EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 44/2022, 11 October 2022
Tags: Data protection and digital governance
Topics: PNR Directive, Case C-817/19, air passenger data, Charter of Fundamental Rights

Repairing the EU Passenger Name Record Directive: the ECJ's judgment in *Ligue des droits humains* (Case C-817/19)

By Kristina Irion

On 21 June 2022, the European Court of Justice (ECJ) handed down its judgment in *Ligue des droits humains* concerning the Directive 2016/681 on passenger name record data (PNR Directive). This is the second time that the ECJ has appraised the conformity of a PNR system with the EU Charter of Fundamental Rights (the Charter). In Opinion 1/15, the Court found the draft PNR Agreement between the EU and Canada to be incompatible with Articles 7, 8, 21 and 52(1) of the Charter. This interpretation cast a shadow on the legality of the PNR Directive as well, as it contains partly identical provisions to the EU-Canada draft PNR Agreement. In *Ligue des droits humains*, the Court now 'repairs' the PNR Directive by means of a Charter-conforming interpretation and, without affecting its validity, significantly modifies the permissible scale and scope of the EU-wide security practice on passengers' data.

This post summarises how the ECJ assesses the validity of the PNR Directive in light of Articles 7, 8 and 52(1) of the Charter (the fundamental right to respect for private life, to protection of personal data, and the principle of proportionality, respectively). For the sake of clarity, the post exclusively focuses on the judgment's implications for the PNR Directive, leaving aside the two other EU legal instruments also considered in the judgment, namely Council Directive 2004/82/EC (API Directive) and Directive 2010/65/EU on reporting formalities for ships.

The PNR Directive in a nutshell

The collection of air passenger data is an integral part of the EU Security Union Strategy. In 2016, the Parliament and the Council adopted the PNR Directive in the wake of the terrorist attacks in Paris in 2015 and Brussels in 2016. This Directive creates

an EU legal framework for the collection and use of passengers' personal data on flights to or from third countries. Member States have the power to apply the PNR Directive to flights within the EU (Article 2). Pursuant to the PNR Directive, Member States designate a competent authority to act as its Passenger Information Unit (PIU). Additionally, Member States must impose a legal obligation on air carriers to transfer the PNR data listed in Annex I of the Directive by electronic means to the database of the PIU (Article 8). PNR data may be processed only for the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crime (Article 1(2)). The PIU must ensure that PNR data is retained for a period of five years and deleted afterwards, and that PNR data is de-personalised six months after receipt (Article 12).

The PIUs are authorised to process the PNR data for three purposes (Article 6(2)):

1. for an advance assessment of passengers to identify persons who require further examination by the competent authorities or Europol;
2. to respond to a duly reasoned request from the competent authorities to provide PNR data or the results of its processing to the competent authorities or Europol; and
3. to analyse PNR data for the purpose of creating new criteria to identify persons who may be involved in a terrorist offence or serious crime.

The PNR Directive "should ensure full respect for fundamental rights" and "meet the objectives of necessity and proportionality" to achieve its objective (Recital 22). The retention and processing of PNR data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life, or sexual orientation is under no circumstances allowed (Articles 6, 7 and 13). Any positive match resulting from the automated processing of PNR data shall be individually reviewed by non-automated means (Articles 6(5) and (6), 12(5)). Requests from competent authorities to provide PNR data older than six months must be approved by a judicial authority or another national authority (Article 12(3)). The PIU must appoint a data protection officer (Article 5), maintain documentation, and keep records of processing operations (Article 13). The PNR Directive guarantees data subject rights (Article 13), and the PIU must be under the supervision of the Member State's data protection authority (Article 15).

Request for a preliminary ruling

The request for a preliminary ruling was made by the Belgian Constitutional Court (*Cour constitutionnelle*) in proceedings between the *Ligue des droits humains* and the Belgian Council of Ministers (*Conseil de ministers*). The referring court raises several fundamental questions about the compatibility of the PNR Directive with Articles 7, 8 and 52(1) of the Charter (para. 62). In particular, the court asks whether the PNR Directive is in conformity with the Charter where it:

- introduces a system of generalised collection, transfer and processing of passenger data, (Question 4),
- provides for an advance assessment of all passengers, which is conducted by comparing PNR data against databases and pre-determined criteria (Question 6), and
- prescribes a general data retention period of five years (Question 8),

all of which takes place regardless of whether there is any objective ground for considering that that a person may present a risk to public security.

Further, the referring court asks questions about the Belgian legislation which transposes the PNR Directive. The Belgian legislation includes activities of intelligence and security services within the remit of the purposes for which PNR data is processed and grants power to the PIU to authorize access to PNR data older than six months (Questions 5 and 7).

Underscoring the importance of the case, aside from the Council and the Commission, 14 Member States joined the proceedings before the ECJ. The European Data Protection Supervisor and the EU Fundamental Rights Agency made an intervention as well.

Opinion of Advocate General Pitruzella

On 27 January 2022, AG Pitruzzella issued his Opinion in *Ligue des droits humains*. He faithfully transposes Opinion 1/15 to the situation of the PNR Directive and develops the contours of an EU law consistent interpretation of the PNR Directive. The AG, however, suggests to the ECJ to invalidate partially the PNR item "general remarks" as being too broad and unspecified and, instead, to keep only information concerning minors listed in point 12 of Annex I of the PNR Directive (points 152-153). The AG, moreover, holds that, while the objective of the PNR Directive "justif[ies] the generalised indiscriminate transfer of PNR data and their automated processing in the context of their advance assessment […]", it does not by itself "justify the generalised and indiscriminate retention of those data after that assessment" (point 241).

The ECJ's Judgment

The Grand Chamber's judgment largely follows the AG's Opinion but is more deferential to the EU legislator as regards the necessity of the initial retention period of six months of all air passengers' PNR data. Considering the validity of the PNR Directive in light of Articles 7, 8 and 52(1) of the Charter (questions 2-4 and 6), the Court recalls that "an EU act must be interpreted, as far as possible, in such a way as not to affect its validity" (para. 86).

The Court finds that the PNR Directive clearly affects the fundamental rights guaranteed by Articles 7 and 8 of the Charter (paras 94-97). Even more so, it concludes that "the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter … as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services" (para. 111). Despite this, the Court specifies that the PNR Directive's objective to ensure the internal security of the EU and to combat terrorist offences and serious crime constitute objectives of general interest of the EU that are capable of justifying even serious interferences with the rights in question (paras 121-122). It further finds that the Directive still respects the essence of the fundamental rights in Articles 7 and 8 of the Charter: the PNR Directive lays down in a precise manner the scope of the limitation on the exercise of the rights in question, the purposes for processing PNR data and detailed rules governing those processing operations (para. 119). Furthermore, PNR data is limited to certain aspects of a person's private life, i.e., a person's air travel, and that the PNR Directive prohibits the processing of protected characteristics (para. 120).

Turning to the question of whether the serious interferences are necessary, the Court first considers the list of PNR items contained in Annex I of the PNR Directive. The deficiencies of certain PNR items are 'repaired' with a Charter-conforming interpretation, affecting open-ended formulations (e.g., "including") and unspecified data categories (e.g., "frequent flyer information", "payment information" and "general remarks") (headings 5, 6, 8, 12 and 18 of Annex I) (paras 130-136). The ECJ also requires Member States to ensure that their national implementations of the PNR Directive are effectively limited to combating terrorist offences and serious crime "having an objective link, even if only an indirect one, with the carriage of passengers by air" (para. 157). Moreover, it may not be applied to combat ordinary crime (para. 152).

Collection of PNR data from extra- and intra-EU flights

Regarding the Directive's application to extra-EU flights, the Court holds that the transfer and advance assessment of the PNR data of air passengers entering or leaving the EU contributes to the objective of combatting terrorist offences and serious crime. Accordingly, the Court finds that "the PNR Directive does not go beyond what is strictly necessary merely because it imposes on Member States the systematic transfer and advance assessment of the PNR data of all those passengers" (para. 162, referring to Opinion 1/15).

Noting that the PNR Directive does not prescribe the application to intra-EU flights, the Court requires Member States to assess whether there is a threat linked to terrorist offences and serious crime, "which is capable of justifying the application of the said directive to intra-EU flights also" and whether it is "effectively necessary and proportionate" (paras 167-168). Analogous to its *La Quadrature du Net and Others* judgment (para. 137), the Court rules that where a Member State "is confronted with

a terrorist threat which is shown to be genuine and present or foreseeable", the application of the PNR Directive to all intra-EU flights "for a limited period of time, does not appear to go beyond what is strictly necessary" (para. 171). In situations other than a terrorist threat, the PNR system can only be applied to selected intra-EU flights relating "to certain routes or travel patterns or to certain airports in respect of which there are indications that are such as to justify that application" (para. 174).

Advance assessment of PNR data through automated processing

Paying critical attention to the advance assessment of PNR data by automated processing, the ECJ considers the safeguards put in place by the PNR Directive (paras 179-180): first, "no decision that produces an adverse legal effect on a person or significantly affects a person may be taken … only by reason of the automated processing of PNR data"; second, the PIU is tasked with an individual review by non-automated means before it may transfer PNR data of persons who require further examination to the competent authorities; and third, a designated data protection officer monitors a PIU's compliance with the PNR Directive, which is subject to supervision by the national supervisory authority, as well as judicial review.

Subsequently, the Court offers crucial clarifications on how the advance assessment of PNR data by automated processing must be organised in conformity the Charter: "the only databases against which the PIU may compare PNR data" are databases "on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such databases" (paras 187-188). Such databases must only be "used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air" (para. 191). This serves to exclude other databases, such as those "managed and exploited by the security and intelligence agencies of Member States" for objectives other than those of the PNR Directive (para. 184). Additionally, the Court carries over a set of requirements intended for the processing of PNR data against pre-determined criteria to the situation of comparing PNR data against databases, which must be "carried out in a non-discriminatory manner", "targeted, proportionate and specific", and "regularly reviewed", in accordance with Article 6(4) PNR Directive and para. 174 of Opinion 1/15 (para. 189).

The Court then considers the processing of PNR data against pre-determined criteria. As a crucial safeguard against discrimination, according to Article 6(4) of the PNR Directive, the pre-determined criteria may not be based on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life, or sexual orientation. To the ECJ, this means that pre-determined criteria "are 'in no circumstances' to be based on those characteristics" and this provision must be understood as covering "both direct and indirect discrimination" (para. 197).

The appropriateness of the PNR system requires the "proper functioning" of the individual review by non-automated means, which fulfils several functions (see paras 203-208). First, it serves to keep "to a minimum the number of innocent people wrongly identified" by a system which produces a "fairly substantial number of 'false positives'" Second, it is a safeguard against a decision "that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data". Third, the individual review should exclude any discriminatory results from the automated processing. The PIU should thus only transfer results to the competent authorities which, following the individual review, give rise, "to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime of persons identified by means of those automated processing operations". Member States must lay down clear and precise rules which "guarantee a uniform administrative practice within the PIU".

In this regard, PIUs must "maintain documentation relating to all processing of PNR data", automated or manually, "for the purpose of verifying its lawfulness and for the purpose of self-monitoring" (para. 206), including by the data protection officer and the national supervisory authority (para. 212). Such documentation is moreover a prerequisite for exercising a person's right to judicial redress (para. 210).

Requests by competent authorities for PNR data and prior review

During the period in which the data is retained, PIUs may also respond, "on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities" and provide PNR data results to these authorities "in specific cases". That such disclosure of PNR data requires "sufficient grounds" is interpreted by the Court as referring to "objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved […] in serious crime […]" (para. 220).

Strengthening prior review as a procedural safeguard, the ECJ interprets Article 12(3)(b) of the PNR Directive as meaning that requests for disclosure of PNR data during the initial six months period require prior approval by a court or independent national authority (paras 222-224). If a court is not tasked with prior review, the competent national authority "must have a status that enables it to act objectively and impartially when carrying out its duties and must, therefore, be free from any external influence" (para. 226). Following an interpretation that is consistent with the Charter, the PNR Directive must thus be interpreted as precluding national legislation pursuant to which the authority, which submits a request for PNR data, as well as the PIU itself, is designated as the competent national authority with power to approve the disclosure of PNR data (paras 227 and 247).

Retention period of six months is necessary, not five years

The Court holds that the retention of PNR data of all air passengers during the initial period of six months without any indication as to their involvement in terrorist offences or serious crime "does not appear, as a matter of principle, to go beyond what is strictly necessary" (para. 255). By contrast, the five-year period of general retention of PNR data of all air passengers set out in Article 12(3) of the PNR Directive, without any connection between the PNR data and the objectives of the PNR Directive, "entails an inherent risk of disproportionate use and abuse" (para. 256). A Charter-conforming interpretation of the PNR Directive, hence, "precludes national legislation, which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers" (para. 262).

Commentary

The judgment is not a victory for those who had hoped the Court would invalidate the PNR Directive. The ECJ, in principle, signs off on the EU-wide security practice surrounding passenger data introduced by the PNR Directive. In relation to extra-EU flights, the Court does not apply its case law on communications data retention to the PNR system, which already transpired from its Opinion 1/15. Concerning the collection of PNR data from intra-EU flights, however, the ECJ formulates requirements, which are consistent with its case law on communications data retention (see *La Quadrature du Net and Others*, para. 137; *SpaceNet and Telekom Deutschland*). Restricting the Member States' power to collect PNR data from intra-EU flights significantly limits the scale and scope of the EU-wide PNR system.

In its judgment, the ECJ does not engage with the argument that the PNR Directive corresponds to international standards which define government access to PNR data as a security practice (see e.g., Security Council resolutions 2396 (2017) and 2482 (2019) or the PNR Guidelines by the International Civil Aviation Organization (ICAO 2010)). Neither is the Court concerned about the fact that PNR data are often non-verified data from air carriers' reservation systems or whether such data can be used to identify persons reliably (see Korff 2021).

Consistent with its Opinion 1/15, the ECJ does not take much issue with the fairly substantial margin of error from the automated processing of PNR data, as long as an individual review by non-automated means can effectively reduce the number of innocent persons identified. Overall, the Court places much confidence in various reviews to safeguard PNR data against unlawful use, as well as monitoring by the PIU's data protection officer, supervision by the national data protection authority, and ultimately judicial review.

The judgment is, however, alert to the use of artificial intelligence technology and notes that, "given the opacity which characterises the way in which artificial intelligence technology works" (para. 195), data subjects could be deprived of their right to an effective judicial remedy pursuant to Article 47 of the Charter. The ECJ shares the AG's

observation that the notion of pre-determined criteria precludes "the use of artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review … the assessment criteria … as well as the weighting of those criteria" (para. 194).

Member States are now tasked with bringing their national laws and practices in line with the ECJ judgment requiring that:

- national implementations of the PNR Directive are limited to combatting terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air;
- air carriers transfer only PNR data items in line with the ECJ's interpretation;
- only PNR data from extra-EU flights are systematically transferred;
- Member States assess whether there is a threat linked to terrorist offences and serious crime that justifies the collection of PNR data from intra-EU flights;
- only databases that meet the objective of the PNR Directive are designated for the advance assessment of PNR data by automated means;
- pre-determined criteria do not discriminate directly or indirectly against persons having protected characteristics;
- the individual review by non-automated means by PIU staff functions effectively and consistently;
- the general retention of PNR data is limited to six months after their initial collection and, after that period, only PNR data of persons are retained where objective evidence establishes a risk of their involvement in terrorist offences or serious crime; and
- requests for PNR data from competent authorities are subject to an independent review by a court or administrative body.

It is unclear how quickly Member States will make the necessary modifications to their national PNR laws and practices or how this will be monitored.

The judgment also has repercussions for the EU Security Union Strategy and the EU's plans to expand the PNR system to cover additional data and alternative modes of transport. The Commission's 2020 review of the PNR Directive (COM(2020) 305 final) hinted at the possibility of mandating the collection of passengers' date of birth by air carriers. Further, the Commission, following a recommendation by the Council (14746/19), embarked on an impact assessment on potentially widening the scope of PNR data legislation to transport forms other than air traffic, such as maritime, rail and road carriers, which could now only be considered for extra-EU transport (if at all). Member States are also likely not too content that their powers to introduce national measures to monitor intra-EU travellers are curbed by EU law. They could nevertheless adopt measures that breach the ECJ's judgment, as has been the case with communications data retention measures adopted by numerous Member States (see Manancourt 2022). *Ligue des droits humains* is thus unlikely to be the last case before the Court on the PNR Directive.