



FACILITATION (FAL) DIVISION — TWELFTH SESSION

Cairo, Egypt, 22 March to 2 April 2004

Agenda Item 2: Facilitation and security of travel documents and border control formalities

2.4: Advance passenger information (API)

HARMONIZATION OF CRITERIA FOR PASSENGER NAME RECORD (PNR) ACCESS

(Presented by the Switzerland)

SUMMARY

This working paper presents to the Division a proposal from Switzerland on a common approach to PNR access requirements, recognizing the need to find harmonization on an international level.

Action by the Division is in paragraph 4.

1. BACKGROUND AND PURPOSE

1.1 Since the terrorist attacks of 11 September 2001, all States have increased their efforts in security. As a part of this process, some States wish to obtain personal data of passengers before they enter into their territory. Before this date, airlines had been transmitting Advanced Passenger Information (API) electronically to the States who had implemented this procedure in order to facilitate the immigration process of their passengers at their borders.

1.2 In order to accomplish their mission of preventing and combatting terrorism and other serious criminal offences and protecting the own borders, authorities may deem it necessary to require additional data of passengers going beyond the API requirements. In such cases it has to be assured that authorities who set up such requirements do not violate national laws of other States when implemented.

2. CATEGORIES OF DATA TRANSMITTED

2.1 Passenger Name Record (PNR) files are stored in the airlines' reservation and departure control databases and allow all the different agents within the air industry – from the travel agent and the computer reservation systems to the air carrier and the handling agents at the airports – to recognize each passenger and have access to all relevant information related to his/her journey, namely departure and return flights. Furthermore, they may contain information concerning frequent flyer programmes, data concerning needs for special assistance on board or special wishes concerning meals, from which conclusions can be

drawn relating to the medical condition, religion, etc. of a passenger. It has to be stressed that the information contained in a PNR is more detailed and goes far beyond that which is contained in an API message.

2.2 Due to their sensitive character, some of these PNR data need highest protection under general provisions of data protection legislation. Therefore the balance between the rights of a passenger not to disclose such information and the interest of agencies of certain third States has to be carefully taken into consideration.

3. POINTS FOR CONSIDERATION

3.1 Huge volumes of personal data (including travel data) are transferred across international boundaries between States every day by the data control systems of the air carriers. However, most national laws require that personal data can be transferred only to States which provide minimal adequate privacy protections for that data. Today air carriers are confronted with two contradictory requirements: On the one hand national data protection legislations require appropriate measures to protect personal data, on the other hand, some receiving States are asking access to PNR data as a prerequisite for granting landing permissions in their territory. Therefore it is urgent and of highest importance that all requirements for PNR access be dealt with according to internationally harmonized standards. This would allow the transmission of such data in a way that is compatible with minimal requirements of data protection on the one hand, and which grants to carriers concerned a worldwide uniform system to be applied when granting access to PNR on the other hand.

3.2 In order to be able to transfer data freely with privacy protection assured, a framework of privacy protection which is consistent with international standards should be put in place by States requiring PNR access.

3.3. As a prerequisite, a number of basic issues has to be considered. These include the following:

- a) The purpose of requiring PNR data has to be clearly defined and the use of such data has to be restricted (e.g. combat of terrorism).
- b) PNR comprises an extensive amount of data which varies from State to State. In view of this large, multifarious amount of data involved, all data cannot be considered to be adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed. There is a need of having a standardized sample of data which may be contained in the part of the PNR to which access shall be granted.
- c) The PNR data will be mainly used by agencies involved in anti-terrorism measures. These agencies may consider to share the information contained in the PNR with other agencies interested in access such as immigration authorities; and in case such access to PNR data should be granted, it is of particular interest to determine clearly
 - 1) the circle of recipients;
 - 2) the purpose for which access shall be granted; and
 - 3) the conditions under which access shall be granted.
- d) The storage of data has to be respected within the framework of purpose limitation. Therefore the period of storage should be defined and data deleted after expiration of the term.

- e) Passengers whose PNR data were disclosed must have the necessary information for ensuring a fair processing of data. In order to adjust incorrect data entries, appropriate provisions have to be developed and passengers have to be informed in due time in order to enable them to correct their PNR data, which were disclosed by the carrier.
- f) There are two options for access to PNR; either the authorities from the State requiring the data can enter the system and collect the data themselves (“pull”), or the air carriers bound to provide data can select and send what is required (“push”). In order to avoid further confusion and facilitate the transmission, the way of giving access to PNR data should be harmonized as much as possible. From a data protection point of view, the “push”-system would be much more appropriate, since it grants a higher degree of protection.

4. ACTION BY THE DIVISION

4.1 The Division is invited to agree that there is an urgent need for a harmonized approach to PNR access and to adopt the following recommendation:

Recommendation B/ —

It is recommended that ICAO develop guidance material for those States that may require access to Passenger Name Record (PNR) data to supplement identification data received through an API system, including guidelines for distribution, use and storage of data and a composite list of data elements which may be transferred from the operator to the receiving State.

4.2 The Division is further invited to adopt a new Standard regarding PNR access as follows:

Recommendation A/ —

3.34.1 Contracting States requiring Passenger Name Record (PNR) access to supplement information received through API shall conform their data requirements and their handling of such data to guidelines developed in ICAO.

— END —