Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15

verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/

Christopher Kuner Mi 26 Jul 2017

Mi 26 Jul 2017

On 26 July the EU Court of Justice (CJEU) issued Opinion 1/15, which is its most significant ruling on the international dimensions of data protection law since its 2015 judgment in Case C-362/14 Schrems (previously discussed in a Verfassungsblog debate). In Opinion 1/15, the Grand Chamber of the Court found that the draft agreement between the EU and Canada for the transfer of passenger name record (PNR) data may not be concluded in its current form, since several of its provisions are incompatible with EU fundamental rights law. As the Court's first ruling on the compatibility of a draft international agreement with the EU Charter of Fundamental Rights, the judgment has important implications for many areas of EU law.

Background

On 6 September 2005 the European Commission adopted an adequacy decision under Article 25 of the EU Data Protection Directive 95/46 finding that the Canadian Customs Border Services Agency (CBSA) provided an adequate level of protection for the transfer of PNR data for flights from the EU to Canada. In 2006 an agreement between the EU and Canada concerning the processing of advance passenger information (API) and PNR data also came into force. The Canadian adequacy decision and the EU-Canada agreement then expired in September 2009, but Canada declared that it would continue to apply these protections voluntarily.

A new agreement for the processing and transfer of PNR data between the EU and Canada was initialed by the EU Council of Ministers and Canada on 6 May 2013 (referred to here as the Draft Agreement) and signed on 25 June 2014, following which the Council sought approval of it by the European Parliament. On 25 November 2014, the Parliament adopted a resolution seeking an opinion from the CJEU pursuant to Article 218(11) on two questions, which application was lodged with the Court on 10 April 2015. The two questions were as follows:

> *'Is the envisaged agreement compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to protection of personal data?*
>
> *Do Articles 82(1)(d) and 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the envisaged agreement or must that act be based on Article 16 TFEU?'*

The Opinion of Advocate General Mengozzi was issued on 8 September 2016 (an excellent analysis of it can be found on the blog of Gabriela Zanfir-Fortuna). In it, the Advocate General responded negatively to both questions, as he found several provisions of the Draft Agreement incompatible with the Charter. He also found that the correct legal basis of the Agreement was provided by Articles 16(2) (the right to data protection) and 87(2)(a) (police cooperation among the Member States in criminal matters) of the Treaty on the Functioning of the European Union (TFEU), but not by Article 82(1)(d) TFEU (judicial cooperation in criminal matters in the Union).

Summary of the judgment

The following is a summary of the judgment's main points; the references in parentheses are to the relevant paragraphs of the judgment unless otherwise stated.

The Court first noted that an international agreement must be entirely compatible with the treaties and constitutional principles of the EU (para. 67). After finding that the request for an Opinion of the Parliament was

admissible, the Court then considered what the correct legal basis for the Draft Agreement should be, which has to be determined based on objective legal factors including the aim and content of the measure envisaged (para. 76). The CJEU found that the Draft Agreement has the dual objectives of protecting public security and data protection, both of which are inextricably linked (para. 94). Thus, agreeing with the Advocate General, the CJEU found that both Article 16(2) TFEU and Article 87(2)(a) TFEU were the correct legal bases of the Draft Agreement, but that Article 82(1)(d) TFEU could not serve as a legal basis (as will be discussed later on, this may have an impact on other PNR agreements of the EU).

The Court then considered the compatibility of the Draft Agreement with the rights to respect for private life and the protection of personal data under the TFEU and the Charter. It found that PNR data may reveal considerable detail about an individual, such as their travel habits, relationships, and financial situation, which may also include sensitive information. It stressed that the data were to be systematically analysed by automated means before arrival in Canada, and that they could be stored for up to five years. Thus, the Court observed that the transfer of PNR data to Canada and the rules foreseen in the Draft Agreement would entail an interference with the fundamental rights to respect for private life under Article 7 (para. 125) and to the protection of personal data under Article 8 of the Charter (para. 126).

Since Article 7 and Article 8 are not absolute rights (para. 136), the Court then examined whether such interferences could be justified. It found that the processing of PNR data under the Draft Agreement pursued a different objective from that for which it was collected by air carriers, and thus requires a different legal basis, such as separate consent by passengers or some other legal basis laid down by law (para. 143). The Court next found that an international agreement may meet the requirements of being a 'law' as defined in Article 8(2) and Article 52(1) of the Charter (paras. 145-147). It went on to note that in this case such interferences are justified by the need to fight terrorism and serious transnational crime in order to ensure public security, and that the transfer of PNR data to Canada and its subsequent processing may be appropriate to meet that objective (paras. 151, 153).

The CJEU then analysed the protections provided in the Draft Agreement, and had the following criticisms:

–The Draft Agreement was not sufficiently precise in specifying the PNR data to be transferred (para. 163).

–It did not provide sufficient protections for the transfer of sensitive data (which, under Article 8 of the Directive 95/46, includes 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership' or data processing concerning 'a person's health or sex life') (para. 167). In addition, it stated that 'a transfer of sensitive data…requires a particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime' (para. 165).

–With regard to automated analyses of PNR data, because of the margin of error, any positive result must be subject to 'individual re-examination by non-automated means' before any measure adversely affecting a passenger is taken (para. 173).

–Language permitting Canada to process PNR data on a case-by-case basis to 'ensure the oversight or accountability of the public administration' and to 'comply with the subpoena or warrant issues, or an order made, by a court' lacked sufficient clarity and precision (para. 181).

The Court also noted that the coverage of all air passengers flying between the EU and Canada is not unacceptably broad, particularly since Article 13 of Convention on Civil Aviation (the Chicago Convention) require signatories (which include Canada and all EU Member States, but not the EU itself) to comply with admission and departure formalities of passengers from their territory, which can include security checks laid down by Canadian law (paras. 188-189).

The Court then discussed at length the compatibility of the Draft Agreement with EU law requirements for data retention. With regard to the retention and use of PNR data before the arrival of passengers, during their stay in Canada, and on their departure, the Court found that some elements of the retention of data under the Draft Agreement were acceptable, such as the use of data for security checks and border control checks (para. 197); verifying the reliability and topicality of models for the automated processing of data (para. 198); or cases when

data are collected by the Canadian authorities during the individuals' stay in Canada indicating that use of it may be necessary to combat terrorism and serious transnational crime (para. 199). However, the Court stated that the use of PNR data should be subject to prior review by a court or an administrative body, and that otherwise it may be found to go beyond what is strictly necessary (paras. 201-203).

With regard to the retention and use of PNR data after passengers' departure from Canada, the Court found that it was not strictly necessary (paras. 206 and 211), but that it may be stored in Canada in cases where certain passengers may present a risk of terrorism of serious transnational crime. It stated that the five-year retention period in the Draft Agreement does not exceed the limits of what is strictly necessary (para. 209), but that use of such data should be subject to prior review by a court or 'independent administrative body' (para. 208).

With regard to the disclosure of PNR data to government authorities, the Court reiterated the standard it set forth in Schrems that data transfers to third countries require a level of protection that is 'essentially equivalent' to that under EU law (paras. 134 and 214), and held that this also applies to PNR transfers to Canada. The Court went on to say that this requires either an international agreement between the EU and a third country, or an adequacy decision of the Commission (para. 214). It held that individuals must have a right to have their data rectified (para. 220), and that they must be notified individually when their data are used by a judicial authority or independent administrative body (para. 223) unless this would jeopardise an investigation (para. 224). Finally, the Court held that the Draft Agreement did not sufficiently guarantee that oversight of compliance with its rules would be carried out by an independent authority within the meaning of Article 8(3) of the Charter (para. 231).

Data protection and international agreements

Opinion 1/15 sets out for the first time the conditions under which international agreements may be used to legalize international data transfers. Article 216(1) TFEU allows authority for the conclusion of an international agreement to be 'provided for in a legally binding Union act', which would allow EU legislation to set out criteria for data protection agreements with third countries. However, no EU data protection legislation that I am aware of deals with the use of international agreements as a legal basis for the transfer of data, including the current EU Data Protection Directive 95/46 or the EU General Data Protection Regulation that will replace the Directive in May 2018 (with the exception of Recital 102 of the GDPR, which states somewhat feebly that international agreements must include 'appropriate safeguards for the data subjects'). This seems like a missed opportunity by the EU legislator.

The CJEU states that the transfer of PNR data from the EU to Canada may be satisfied either by an international agreement of the EU or by a Commission adequacy decision (para. 214), which raises the question of the relationship between the two, and seems to suggest that an adequacy decision may not always be necessary. The Court also provides an incentive for the expanded use of international agreements to transfer personal data by clarifying that they may meet the requirements of being a 'law' under Article 8(2) and Article 52(1) of the Charter. The Court's affirmation of the possibility of using an international agreement to transfer data without an adequacy decision may lead to political tensions between the EU institutions in areas such as data sharing for law enforcement purposes, where the Commission now has the power to issue adequacy decisions under Article 36 of the new 'Police Directive' 2016/680.

Affirming the fundamental right to data protection

The Court's judgment in Opinion 1/15 generally followed Advocate General Mengozzi in extending its rulings in cases such as Schrems and Joined Cases C-293/12 and C-594/12 Digital Rights Ireland to international agreements. It also cites liberally to its relatively recent decision in Joined Cases C-203/15 and C-698/15 Tele2 Sverige and Watson and Others, leaving no doubt that it views Tele2 as part of the mainstream of judgments affirming the fundamental right to data protection. At the same time, the Court pulled back a bit from the prohibition in Tele2 against 'general and indiscriminate retention' of data (see para. 103 of that judgment), and found that interference with the fundamental rights to privacy and data protection may, under the right circumstances, be justified by a general objective of the EU such as the fight against terrorism, even though this involved a data retention period of five years.

In some parts of the judgment dealing with fundamental rights the Court seems hesitant to give clear direction. This can be seen, for example, in the section dealing with data retention (paras. 190-211), where the Court states rules, then exceptions to them, and then exceptions to the exceptions, so that even a careful reader may have difficulty understanding exactly what it means. One can only conclude that any parties having to apply the judgment in practice (such as law enforcement authorities) may be left scratching their heads.

Implications for other international agreements

The Court found that the correct legal bases for Draft Agreement were Article 16(2) TFEU and Article 87(2)(a) TFEU, but not Article 82(1)(d) TFEU. This could spell trouble for other PNR agreements of the EU that rely on Article 82(1)(d) TFEU as a legal basis, such as those with Australia and the United States. It may also create risks for the EU-US Privacy Shield, given that the Court was critical of supervision under the Draft Agreement as being carried out 'by an authority which does not carry out its tasks with complete independence' (para. 68), a point on which the Privacy Shield has also been criticized. Finally, it seems that many international agreements of the EU could potentially be open to challenge in light of the strict standard the Court applied.

Third country law in the CJEU

The judgment throws further light on how the Court deals with third country law in its data protection cases, which I have commented on elsewhere. The interpretation of Canadian law was crucial to the Court's judgment as to whether it fulfilled the criteria of EU law that were the substance of the European Parliament's questions, and from what I have been told, there were significant disagreements between the European Parliament and some of the Member States about issues of Canadian law.

The Opinion of Advocate General Mengozzi shows that the Court used different sources to gain information about Canadian law, including explanations by the European Commission (para. 318 of his Opinion), Canadian government web sites (footnote 92), and a letter from the Canadian Mission to the EU (para. 312), but this hardly seems sufficient given the importance of the case. One can ask why the Court didn't take expert evidence or conduct further investigation into Canadian law and practice, which is permissible in opinions (see Articles 196-200 of the Rules of Procedure of the Court of Justice applicable to opinions). Indeed, the Court states that it did put a number of questions in writing to the Member States and the European Data Protection Supervisor, though it does not explain what they concerned (para. 45).

Conclusions

The judgment has narrowed the EU's leeway to negotiate international agreements in a variety of important areas involving the transfer of personal data, such as international trade, data sharing with third countries, and arrangements post Brexit. It also demonstrates the difficulties caused by the failure to deal more explicitly in EU legislation with the place of international agreements in the data protection framework.

The political implications of the judgment are also significant. By examining the Draft Agreement in such minute detail, both the Court and the Advocate General in effect performed a redline revision of it. In the judgment, this went into such a level of detail that the Court objected to the use of the term 'etc.' in one heading of the Annex to the Draft Agreement referring to PNR data elements, which reads 'Available frequent flyer and benefit information (free tickets, upgrades, etc.)' (para. 157).

One wonders how many international agreements of the EU could withstand this degree of second-guessing. It is in the nature of international agreements that they tend to be finely-balanced, with a concession in one provision offset by a gain in another one. Following the judgment, some third countries may be hesitant to invest the time and resources necessary to conclude an international agreement on data protection with the EU knowing that it may later be picked apart by the Court. The ultimate effects of the judgment will be seen in the coming years as the EU seeks to negotiate further agreements on data protection and data sharing with third countries and international organisations.

SUGGESTED CITATION Kuner, Christopher: *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15, VerfBlog,* 2017/7/26, http://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/.