At a glance
September 2017

CJEU Opinion on EU-Canada PNR agreement

A new agreement on the transfer of passenger name records (PNR) was signed by the EU Council and Canada in 2014, but conclusion of the agreement requires the European Parliament's consent. Consulted by Parliament, the Court of Justice of the EU held in July 2017 that the envisaged agreement needs to be revised.

PNR data, counter-terrorism policy and the European data protection framework

PNR consist of information on passengers held by air carriers for operational purposes, such as passengers' names, travel dates, itinerary and payment method. In many countries information-sharing involving PNR is increasingly, but not without criticism, an essential component of anti-terrorism and security policies, leading to the adoption of specific agreements regulating their exchange. The relevance of PNR for security purposes is also stressed in the European Commission's recent ninth security progress report, drawing on a comprehensive assessment of EU security policy, including its external dimension. The report states that cooperation with third countries through information exchange aims at reinforcing EU security, yet poses challenges as regards EU data protection law.

The rights to private life and data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights (CFR), binding as EU primary law since 2009. Article 16 of the Treaty on the Functioning of the EU (TFEU), imposes the ordinary legislative procedure on the EU when adopting rules **relating** to data protection, and states that these rules are subject to control by independent authorities.

At the level of secondary law, the 1995 Data Protection Directive (and its replacement which will apply from 2018), provides for a high level of personal data protection, to the extent that data transfer outside the EU is allowed only if the third country can ensure an **adequate** level of protection. Such **adequacy** is assessed under Article 25 of the directive, in light of all the circumstances and of the rules of law in force in the third country or of international commitments. According to the EU Court of Justice (CJEU), this requirement should be read in light of the CFR, which justifies limitations to privacy and data protection rights if provided by law, and if strictly necessary and proportionate to meeting objectives of general interest (Article 52).

New EU-Canada PNR agreement: a long path

Since the Lisbon Treaty, the conclusion by the Council of agreements with third countries covering fields subject to the ordinary legislative procedure requires the European Parliament's consent (Article 218(6.a) TFEU). The previous 2006 Canada PNR agreement was based on the Commission adequacy decision that expired in 2009, with the consequence that the agreement ceased to have effect (although Canada committed to respecting its principles). In a 2010 resolution, the EP urged the Commission to adopt a coherent approach on the use of PNR data for law enforcement and security purposes, including as regards PNR agreements with third countries: in particular, that the latter should be negotiated in view of the EU data protection standards (e.g. purpose limitation, proportionality, legal redress). In its 2010 communication on external PNR strategy, the Commission indicated data protection among the general principles. The Council authorised the Commission to open negotiations with Canada for a new PNR agreement in December 2010. Following negotiations, the Commission adopted proposals for Council decisions on the conclusion and the signature of the new deal in July 2013. The new PNR agreement was signed by the Council Presidency and Canada on 25 June 2014 and sent to the EP for consent.

Under the envisaged EU-Canada PNR agreement, EU airlines are obliged to transfer ('push') PNR of passengers to the competent Canadian authorities. The agreement also provides for Canada to share PNR with Europol, Eurojust, or the police and judicial authorities of the Member States. In particular, the agreement provides for a set of rules on the sharing of PNR strictly for the purpose of countering terrorist offences or serious transnational crimes (as defined therein). The EU shall ensure that airlines, operating flights to and from the EU, transfer PNR data they collect on all EU-Canada travellers upon request by a Canadian authority ('push system'); if compliant with the agreement, Canada

EPRS | European Parliamentary Research Service
Author: Shara Monteleone, **Members' Research Service**
PE 608.673

is deemed to provide an **adequate** level of data protection; Canada shall ensure the safeguard of passengers' PNR according to non-discrimination and transparency principles; allow individuals to access their data (within limits); and to lodge complaints with an independent authority. Data should be retained in masked form and for up to five years – renewable; finally, the agreement includes a reciprocity clause (introduced in view of the adoption of the EU-PNR regime).

The role of the European Parliament

In November 2014, pursuant to Article 218(11) TFEU, the EP decided to seek, for the first time, the opinion of the Court of Justice of the European Union (CJEU), on the compatibility of the agreement with the Treaties and the CFR. The EP has consistently sought to ensure that PNR agreements comply with the EU data protection legal framework, and *in specie* with the proportionality principle. The EP decision to refer to the CJEU was taken following the CJEU ruling invalidating the 2006 Data Retention Directive permitting unlimited data collection and storage, and particularly following the European Data Protection Supervisor's critical opinion, which questioned the proportionality of PNR schemes and the choice of the legal basis, proposing inclusion of Article 16 TFEU (personal data protection). The EP has expressed its position on data transfers on several occasions, e.g., in resolutions on data transfers via the SWIFT network. In its 2010 resolution on the global approach to PNR transfers, the EP held that the purpose of these agreements is to ensure that data transfer is in line with EU data protection and privacy rules. A 2015 resolution on anti-terrorism measures called for better information sharing, but subject to appropriate safeguards. Parliament also reiterated the need to respect fundamental rights on the occasion of the debate surrounding the adoption of the EU PNR Directive on the sharing of PNR data by Member States in the fight against terrorism and serious crimes.

2017 Court of Justice opinion

On 26 July 2017, the CJEU, sitting in Grand Chamber, issued opinion 1/15 further to the EP's request. The Court, largely endorsing the Advocate-General's earlier opinion, held that, although systematic transfers, retention and use of PNR are, per se, admissible, the EU-Canada agreement in its current form was not in line with the fundamental rights requirements of EU law. In particular, its interferences with privacy and data protection rights would go beyond what could be justified for fighting terrorism, lacking necessity and proportionality in many cases. More in detail, the Court stated that the agreement must be based jointly on Article 16(2) and 87 TFEU (police cooperation); the current text violates Articles 7, 8, 21 and 52 CFR, as it does not preclude the transfer of sensitive data (e.g. on racial origin, health, religion, sex life); it must clearly specify the PNR data to be transferred; the agreement must provide that automated processing of PNR is specific, reliable and non-discriminatory and that the databases used are only those relating to counter-terrorism and serious transnational crimes; it must impose specific conditions for further use of data and for disclosure to other authorities; PNR retention must be limited to cases of objective evidence of risk in terms of terrorism or serious crimes; disclosure of PNR by Canada to third countries' authorities must be allowed only in the presence of a PNR agreement with the EU or of a Commission adequacy decision; the agreement must provide for individuals to be notified if their data are used by a judicial authority; and finally, it must guarantee oversight of the related rules by an independent supervisory authority.

Policy implications

Pursuant to Article 218(11) TFEU, where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless amended. The text of the agreement must therefore be revised. The Court's opinion is likely to have an impact on similar current (with Australia and the USA) and future PNR deals. EU Security Commissioner, Julian King, is ready to address the concerns with Canada, but also stated that the opinion does not affect the application of the EU PNR Directive (adopted after the Canada agreement was signed). As some scholars stress, the CJEU opinion, which shed some light on the thorny issue of balancing fundamental rights, security and external relations, is part of consistent CJEU jurisprudence on data protection: in *Schrems*, declaring the adequacy decision on the EU-US agreement invalid, prompting the adoption of the new *Privacy Shield* deal, the annual review of which is approaching; *Digital Rights Ireland* and *Tele2* also fix limits to data retention obligations in the Member States. EP rapporteur, Sophia in 't Veld (ALDE, the Netherlands), criticised both Commission and Council for persisting with a flawed agreement, stressing that upholding privacy rules and fighting terrorism are not contradictory. As it corroborates conditions on data transfers in general, the opinion may also have implications on data flows with the United Kingdom following Brexit. For this reason, announcement of an upcoming data protection bill aiming to harmonise British and EU law is critical (in view of a future Commission adequacy decision) for both commercial and security cooperation.