



The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form

Although the systematic transfer, retention and use of all passenger data are, in essence, permissible, several provisions of the draft agreement do not meet requirements stemming from the fundamental rights of the European Union

The EU and Canada negotiated an agreement on the transfer and processing of Passenger Name Record data (PNR agreement) which was signed in 2014. The Council of the European Union requested the European Parliament's approval of the agreement, and the European Parliament decided to refer the matter to the Court of Justice in order to ascertain whether the envisaged agreement was compatible with EU law and, in particular, with provisions relating to respect for private life and the protection of personal data. It is to be noted that this is the first time the Court has been called upon to give a ruling on the compatibility of a draft international agreement with the EU Charter of Fundamental Rights.

The answer given by the Court in today's Opinion is that **the PNR agreement may not be concluded in its current form because several of its provisions are incompatible with the fundamental rights recognised by the EU.**

The envisaged agreement permits the systematic and continuous transfer of PNR data of all air passengers to a Canadian authority with a view to that data being used and retained, and possibly transferred subsequently to other authorities and to other non-member countries, for the purpose of combating terrorism and forms of serious transnational crime. To that end, the envisaged agreement, amongst other things, provides for a data storage period of five years and lays down requirements in relation to PNR data security and integrity, immediate masking of sensitive data, rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

Taken as a whole, PNR data may reveal, inter alia, a complete travel itinerary, travel habits, relationships existing between two or more individuals, and information on the financial situation of air passengers, their dietary habits or their state of health, and may even provide sensitive information about those air passengers. Furthermore, the PNR data transferred is intended to be analysed systematically by automated means, based on pre-established models and criteria, before the passengers' arrival in Canada. Such analyses may provide additional information on the private lives of passengers. Lastly, since the period during which PNR data may be retained may last for up to five years, that agreement makes it possible for information on the private lives of passengers to be available for a particularly long period of time.

The Court observes, therefore, that the transfer of PNR data from the EU to Canada, and the rules laid down in the envisaged agreement on the retention of data, its use and its possible subsequent transfer to Canadian, European or foreign public authorities entail an **interference with the fundamental right to respect for private life**. Similarly, the envisaged agreement entails an **interference with the fundamental right to the protection of personal data**.

The Court then examines whether those interferences can be justified. It observes, in this connection, that **the interferences in question are justified by the pursuit of an objective of general interest** (to ensure public security in the context of the fight against terrorist offences and serious transnational crime) and that the transfer of PNR data to Canada and its subsequent processing is appropriate for the purposes of ensuring that that objective is achieved.

As regards the necessity of those interferences, the Court considers that **several provisions of the agreement are not limited to what is strictly necessary and do not lay down clear and precise rules**.

In particular, the Court points out that the parties to the agreement have accepted that **sensitive data** may be transferred to Canada (sensitive data covers any information that reveals 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership' or concerning 'a person's health or sex life'). Having regard to the risk of processing contrary to the principle of non-discrimination, a transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this instance, however, there is no such justification. The Court concludes from this that **the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of that data are incompatible with fundamental rights**.

The Court also considers that the envisaged agreement does not exceed the limits of what is strictly necessary in so far as it permits the transfer of the PNR data of all air passengers to Canada. The automated analysis of PNR data is intended to identify the risk to public security that persons who are not known to the competent services may potentially present, and who may, on account of that risk, be subject to further examination at borders. That processing of data facilitates and expedites the security checks (in particular at borders) to which, in accordance with Article 13 of the Chicago Convention,¹ all air passengers who wish to enter or depart from Canada are subject, those passengers being required to comply with the conditions on entry and departure laid down by the Canadian law in force.

For the same reasons, for as long as the passengers are in Canada or are due to leave that non-member country, the necessary connection between that data and the objective pursued by the envisaged agreement exists, so that that agreement does not exceed the limits of what is strictly necessary merely because it permits the systematic retention and use of their PNR data.

However, as regards the use of PNR data during the air passengers' stay in Canada, the Court points out that, since following verification of their PNR data the air passengers have been allowed to enter the territory of that non-member country, the use of that data during their stay in Canada must be based on new circumstances justifying that use. That use therefore requires, as does the case-law of the Court, rules laying down the substantive and procedural conditions governing such use in order, inter alia, to protect the data in question against the risk of abuse. Such rules must be based on objective criteria in order to define the circumstances and conditions under which the Canadian authorities referred to in the envisaged agreement are authorised to use that data. In order to ensure that those conditions are fully respected in practice, the use of retained PNR data during the air passengers' stay in Canada must, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out by a court or by an independent administrative body, the decision of that court or body being made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.

The continued storage of the PNR data of all air passengers after their departure from Canada which the envisaged agreement permits is not limited to what is strictly necessary. As regards air passengers in respect of whom no risk has been identified as regards terrorism or serious transnational crime on their arrival in Canada and up to their departure from that country, there

¹ The Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (*United Nations Treaty Series*, Volume 15, No 102).

would not appear to be, once they have left, a connection – even a merely indirect connection – between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained. By contrast, the storage of the PNR data of air passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada is permissible beyond their stay in Canada, even for a period of five years. The use of the PNR data is therefore subject to the same conditions as those concerning the use of PNR data during the air passengers' stay in Canada.

The Court also considers that **other provisions of the envisaged agreement are incompatible with fundamental rights unless the agreement is revised in order to better delimit and define the interferences**. Accordingly, the Court considers that the agreement should:

- determine in a more clear and precise manner certain of the PNR data to be transferred;
- provide that the models and criteria used for the automated processing of PNR data will be specific, reliable and non-discriminatory;
- provide that the databases used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;
- provide that PNR data may be disclosed by the Canadian authorities to the government authorities of a non-EU country only if there is an agreement between the European Union and that country equivalent to the envisaged agreement or a decision of the European Commission in that field;
- provide for a right to individual notification for air passengers in the event of use of PNR data concerning them during their stay in Canada and after their departure from that country, and in the event of disclosure of that data to other authorities or to individuals;
- guarantee that the oversight of the rules relating to the protection of air passengers with regard to the processing of their PNR data is carried out by an independent supervisory authority.

Since the interferences which the envisaged agreement entails are not all limited to what is strictly necessary and are therefore not entirely justified, the Court concludes that **the envisaged agreement may not be concluded in its current form**.

Lastly, it should be noted that the Parliament also wished to know whether the legal basis for the envisaged agreement must be Article 82 TFEU and Article 87 TFEU (judicial cooperation in criminal matters and police cooperation) or Article 16 TFEU (protection of personal data). In this connection, the Court states that the agreement must be concluded both on the basis of Article 16 TFEU and Article 87 TFEU. The envisaged agreement pursues two equally important aims each inseparable from the other, namely, the fight against terrorism and serious transnational crime – which falls under Article 87 TFEU – and the protection of personal data – which falls under Article 16 TFEU.

NOTE: A Member State, the European Parliament, the Council or the Commission may obtain the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Treaties or as to competence to conclude that agreement. Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised.

Unofficial document for media use, not binding on the Court of Justice.

The [full text](#) of the opinion is published on the CURIA website on the day of delivery.

Press contact: Holly Gallagher ☎ (+352) 4303 3355

Pictures of the delivery of the opinion are available from "[Europe by Satellite](#)" ☎ (+32) 2 2964106