I

*(Resolutions, recommendations and opinions)*

OPINIONS

# EUROPEAN DATA PROTECTION SUPERVISOR

## Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on a code of conduct for computerised reservation systems

(2008/C 233/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 20 November 2007 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

### I. INTRODUCTION

#### Consultation of the EDPS

1. The Proposal for a Regulation on a code of conduct for computerised reservation systems was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001 (hereinafter 'the proposal').

2. The proposal concerns the processing of passenger data by computerised reservation systems (hereafter CRSs) and is closely related to other schemes of collection and use of passenger data, within the EU or in relation with third countries. These schemes present a high interest for the EDPS, who welcomes the consultation of the Commission.

#### The proposal in its context

3. The objective of the proposal is to update the provisions of the code of conduct for Computerized Reservation Systems that was established in 1989 by Council Regulation (EEC) No 2299/89. The code appears to be increasingly ill-adapted to the new market conditions, and would need simplification in order to reinforce competition — while maintaining basic safeguards, and ensuring the provision of neutral information to consumers.

4. The main focus of the proposal is not on protection of personal data. However, considering that CRSs do process a vast amount of personal data, a specific Article on data protection has been developed in the proposal, with a view to complementing the provisions of Directive 95/46/EC which continues to apply as a *lex generalis*.

5. Other provisions in the proposal also have an impact on data protection, even if their main objective is to ensure equal information to all actors involved in a fair competition perspective: the protection of the identity of subscribers, being natural persons or undertakings, is also welcome in terms of privacy protection.

6. The EDPS notes that the proposal only addresses the activities of CRSs in their quality of interface between airlines and travel agents. It does not cover the provision of other IT services like the hosting of the reservation system of airlines. Personal data processed in this distinct context will therefore not benefit from some safeguards provided for in the code of conduct. They will nevertheless be covered by the general data protection regime of Directive 95/46/EC.

### Focus of the opinion

7. The opinion of the EDPS will start with the scope and conditions of application of the proposal in relation with the application of Directive 95/46/EC. It will then focus on substance, with the analysis of the Articles of the proposal related to data protection issues. Positive aspects are identified, and possible improvements also suggested. Specific attention will be given to the conditions of enforcement of these provisions.

8. As a last point, the opinion will extend beyond the concrete provisions of the proposal, and address some wider implications of the processing of passenger data by CRSs, be it in their capacity of interface for travel agencies or as IT service providers. Access by third countries to passenger data held by CRSs will be subject to a specific analysis.

## II. SCOPE AND CONDITIONS OF APPLICATION

9. The proposal includes detailed provisions on the protection of personal data. These provisions 'particularise and complement' those of Directive 95/46/EC, and are without prejudice to the provisions of the said Directive ([1]). This explicit relationship between the two instruments is a positive element.

10. However, the EDPS notes that the scope of application of the code of conduct is not identical to the scope of Directive 95/46/EC. Indeed, the determining criterion for application of the code of conduct is the *use or offering for use of the system* in the territory of the EU ([2]). The provisions of the Directive apply when the controller is *established* in a Member State, or when the controller is established outside the EU but *makes use of equipment* situated in the EU ([3]).

11. Different scenarios could therefore be envisaged with regard to the application of the code of conduct and the Directive:

— when the CRS is established in the EU, both the code of conduct and the Directive will apply as the criteria of these two texts are fulfilled,

— when the CRS is established outside the EU, the offering of services in the EU, and the use of equipment in the EU will determine the application of both legal instruments.

Although the criteria for application of the code of conduct and the Directive are different, in practice they should result in the combined application of the two instruments: *offering of CRS services in the EU* will trigger the application of the code of conduct, and this offering of services will in practice take place through the use of (computer) equipment situated in the EU, which will also have as a consequence the application of the Directive.

12. Another consequence of the broad scope of application of the code of conduct and the Directive is their impact on airlines, which can be established inside or outside the EU. Airlines established outside the EU are in principle not subject to European data protection principles, except if they *make use of equipment situated in the EU* to process personal data (application of the Directive). This would be the case e.g. if they make use of a CRS established in the EU in its quality of 'host' for a reservation service. It should be noted as well that data related to airline flights will be subject to EU legislation as soon as they are processed by a CRS established in the EU — or offering services within the EU (application of the code of conduct).

## III. ANALYSIS OF THE PROPOSAL

### Basic data protection principles

13. Article 11 of the proposal provides for a list of guarantees relating to the processing of personal data, including purpose limitation, necessity of the data, specific protection of sensitive data, limited storage, information and access rights of the data subjects.

14. Article 11 also gives a welcome precision on the quality of CRSs, which are to be considered as data controllers with regard to the making of reservations or issuing of tickets for transport products. Data subjects will therefore be able to exercise their rights not only towards travel agents or air carriers, but also towards CRSs, where appropriate.

15. The obligation for participating carriers and intermediaries to ensure the accuracy of data (although not limited to personal data), as provided for in Article 9, is an explicit reference to Directive 95/46/EC, according to which personal data must be accurate.

16. It must be noted that these provisions of the proposal are in line with the remarks made by the Article 29 Working Party in its Recommendation No 1/98 ([4]). They are all the more welcome in that they specify some provisions of Directive 95/46/EC: reference is made in particular to the limited storage period of personal data off-line (72 hours) and the deletion of the information after three years, with limited conditions of access linked with the original purpose of the processing (billing dispute resolution). The transparency of the processing is also foreseen, with indication by the subscriber of the contact details of the system vendor and information on the exercise of access rights.

([1]) Article 11, paragraph 9 of the proposal.
([2]) Article 1 of the proposal.
([3]) Article 4, paragraph 1, subparagraph (a) and (c) of Directive 95/46/EC.
([4]) Recommendation of 28 April 1998 on Airline Computerised Reservation Systems, WP10.

17. In addition to these elements already included in the proposal, the latter could be completed with regard to three aspects.

**Sensitive data**

18. Firstly, with regard to the possibility for the data subject to consent to the processing of sensitive data, it should be explicitly stated that the consent must be based on adequate information. Although Article 2, subparagraph (h) of Directive 95/46/EC implies that any consent should be *'freely given, specific and informed'*, this may not always happen in practice. Article 11, paragraph 3, could thus be completed as follows: '… such data shall only be processed where the data subject has given his explicit consent to the processing of those data *on an informed basis*'.

**Security measures**

19. Secondly, with regard to security issues, it is assumed that the general principles of Directive 95/46/EC will apply. The EDPS would recommend complementing these principles with obligations more directly focussed on the particularities of personal data processed by CRSs. Since CRSs can act as a global interface for airlines, but also as a service provider or 'host' for a specific airline, the large quantity of data processed with regard to these two different functions should be clearly isolated, using 'Chinese' walls and other appropriate security measures. The EDPS recommends adding this as an additional paragraph in Article 11.

20. Article 11 could thus be completed with a new paragraph after paragraph 4 that would read as follows: '*Where a CRS operates databases in different capacities such as interface or host for airlines, technical and organisational measures must be taken to prevent interconnection between the databases, and to ensure that personal data are only accessible for the specific purpose for which they were collected*'.

**Marketing information**

21. Thirdly, the EDPS welcomes the conditions put in Articles 7 and 11(5) to the processing of data in a market analysis perspective. These data can only be provided by system vendors to third parties in a non identifiable format, be they about organisations, companies or natural persons. While the objective here is mainly to prevent the identification of travel agents ([1]), it is assumed that anonymisation concerns any kind of personal data processed in the course of a reservation, thus also personal data of clients of travel agents. This should be specified in the proposal, by completing Article 11(5) as follows: '*Anonymisation shall apply to all data subjects involved in the reservation procedure, including the final consumer*'.

([1]) Explanatory Memorandum, 5. Additional information. 'Detailed explanation of the proposal'.

## IV. **ENFORCEMENT**

22. As a consequence of the broad scope of application of the Regulation, the competence of the Commission and Data Protection Authorities to ensure the compliance of actors involved, extends to data controllers established outside the EU. It is essential that the Commission, explicitly mentioned in the proposal as responsible for the enforcement of the code of conduct, will have effective means to ensure compliance with data protection principles.

23. To ensure an effective enforcement of the code of conduct, control and traceability of personal data within the CRS network should be ensured. Personal data are indeed transmitted and accessed by different actors, like airlines, travel agencies, and are processed by CRSs in different qualities, acting or not on behalf of the airlines.

24. In addition to the need for a clear distinction between the different activities of CRSs, a scheme of data flows within the system appears to be a prerequisite in order to have a clear picture of the circulation of personal data between airlines, travel agencies and CRSs. This is essential in order to assess the competence of the different enforcement authorities (DPAs and Commission).

25. This is all the more needed considering the fact that CRSs are interconnected, and in view of the complexity of the CRS network. The extent to which e.g. personal data entered via an airline or a travel agency, client of a CRS, can be accessed and processed at a different stage via a CRS, distinct from the original one, must be made clear.

26. According to Article 12 of the proposal, the Commission will be competent to initiate enforcement procedures in case of infringement of the Regulation. The competence of the Commission will therefore include, among others, control of compliance with data protection principles included in the Regulation.

27. While doing so, its role may compete with national data protection authorities, in so far as the activities of a CRS or system vendor falls within the scope of a national data protection legislation. Coherent procedures of enforcement and mutual collaboration should be ensured in such a case. The Article 29 Working Party could be an appropriate forum to facilitate such coordination.

28. Besides, in the course of the exercise of its competences, the Commission will handle specific files including all the elements of an alleged infringement (e.g. access to the files by the concerned parties being addressed in Article 15 of the proposal). Personal data will inevitably be included in these files, which would imply the competence of the EDPS to supervise the processing, as an aspect of his tasks with regard to the European Institutions in accordance with Regulation (EC) No 45/2001, like for all other cases where the Commission acts as a data controller.

## V. ACCESS TO PASSENGERS' DATA BY THIRD COUNTRIES

29. Access to passengers' data by third countries has led to the conclusion of specific agreements between the European Union and these third countries and in particular an agreement concluded between the EU and Canada in July 2005, and between the EU and the United States in July 2007. According to these agreements, PNR data communicated to foreign authorities by airlines must comply with specific conditions in relation with data protection.

30. The role of CRS in this context would be different, depending on their quality of host or interface for the airlines.

### CRS as host for the airlines

31. As already mentioned, airlines that do not manage their own reservation system are used to outsource it to a third party that can be a CRS. The CRS does not act here in its capacity of interface for travel agents, but as a service provider for the airline. In this 'host' capacity, the CRS might communicate PNR information to the authorities of a third country.

32. According to the Commission ([1]), this activity of CRS does not fall within the scope of the Regulation, and its obligations with regard to transfers to third parties are therefore not violated in these circumstances. However, the general data protection principles of Directive 95/46/EC remain applicable, as well as those of the Council of Europe's Convention No 108 as far as the conditions of transfer to third countries are concerned.

33. The EDPS considers that the entities providing such IT services are responsible for the service they offer and for the further transfer of data to a third party. In that sense, they should be considered as co-controllers with the airlines concerned with regard to the service provided. This implies that the transfer of passenger data by a service provider — be it a CRS or another IT service provider — to a third country must comply with the conditions of any international agreement concluded with that country.

([1]) Decision C(2005) 652/1 on the compatibility of US access to Passenger Name Record (PNR) with Regulation (EEC) No 2299/89 on a code of conduct for computerized reservation systems.

34. Obligations might include the resolution of practical issues, such as the modalities of transfer of data and the transition from 'push' to 'pull', implying that the IT service controls the conditions of transfer and the quality of data transferred. Transparency obligations should also be taken into account, in concertation with airlines and to the extent airlines' reservation services are effectively performed by the IT service. Redress against the CRS should also be available to the data subject in relation with the processing of data performed by the CRS in this context of transfer to a third party.

### CRS acting as interface

35. Independently of the situation where CRSs act in their capacity of service provider and have to take into account international agreements concluded between the EU and third countries, one should also envisage the case where CRSs act in their quality of interface: in this case, any request for personal data from a third party falls within the conditions of the Regulation, and in principle the transfer should not be allowed. Indeed, according to Article 11(4) of the proposal, access to CRS data is allowed only for billing dispute reasons. Important is the fact that this provision applies independently of the situation of the CRS (be it situated in the EU or in the United States), as far as services are offered for use in the territory of the Community.

## VI. CONCLUSION

36. The EDPS welcomes the inclusion in the proposal of data protection principles that specify the provisions of Directive 95/46/EC. These provisions enhance legal certainty, and could usefully be complemented by additional safeguards on three points: ensuring the fully informed consent of data subjects for the processing of sensitive data; providing for security measures taking into account the different services offered by CRSs, and the protection of marketing information (see points 18-21 of this opinion).

37. With regard to the scope of application of the proposal, the criteria that make the proposal applicable to CRSs established in third countries raise the question of its practical application, in a coherent way with the application of the *lex generalis*, i.e. the Directive 95/46/EC (see points 9-12).

38. To ensure the effective implementation of the proposal, the EDPS considers that there is a need for a clear and comprehensive view on the whole CRSs problematic, taking into account the complexity of the CRS network and the conditions of access by third parties to personal data processed by CRSs.

39. Even if these issues go beyond the concrete provisions of the proposal, it is nevertheless deemed as essential to put the CRS question in its global context and to be aware of the implications and the challenges of having such a large amount of personal data, some of them sensitive, processed in a global network practically accessible to third State authorities.

40. It is therefore decisive that effective compliance is ensured, not only with regard to competition aspects of the proposal but with regard to data protection principles, by authorities competent for enforcement, i.e. the Commission, as foreseen in the proposal, and Data Protection Authorities (see points 22-35).

Done at Brussels, 11 April 2008.

Peter HUSTINX

*European Data Protection Supervisor*