International Civil Aviation Organization

WORKING PAPER

A40-WP/530
EX/226
10/9/19
(Information paper)
English only

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Facilitation Programmes

STANDARDS AND PRINCIPLES ON THE COLLECTION, USE, PROCESSING AND PROTECTION OF PASSENGER NAME RECORD (PNR) DATA

(Presented by Finland on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2])

EXECUTIVE SUMMARY

More and more States are setting up Passenger Name Data (PNR) systems and requiring air carriers to transfer PNR data to them. This paper sets out our position on core principles compliance with which would ensure respect for the regulatory requirements concerning fundamental rights to privacy and data protection when processing PNR data for the purposes of countering terrorism and serious crime. These principles are increasingly shared by countries around the world and form part of various regional and global arrangements such as the Ibero-American Data Protection Standards or the Council of Europe Convention 108 as the only binding international agreement on data protection.

Strategic Objectives:	This working paper relates to Strategic Objective — *Security and Facilitation*.
Financial implications:	Not applicable.
References:	Annex 9 — *Facilitation*

1. INTRODUCTION

1.1. Passenger Name Record (PNR) data – information provided by passengers, collected by and held in the carriers' reservation and departure control systems for their own commercial purposes - is

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, North Macedonia, Norway, San Marino, Serbia, Switzerland, Turkey and Ukraine.

increasingly being used for law enforcement purposes globally as a tool to prevent and counter continuing security threats. The processing of PNR data has been recognised by European countries as well as the United Nations (UN) and its Member States as a powerful tool to fight terrorism and serious crimes. Identifying and tracing suspicious travel patterns by processing PNR to gather evidence and, where relevant, find associates of criminals and unravel criminal networks is proving essential to prevent, detect, investigate and prosecute terrorist and serious crime offences.

1.2. According to UN Security Council Resolution 2396 (2017), Member States shall develop the capability to collect, process and analyse, in furtherance of ICAO standards and recommended practices, PNR data, with full respect for human rights and fundamental freedoms.[3] The Resolution also encourages Member States to share PNR data with relevant or concerned Member States to detect foreign terrorist fighters returning to their countries of origin or nationality, or traveling to a third country. In addition, ICAO was urged to work with the Member States to establish a standard for the collection, use, processing and protection of PNR data. In this context, ICAO has set up a Task Force which will provide input to the development of such a PNR standard.

1.3. A growing number of States are requiring airlines to provide PNR data in order to detect and trace the travel routes of criminal and terrorist networks using international air travel, while ICAO is taking steps to review and complement the existing standards, recommended practices and additional guidance on the collection, use, processing and protection of PNR data.

1.4. In this context, we invite the Assembly to ensure that the principles outlined in this paper are embedded in any future ICAO standard(s), and reaffirm the need for Contracting States seeking to establish a PNR system to adhere to such principles. These principles are increasingly shared by countries around the world and also from part of various regional and global arrangements such as the Ibero-American Data Protection Standards or the Council of Europe Convention 108 as the only binding international agreement on data protection.

2. PRINCIPLES UNDERPINNING A GLOBAL STANDARD FOR THE COLLECTION, USE, PROCESSING AND PROTECTION OF PNR DATA

2.1 General

PNR data are personal data of passengers collected by airlines for their business purposes, unlike other travel-related data collected on behalf of Governments such as Advance Passenger Information. Such data include a number of different elements that can be further processed and analysed to provide important information from a criminal intelligence point of view. Therefore, the collection and further processing of PNR data by public authorities for the purpose of (criminal) law enforcement – with possible consequences for the individual such as denial of entry, arrest, criminal prosecution, etc. – constitutes a serious interference with the fundamental right to privacy and the protection of personal data of the persons concerned.

Furthermore, air carriers can face a conflict of laws when confronted with differing legal requirements between States on how personal data must be protected. This can prevent air carriers from transferring PNR data to requesting authorities and lead to sanctions for not disclosing PNR. In this context, any rules ICAO might develop with a view to addressing this issue should ensure that the interferences with the right to privacy and protection of personal data are kept to the minimum necessary to achieve its purposes and in that way to facilitate compliance by air carriers

[3] Resolution 2396 (2017) adopted by the Security Council at its 8148th meeting, on 21 December 2017 [on threats to international peace and security caused by returning foreign terrorist fighters].

with the various PNR regimes. As regards the modalities of PNR transmission, in particular, they also reflect the desire to minimise the financial burden on air carriers.

2.2. **Modalities of PNR transmission**

The method of transmission: To protect the personal data that is contained in the carriers' systems and to ensure that they remain in control of those systems, data should be transmitted using the 'push' system exclusively.

Transmission protocols: The use of suitable, secure and open standard protocols as part of internationally accepted reference protocols for the transmission of PNR data should be encouraged with the aim of gradually increasing their uptake and eventually replacing proprietary standards.

The frequency of transmission: The frequency and the timing of PNR data transmissions should not create an unreasonable burden on carriers and should be limited to that strictly necessary for the purpose described in section 2.3 below.

No obligation on the carriers to collect additional data: Carriers should not be required to collect additional data compared to what they already do or to collect certain types of data, but only to transmit what they already collect as part of their business.

2.3 **Modalities of PNR processing**

The processing of PNR data using evidence-based criteria and its comparison against databases relevant for the fight against terrorism and serious crime help law enforcement authorities to detect persons suspected for their involvement in criminal activities. Furthermore, subject to the appropriate guarantees for the protection of privacy of the persons concerned, PNR data can be made available well in advance of a flight's arrival or departure, and hence provide authorities with more time for processing and analysing the data, and potentially taking action.

2.4 **General principles concerning the protection of personal data**

The collection and transfer of PNR data affects a very large number of individuals against whom there is no prior suspicion. Therefore, such processing should be limited and only be allowed under strict conditions in accordance with the applicable legal frameworks. While it must always respect legal requirements imposed on air carriers under the specific rules of the source country, the following sets out a number of general principles should constitute the basis for the development of ICAO standards in this area:

Lawfulness, fairness and transparency of processing: the need to have a lawful basis for the processing of personal data and to make individuals aware of the risks, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing.

Purpose limitation: the purposes for which PNR data may be used by authorities should be clearly spelt out and should be no wider than what is necessary in view of the aims to be achieved, in particular for law enforcement and border security purposes to fight terrorism and serious crime.

Scope of PNR data: the PNR data elements to be transferred by airlines should be clearly identified and exhaustively listed. This list should be standardised to ensure that such data is kept to the minimum, while preventing the processing of sensitive data, including data revealing a person’s racial or ethnic origins, political opinions or religious or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.

Use of PNR data: the further processing of the data should be limited to the purposes of the original transfer, based on objective criteria and subject to substantive and procedural conditions in line with the requirements applicable to the transfers of personal data.

Automated processing of PNR data: automated processing should be based on objective, non-discriminatory and reliable, pre-established criteria and should not be used as the sole basis for any decisions with adverse legal effects or seriously affecting a person.
Data retention: the period of retention of the PNR data should be restricted and not be longer than necessary for the original objective pursued. Deletion of the data should be ensured according to the legal requirements of the source country. At the end of the retention period, the PNR data should be deleted or anonymised.
Disclosure of PNR data to authorized authorities: the further disclosure of PNR data to other government authorities within the same country or to other countries on a case-by-case basis may only take place if the recipient authority exercises functions related to the fight against terrorism or serious transnational crime and ensures the same protections as those afforded by the disclosing authority.
Data security: appropriate measures must be taken to protect the security, confidentiality and integrity of the PNR data.
Transparency and notice: subject to necessary and proportionate restrictions**,** individuals should be notified of the processing of their PNR data and be informed about the rights and means of redress afforded to them.
Access, rectification and deletion: subject to necessary and proportionate restrictions, individuals should have the right to get access to, and the right to rectification of, their PNR data.
Redress: individuals should have the right to effective administrative and judicial redress in case they consider that their rights to privacy and data protection have been infringed.
Oversight and accountability: the authorities using PNR data should be accountable to and supervised by an independent public authority with effective powers of investigation and enforcement, which should be in a position to execute its tasks free from any influence, in particular from law enforcement authorities.

2.5 **Information sharing**

Enhancing the exchange of PNR-related information on a case-by case basis could improve the ability of law enforcement authorities to cooperate to prevent, detect, investigate and prosecute acts of terrorism and serious crime. Information sharing should take place through appropriate channels ensuring adequate data security and be fully compliant with international and national legal frameworks for the protection of personal data.

3. CONCLUDING REMARKS

3.1. The principles outlined in this paper, in particular those on the protection of personal data, should be embedded in any future ICAO Standard(s) and Recommended Practices on the collection, use, processing and protection of PNR data for the purposes of countering terrorism and serious crime. This includes the need, for Contracting States seeking to establish and operate a PNR system, to adhere to such principles and notably comply with the applicable privacy and data protection legal requirements of the source country.

3.2. The ICAO Guidelines on Passenger Name Record Data (Doc 9944) cover a wide range of issues related to the transfer of passenger data. They offer a starting point for the harmonisation of the modalities of transmissions of PNR data. However, in the current context, these guidelines are insufficient. They should therefore be complemented with more far-reaching principles and considerations for the collection, use, processing and protection of PNR data outlined in this paper.