International Civil Aviation Organization

INFORMATION PAPER

FALP/7-IP/9
12/10/12
English only

FACILITATION PANEL (FALP)

SEVENTH MEETING

Montréal, 22-26 October 2012

Agenda Item 4: Developments on Advance Passenger Information (API) and Passenger Name Record (PNR) data

DATA PROTECTION

(Presented by the Secretary)

1. INTRODUCTION

1.1 In 2010, the 37th Session of the ICAO Assembly, in Resolution A37-17, *Consolidated statement on the continuing ICAO policies related to the safeguarding of international civil aviation against acts of unlawful interference*, at Appendix C, called upon Contracting States to examine the "further use of Advance Passenger Information (API) provided by air carriers, to reduce the risk to passengers, while ensuring the protection of privacy and civil liberties." Additionally, in its *Declaration on Aviation Security*, the Assembly urged Member States to enhance international cooperation to counter threats to civil aviation by, *inter alia*, promoting the increased use of "cooperation mechanisms for information exchange" and for early detection and dissemination of information on security threats to civil aviation, including through the "collection and transmission of advance passenger information (API) and passenger name record (PNR) data, as an aid to security, whilst ensuring the protection of passengers' privacy and civil liberties."

1.2 In September 2012, the High-level Conference on Aviation Security (HLCAS) noted that the collection and transmission of PNR data is increasingly being deemed important for the threat assessment value that can be derived from data analysis, in relation to the fight against terrorism. It emphasized that in the exchange of such data, due regard should be given to the protection of individual rights and privacy. The Conference recommended that States should align the various data exchange systems that currently exist with the international data transmission standards adopted by relevant United Nations agencies, while ensuring the protection of the privacy and civil liberties of passengers.

1.3 As a follow-up of the Assembly's resolutions and the HLCAS's recommendation, the Secretariat conducted a general review of existing documentation on the security and integrity of PNR and API data and its protection. The Appendix contains basic reference material on the matter, for information of the FAL Panel.

— — — — — — — —

APPENDIX

1. Extracts from ICAO Doc 9944, *Guidelines on Passenger Name Record (PNR) Data*

[. . . . .]

2.1.9 PNRs should not contain any information that an aircraft operator does not need to facilitate a passenger's travel, e.g. racial or ethnic origin, political opinions, religious or political beliefs, trade-union membership, marital status or data relating to a person's sexual orientation. Contracting States should not require aircraft operators to collect such data in their PNRs.

2.1.10 PNRs may contain data, e.g. meal preferences and health issues as well as free text and general remarks, legitimately entered to facilitate a passenger's travel. Some of these data may be considered sensitive and require appropriate protection. It is particularly important that carriers and States protect these data. Although they can be relevant in determining the risk that a passenger might represent, such data should be taken into consideration only if concrete indications exist which require the use of such data for the purposes listed in 2.2.2 a) to d).

[. . . . .]

2.4.1 The requirement for PNR data transfer should be governed by explicit legal provisions. The reasons for requiring PNR data should be clearly expressed in the appropriate laws or regulations of the State or in explanatory material accompanying such laws or regulations, as appropriate.

2.4.2 States should ensure that their public authorities have the appropriate legal authority to process the PNR data requested from aircraft operators, in a manner that observes these guidelines. States are invited to forward the full text of such legislation to ICAO for online dissemination to other States for information. All queries arising from such legislation should be addressed to the State and not to ICAO.

[. . . . .]

2.5.1 As seen in section 2.1, PNRs can contain an extensive amount of data. States should limit their requirements to the transfer of those PNR elements which are necessary and relevant for the purposes listed in section 2.2. . . . .

[. . . . .]

2.6.2 It is particularly important that these data be protected, and therefore a State obtaining PNR information should, as a minimum:

a) limit the use of the data to the purpose for which it collects them;

b) restrict access to such data;

c) limit the period of data storage, consistent with the purposes for which data are transferred;

d) ensure that individuals are able to request disclosure of the data that are held concerning them, consistent with 2.14.3 of these guidelines, in order to request corrections or notations, if necessary;

e) ensure that individuals have an opportunity for redress (2.14.4 refers); and

f) ensure that data transfer protocols and appropriate automated systems are in place to access or receive the data in a manner consistent with these guidelines.

[. . . . .]

2.9 FILTERING OF PNR DATA

2.9.1 The State requiring PNR data should consult with operators providing these data regarding the most efficient method(s) for the filtering of data taking into full consideration available technological solutions and applicable laws or regulations (2.4.3 also refers).

2.9.2 Appropriate mechanisms should be installed to ensure that only required PNR data elements are pushed by the aircraft operator to, or pulled by, the relevant State authorities.

2.9.3 States may decide whether the filtering will take place within the individual systems of aircraft operators or of their authorized agents or within the system of the receiving State. States may also consider whether a regional filtering system under the control of interested operators should be developed.

2.10 STORAGE OF PNR DATA

PNR data should be stored by the receiving State for no longer than is reasonably necessary for the stated purposes related to their collection by the State and for auditing or redress purposes, in accordance with its laws.

2.11 ONWARD TRANSFER

2.11.1 Appropriate safeguards for limiting the onward transfer of PNR data only to authorized public authorities should be put in place. Such safeguards should take account of agreements or undertakings entered into with the State from which the data are transferred.

2.11.2 When PNR data acquired by one State are to be transferred to another, the purposes for such onward intergovernmental transfer or sharing should be consistent with those set out in 2.2.2, and the conditions under which such a transfer will take place should be resolved during the process contemplated in 2.4.4 and 2.4.5. States should bear in mind that the onward transfer of data could expose the aircraft operator to civil liabilities.

2.12 PNR DATA PROTECTION: GENERAL PRINCIPLES

2.12.1 A State should ensure that each public authority with access to PNR data provide an appropriate level of data management and protection.

2.12.2 Where no national data protection legislation is in place, States should have procedures in place to protect a passenger's PNR data. Using these guidelines as a basis, as appropriate, States should develop data protection laws or regulations concerning PNR data transfer and data processing.

2.12.3 A reasonable balance should be achieved between the need to protect a passenger's PNR data and a State's prerogative to require disclosure of passenger information. Accordingly, States should not unduly restrict PNR data transfer by aircraft operators to relevant authorities of another State, and States should ensure that a passenger's PNR data are protected.

2.13 SECURITY AND INTEGRITY OF PNR DATA

2.13.1 States should put in place regulatory, procedural and technical measures to ensure that the processing of PNR data for the purposes identified in section 2.2 is carried out in accordance with appropriate safeguards, notably with respect to the security, authenticity, integrity and confidentiality of the PNR data. Precautions should also be taken against the misuse or abuse of the data by State authorities.

2.13.2 States should ensure that their PNR data computer systems and networks are designed to prevent aircraft operators from having access through these systems to the data or information systems of another operator.

2.13.3 To prevent the unauthorized disclosure, copying, use or modification of data provided to a State, a receiving State should restrict access to such information on a "need-to-know" basis and use recognized security mechanisms, such as passwords, encryption or other reasonable safeguards, to prevent unauthorized access to PNR data contained in its computer systems and networks.

2.13.4 A State should, pursuant to its national laws or regulations, maintain a system of database control that provides for the orderly disposal of PNR data received.

2.13.5 Under the "pull" method, PNR access systems operated by State authorities should be so designed that they do not adversely affect the normal operation or security of aircraft operators' systems. The access systems should also be designed such that operators' data cannot be modified or other actions undertaken that would threaten the integrity of operators' data or their systems (i.e. they are "read-only" systems).

2.13.6 States should ensure that an appropriate audit programme is in place to monitor the transfer, removal and destruction of PNR data from their databases. Audit system access should be limited to authorized users.

2.14 TRANSPARENCY AND PASSENGER REDRESS

2.14.1 An aircraft operator or its agent should provide adequate notice to passengers (for example at the time of booking of a flight or purchase of the ticket) that the operator might be required, by law, to provide the public authorities of a State with any or all of the passenger PNR data held by the operator in relation to a flight to, from, or in transit through an airport within the territory of the State and that the information might be passed to other authorities when necessary to satisfy the State's purpose for acquiring the information. This notice should also include the specified purpose for obtaining the information as well as appropriate guidance to passengers on how they might access their data and seek redress.

2.14.2 Model passenger information/notice forms that operators might wish to use are found in Appendix 2 to these guidelines.

2.14.3 States should provide for appropriate mechanisms, established by legislation where feasible, for passengers to request access to and consult personal information about them and request corrections or notations, if necessary.

2.14.4 Redress mechanisms should be set up to enable passengers to obtain adequate remedy for the unlawful processing of their PNR data by public authorities.

[. . . . .]

2. Extracts from the WCO/IATA/ICAO Guidelines on Advance Passenger Information (2010)

[. . . . .]

8.1. Data privacy and data protection legislation have been enacted in many countries in recent years in order to protect the individual's right to privacy and to allow individuals to have access to their own personal data held in computer systems and databases in order to verify its accuracy.

8.3. This legislation can vary from country to country. However, there is a large degree of commonality of provisions of such legislation. Data privacy and data protection legislation typically requires that personal data undergoing automated (computer) processing:

- should be obtained and processed fairly and lawfully;
- should be stored for legitimate purposes and not used in any way incompatible with those purposes;
- should be adequate, relevant and not excessive in relation to the purposes for which they are stored;
- should be accurate and, where necessary, kept up to date;
- should be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which that data is stored.

8.4. Such legislation also usually incorporates provisions concerning the right of access by data subjects to their own personal data. There may also be provisions regarding disclosure of personal data to other parties, and about transmission of such data across national borders and beyond the jurisdiction of the country in which it was collected.

8.5. It is clear from the above that the existence of such legislation may well have an impact on a carrier’s ability to capture personal details of passengers and to transmit this data to a foreign government. However, it is also clear that the nature of API data (basic personal information that appears in an official document) and the use to which it is put, should conform to the national law of most countries. The long-term archiving of passenger manifests on computer media and the use of such data for purposes other than national security or passenger clearance may pose problems in certain countries.

8.6. Because of the differences in the provisions and interpretation of data privacy laws from country to country, carriers being required to participate in API should enquire on a case-by-case basis whether the capture, storage and transmission overseas of the passenger details mentioned in this Guideline is in contravention of national law. Where such contravention is determined, the country requiring the API data should, to the best of its abilities, seek to address and resolve those legal concerns.

[. . . . .]

3. Other sources of guidance

3.1 Other sources of guidance in this area include, but are by no means limited to the following:

a) *IATA Recommended Practice 1674* (from the Cargo Services Conference Resolutions Manual) on the Protection of privacy and transborder data flows of personal data used in international air transport of passengers and cargo (32nd edition, 2011);

b) *ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management in an organization* (intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to build confidence in inter-organizational activities); and,

c) *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security* (8 December 2011), including, amongst other things, requirements relating to the handling and use of personal sensitive data (Art. 6), data retention (including time periods and uses and depersonalization in connection with law enforcement operations) (Art. 8), and redress for individuals (Art. 13). (This Agreement provides clauses relating to the range of issues concerning the protection of data and privacy.)

— END —