



Council of the
European Union

Brussels, 16 September 2019
(OR. en)

Interinstitutional File:
2019/0195(NLE)

12197/19
ADD 1

AVIATION 184
DAPIX 260
RELEX 836

PROPOSAL

From: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director

date of receipt: 13 September 2019

To: Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of
the European Union

No. Cion doc.: COM(2019) 416 final - ANNEX

Subject: ANNEX to the Proposal for a Council Decision on the position to be taken
on behalf of the European Union in the Council of the International Civil
Aviation Organization, in respect of the revision of Chapter 9 of Annex 9
(‘Facilitation’) to the Convention on International Civil Aviation with regard
to standards and recommended practices on passenger name record data

Delegations will find attached document COM(2019) 416 final - ANNEX.

Encl.: COM(2019) 416 final - ANNEX



Brussels, 13.9.2019
COM(2019) 416 final

ANNEX

ANNEX

to the

Proposal for a Council Decision

on the position to be taken on behalf of the European Union in the Council of the International Civil Aviation Organization, in respect of the revision of Chapter 9 of Annex 9 ('Facilitation') to the Convention on International Civil Aviation with regard to standards and recommended practices on passenger name record data

ANNEX

Position to be taken on behalf of the European Union in the Council of the International Civil Aviation Organization, in respect of the revision of Chapter 9 of Annex 9 ('Facilitation') to the Convention on International Civil Aviation with regard to standards and recommended practices on passenger name record data

General principles

Within the framework of the activities of the International Civil Aviation Organisation (ICAO) in respect of the revision of Chapter 9 of Annex 9 ('Facilitation') to the Chicago Convention concerning the development of standards and recommended practices (SARPs) on passenger name record (PNR) data, the Member States, acting jointly in the interests of the Union:

- (a) act in accordance with the objectives pursued by the Union within the framework of its PNR policy, notably to ensure security, to protect the life and safety of persons, and ensure full respect for fundamental rights, in particular the rights to privacy and the protection of personal data;
- (b) raise awareness, among all ICAO contracting States, of the Union standards and principles related to the transfer of PNR data, as resulting from the relevant Union law and the case law of the Court of Justice of the European Union;
- (c) promote the development of multilateral solutions compliant with fundamental rights concerning the transfer of PNR data by airlines to law enforcement authorities, in the interest of providing legal certainty, respect of fundamental rights and to streamline the obligations placed on air carriers;
- (d) promote the exchange of PNR data and the results of processing those data among the ICAO contracting States, where that is deemed necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime, in full respect of fundamental rights and freedoms;
- (e) continue to support the development by ICAO of standards for the collection, use, processing and protection of PNR data, in line with the United Nations Security Council Resolution 2396 (2017) of 21 December 2017;
- (f) continue to support the development, in all ICAO contracting States, of the capability to collect, process and analyse, in furtherance of ICAO SARPs, PNR data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel, as required by the United Nations Security Council Resolution 2396 (2017) of 21 December 2017;
- (g) promote the development of an environment in which international air transport may develop in an open, liberalised and global market and continue to grow without compromising security, and while ensuring the introduction of relevant safeguards.

Orientations

The Member States, acting jointly in the interests of the Union, shall support the inclusion of the following standards and principles in any future ICAO standards and recommended practices on PNR data:

1. Concerning the modalities of PNR transmission:

- (a) **Method of transmission:** In order 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.
- (b) **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.
- (c) **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 what is strictly necessary for the purposes of law enforcement and border security to fight terrorism and serious crime.
- (d) **No obligation on the carriers to collect additional data:** Carriers should not be required to collect additional PNR 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. Concerning the modalities of PNR processing:

- (a) **Timing of transmission and processing:** 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.
- (b) **Comparison against pre-determined criteria and databases:** the authorities should process PNR data using evidence-based criteria and databases that are relevant for the fight against terrorism and serious crime.

3. Concerning the protection of personal data:

- (a) **Lawfulness, fairness and transparency of processing:** there needs to be a lawful basis for the processing of personal data, in order to make individuals aware of the risks, safeguards and rights in relation to the processing of their personal data and of how to exercise their rights in relation to the processing.
- (b) **Purpose limitation:** the purposes for which PNR data may be used by authorities should be clearly set 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.
- (c) **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.

- (d) **Use of PNR data:** the further processing of the PNR 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.
 - (e) **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.
 - (f) **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 in accordance with the legal requirements of the source country. At the end of the retention period, the PNR data should be deleted or anonymised.
 - (g) **Disclosure of PNR data to authorized authorities:** the further disclosure of PNR data to other government authorities within the same State or to other ICAO contracting States 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.
 - (h) **Data security:** appropriate measures must be taken to protect the security, confidentiality and integrity of the PNR data.
 - (i) **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.
 - (j) **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.
 - (k) **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.
 - (l) **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 that should be in a position to execute its tasks free from any influence, in particular from law enforcement authorities.
- 4. Concerning PNR information sharing among the law enforcement authorities:**
- (a) **Promotion of information sharing:** case-by-case exchanges of PNR data among the law enforcement authorities of different ICAO contracting States should be promoted in order to improve international cooperation on the prevention, detection, investigation and prosecution of terrorism and serious crime.
 - (b) **Security of information exchange:** 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.