Fifth anniversary of the EU PNR Directive – la route vers la CJUE

Summary by Alessandra Calvi (VUB/LSTS) and Juraj Sajfert (VUB/University of Luxembourg)

On 12 May 2021, the Brussels Privacy Hub, in cooperation with the **University of Luxembourg** within the framework of the FWO/FNR-funded MATIS project, the **Cyber & Data Security Lab** (CDSL) and in media partnership with **Privacy Laws & Business** organised the fifth webinar within the series **Enforcing Europe - Webinar Series 1**.

The fifth webinar, entitled the **Fifth anniversary of the EU PNR Directive – la route vers la CJUE** discussed the EU **Passenger Name Records Directive** (PNR Directive (EU) 2016/681). Now that most of the Member States transposed it, this Directive is being challenged before the Court of Justice of the European Union (CJEU) by NGOs from Belgium (Ligue des Droits Humains), Austria (Epicenter.works) and Germany (Gesellschaft für Freiheitsrechte (GFF, Society for Civil Rights)). How did we get there (again)? Ahead of the hearing, could we, and why, expect a similar outcome to the one in Digital Rights Ireland? Are there any lessons to be (finally) learned?

Juraj Sajfert (VUB/University of Luxembourg) moderated the discussion. Invited speakers were **Catherine Forget** (lawyer from Brussels, representing la Ligue des Droits Humains in the PNR case before the CJEU) and **Vagelis Papakonstatinou** (VUB, CDSL).

Vagelis Papakonstantinou observed that the PNR domain is at the intersection of data protection and criminal justice. This field is becoming more and more specialised. He noted that whereas the GDPR and the ePrivacy directive apply to everybody, the PNR Directive is just for passengers (travellers). More specifically, air travellers (although some countries expanded PNR to other ways of travelling). Therefore, travelling by car is a way to avoid the processing of personal data under the PNR. Conversely, individuals cannot circumvent the application of the GDPR or the ePrivacy directive. He added that sensitive data can be inferred from PNR (e.g. meal preference) but that PNR as such are not considered sensitive data. He noted how all personal data risk becoming sensitive data and that the approach of the GDPR is not dynamic: that is why the GDPR refers to a closed list of sensitive data. PNR Directive roots 20 years ago when, after 9/11, US border control authorities suddenly demanded EU airlines, as a condition to continue flying to the US, to provide information about their passengers. As this created a data protection problem, the Commission started to negotiate interim agreements to close this gap. Beforehand, there was Advanced Passenger Information (API) but they were not so detailed. In 2009, the discussion moved towards the creation of an intra-EU PNR. Whereas the Commission did not create a mandatory intra-EU PNR framework, it gave the Member States this possibility. He noted how PNR are processed in EU Star Alliance by a non-EU company located in Switzerland. These data are then transferred to Passenger Information Units (PIUs).

Caterine Forget stated that the request of preliminary ruling regards the compatibility of the Directive with human rights, in particular with the Charter of Fundamental Rights. She referred to the 2015 Opinion on the PNR agreement with Canada, where the CJEU acknowledged that PNR represented an intrusion in the rights to privacy and personal data protection. She added that the effectiveness of PNR in the fight against crime is not demonstrated, questioning the overall necessity and proportionality of their collection. She explained that the Ligue des droits humains has introduced an action before the Belgian Constitutional Court for annulment of the federal Act of 25 December 2016, transposing the PNR and API Directives.[1]
From a data protection point of view, the most interesting issues include: the quality and quantity of the data to be collected under the PNR framework, open formulation of the directive (see in particular

[1] https://gdprhub.eu/index.php?title=Constitutional_Court_-_135/2019

Point 12[2] and 18[3] Annex 1 PNR Directive) open, leaving the rules on sensitive data uncertain; the broadness of the system of collection, transfer and processing – and retention – of passenger data, that applies to any air traveller, regardless of whether there is any objective ground for considering that that person may present a risk to public security; the system of *a posteriori* notification, that is under evaluation; the compatibility of the intra-EU exchange of PNR data with the freedom of movement.

During the Q&A Juraj Sajfert observed that under the LED there is an obligation of *ex post* notification. This is controversial because, as rightly pointed out by La Quadrature du Net and the European Court of Human Rights, the lack of implementation of this system would jeopardise the right to an effective remedy. Other participants observed that EU large-scale databases appear outside the scope of the PNR Directive and wondered whether algorithms used by PIUs will fall under the upcoming AI Act. Concerns over the repurposing, in particular as to the possible expansion of the scope of the PNR Directive for purposes of public health protection, as happened in Germany to allow the PIUs to transfer data to health authorities were raised, too.

[2] General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

[3] Any advance passenger information (API) data collected (including the type, number, country of issuance and expiry date of any identity document, nationality, family name, given name, gender, date of birth, airline, flight number, departure date, arrival date, departure port, arrival port, departure time and arrival time)