons wishing to gain entry to their country. However, the current proposals concerning the APIS system, though developed in the context of terrorist atrocities, would lead to the disproportionate and routine disclosure of information by airlines who are subject to the requirements of Directive 95/46/EC. This information could be used for routine purposes related to immigration, customs as well as more generally for US national security and may at least be shared amongst all US federal agencies.

2. In the light of the recent development of the APIS system, the Working Party is of the opinion that the compliance with the US requirements creates problems in respect of Directive 95/46/EC. Most issues at stake are beyond the competence of airline companies and should be addressed by the Member States and as necessary by the Commission.

3. On substance, the Working Party is of the opinion that the transfers of data relating to persons not travelling to the United States should be ruled out except under specific co-operation agreements concerning justice and home affairs.

4. Other transmission of data from reservation and departure control systems relating to passengers and cabin crew could only be envisaged in accordance with the legislation of the Member States.

   This legislation should provide that any necessary restrictions on the rights and obligations of Directive 95/46/EC be in accordance with Article 13 of the directive, and that guarantees for individuals are in place.

   A common approach at EU level should be sought.

---

[20] See Recommendation 1/98 on Airline Computerised Reservation Systems, which also mentions archiving data for a certain time to settle disputes and process data relating to frequent flyers after obtaining the consent of the data subjects. The Article 29 Working Party in principle advocates storing data on-line for 72 hours only and destroying it within no more than three years (with limited access to requests for investigation) or even longer (only for compliance with a legal obligation).

[21] The Working Party is presently discussing the issue of biometrics data.

5. Transfers of data that may be considered as sensitive data should be approached with greater caution. Such transfers also presuppose that proof can be supplied that there are 1) reasons of substantial public interest to Member States, 2) suitable guarantees and that 3) national legislation or a decision of the supervisory authority is required.

6. Where direct access by US Customs and US Immigration and Naturalization Service is additionally envisaged with regard to data in reservation and departure control systems, these authorities are committed to ensuring respect for the directive as a whole.

7. The system should be negotiated with the US authorities. Discussions should, in particular, focus on clarifying and defining objectives, finalities and the recipients of the data, on the categories of data which may be transferred having taken account of these explanations and on the conditions and guarantees surrounding the processing of personal data, in particular, disclosing them to the US federal authorities (and if so, limiting disclosure to law enforcement authorities).

8. A comprehensive approach should be taken when addressing the transfer of personal data from airlines to the United States. It would first be necessary to take account of other existing or planned transfers to the United States. It would be particularly necessary to incorporate the concept of the third pillar. In essence, data transfers made to the public authorities of third countries for reasons of public order in this country should be understood in the context of cooperation mechanisms set up under the third pillar (judicial and police cooperation). In addition, these mechanisms should go hand-in-hand with guarantees for the protection of transferred data[22]. It appears to be important for the co-operation mechanisms laid down in the third pillar not to be circumvented via the first pillar. Finally, the solution arrived at for data transfers to the United States could be appropriate to serve as a model for transfers through APIS to other third countries.

Done at Brussels, 24 October 2002

For the Working Party

The Chairman

Stefano RODOTA

[22] Personal data is exported by Member States for the purpose of judicial and police cooperation. Data is being transferred by Europol to examine the events of 11 September 2001 as part of an exceptional procedure and discussions are being held to set up cooperation on a stable basis in accordance with the requirements of the Europol Convention (Article 18). See also the Eurojust Decision (Article 27) and, finally, the negotiations currently being held on Article 38 of the Treaty.