



Brussels, 27.9.2019
COM(2019) 420 final

ANNEX

ANNEX

to the

**Recommendation
for a
COUNCIL DECISION**

**to authorise the opening of negotiations for an Agreement between the European Union
and Japan for the transfer and use of Passenger Name Record (PNR) data to prevent
and combat terrorism and other serious transnational crime**

ANNEX

Directives for the negotiation of an Agreement between the European Union and Japan for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime

In the course of the negotiations the European Commission should aim to achieve the objectives set in detail below:

- (1) The objective of the Agreement should be to provide the legal basis, conditions and safeguards for the transfer of PNR data to Japan.
- (2) The Agreement should duly reflect the necessity and importance of the use of PNR data in preventing and combating terrorism and other serious transnational crime.
- (3) To this end, the objective of this Agreement should be to regulate the transfer and use of PNR data for the sole purpose of preventing and combating terrorism and other serious transnational crime, with full respect of the protection of privacy, personal data and fundamental rights and freedoms of individuals under the conditions to be set out in the Agreement.
- (4) The Agreement should also acknowledge the transfer of PNR data to Japan as fostering police and judicial cooperation which will be achieved through the transfer of analytical information flowing from PNR data. Therefore, the Agreement should ensure the transfer of analytical information flowing from competent authorities of Japan to police and judicial authorities of the Member States, as well as to Europol and Eurojust within their respective competences.
- (5) To guarantee compliance with the purpose limitation principle, the Agreement should limit the processing of PNR data exclusively to the prevention, detection, investigation or prosecution of terrorism and other serious transnational crime as based on definitions laid down in relevant EU instruments.
- (6) The Agreement should ensure full respect for fundamental rights and freedoms as enshrined in Article 6 of the Treaty on the EU, in particular the right to the protection of personal data as stipulated in Article 16 of the Treaty of the Functioning of the EU and Article 8 of the Charter of Fundamental Rights of the EU. It should also ensure full respect for the principles of necessity and proportionality regarding the right for private and family life and the protection of personal data as set out Article 7 and Article 8 of the Charter of Fundamental Rights of the EU as interpreted by the Court of Justice in its Opinion 1/15 on the envisaged EU-Canada PNR Agreement.
- (7) The Agreement should provide for legal certainty, notably for air carriers, by providing a legal basis for them to transfer PNR data contained in their automated reservation and departure control systems.
- (8) The Agreement should spell out clearly and precisely the necessary safeguards and controls with respect to the protection of personal data, fundamental rights and freedoms of individuals, irrespective of nationality and place of residence, in the context of the transfer of PNR data to Japan. These safeguards should ensure the following:
 - (a) The categories of PNR data to be transferred should be specified exhaustively and in a clear and precise manner, in line with international standards. Data transfers should be kept to the minimum necessary and should be proportionate to the specified purpose of the Agreement.

- (b) Sensitive data within the meaning of EU law, including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning a person's health or sexual life or orientation, should not be processed.
- (c) The Agreement should include provisions on data security, especially allowing only a limited number of specially authorised individuals to have access to PNR data and providing for an obligation to notify without delay the European data protection supervisory authorities of breaches of data security affecting PNR data unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons as well as referring to effective and deterrent sanctions.
- (d) The Agreement should contain provisions for the adequate and transparent information to passengers in relation to the processing of their PNR data, as well as the right of individual notification in case of use after arrival, access, and where appropriate, rectification and deletion.
- (e) The Agreement should ensure the rights of effective administrative and judicial redress on a non-discriminatory basis regardless of nationality or place of residence for any person whose data are processed pursuant to the Agreement, in line with Article 47 of the Charter of Fundamental Rights of the EU.
- (f) The Agreement should ensure that automated processing should be based on specific, 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 an individual. The databases against which PNR data are compared should be only those relevant for purposes covered by the Agreement and should be reliable and up to date.
- (g) The use of PNR data by the Japanese competent authority beyond security and border control checks should be based on new circumstances and subject to substantive and procedural conditions based on objective criteria. In particular, such use should be subject to a prior review carried out either by a court or by an independent administrative body, except in cases of validly established urgency.
- (h) The period of retention of the PNR data should be restricted and not be longer than necessary for the original objective pursued. The retention of PNR data after the air passengers' departure from Japan should be in line with the requirements set in the case law of the Court of Justice. The Agreement should require that the data are deleted upon expiry of the retention period or rendered anonymous in such a manner that the individual concerned is no longer identifiable.
- (i) The Agreement should ensure that further disclosure of PNR data to other government authorities within the same country or to other countries may only take place on a case-by-case basis and under certain conditions and safeguards. In particular, such disclosure 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 set out in the Agreement. Onward transfers to competent authorities of other third countries should be limited to those countries with which the EU has an equivalent PNR Agreement or for which the EU has adopted an adequacy decision under EU

data protection law covering the relevant authorities to which PNR data is intended to be transferred.

- (9) The Agreement should ensure a system of oversight by an independent public authority responsible for data protection with effective powers of investigation, intervention and enforcement to exercise oversight over those public authorities that use PNR data. That authority should have powers to hear complaints from individuals, in particular concerning the processing of their PNR data. Public authorities that use PNR data should be accountable for complying with the rules on protection of personal data under this Agreement.
- (10) The Agreement should require that the data be transferred exclusively on the basis of a 'push' system.
- (11) The Agreement should ensure that 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.
- (12) The Agreement should ensure that air carriers are not 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.
- (13) The Agreement should include provisions for regular joint review on all aspects of the implementation of the Agreement, including the reliability and topicality of pre-established models and criteria and databases and comprising a proportionality assessment of the retained data based on their value for the prevention and combat of terrorism and other serious transnational crime.
- (14) The Agreement should provide for a dispute settlement mechanism with respect to its interpretation, application and implementation.
- (15) The Agreement should be concluded for a period of 7 years and should include a provision whereby the Agreement maybe renewed for a similar period unless a Party terminates it.
- (16) The Agreement should include a clause addressing its territorial application.
- (17) The Agreement should be authentic in the Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages and should include a language clause to that effect.