DOI:10.1017/ilm.2023.8

INTRODUCTORY NOTE TO CASE C-817/19, LIGUE DES DROITS HUMAINS V. COUNCIL OF MINISTERS (C.J.E.U.)

BY SOPHIE DUROY*

[June 21, 2022]

Introduction

On June 21, 2022, the Court of Justice of the European Union (CJEU), sitting as a Grand Chamber, rendered its decision in the preliminary ruling procedure C-817/19, *Ligue des Droits Humains* v. *Council of Ministers*.[1] In its ruling, the CJEU held that the surveillance regime established by the Passenger Name Record Directive 2016/681[2] (PNR Directive) was compatible with the Charter of Fundamental Rights of the European Union (CFREU/EU Charter).[3] Nevertheless, the CJEU strictly circumscribed the Directive's transposition within EU member states' domestic laws. While restricting permissible interpretations of the PNR Directive's provisions and imposing strict limitations on its scope to ensure its conformity with the EU Charter, for the first time the Court upheld an instrument of indiscriminate surveillance as compatible with EU primary law. This represents a significant development in the CJEU's case law on privacy rights, which is likely to affect the negotiation and development of future PNR agreements with third countries, as well as the development of the ePrivacy Regulation, discussions surrounding the regulation of AI, and negotiations for international instruments aiming to address serious crimes. Further, the ruling confirms the CJEU's increasing convergence with the European Court of Human Rights' (ECtHR) case law on the matter, thus inscribing national security as a legitimate exception to the general prohibition of indiscriminate bulk data collection and retention in Europe.

Background

Since its original 2014 pronouncement in *Digital Rights Ireland*,[4] the CJEU has grappled with a number of instruments and domestic laws concerning indiscriminate data collection and retention. Originally extremely protective of privacy rights, the Court has slowly evolved towards a stance more deferential to states' national security concerns.

In *Digital Rights Ireland*, the CJEU rejected a model of mass surveillance based on the general and indiscriminate retention of communication metadata as incompatible with the EU Charter. As a result, it annulled the Data Retention Directive.[5] In this landmark judgment, the CJEU thus rejected the possibility that indiscriminate data retention could constitute a proportionate interference with the right to respect for private and family life (Article 7 CFREU) and to the protection of personal data (Article 8 CFREU). The Court's principled opposition to mass surveillance was reaffirmed in further cases concerning EU member states' data-retention regimes;[6] international data sharing;[7] and the transfer of Passenger Name Record data.[8]

This principled position was, however, undermined in October 2020. In *La Quadrature du Net and Others*,[9] concerning the compatibility with EU law of French and Belgian laws on data processing, the Court held for the first time that bulk retention of communications data could be justified on national security grounds. The Court was careful to mandate strong procedural safeguards. Nevertheless, *La Quadrature du Net* resulted in the principled acceptance of bulk data retention (and thus bulk data collection as a necessary prior step) as a proportionate interference with fundamental rights when the objective of general interest pursued is the protection of national security. The national security exception was reaffirmed in a later decision, a preliminary ruling concerning Germany's telecommunications data retention law (*SpaceNet AG* and *Telekom Deutschland*).[10]

Unlike *La Quadrature du Net* and *SpaceNet AG* and *Telekom Deutschland*, the Belgian court's referral for a preliminary ruling in *Ligue des Droits Humains* pertained not only to the conformity of national legislation with EU law but also to the validity of an EU instrument, namely the PNR Directive, which requires the systematic processing of PNR data relating to air passengers on extra-EU flights entering and leaving the EU for the purposes of combating terrorist

*Sophie Duroy is a post-doctoral fellow at the KFG Berlin-Potsdam Research Group 'The International Rule of Law: Rise or Decline?', Germany. She holds a PhD in Law from the European University Institute.

offenses and serious crime, and authorizes similar measures for intra-EU flights. The CJEU therefore had to pronounce itself on the validity of the PNR Directive with regard to EU primary law, in this case the EU Charter.

Ruling

In its ruling, the CJEU found the PNR Directive to be compatible with the EU Charter. While noting the seriousness of the Directive's interferences with the rights to privacy and the protection of personal data,[11] the Court provided a detailed analysis of the justification for these interferences.[12] In particular, the CJEU found that the interferences are necessary and proportionate to the objective of legitimate interest that the Directive seeks to achieve, namely "to ensure the internal security of the European Union and thus protect the life and safety of persons."[13] Hence, despite the Directive seeking to introduce "a surveillance regime that is continuous, untargeted and systematic, including the automatic assessment of the personal data of everyone using air transport services,"[14] the CJEU ultimately concluded that the Directive is consistent with the Charter.

Nevertheless, in doing so, the Court strictly circumscribed the transposition of the PNR Directive by member states. The CJEU thus imposed numerous limitations and restrictive interpretations, many of which derived from Opinion 1/15 in which it had invalidated the proposed PNR agreement between the EU and Canada.[15] First, as regards the material scope of the PNR regime, the CJEU limited the information that can be collected to the data listed in the Directive's Annex I.[16] It also specified that this regime can only be applied for the purpose of combating serious crime and should not be extended to ordinary crime.[17] Further, despite Article 2 of the Directive unreservedly allowing member states to apply the PNR regime to intra-EU flights, the Court held that this regime may only apply to intra-EU flights and/or other means of transport in the presence of "a genuine and present or foreseeable threat."[18]

Then, with regard to the processing of PNR data, the CJEU held that member states may not add processing purposes other than those exhaustively listed in Article 1(2) of the Directive.[19] Nor can they empower their Passenger Information Units (PIUs) to authorize the disclosure of PNR data after the six-month period provided for in the Directive.[20] Then, in direct contradiction with the text of Article 12(1) of the Directive mandating a five-year retention period for all PNR data, the Court held that member states may not set a general retention period for data for all air passengers, regardless of whether they pose a terrorist risk or present no risk at all.[21]

The Court also specified limitations concerning the means and methods used to process PNR data. It thus stated that, to compare PNR data with existing databases, PIUs may only use databases "on persons or objects sought or under alert."[22] Furthermore, the Court excluded the possibility of using self-learning AI technologies to process PNR data if these technologies can modify their processing methods without human intervention or control.[23] In addition, the results of any automated processing of PNR data must be thoroughly and effectively reviewed by a PIU official.[24] Hence, while AI processing is authorized, human oversight remains mandatory.

Conclusion

The CJEU's ruling in *Ligue des Droits Humains* is part of a broader judicial movement legitimating bulk data collection and retention for national security purposes in Europe. Aligning itself with ECtHR's case-law on mass surveillance regimes,[25] the CJEU confirms that the protection of national security constitutes an objective capable of rendering bulk data collection and retention necessary and proportionate under the EU Charter. Nevertheless, the ruling presents itself as a complex balancing exercise. On the one hand, the Court finds the PNR Directive compatible with the EU Charter. On the other hand, and through the same reasoning, the Court imposes extremely restrictive interpretations of the Directive's provisions to EU member states to ensure such compatibility. By so doing, the Court adopts a rule-creating role. Indeed, these restrictive interpretations are sometimes in direct contradiction to the text of the Directive (for instance concerning the retention period for PNR data or the limitations on EU member states' competence to apply the PNR regime to intra-EU flights). Since member states' transposition laws will need to reflect these interpretations, their lack of textual basis is likely to trigger further litigation.

The development and confirmation of a national security exception to the general prohibition of indiscriminate bulk data collection and retention by the CJEU in its recent case-law also has the potential to influence law-making efforts at both EU and international levels. In the European Union, future agreements, directives, and regulations will necessarily take into account the CJEU's latest case-law to ensure conformity with the EU Charter. Discussions on AI

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

and PNR agreements with third countries will be directly affected by the ruling. *Ligue des Droits Humains* could also affect the new ePrivacy Regulation[26] currently being developed to replace the ePrivacy Directive,[27] with regard to which the Council of the European Union had already proposed to exclude national security activities from its scope.[28] Beyond Europe, the ruling might have consequences in multilateral negotiation fora, for instance in the UN Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes.[29] Indeed, European courts' principled acceptance of indiscriminate data collection and retention as compatible with fundamental rights when national security is at stake could further hinder civil society's efforts to bring privacy rights to the forefront of discussions.

ENDNOTES

1 Case C-817/19, Ligue des Droits Humains v. Council of Ministers, ECLI:EU:C:2022:491 [hereinafter Judgment].

2 Directive (EU) 2016/681 of the European Parliament and of the Council of Apr. 27, 2016, on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

3 Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

4 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung and Others ECLI:EU:C:2014:238 (Apr. 8, 2014).

5 Directive 2006/24/EC of the European Parliament and of the Council of Mar. 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 (Data Retention Directive).

6 Joined Cases C-203/15 and C-689/15, Tele2 Sverige AB v. Postoch telestyrelsen and Secretary of State for the Home Dept. v. Watson, ECLI:EU:C:2016:970 (Dec. 21, 2016).

7 Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015) and Case C-311/18, Data Protection Commissioner v. Facebook Ir. Ltd. & Schrems, ECLI:EU:C:2020:559 (July 16, 2020).

8 Opinion 1/15, ECLI:EU:C:2016:656 (Sept. 8, 2016).

9 Joined Cases C-511/18, C-512/18, and C-520/18, La Quadrature du Net v. Premier Ministre, ECLI:EU:C:2020:791 (Oct. 6, 2020). *See also* 60 I.L.M. 464 (2021).

10 Joined Cases C-793/19 (SpaceNet AG) and C-794/19 (Telekom Deutschland), ECLI:EU:C:2022:702 (Sept. 20, 2022).

11 Judgment ¶ 111.

12 *Id.* ¶¶ 112–128.

13 *Id.* ¶ 121.

14 *Id.* ¶ 111.

15 Opinion 1/15, ECLI:EU:C:2016:656 (Sept. 8, 2016).

16 Judgment ¶¶ 131–139.

17 *Id.* ¶ 152.

18 *Id.* ¶¶ 173–174.

19 *Id.* ¶¶ 236–237.

20 *Id.* ¶ 247.

21 *Id.* ¶ 262.

22 *Id.* ¶¶ 187–188.

23 *Id.* ¶¶ 193–201.

24 *Id.* ¶¶ 202–213.

25 *See*, *in particular*, Big Brother Watch v. U.K. [GC], App. Nos. 58170/13, 62322/14, and 24960/15 (May 25, 2021); Centrum för Rättvisa v. Swed. [GC], App. No. 35252/08 (May 25, 2021).

26 *Commission proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM (2017) 010 final (Oct. 1, 2017).

27 Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

28 *Commission proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)—Mandate for negotiations with the European Parliament*, ST 6087 2021 INIT (Feb. 10, 2021).

29 *See*: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

DOI:10.1017/ilm.2023.8

CASE C-817/19, LIGUE DES DROITS HUMAINS V. COUNCIL OF MINISTERS (C.J.E.U.)*
[June 21, 2022]

JUDGMENT OF THE COURT (Grand Chamber)

21 June 2022**

Table of contents

(Reference for a preliminary ruling – Processing of personal data – Passenger Name Records (PNR) – Regulation (EU) 2016/679 – Article 2(2)(d) – Scope – Directive (EU) 2016/681 – Use of PNR data of air passengers of flights operated between the European Union and third countries – Power to include data of air passengers of flights operated within the European Union – Automated processing of that data – Retention period – Fight against terrorist offences and serious crime – Validity – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 21 as well as Article 52(1) – National legislation extending the application of the PNR system to other transport operations within the European Union – Freedom of movement within the European Union – Charter of Fundamental Rights – Article 45)

In Case C-817/19,

REQUEST for a preliminary ruling under Article 267 TFEU from the Cour constitutionnelle (Constitutional Court, Belgium), made by decision of 17 October 2019, received at the Court on 31 October 2019, in the proceedings

Ligue des droits humains

v

Conseil des ministres,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, A. Arabadjiev, S. Rodin, I. Jarukaitis and N. Jääskinen, Presidents of Chambers, T. von Danwitz (Rapporteur), M. Safjan, F. Biltgen, P.G. Xuereb, N. Piçarra, L.S. Rossi, A. Kumin and N. Wahl, Judges,

Advocate General: G. Pitruzzella,

Registrar: M. Krausenböck, Administrator,

having regard to the written procedure and further to the hearing on 13 July 2021,

after considering the observations submitted on behalf of:

– the Ligue des droits humains, by C. Forget, avocate,

– the Belgian Government, by P. Cottin, J.-C. Halleux, C. Pochet, M. Van Regemorter, acting as Agents, and by C. Caillet, advocaat, E. Jacubowitz, avocat, G. Ceuppens, V. Dethy and D. Vertongen,

– the Czech Government, by T. Machovičová, O. Serdula, M. Smolek and J. Vláčil, acting as Agents,

– the Danish Government, by M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen and M. Søndahl Wolff, acting as Agents,

– the German Government, by D. Klebs and J. Möller, acting as Agents,

*This text was reproduced and reformatted from the text available at the Court of Justice of the European Union website (visited February 6, 2023), https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=13059170.
**Language of the case: French.

– the Estonian Government, by N. Grünberg, acting as Agent,
– Ireland, by M. Browne, A. Joyce, J. Quaney, acting as Agents, and D. Fennelly, Barrister-at-Law,
– the Spanish Government, by L. Aguilera Ruiz, acting as Agent,
– the French Government, by D. Dubois, E. de Moustier and T. Stéhelin, acting as Agents,
– the Cypriot Government, by I. Neofytou, acting as Agent,
– the Latvian Government, by E. Bārdiņš, K. Pommere and V. Soņeca, acting as Agents,
– the Netherlands Government, by M.K. Bulterman, A. Hanje, J. Langer and C.S. Schillemans, acting as Agents,
– the Austrian Government, by G. Kunnert, A. Posch and J. Schmoll, acting as Agents,
– the Polish Government, by B. Majczyna, acting as Agent,
– the Slovak Government, by B. Ricziová, acting as Agent,
– the Finnish Government, by A. Laine and H. Leppo, acting as Agent,
– the European Parliament, by O. Hrstková Šolcová and P. López-Carceller, acting as Agents,
– the Council of the European Union, by J. Lotarski, N. Rouam, E. Sitbon and C. Zadra, acting as Agents,
– the European Commission, by D. Nardi and M. Wasmeier, acting as Agents,
– the European Data Protection Supervisor, by P. Angelov, A. Buchta, F. Coudert and C.-A. Marnier, acting as Agents,
– the European Union Agency for Fundamental Rights, by L. López, T. Molnar, M. Nespor and M. O'Flaherty, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 27 January 2022,

gives the following

Judgment

1 This reference for a preliminary ruling, in essence, concerns:

– the interpretation of Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1; 'the GDPR'), of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24; 'the API Directive') and of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC (OJ 2010 L 283, p. 1);

– the interpretation and validity, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter'), of Article 3(4) and Articles 6 and 12 of, as well as Annex I to, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132; 'the PNR Directive'), and

– the interpretation and validity, in the light of Article 3(2) TEU and Article 45 of the Charter, of the API Directive.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

2 The request has been made in proceedings between the Ligue des droits humains and the Conseil des ministres (Council of Ministers, Belgium) concerning the legality of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data).

I. Legal context

A. European Union law

1. Directive 95/46/EC

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3(2) of that directive provided:

'This Directive shall not apply to the processing of personal data:

– in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

– by a natural person in the course of a purely personal or household activity.'

2. The API Directive

4 Recitals 1, 7, 9 and 12 of the API Directive state:

'(1) In order to combat illegal immigration effectively and to improve border control, it is essential that all Member States introduce provisions laying down obligations on air carriers transporting passengers into the territory of the Member States. In addition, in order to ensure the greater effectiveness of this objective, the financial penalties currently provided for by the Member States for cases where carriers fail to meet their obligations should be harmonised to the extent possible, taking into account the differences in legal systems and practices between the Member States.

...

(7) The obligations to be imposed on carriers by virtue of this Directive are complementary to those established pursuant to the provisions of Article 26 of the 1990 Schengen Convention implementing the Schengen Agreement of 14 June 1985, as supplemented by Council Directive 2001/51/EC [of 28 June 2001 supplementing the provisions of Article 26 of the Convention implementing the Schengen Agreement of 14 June 1985 (OJ 2001 L 187, p. 45)], the two types of obligation serving the same objective of curbing migratory flows and combating illegal immigration.

...

(9) In order to combat illegal immigration more effectively and in order to ensure the greater effectiveness of this objective, it is essential that, without prejudice to the provisions of Directive [95/46], account be taken at the earliest opportunity of any technological innovation, especially with reference to the integration and use of biometric features in the information to be provided by the carriers.

...

(12) Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States. This means, that whereas it would be legitimate to process the passenger data transmitted for the performance of border checks also for the purposes of allowing their use as evidence in proceedings aiming at the enforcement of the laws and regulations on entry and immigration, including their provisions on the protection of public policy (*ordre public*) and national security, any further processing in a way incompatible with those purposes would run counter to the principle set out in

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

Article 6(1)(b) of Directive [95/46]. Member States should provide for a system of sanctions to be applied in the event of use contrary to the purpose of the present Directive.'

5 Article 1 of the API Directive, entitled 'Objective', provides:

'This Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities.'

6 Article 2 of that directive, entitled 'Definitions', states:

'For the purpose of this Directive:

(a) "carrier" means any natural or legal person whose occupation it is to provide passenger transport by air;

(b) "external borders" means the external borders of the Member States with third countries;

(c) "border control" means a check carried out at a border in response exclusively to an intention to cross that border, regardless of any other consideration;

(d) "border crossing point" means any crossing point authorised by the competent authorities for crossing external borders;

(e) "personal data", "processing of personal data" and "personal data filing system" have the meaning as stipulated under Article 2 of Directive [95/46].'

7 Article 3 of that directive, entitled 'Data transmission', provides, in its paragraphs 1 and 2:

'1. Member States shall take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State.

2. The information referred to above shall comprise:

– the number and type of travel document used,

– nationality,

– full names,

– the date of birth,

– the border crossing point of entry into the territory of the Member States,

– code of transport,

– departure and arrival time of the transportation,

– total number of passengers carried on that transport,

– the initial point of embarkation.'

8 Article 6 of the API Directive, entitled 'Data processing', provides:

'1. The personal data referred to in Article 3(1) shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks with the objective of combating illegal immigration more effectively.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

Member States shall ensure that these data are collected by the carriers and transmitted electronically or, in case of failure, by any other appropriate means to the authorities responsible for carrying out border checks at the authorised border crossing point through which the passenger will enter the territory of a Member State. The authorities responsible for carrying out checks on persons at external borders shall save the data in a temporary file.

After passengers have entered, these authorities shall delete the data, within 24 hours after transmission, unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive [95/46].

Member States shall take the necessary measures to oblige carriers to delete, within 24 hours of the arrival of the means of transportation pursuant to Article 3(1), the personal data they have collected and transmitted to the border authorities for the purposes of this Directive.

In accordance with their national law and subject to data protection provisions under Directive [95/46], Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.

2. Member States shall take the necessary measures to oblige the carriers to inform the passengers in accordance with the provisions laid down in Directive [95/46]. This shall also comprise the information referred to in Article 10(c) and Article 11(1)(c) of Directive [95/46].'

3. Directive 2010/65

9 Directive 2010/65 is to be repealed, pursuant to Article 25 of Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65 (OJ 2019 L 198, p. 64), from 15 August 2025.

10 Recital 2 of that directive states:

'For the facilitation of maritime transport and in order to reduce the administrative burdens for shipping companies, the reporting formalities required by legal acts of the [European] Union and by Member States need to be simplified and harmonised to the greatest extent possible. . . .'

11 Article 1 of that directive, entitled 'Subject matter and scope', provides, in its paragraphs 1 and 2:

'1. The purpose of this Directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities.

2. This Directive shall apply to the reporting formalities applicable to maritime transport for ships arriving in and ships departing from ports situated in Member States.'

12 Under Article 8 of that directive, entitled 'Confidentiality':

'1. Member States shall, in accordance with the applicable legal acts of the [European] Union or national legislation, take the necessary measures to ensure the confidentiality of commercial and other confidential information exchanged in accordance with this Directive.

2. Member States shall take particular care to protect commercial data collected under this Directive. In respect of personal data, Member States shall ensure that they comply with Directive [95/46]. The [EU] institutions and bodies shall ensure that they comply with Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)].'

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

4. The GDPR

13 Recital 19 of the GDPR states:

> 'The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific [EU] legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific [EU] legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council [of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89)]. Member States may entrust competent authorities within the meaning of [Directive 2016/680] with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of [EU] law, falls within the scope of this Regulation.
> . . .'

14 Article 2 of that regulation, entitled 'Material scope', provides in its paragraphs 1 and 2:

> '1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> 2. This Regulation does not apply to the processing of personal data:
>
> (a) in the course of an activity which falls outside the scope of [EU] law;
>
> (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V [TEU]; . . .
>
> (c) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

15 Article 4 of that regulation, entitled 'Definitions', provides:

> 'For the purposes of this Regulation:
>
> (1) "personal data" means any information relating to an identified or identifiable natural person . . .;
>
> (2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
>
> . . .'

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

16 Article 23 of the GDPR, entitled 'Restrictions', provides:

'1. [EU] or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as in Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; . . .

(e) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); . . .

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'

17 Article 94 of that regulation, entitled 'Repeal of Directive [95/46]' provides:

'1. Directive [95/46] is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive [95/46] shall be construed as references to the European Data Protection Board established by this Regulation.'

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

5. Directive 2016/680

18 Directive 2016/680, in accordance with Article 59 thereof, repealed and replaced Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60), from 6 May 2018.

19 Recitals 9 to 11 of Directive 2016/680 state:

> '(9) On that basis, [the GDPR] lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the [European] Union.
>
> (10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and on the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields.
>
> (11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] applies. [The GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of [the GDPR] remains unaffected for the processing of personal data by the processor outside the scope of this Directive.'

20 Article 1 of that directive, entitled 'Subject matter and objectives', which corresponds, in essence, to Article 1 of Framework Decision 2008/977, provides, in its paragraph 1:

> 'This Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

21 Under Article 3 of that directive, entitled 'Definitions':

> 'For the purposes of this Directive:
>
> . . .
>
> 7. "competent authority" means:
>
> (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
>
> (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

. . .'

6. The PNR Directive

22 Recitals 4 to 12, 15, 19, 20, 22, 25, 27, 28, 33, 36 and 37 of the PNR Directive state:

'(4) [The API Directive] regulates the transfer of advance passenger information (API) data by air carriers to the competent national authorities for the purpose of improving border controls and combating illegal immigration.

(5) The objectives of this Directive are, inter alia, to ensure security, to protect the life and safety of persons, and to create a legal framework for the protection of PNR data with regard to their processing by competent authorities.

(6) Effective use of PNR data, for example by comparing PNR data against various databases on persons and objects sought, is necessary to prevent, detect, investigate and prosecute terrorist offences and serious crime and thus enhance internal security, to gather evidence and, where relevant, to find associates of criminals and unravel criminal networks.

(7) Assessment of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities. By using PNR data it is possible to address the threat of terrorist offences and serious crime from a different perspective than through the processing of other categories of personal data. However, to ensure that the processing of PNR data remains limited to what is necessary, the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of such criteria is relevant. Furthermore, the assessment criteria should be defined in a manner which keeps to a minimum the number of innocent people wrongly identified by the system.

(8) Air carriers already collect and process their passengers' PNR data for their own commercial purposes. This Directive should not impose any obligation on air carriers to collect or retain any additional data from passengers or any obligation on passengers to provide any data in addition to that already being provided to air carriers.

(9) Some air carriers retain as part of the PNR data the API data they collect, while others do not. The use of PNR data together with API data has added value in assisting Member States in verifying the identity of an individual, thus reinforcing the law enforcement value of that result and minimising the risk of carrying out checks and investigations on innocent people. It is therefore important to ensure that where air carriers collect API data, they transfer it irrespective of whether they retain API data by different technical means as for other PNR data.

(10) To prevent, detect, investigate and prosecute terrorist offences and serious crime, it is essential that all Member States introduce provisions laying down obligations on air carriers operating extra-EU flights to transfer PNR data they collect, including API data. Member States should also have the possibility to extend this obligation to air carriers operating intra-EU flights. Those provisions should be without prejudice to [the API Directive].

(11) The processing of personal data should be proportionate to the specific security goals pursued by this Directive.

(12) The definition of terrorist offences applied in this Directive should be the same as in Council Framework Decision 2002/475/JHA [of 13 June 2002 on combating terrorism (OJ 2002 L 164, p. 3)]. The definition of serious crime should encompass the categories of offence listed in Annex II to this Directive.

. . .

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

(15) A list of the PNR data to be obtained by a [passenger information unit (PIU)] should be drawn up with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data. To that end, high standards should be applied in accordance with [the Charter], the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No 108"), and the European Convention for the Protection of Human Rights and Fundamental Freedom[, signed at Rome on 4 November 1950] (the "ECHR"). Such a list should not be based on a person's race or ethnic origin, religion or belief, political or any other opinion, trade union membership, health, sexual life or sexual orientation. The PNR data should only contain details of passengers' reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security.

. . .

(19) Each Member State should be responsible for assessing the potential threats related to terrorist offences and serious crime.

(20) Taking fully into consideration the right to the protection of personal data and the right to non-discrimination, no decision that produces an adverse legal effect on a person or significantly affects that person should be taken only by reason of the automated processing of PNR data. Moreover, in respect of Articles 8 and 21 of the Charter, no such decision should discriminate on any grounds such as a person's sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. The [European] Commission should also take those principles into account when reviewing the application of this Directive.

. . .

(22) Taking fully into consideration the principles outlined in recent relevant case-law of the Court of Justice of the European Union, the application of this Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality. It should also genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime. The application of this Directive should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data.

. . .

(25) The period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Because of the nature of the data and their uses, it is necessary that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations. To avoid disproportionate use, after the initial retention period the PNR data should be depersonalised through masking out of data elements. To ensure the highest level of data protection, access to the full PNR data, which enable direct identification of the data subject, should be granted only under very strict and limited conditions after that initial period.

. . .

(27) The processing of PNR data in each Member State by the PIU and by competent authorities should be subject to a standard of protection of personal data under national law in line with Framework Decision [2008/977] and the specific data protection requirements laid down in this Directive. References to Framework Decision [2008/977] should be understood as references to legislation currently in force as well as to legislation that will replace it.

(28) Taking into consideration the right to the protection of personal data, the rights of data subjects concerning the processing of their PNR data, such as the rights of access, rectification, erasure and restriction and the rights

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

to compensation and judicial redress, should be in line both with Framework Decision [2008/977] and with the high level of protection provided by the Charter and the ECHR.

. . .

(33) This Directive does not affect the possibility for Member States to provide, under their national law, for a system of collecting and processing PNR data from non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services – including the booking of flights – for which they collect and process PNR data, or from transportation providers other than those specified in this Directive, provided that such national law complies with [EU] law.

. . .

(36) This Directive respects the fundamental rights and the principles of the Charter, in particular the right to the protection of personal data, the right to privacy and the right to non-discrimination as protected by Articles 8, 7 and 21 thereof; it should therefore be implemented accordingly. This Directive is compatible with data protection principles and its provisions are in line with Framework Decision [2008/977]. Furthermore, to comply with the proportionality principle, on specific issues this Directive provides for stricter rules on data protection than Framework Decision [2008/977].

(37) The scope of this Directive is as limited as possible since: it provides for the retention of PNR data in the PIUs for a period of time not exceeding five years, after which the data should be deleted; it provides for the data to be depersonalised through masking out of data elements after an initial period of six months; and it prohibits the collection and use of sensitive data. To ensure efficiency and a high level of data protection, Member States are required to ensure that an independent national supervisory authority and, in particular, a data protection officer are responsible for advising and monitoring the way PNR data are processed. All processing of PNR data should be logged or documented for the purposes of verifying its legality, self-monitoring and ensuring proper data integrity and secure processing. Member States should also ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.'

23 Article 1 of the PNR Directive, entitled 'Subject matter and scope', is worded as follows:

1. '1. This Directive provides for:
   (a) the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights,
   (b) the processing of the data referred to in point (a), including its collection, use and retention by Member States and its exchange between Member States.
2. PNR data collected in accordance with this Directive may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2).'

24 In accordance with Article 2 of that directive, entitled 'Application of this Directive to intra-EU flights':

1. If a Member State decides to apply this Directive to intra-EU flights, it shall notify the Commission in writing. A Member State may give or revoke such a notification at any time. The Commission shall publish that notification and any revocation of it in the *Official Journal of the European Union*.
2. Where a notification referred to in paragraph 1 is given, all the provisions of this Directive shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights.
3. A Member State may decide to apply this Directive only to selected intra-EU flights. In making such a decision, the Member State shall select the flights it considers necessary in order to pursue the objectives of this Directive. The Member State may decide to change the selection of intra-EU flights at any time.'

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

25 Under Article 3 of that directive, entitled 'Definitions':

'For the purposes of this Directive the following definitions apply:

(1) "air carrier" means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage of passengers by air;

(2) "extra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stop-overs in the territory of Member States or third countries;

(3) "intra-EU flight" means any scheduled or non-scheduled flight by an air carrier flying from the territory of a Member State and planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country;

(4) "passenger" means any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried in an aircraft with the consent of the air carrier, such consent being manifested by that person's registration in the passengers list;

(5) "passenger name record" or "PNR" means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;

(6) "reservation system" means the air carrier's internal system, in which PNR data are collected for the handling of reservations;

(7) "push method" means the method whereby air carriers transfer PNR data listed in Annex I into the database of the authority requesting them;

(8) "terrorist offences" means the offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475];

(9) "serious crime" means the offences listed in Annex II that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State;

(10) "to depersonalise through masking out of data elements" means to render those data elements which could serve to identify directly the data subject invisible to a user.'

26 Article 4 of the PNR Directive, entitled 'Passenger information unit', provides in paragraphs 1 to 3:

1. Each Member State shall establish or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime or a branch of such an authority, to act as its passenger information unit ("PIU").

2. The PIU shall be responsible for:

(a) collecting PNR data from air carriers, storing and processing those data and transferring those data or the result of processing them to the competent authorities referred to in Article 7;

(b) exchanging both PNR data and the result of processing those data with the PIUs of other Member States and with Europol in accordance with Articles 9 and 10.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

3. Staff members of a PIU may be seconded from competent authorities. Member States shall provide the PIUs with adequate resources for them to fulfil their tasks.'

27 Article 5 of that directive, entitled 'Data protection officer in the PIU' is worded as follows:

1. The PIU shall appoint a data protection officer responsible for monitoring the processing of PNR data and implementing relevant safeguards.

2. Member States shall provide data protection officers with the means to perform their duties and tasks in accordance with this Article effectively and independently.

3. Member States shall ensure that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data.'

28 Article 6 of that directive, entitled 'Processing of PNR data', provides that:

1. The PNR data transferred by the air carriers shall be collected by the PIU of the relevant Member State as provided for in Article 8. Where the PNR data transferred by air carriers include data other than those listed in Annex I, the PIU shall delete such data immediately and permanently upon receipt.

2. The PIU shall process PNR data only for the following purposes:

   (a) carrying out an assessment of passengers prior to their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent authorities referred to in Article 7, and, where relevant, by Europol in accordance with Article 10, in view of the fact that such persons may be involved in a terrorist offence or serious crime;

   (b) responding, on a case-by-case basis, to a duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime, and to provide the competent authorities or, where appropriate, Europol with the results of such processing; and

   (c) analysing PNR data for the purpose of updating or creating new criteria to be used in the assessments carried out under point (b) of paragraph 3 in order to identify any persons who may be involved in a terrorist offence or serious crime.

3. When carrying out the assessment referred to in point (a) of paragraph 2, the PIU may:

   (a) compare PNR data against databases relevant for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases; or

   (b) process PNR data against pre-determined criteria.

4. Any assessment of passengers prior to their scheduled arrival in or departure from the Member State carried out under point (b) of paragraph 3 against pre-determined criteria shall be carried out in a non-discriminatory manner. Those pre-determined criteria must be targeted, proportionate and specific. Member States shall ensure that those criteria are set and regularly reviewed by the PIU in cooperation with the competent authorities referred to in Article 7. The criteria shall in no circumstances 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.

5. Member States shall ensure that any positive match resulting from the automated processing of PNR data conducted under point (a) of paragraph 2 is individually reviewed by non-automated means to verify whether the competent authority referred to in Article 7 needs to take action under national law.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

6. The PIU of a Member State shall transmit the PNR data of persons identified in accordance with point (a) of paragraph 2 or the result of processing those data for further examination to the competent authorities referred to in Article 7 of the same Member State. Such transfers shall only be made on a case-by-case basis and, in the event of automated processing of PNR data, after individual review by non-automated means.

7. Member States shall ensure that the data protection officer has access to all data processed by the PIU. If the data protection officer considers that processing of any data has not been lawful, the data protection officer may refer the matter to the national supervisory authority. . . .

8. The consequences of the assessments of passengers referred to in point (a) of paragraph 2 of this Article shall not jeopardise the right of entry of persons enjoying the [EU] right of free movement into the territory of the Member State concerned as laid down in Directive 2004/38/EC of the European Parliament and of the Council [of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ 2004 L 158, p. 77)]. In addition, where assessments are carried out in relation to intra-EU flights between Member States to which Regulation (EC) No 562/2006 of the European Parliament and of the Council [of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) (OJ 2006 L 105, p. 1)] applies, the consequences of such assessments shall comply with that Regulation.'

29 Under Article 7 of the PNR Directive, entitled 'Competent authorities':

1. Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

2. The authorities referred to in paragraph 1 shall be authorities competent for the prevention, detection, investigation or prosecution of terrorist offences or serious crime. . . .

3. The PNR data and the result of processing those data received by the PIU may be further processed by the competent authorities of the Member States only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.

4. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

5. The competent authorities shall not take any 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. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.'

30 Article 8 of that directive, entitled 'Obligations on air carriers regarding transfers of data', provides in its paragraphs 1 to 3:

1. Member States shall adopt the necessary measures to ensure that air carriers transfer, by the "push method", the PNR data listed in Annex I, to the extent that they have already collected such data in the normal course of their business, to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers, the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where an extra-EU flight has one or more stop-overs at airports of the Member States, air carriers shall transfer the PNR data of all passengers to

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

the PIUs of all the Member States concerned. This also applies where an intra-EU flight has one or more stop-overs at the airports of different Member States, but only in relation to Member States which are collecting PNR data from intra-EU flights.

2. In the event that the air carriers have collected any [API] data listed under item 18 of Annex I but do not retain those data by the same technical means as for other PNR data, Member States shall adopt the necessary measures to ensure that air carriers also transfer, by the "push method", those data to the PIU of the Member States referred to in paragraph 1. In the event of such a transfer, all the provisions of this Directive shall apply in relation to those API data.

3. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the examination procedure referred to in Article 17(2) or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:

   (a) 24 to 48 hours before the scheduled flight departure time; and

   (b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for passengers to board or leave.'

31 Article 12 of that directive, entitled 'Period of data retention and depersonalisation', provides:

1. Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database at the PIU for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing.

2. Upon expiry of a period of six months after the transfer of the PNR data referred to in paragraph 1, all PNR data shall be depersonalised through masking out of the following data elements which could serve to identify directly the passenger to whom the PNR data relate:

   (a) name(s), including the names of other passengers on the PNR and number of travellers on the PNR travelling together;

   (b) address and contact information;

   (c) all forms of payment information, including billing address, to the extent that it contains any information which could serve to identify directly the passenger to whom the PNR relate or any other persons;

   (d) frequent flyer information;

   (e) general remarks to the extent that they contain any information which could serve to identify directly the passenger to whom the PNR relate; and

   (f) any API data that have been collected.

3. Upon expiry of the period of six months referred to in paragraph 2, disclosure of the full PNR data shall be permitted only where it is:

   (a) reasonably believed that it is necessary for the purposes referred to in point (b) of Article 6(2) and

   (b) approved by:

   (i) a judicial authority; or

   (ii) another national authority competent under national law to verify whether the conditions for disclosure are met, subject to informing the data protection officer of the PIU and to an *ex post* review by that data protection officer.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

4. Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case the retention of such data by the competent authority shall be regulated by national law.

5. The result of the processing referred to in point (a) of Article 6(2) shall be kept by the PIU only as long as necessary to inform the competent authorities and, in accordance with Article 9(1), to inform the PIUs of other Member States of a positive match. Where the result of automated processing has, further to individual review by non-automated means as referred to in Article 6(5), proven to be negative, it may, however, be stored so as to avoid future "false" positive matches for as long as the underlying data are not deleted under paragraph 4 of this Article.'

32 Article 13 of the PNR Directive, entitled 'Protection of personal data', provides in paragraphs 1 to 5:

1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in [EU] and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision [2008/977]. Those Articles shall therefore apply.

2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of Framework Decision [2008/977] regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive.

3. This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers, in particular their obligations to take appropriate technical and organisational measures to protect the security and confidentiality of personal data.

4. Member States shall prohibit the 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. In the event that PNR data revealing such information are received by the PIU, they shall be deleted immediately.

5. Member States shall ensure that the PIUs maintain documentation relating to all processing systems and procedures under their responsibility. That documentation shall contain at least:

   (a) the name and contact details of the organisation and personnel in the PIU entrusted with the processing of the PNR data and the different levels of access authorisation;

   (b) the requests made by competent authorities and PIUs of other Member States;

   (c) all requests for and transfers of PNR data to a third country.

The PIU shall make all documentation available, upon request, to the national supervisory authority.'

33 According to Article 15 of that directive, entitled 'National supervisory authority':

1. Each Member State shall provide that the national supervisory authority referred to in Article 25 of Framework Decision [2008/977] is responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. Article 25 of Framework Decision [2008/977] shall apply.

2. Those national supervisory authorities shall conduct activities under paragraph 1 with a view to protecting fundamental rights in relation to the processing of personal data.

3. Each national supervisory authority shall:

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

(a) deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period;

(b) verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint referred to in point (a).

4. Each national supervisory authority shall, upon request, advise any data subject on the exercise of the rights laid down in provisions adopted pursuant to this Directive.'

34 Article 19 of the directive, entitled 'Review', provides:

1. On the basis of information provided by the Member States, including the statistical information referred to in Article 20(2), the Commission shall by 25 May 2020 conduct a review of all the elements of this Directive and submit and present a report to the European Parliament and to the Council [of the European Union].

2. In conducting its review, the Commission shall pay special attention to:

(a) compliance with the applicable standards of protection of personal data,

(b) the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive,

(c) the length of the data retention period,

(d) the effectiveness of exchange of information between the Member States, and

(e) the quality of the assessments including with regard to the statistical information gathered pursuant to Article 20.

3. The report referred to in paragraph 1 shall also include a review of the necessity, proportionality, and effectiveness of including within the scope of this Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights. The Commission shall take into account the experience gained by Member States, especially those Member States that apply this Directive to intra-EU flights in accordance with Article 2. The report shall also consider the necessity of including non-carrier economic operators, such as travel agencies and tour operators which provide travel-related services, including the booking of flights, within the scope of this Directive.

4. If appropriate, in light of the review conducted pursuant to this Article, the Commission shall make a legislative proposal to the European Parliament and to the Council with a view to amending this Directive.'

35 Article 21 of that directive, entitled 'Relationship to other instruments', provides, in paragraph 2:

'This Directive is without prejudice to the applicability of Directive [95/46] to the processing of personal data by air carriers.'

36 Annex I to the PNR Directive, entitled 'Passenger name record data as far as collected by air carriers', provides:

1. PNR record locator

2. Date of reservation/issue of ticket

3. Date(s) of intended travel

4. Name(s)

5. Address and contact information (telephone number, email address)

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

6. All forms of payment information, including billing address
7. Complete travel itinerary for specific PNR
8. Frequent flyer information
9. Travel agency/travel agent
10. Travel status of passenger, including confirmations, check-in status, no-show or go-show information
11. Split/divided PNR information
12. 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)
13. Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, automated ticket fare quote fields
14. Seat number and other seat information
15. Code share information
16. All baggage information
17. Number and other names of travellers on the PNR
18. 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)
19. All historical changes to the PNR listed in numbers 1 to 18.'

37 Annex II to that directive, entitled 'List of offences referred to in point (9) of Article 3', is worded as follows:

1. participation in a criminal organisation,
2. trafficking in human beings,
3. sexual exploitation of children and child pornography,
4. illicit trafficking in narcotic drugs and psychotropic substances,
5. illicit trafficking in weapons, munitions and explosives,
6. corruption,
7. fraud, including that against the financial interests of the Union,
8. laundering of the proceeds of crime and counterfeiting of currency, including the euro,
9. computer-related crime/cybercrime,
10. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
11. facilitation of unauthorised entry and residence,
12. murder, grievous bodily injury,
13. illicit trade in human organs and tissue,

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

14. kidnapping, illegal restraint and hostage-taking,
15. organised and armed robbery,
16. illicit trafficking in cultural goods, including antiques and works of art,
17. counterfeiting and piracy of products,
18. forgery of administrative documents and trafficking therein,
19. illicit trafficking in hormonal substances and other growth promoters,
20. illicit trafficking in nuclear or radioactive materials,
21. rape,
22. crimes within the jurisdiction of the International Criminal Court,
23. unlawful seizure of aircraft/ships,
24. sabotage,
25. trafficking in stolen vehicles,
26. industrial espionage.'

7. Framework Decision 2002/475

38 Article 1 of Framework Decision 2002/475 defined the concept of 'terrorist offence' by listing intentional acts referred to in points (a) to (i) of that article, committed with the aim of 'seriously intimidating a population', 'unduly compelling a Government or international organisation to perform or abstain from performing any act', or 'seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation'. Articles 2 and 3 of that framework decision defined the concepts of 'offences relating to a terrorist group' and of 'offences linked to terrorist activities', respectively. Article 4 of the said framework decision governed the charges of inciting and aiding or abetting those offences as well as that of attempting to commit them.

39 Framework Decision 2002/475 was repealed by Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Framework Decision 2002/475 and amending Council Decision 2005/671/JHA (OJ 2017 L 88, p. 6), Articles 3 to 14 of which include similar definitions.

B. BELGIAN LAW

1. The Constitution

40 Article 22 of the Constitution provides as follows:

> 'Everyone is entitled to respect for private and family life except in the cases and under the circumstances laid down by law.
>
> The laws, decrees and rules referred to in Article 134 guarantee the protection of this right.'

2. The Law of 25 December 2016

41 Article 2 of the loi du 25 décembre 2016, relative au traitement des données des passagers (Law of 25 December 2016 on the processing of passenger data, *Moniteur belge* of 25 January 2017, p. 12905; 'the Law of 25 December 2016') is worded as follows:

> 'The present law and the royal decrees which shall be adopted in implementation of the present law transpose [the API Directive] and [the PNR Directive]. The present law and the royal decree concerning the maritime sector partially transpose Directive [2010/65].'

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

42 Article 3 of that law provides:

1. This law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers travelling to or from or transiting through Belgian territory.

2. The King shall prescribe, by decree deliberated in the Council of Ministers, in respect of each sector of the transport industry and in respect of tour operators, the passenger data to be transferred and how they are to be transferred, after an opinion has been given by the Commission de la protection de la vie privée [(Commission for the protection of privacy)].'

43 Under Article 4 of that law:

'For the purposes of this law and its implementing decrees, the following definitions shall apply:

. . .

(8) "the competent services": the services under Article 14(1)(2);

(9) "PNR": a record of each passenger's travel requirements which contains the information referred to in Article 9, which is necessary to enable reservations to be processed and controlled by the booking and participating carriers and tour operators for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities;

(10) "passenger": any person, including persons in transfer or transit and excluding members of the crew, carried or to be carried by the carrier with its consent, such consent being manifested by that person's registration in the passengers list; . . .'

44 Article 8 of the Law of 25 December 2016 states:

1. Passenger data shall be processed for the purposes of:

(1) detection and prosecution (including the execution of penalties or measures depriving the person concerned of his or her liberty) of the offences referred to Article 90*ter*(2), . . .(7), . . .(8), . . .(11), . . .(14), . . .(17), (18), (19) and Article 90*ter*(3) of the Code d'instruction criminelle [(Criminal Procedure Code)];

(2) detection and prosecution (including the execution of penalties or measures depriving the person of his or her liberty) of the offences referred to in Article 196, in so far as concerns the offences of forgery of authentic and public documents, Article 198, 199, 199*bis*, 207, 213, 375 and 505 of the Code pénal [(Criminal Code)];

. . .

(4) monitoring the activities referred to in Article 7(1) and (3/l) and Article 11(1)(1) to (3) and (5) of the loi du 30 novembre 1998 organique des services de renseignement et de sécurité [(Organic law of 30 November 1998 on the intelligence and security services)];

(5) detection and prosecution of the offences referred to in Article 220(2) of the loi générale sur les douanes et accises du 18 juillet 1977 [(General customs and excise law of 18 July 1977)] and the third paragraph of Article 45 of the loi du 22 décembre 2009 relative au régime général d'accise [(Law of 22 December 2009 on the general excise regime)] . . .

2. Subject to the conditions in Chapter 11, passenger data shall also be processed with a view to improving external border controls on individuals, and with a view to combating illegal immigration.'

45 Article 14(1) of that law states:

'The PIU shall be made up of:

. . .

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

(2) members seconded from the following competent services:

(a) the police services covered by the loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux [(Law of 7 December 1998 organising an integrated police service, with a two-tier structure)];

(b) the Sûreté de l'État [(State security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];

(c) the Service général de Renseignement et de Sécurité [(General intelligence and security services)] covered by the [Organic law of 30 November 1998 on the intelligence and security services];
. . .'

46 Article 24 of the said law, in Section 1 thereof, entitled 'Processing of passenger data in connection with the advance assessment of passengers', of Chapter 10 of that law, on data processing, is worded as follows:

1. Passenger data shall be processed with a view to carrying out an assessment of passengers prior to their scheduled arrival in, departure from, or transit through Belgian territory, in order to identify persons who require further examination.

2. For the purposes referred to in Article 8(1)(1), (4) and (5), or relating to the threats referred to in Article 8(1)(a), (b), (c), (d), (f) and (g) and Article 11(2) of the [Organic law of 30 November 1998 on the intelligence and security services], the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against:

   (1) the databases managed by the competent services or which are directly available or accessible to those services in the course of their functions or against the lists of individuals drawn up by the competent services in the course of their functions.

   (2) the assessment criteria pre-determined by the PIU, as referred to in Article 25.

3. For the purposes referred to in Article 8(1)(3), the advance assessment of passengers shall be based on a positive match resulting from comparing passenger data against the databases referred to in Article 8(2)(1).

4. Positive matches shall be validated by the PIU within 24 hours of receipt of the automated notification of the positive match.

5. From the moment of that validation, the competent service which originally identified the positive match shall take further action without delay.'

47 Chapter 11 of the Law of 25 December 2016, entitled 'Processing of passenger data with a view to improving border controls and combating illegal immigration', comprises Articles 28 to 31 thereof.

48 Article 28 of that law provides:

1. This Chapter applies to the processing of passenger data by the police services responsible for carrying out border checks and by the Office des étrangers [(Immigration Office)], carried out with a view to improving the checks on persons at external borders and with a view to combating illegal immigration.

2. It applies without prejudice to the obligations incumbent on the police services responsible for carrying out border checks and on the [Immigration Office] to transfer personal data or information in accordance with legal or statutory provisions.'

49 Under Article 29 of that law:

1. For the purposes of Article 28(1) passenger data are transferred to the police services responsible for carrying out border checks and to the [Immigration Office] to enable them to perform their statutory duties, within the limits provided for in this article.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

2. Only the passenger data referred to in Article 9(1)(18) concerning the following passenger categories shall be transferred:

   (1) passengers who intend to enter or have entered Belgian territory at an external border;

   (2) passengers who intend to leave or have left Belgian territory at an external border;

   (3) passengers who intend to pass through, are located in, or have passed through an international transit area situated on Belgian territory.

3. The passenger data referred to in paragraph (2) shall be transferred to the police services responsible for carrying out checks at Belgium's external border immediately after they have been entered in the passenger database. The said services shall save those data in a temporary file and delete them within 24 hours of the transfer.

4. When it needs them to perform its statutory duties, the passenger data referred to in paragraph (2) shall be transferred to the [Immigration Office] immediately after they have been entered in the passenger database. The Office shall save those data in a temporary file and delete them within 24 hours of the transfer.

After that period has passed, if the [Immigration Office] requires access to the passenger data referred to in paragraph (2) for the purposes of performing its statutory duties, it shall send a duly reasoned request to the PIU.

. . .'

50 The Law of 25 December 2016 became applicable to airlines, carriers operating international passenger service (HST carriers) and travel intermediaries in a contract with those carriers (HST ticket distributors), and bus carriers, respectively, by the arrêté royal du 1 juillet 2017 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les compagnies aériennes (Royal Decree of 18 July 2017 implementing the Law of 25 December 2016 on the obligations incumbent on airlines, *Moniteur belge* of 28 July 2017, p. 75934), by the arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs HST et distributeurs de tickets HST (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on HST carriers and HST ticket distributors, *Moniteur belge* of 12 Feburary 2019, p. 13018) and by the arrêté royal du 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016, reprenant les obligations pour les transporteurs par bus (Royal Decree of 3 February 2019 implementing the Law of 25 December 2016 on the obligations incumbent on bus carriers, *Moniteur belge* of 12 February 2019, p. 13023).

II. The dispute in the main proceedings and the questions referred for a preliminary ruling

51 By application of 24 July 2017, the Ligue des droits humains brought an action before the Cour constitutionnelle (Constitutional Court, Belgium) seeking annulment in full or in part of the Law of 25 December 2016.

52 The referring court states that that law transposes, into domestic law, the PNR Directive and the API Directive as well as, in part, Directive 2010/65. According to the referring court, it follows from the *travaux préparatoires* that that law seeks to 'create a legal framework requiring international passenger transport carriers in various sectors (air, rail, international road and sea), as well as tour operators, to transfer data on their passengers to a database managed by the [Service public fédéral intérieur (Home Affairs Federal Public Service, Belgium)]'. The national legislature also stated that the intended purposes of the Law of 25 December 2016 fall into three categories, namely (i) the prevention, detection, investigation and prosecution of criminal offences or the enforcement of criminal penalties; (ii) the tasks of the intelligence and security services; and (iii) improving external border controls and combating illegal immigration.

53 In support of its action, the Ligue des droits humains raises two pleas, the first, alleging breach of Article 22 of the Constitution, read in conjunction with Article 23 of the GDPR, Articles 7, 8 as well as Article 52(1) of the Charter as well as Article 8 ECHR, and the second, alleging, in the alternative, breach of Article 22 of the Charter, read in conjunction with Article 3(2) TEU and Article 45 of the Charter.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

54 By its first plea, the Ligue des droits humains submits, in essence, that that law entails an interference with the rights to respect for private life and the protection of personal data, which does not comply with Article 52(1) of the Charter and, inter alia, the principle of proportionality. The scope of that law and the definition of the data collected, which may reveal sensitive information, are too broad. Similarly, the concept of 'passenger', within the meaning of that same law, leads to systematic, non-targeted automated processing of the data of all passengers. Moreover, the nature and detailed rules of the 'pre-screening' method and the databases against which those data are compared, once transmitted, are not defined in a sufficiently clear manner. Furthermore, the Law of 25 December 2016 pursues objectives other than those of the PNR Directive. Finally, the five-year period laid down by that law for the retention of those data is disproportionate.

55 By its second plea, concerning Article 3(1), Article 8(2) and Articles 28 to 31 of the Law of 25 December 2016, the Ligue des droits humains submits that, by extending the system provided for by the PNR Directive to intra-EU transport operations, those provisions have the effect of indirectly restoring internal border control, in breach of the free movement of persons. Once a person is on Belgian territory, whether on arrival, departure or during a stop-over, their data are automatically collected.

56 The Council of Ministers disputes those arguments. It considers, in particular, that the first plea is inadmissible in so far as it concerns the GDPR, which is not applicable to the Law of 25 December 2016. Furthermore, the processing of data provided for by that law, in accordance with the PNR Directive, is an essential tool for, inter alia, the fight against terrorism and serious crime, and the measures stemming from that law are necessary to achieve the aims pursued and are proportionate.

57 As regards the first plea, the referring court asks, first of all, whether the protection provided for by the GDPR applies to the processing of data established by the Law of 25 December 2016, which is intended to implement, primarily, the PNR Directive. Next, that court notes, with reference to the case-law stemming from Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017 (EU:C:2017:592), that the definition of PNR data in Article 3(5) of and Annex I to that directive may, first, not be sufficiently clear and precise, on account of the non-exhaustive nature of the description of some of those data contained in those provisions and, secondly, lead indirectly to the disclosure of sensitive data. Furthermore, the definition of the concept of 'passenger' in Article 3(4) of that directive may result in the collection, transfer, processing and retention of PNR data constituting generalised and indiscriminate obligations, applying to every person carried or to be carried who appears on the passengers list, regardless of whether there are serious grounds for believing that that person has committed or is about to commit an offence or has been found guilty of an offence.

58 The referring court also observes that PNR data, in accordance with the provisions of the PNR Directive, are systematically subject to advance assessment involving cross-checks with databases or pre-determined criteria with a view to finding matches. The Consultative Committee of Convention No 108 of the Council of Europe indicated in its Opinion of 19 August 2016 on the Data protection implications of the processing of Passenger Name Records (T-PD(2016)18rev) that the processing of personal data concerns all passengers and not only the targeted individuals suspected of involvement in a criminal offence or posing an immediate threat to national security or public order, and that PNR data may not only be compared ('data matching') to databases but also be processed by 'data mining' according to selectors or predictive algorithms, with the aim of identifying anyone who may be involved or might engage in criminal activities, as this assessment of passengers by data mining may raise the question of predictability, in particular when operated on the basis of predictive algorithms using dynamic criteria that may constantly evolve in light of self-learning capacities. In that context, the referring court considers that, although the predetermined criteria for identifying high-risk profiles must be specific, reliable and non-discriminatory, in accordance with Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017 (EU:C:2017:592), it seems to be impossible technically to define those criteria further.

59 As regards the five-year retention period and access to the data provided for in Article 12 of the PNR Directive, the referring court notes that the Commission for the protection of privacy (Belgium), in its avis d'initiative n° 01/2010 du 13 janvier 2010 relatif au projet de loi portant assentiment à l'accord PNR UE-États-Unis d'Amérique (own-initiative Opinion No 01/2010 of 13 January 2010 on the Draft law ratifying the PNR Agreement between the European Union and the United States of America), considered that when data is retained for a long period and is

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

stored *en masse*, the risk of the data subjects being profiled rises, as does the potential for improper use of the data for purposes other than those originally intended. It is also apparent from the Opinion of 19 August 2016 of the Consultative Committee of Convention No 108 of the Council of Europe that masked out data still enables individuals to be identified and continue as such to constitute personal data, and that their retention should be limited in time in order to avoid permanent and general surveillance.

60 In those circumstances, having regard to the case-law resulting in particular from Opinion 1/15 *(EU-Canada PNR Agreement)*) of 26 July 2017 (EU:C:2017:592), the referring court asks whether the system for the collection, transfer, processing and retention of PNR data established by the PNR Directive may be regarded as coming within the limits of what is strictly necessary. That court considers that it is also appropriate to ascertain whether that directive precludes national legislation authorising the processing of PNR data for a purpose other than that provided for by that directive and whether disclosure of the full data after they have been depersonalised, pursuant to Article 12 of that directive, may be approved by a national authority such as the PIU created by the Law of 25 December 2016.

61 As regards the second plea, the referring court states that Article 3(1) of that law lays down the obligations of carriers and tour operators regarding the transfer of data relating to passengers 'travelling to or from or transiting through Belgian territory'. That court adds, with regard to the scope of that law, that the national legislature decided to 'inclu[de] intra-EU travel in the data collection' in order to obtain 'a fuller picture of passenger movements representing a potential threat to intra-Community and national security', as envisaged by Article 2 of the PNR Directive, read in conjunction with recital 10 thereof, for flights within the European Union. The referring court also states that the Commission for the protection of privacy, in its Opinion No 55/2015 of 16 December 2015 on the draft bill which became the Law of 25 December 2016, had raised the issue of whether the Belgian PNR system might conflict with the principle of the free movement of persons, in so far as that system includes transport operations carried out within the European Union.

62 It is in those circumstances that the Cour constitutionnelle (Constitutional Court) decided to stay proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) Is Article 23 of [the GDPR], read in conjunction with Article 2(2)(d) of that regulation, to be interpreted as applying to national legislation such as the [Law of 25 December 2016], which transposes [the PNR Directive] as well as [the API Directive] and Directive [2010/65]?

(2) Is Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the data it refers to are very wide in scope – particularly the data referred to in paragraph 18 of Annex I to [that directive], which go beyond the data referred to in Article 3(2) of [the API Directive] – and also given that, taken together, they may reveal sensitive information, and thus go beyond what is "strictly necessary"?

(3) Are paragraphs 12 and 18 of Annex I to [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that, having regard to the word "including", the data referred to in those paragraphs is given by way of example and not exhaustively, such that the requirement for precision and clarity in rules which interfere with the right to respect for private life and the right to protection of personal data is not satisfied?

(4) Are Article 3(4) of [the PNR Directive] and Annex I to that directive compatible with Articles 7, 8 and 52(1) of [the Charter], given that the system of generalised collection, transfer and processing of passenger data established by those provisions relates to any person using the mode of transport concerned, regardless of whether there is any objective ground for considering that that person may present a risk to public security?

(5) Is Article 6 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law, which includes, among the purposes for which PNR data is processed, [monitoring] activities within the remit of the intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime?

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

(6) Is Article 6 of [the PNR Directive] compatible with Articles 7, 8 and 52(1) of [the Charter], given that the advance assessment for which it provides, which is made by comparing passenger data against databases and pre-determined criteria, applies to such data in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security?

(7) Can the expression "another national authority competent under national law" in Article 12(3) of [the PNR Directive] be interpreted as including the PIU created by the Law of 25 December 2016, which would then have power to authorise access to PNR data after six months had passed, for the purposes of ad hoc searches?

(8) Is Article 12 of [the PNR Directive], read in conjunction with Articles 7, 8 and 52(1) of [the Charter], to be interpreted as precluding national legislation such as the contested law which provides for a general data retention period of five years, without making any distinction in terms of whether the advance assessment indicated that the passengers might present a risk to public security?

(9) (a) Is [the API Directive] compatible with Article 3(2) [TEU] and Article 45 of [the Charter], given that the obligations for which it provides apply to flights within the European Union?
(b) Is [the API Directive], read in conjunction with Article 3(2) [TEU] and Article 45 of [the Charter], to be interpreted as precluding national legislation such as the contested law which, for the purposes of combating illegal immigration and improving border controls, authorises a system of collection and processing of data relating to passengers "travelling to, from or transiting through Belgian territory", which may indirectly involve a re-establishment of internal border controls?

(10) If, on the basis of the answers to the preceding questions, the Cour constitutionnelle (Constitutional Court) concludes that the contested law, which transposes, inter alia, [the PNR Directive], fails to fulfil one or more of the obligations arising under the provisions referred to in those questions, would it be open to it to maintain the effects of the [Law of 25 December 2016], on a temporary basis, in order to avoid legal uncertainty and enable the data hitherto collected and retained to continue to be used for the purposes envisaged by the law?'

III. Consideration of the questions referred

A. Question 1

63 By its Question 1, the referring court asks, in essence, whether Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, in particular, the transfer, the retention and the processing of PNR data.

64 As is apparent from Article 2(1) of the GDPR, that regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of such data which form part of a filing system or are intended to form part of a filing system. The concept of 'processing' is defined in broad terms in Article 4(2) of that regulation as including, inter alia, collection, recording, storage, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or erasure of such data or sets of data.

65 The Belgian Government submits however that the transfer of PNR data by economic operators to the PIU, for the purposes of the prevention and detection of criminal offences, as provided for in Article 1(1)(a) and (2) and Article 8 of the PNR Directive, which constitutes 'processing' of personal data within the meaning of Article 4(2) of the GDPR, as well as the advance collection thereof, fall outside the scope of Article 2(2)(d) of the said regulation, on the ground that the case-law stemming from the judgment of 30 May 2006, Parliament v Council and Commission, C-317/04 and C-318/04, EU:C:2006:346 (paragraphs 57 to 59), relating to the first indent of Article 3(2) of Directive 95/46, is applicable to that provision of the regulation.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

66 In that regard, it is true that, as previously held by the Court, the first indent of Article 3(2) of Directive 95/46, which was repealed and replaced by the GDPR with effect from 25 May 2018, generally excluded from its scope 'processing operations concerning public security, defence [and] State security', without drawing any distinction according the person carrying out the data processing operation concerned. Thus, processing operations carried out by private operators resulting from obligations imposed by the public authorities could, where appropriate, fall within the scope of the exception laid down in that provision, given that the wording of that provision covered all processing operations concerning public security, defence or State security, regardless of the person carrying out those operations (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 101).

67 However, Article 2(2)(d) of the GDPR draws such a distinction, since, as noted by the Advocate General in points 41 and 46 of his Opinion, it is clearly apparent from the wording of that provision that two conditions need to be met for data processing to fall within the scope of the exception it lays down. While the first one of those conditions related to the purposes of the processing operation, namely, the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, the second condition relates to the person carrying out that operation, namely a 'competent authority' within the meaning of that provision.

68 As the Court has also held, it is apparent from Article 23(1)(d) and (h) of the GDPR that the processing of personal data carried out by individuals for the purposes set out in Article 2(2)(d) of that regulation falls within the scope of thereof (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 102).

69 It follows that the case-law stemming from the judgment of 30 May 2006, Parliament v Council and Commission (C-317/04 and C-318/04, EU:C:2006:346), relied on by the Belgian Government, is not applicable to the exception to the scope of the GDPR set out in Article 2(2)(d) thereof.

70 In addition, that exception, like the other exceptions to the scope of the GDPR laid down in Article 2(2) of that regulation, must be interpreted strictly.

71 As is apparent from recital 19 of the GDPR, the reason for that exception is that the processing of personal data by authorities competent for the purposes, inter alia, of the prevention and detection of criminal offences, including the safeguarding against and the prevention of threats to public security is governed by a more specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR (judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 69).

72 As is stated, moreover, in recitals 9 to 11 of Directive 2016/680, the latter lays down the specific rules relating to the protection of natural persons with regard to such processing operations, respecting the specific nature of those activities in the fields of judicial cooperation in criminal matters and police cooperation, while the GDPR defines general rules concerning the protection of those persons which are intended to apply to those processing operations when Directive 2016/680, as a more specific legal act, does not apply. In particular, according to recital 11 of that directive, the GDPR applies to processing of personal data that is carried out by a 'competent authority' within the meaning of Article 3(7) of the said directive, but for purposes other than those of that directive (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 70).

73 As regards the first condition set out in paragraph 67 above, and, specifically, the purposes for which the personal data are to be processed under the PNR Directive, it is appropriate to recall that, in accordance with Article 1(2) of that directive, PNR data may be processed only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes are covered by those set out in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680, with the result that such processing operations may be caught by the exception laid down in Article 2(2)(d) of that regulation and, consequently, be within the scope of that directive.

74 By contrast, that is not the case with regard to the processing operations covered by the API Directive and Directive 2010/65, the purposes of which are other than those in Article 2(2)(d) of the GDPR and Article 1(1) of Directive 2016/680.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

75 Indeed, the API Directive aims at improving border controls and combating illegal immigration, as is apparent from recitals 1, 7 and 9 as well as Article 1 thereof, by the transmission of advance passenger data by carriers to the competent national authorities. Moreover, several recitals and provisions of that directive make clear that the data processing operations envisaged for its implementation are within the scope of the GDPR. Recital 12 of that directive states that 'Directive [95/46] applies with regard to the processing of personal data by the authorities of the Member States'. In addition, the fifth subparagraph of Article 6(1) of the API Directive specifies that Member States may also use API data for law enforcement purposes, 'subject to data protection provisions under Directive [95/46]', that phrase being used also in the third subparagraph of that provision. Similarly, the phrase 'without prejudice to the provisions of Directive [95/46]' is used, inter alia, in recital 9 of the API Directive. Article 6(2) of the API Directive provides, lastly, that passengers must be informed by carriers 'in accordance with the provisions laid down in Directive [95/46]'.

76 As to Directive 2010/65, it follows from recital 2 and Article 1(1) thereof that the purpose of that directive is to simplify and harmonise the administrative procedures applied to maritime transport by making the electronic transmission of information standard and by rationalising reporting formalities, for the facilitation of maritime transport, and in order to reduce the administrative burden for shipping companies. Article 8(2) of the said directive confirms that the data processing operations envisaged for its implementation fall within the scope of the GDPR, since that provision require Member States, concerning personal data, to ensure compliance with Directive 95/46.

77 It follows that the data processing operations envisaged by national legislation transposing, into domestic law, the provisions of the API Directive and of Directive 2010/65 are within the scope of the GDPR. By contrast, data processing operations envisaged by national legislation that transpose, into domestic law, the PNR Directive may, pursuant to the exception in Article 2(2)(d) of that regulation, fall outside the scope of the regulation, subject to compliance with the second condition recalled in paragraph 67 above, namely that the person carrying out the processing operations is a competent authority within the meaning of the latter provision.

78 As regards that second condition, the Court has held that, in so far as Directive 2016/680 defines, in Article 3(7) thereof, the concept of 'competent authority', such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 69).

79 Pursuant to Articles 4 and 7 of the PNR Directive, each Member State must, respectively, designate, as its PIU, an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime and adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU, the latter authorities being also competent for those purposes, as specified in Article 7(2) of that directive.

80 It follows therefrom that the processing of PNR data by the PIU and the said competent authorities for such purposes satisfy both conditions referred to in paragraph 67 above, with the result that those operations are covered by the provisions of the PNR Directive itself as well as those of Directive 2016/680 and not those of the GDPR, as confirmed, moreover, by recital 27 of the PNR Directive.

81 By contrast, since economic operators such as air carriers, although they have a legal obligation to transfer PNR data, are neither in charge of exercising public authority nor entrusted with public powers by that directive, they cannot be regarded as being competent authorities within the meaning of Article 3(7) of Directive 2016/680 and Article 2(2)(d) of the GDPR, with the result that the collection of those data and transfer to the PIU, by air carriers, are covered by that regulation. The same applies in a situation, such as that provided for by the Law of 25 December 2016, where the collection and transfer of the said data are operated by other carriers or by tour operators.

82 The referring, lastly, raises the question of the impact, if any, of the adoption of national legislation intended to transpose the provisions of the PNR Directive, those of the API Directive and also those of Directive 2010/65, such as the Law of 25 December 2016. In that regard, it should be borne in mind that, as is apparent from paragraphs 72 and 75 to 77 above, the data processing operations provided for under those last two directives fall within the scope of the GDPR, which entails general rules on the protection of natural persons with regard to the processing of personal data.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

83 Thus, when a data processing operation carried out on the basis of that legislation is covered by the API Directive and/or Directive 2010/65, the GDPR applies to that operation. The same is true of a data processing operation carried out on that same basis and, in terms of its purpose and in addition to the PNR Directive, falls within the API Directive and/or Directive 2010/65. Lastly, when a data processing operation carried out on the basis of that same legislation, in terms of its purpose, falls outside the PNR Directive, the GDPR applies if the operation relates to the collection of PNR data and transfer to the PIU, by air carriers. By contrast, where such a processing operation is carried out by the PIU or the authorities competent for the purposes referred to in Article 1(2) of the PNR Directive, that operation is covered by Directive 2016/680, in addition to national law.

84 In the light of the foregoing, the answer to Question 1 is that Article 2(2)(d) and Article 23 of the GDPR must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of the API Directive, those of Directive 2010/65 and also those of the PNR Directive in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by the API Directive or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by the PNR Directive and are carried out by the PIU or by the authorities competent for the purposes referred to in Article 1(2) of that directive.

B. QUESTIONS 2 TO 4 AND QUESTION 6

85 By its Questions 2 to 4 and Question 6, which it is appropriate to consider together, the referring court asks the Court, in essence, whether the PNR Directive is valid in the light of Articles 7 and 8 as well as Article 52(1) of the Charter. Those questions concern, inter alia:

– Annex I to that directive and the data listed in that annex, in particular those referred to in paragraphs 12 and 18 thereof, concerning the requirements for clarity and precision (Questions 2 and 3);

– Article 3(4) of the said directive and Annex I thereto, in that the system of generalised collection, transfer and processing of PNR data established by those provisions may apply to any person on a flight covered by the provisions of that directive (Question 4), and

– Article 6 of the PNR Directive in that it provides for advance assessment, by comparing PNR data against databases and/or processing them against pre-determined criteria, which applies to such data in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security (Question 6).

86 It should be noted as a preliminary point that, in accordance with a general principle of interpretation, an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter Thus, if the wording of secondary EU legislation is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with primary law (judgment of 2 February 2021, *Consob*, C-481/19, EU:C:2021:84, paragraph 50 and the case-law cited).

87 In addition, it is settled case-law that, when a directive allows the Member States discretion to define transposition measures adapted to the various situations possible, they must, when implementing those measures, not only interpret their national law in a manner consistent with the directive in question but also ensure that they do not rely on an interpretation of the directive that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law (see, to that effect, judgments of 15 February 2016, *N.*, C-601/15 PPU, EU:C:2016:84, paragraph 60 and the case-law cited, and of 16 July 2020, *État belge (Family reunification – Minor child)*, C-133/19, C-136/19 and C-137/19, EU:C:2020:577, paragraph 33 and the case-law cited).

88 As regards the PNR Directive, it should be noted that recitals 15, 20, 22, 25, 36 and 37 thereof stress the importance that the EU legislature, by referring to the high level of data protection, gives to the full respect for

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

fundamental rights enshrined in Articles 7, 8 and 21 of the Charter as well as the principle of proportionality, with the result that, as stated in recital 36, that directive 'should . . . be implemented accordingly'.

89 In particular, recital 22 of the PNR Directive points out that, '[by] taking fully into consideration the principles outlined in recent relevant case-law of the [Court], the application of th[at] Directive should ensure full respect for fundamental rights, for the right to privacy and for the principle of proportionality' and 'genuinely meet the objectives of necessity and proportionality in order to achieve the general interests recognised by the [European] Union and the need to protect the rights and freedoms of others in the fight against terrorist offences and serious crime'. That recital adds that that application 'should be duly justified and the necessary safeguards put in place to ensure the lawfulness of any storage, analysis, transfer or use of PNR data'.

90 Moreover, under Article 19(2) of the PNR Directive, the Commission, when reviewing the directive, must pay special attention to 'compliance with the applicable standards of protection of personal data', 'the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in this Directive' and 'the length of the data retention period'.

91 It is therefore appropriate to determine whether the PNR Directive, in accordance with, in particular, the requirements set out in its recitals and its provisions referred to in paragraphs 88 to 90 above, may be interpreted in a way that ensures full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter as well as the principle of proportionality enshrined in Article 52(1) thereof.

1. Interferences with the fundamental rights guaranteed in Articles 7 and 8 of the Charter resulting from the PNR Directive

92 Article 7 of the Charter guarantees everyone the right to respect for his or her private and family life, home and communications, while Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her.

93 As is apparent from Article 3(5) of the PNR Directive and the list in Annex I thereto, the PNR data covered by that directive include, inter alia, besides the name(s) of the air passenger(s), information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.

94 Since the PNR data therefore include information on identified individuals, namely the air passengers concerned, the various forms of processing to which those data may be subject affect the fundamental right to respect for private life, guaranteed in Article 7 of the Charter (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraphs 121 and 122 and the case-law cited).

95 Furthermore, the processing of PNR data such as that covered by the PNR Directive also falls within the scope of Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 123 and the case-law cited).

96 It is settled case-law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to those data with a view to their use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference (Opinion 1/15, *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraphs 124 and 126 and the case-law cited).

97 Thus, both the transfer of PNR data by air carriers to the PIU of the Member State concerned, provided for in Article 1(1)(a) of the PNR Directive, read in conjunction with Article 8 thereof, and the framework of conditions governing the retention of those data, their use and any further transfer to the competent authorities of that

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

Member State, to the PIUs and the competent authorities of the other Member States, to Europol or to the authorities of third countries, which are permitted, inter alia, by Articles 6, 7, 9 and 10 to 12 of that directive, constitute interferences with the rights guaranteed in Articles 7 and 8 of the Charter.

98 As regards the seriousness of those interferences, it should be noted, first, that according to Article 1(1)(a), read in conjunction with Article 8 thereof, the PNR Directive provides for the systematic and continuous transfer to the PIUs of PNR data relating to any air passenger on an extra-EU flight within the meaning of Article 3(2) of that directive, operated between third countries and the European Union. As noted by the Advocate General in point 73 of his Opinion, such a transfer involves general and full access, by the PIUs, to the PNR data disclosed, concerning all the persons using air transport services, irrespective of subsequent use of those data.

99 Secondly, Article 2 of the PNR Directive provides, in paragraph 1 thereof, that Member States may decide to apply the directive to intra-EU flights within the meaning of Article 3(3) thereof, and specifies, in paragraph 2 thereof, that in that case all the provisions of the said directive 'shall apply to intra-EU flights as if they were extra-EU flights and to PNR data from intra-EU flights as if they were PNR data from extra-EU flights'.

100 Thirdly, even if some of the PNR data listed on Annex I to the PNR Directive, as summarised in paragraph 93 above, taken in isolation, do not appear to be liable to reveal precise information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between one or more persons and the financial situation of air passengers, their dietary habits or state of health, and may even reveal sensitive information about those passengers (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 128).

101 Fourthly, under Article 6(2)(a) and (b) of the PNR Directive, the data transferred by air carriers are intended for advance assessment, prior to the passengers' scheduled arrival or departure, as well as subsequent assessment.

102 As regards advance assessment, it is apparent from Article 6(2)(a) and (3) of the PNR Directive that that assessment is carried out by the PIUs of the Member States, systematically and by automated means, that is to say continuously and regardless of whether there is any indication that there is a risk that the person concerned is involved in terrorist offences or serious crime. To that end, those provisions provide that PNR data may be compared against 'relevant databases' and be processed against 'pre-determined' criteria.

103 Against this background, it should be borne in mind that the Court has already held that the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-determined models and criteria and on the databases on which that type of data processing is based (Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 172).

104 As noted by the Advocate General in point 78 of his Opinion, the processing operation provided for in Article 6(3)(a) of the PNR Directive, namely the comparison of PNR data against 'relevant databases', may provide additional information on the private lives of air passengers and may allow very precise conclusions to be drawn in that regard.

105 As to the processing of PNR data against 'pre-determined criteria' provided for in Article 6(3)(b) of the PNR Directive, it is true that Article 6(4) of that directive requires that any assessment of passengers by those means must be carried out in a non-discriminatory manner and, in particular, should not be based on a series of characteristics referred to in the last sentence of that paragraph 4. In addition, the criteria used must be targeted, proportionate and specific.

106 That being said, the Court has already held that, since automated analyses of PNR data are carried out on the basis of unverified personal data and are based on pre-determined models and criteria, they necessarily present some margin of error (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 169). In particular, as noted, in essence, by the Advocate General in point 78 of his Opinion, it is apparent from Commission Working Document (SWD(2020) 128 final) annexed to its report of 24 July 2020 on the review of the PNR Directive that the number of positive matches from automated processing under Article 6(3)(a) and (b) of that directive which prove to be incorrect following individual review by non-automated means is fairly substantial,

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

amounting in 2018 and 2019 to at least five out of six individuals identified. Those processing operations thus lead to a careful analysis of the PNR data relating to the said persons.

107 As regards the subsequent assessment of PNR data provided for in Article 6(2)(b) of the PNR Directive, it is apparent from that provision that, during the period of six months after the transfer of the PNR data, referred to in Article 12(2) of that directive, the PIU is required, upon request from the competent authorities, to provide them with the PNR data and process those data in specific cases, for the purposes of combating terrorist offences and serious crime.

108 In addition, even if, upon expiry of that period of six months, PNR data are depersonalised through masking out of certain data elements, the PIU may be required, pursuant to Article 12(3) of the PNR Directive, to disclose, following such a request, full PNR data in a form which permits the identification of the data subject by the competent authorities where it is reasonably believed that it is necessary for the purposes referred to Article 6(2)(b) of that directive, such disclosure being however subject to approval granted by a judicial authority or 'another [competent] national authority'.

109 Fifthly, by providing, in Article 12(1) thereof, without providing further details in that regard, that PNR data are to be retained in a database for a period of five years following their transfer to the PIU of the Member State on the territory of which the flight is landing or departing, the PNR Directive, given the fact that, despite being depersonalised upon expiry of the initial period of six months though masking out of certain data elements, full PNR data may still be disclosed in the scenario referred to in the preceding paragraph, makes it possible for information on the private life of air passengers to be available for a period of time which the Court, in its Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017 (EU:C:2017:592, paragraph 132), has already described as being particularly long.

110 Given how common use of air transport services is, the effect of a retention period that long is that a very large part of the population of the European Union is liable to have its PNR data retained, repeatedly, under the system established by the PNR Directive and, accordingly, be accessible for analyses carried out in the context of advance and subsequent assessments by the PIU and competent authorities over a considerable – even indefinite – period of time, in the case of persons who travel by air more than once every five years.

111 In the light of all of the foregoing, it is appropriate to find that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, 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.

2. Justification for the interferences resulting from the PNR Directive

112 It must be borne in mind that the fundamental rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 136 and the case-law cited, and judgment of 6 October 2020, *Privacy International*, C-623/17, EU:C:2020:790, paragraph 63 and the case-law cited).

113 Under the first sentence of Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. In this connection, Article 8(2) of the Charter states that personal data must, inter alia, be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.

114 It should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned, bearing in mind, on the one hand, that that requirement does not preclude the limitation in question from being formulated in terms which are sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances (see, to that effect, judgment of 26 April

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

2022, *Poland* v *Parliament and Council*, C-401/19, EU:C:2022:297, paragraphs 64 and 74 and the case-law cited) and, on the other hand, that the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter.

115 As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue (Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 140, and judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others,* C-140/20, *EU:C:2022:258*, paragraph 52 and the case-law cited).

116 More specifically, the question whether the Member States may justify a limitation on the rights guaranteed in Articles 7 and 8 of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness (see, to that effect, judgments of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, paragraph 55 and the case-law cited, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 53 and the case-law cited).

117 In order to satisfy the proportionality requirement, the legislation in question entailing the interference must lay down clear and precise rules governing the scope and application of the measures provided for and imposing minimum safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data are subject to automated processing. Those considerations apply especially where the PNR data are liable to reveal sensitive passenger data (Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 141, and judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 132 and the case-law cited).

118 Thus, legislation that provides for the retention of personal data must continue to satisfy objective criteria that establish a connection between the data to be retained and the objective pursued (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 191 and the case-law cited, and judgments of 3 October 2019, *A and Others*, C-70/18, EU:C:2019:823, paragraph 63, and of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 133).

(a) Observance of the principle of legality and respect for the essence of the fundamental rights in question

119 Provision is made in an EU legislative act for the limitation of the exercise of the fundamental rights guaranteed in Articles 7 and 8 of the Charter stemming from the system established by the PNR Directive. As to the question whether, in accordance with the case-law referred to in paragraph 114 above, that directive, as an act of EU law which permits interference with those rights, itself defines the scope of the limitation on the exercise of the rights concerned, it must be noted that the provisions of the said directive as well as Annexes I and II thereto, first, list PNR data and, secondly, provide a framework for processing those data, inter alia, by laying down the purposes and detailed rules governing those processing operations. Moreover that question is largely the same as that of compliance with the proportionality requirement referred to in paragraph 117 above (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 180), and will be examined in paragraph 125 et seq. below.

120 As regards respect for the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter, it is true that PNR data may, in some circumstances, reveal very specific information on the private life of a person. However, in so far as, on the one hand, the nature of that information is limited to certain aspects of a person's

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

private life, concerning that person's air travel in particular, and, on the other hand, the PNR Directive expressly prohibits in Article 13(4) thereof the processing of sensitive data within the meaning of Article 9(1) of the GDPR, the data covered by that directive do not by themselves allow for a full overview of the private life of a person. In addition, that directive, in Article 1(2) thereof read in conjunction with Article 3(8) and (9) thereof as well as Annex II thereto, circumscribes the purposes for which those data are to be processed. Lastly, that same directive, in Articles 4 to 15 thereof, lays down the rules governing the transfer, processing and retention of those data as well as the rules intended to ensure, inter alia, the security, confidentiality and integrity of those data, and to protect them against unlawful access and processing. In those circumstances, the interferences which the PNR Directive entails do not adversely affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter.

(b) Objective of general interest and appropriateness of the processing of PNR data having regard to that objective

121 As to the question whether the system established by the PNR Directive pursues an objective of general interest, it is apparent from recitals 5, 6 and 15 of that directive that the objectives thereof are to ensure the internal security of the European Union and thus protect the life and safety of persons, while creating a legal framework that guarantees a high level of protection of passengers' fundamental rights, in particular the right to the respect for private life and that of the protection of personal data, where PNR data are processed by the competent authorities.

122 To that end, Article 1(2) of the PNR Directive provides that PNR data collected in accordance with that directive may be subject to the processing operations referred to in Article 6(2)(a) to (c) thereof only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Those purposes undoubtedly constitute objectives of general interest of the European Union that are capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter (see, to that effect, judgment of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 42, and Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, *EU:C:2017:592*, paragraphs 148 and 149).

123 As to the whether the system established by the PNR Directive is appropriate for the purpose of attaining the objectives pursued, it should be noted that while the possibility of 'false negatives' and the fairly substantial number of 'false positives' resulting, as noted in paragraph 106 above, from automated processing under that directive in 2018 and 2019, are liable to limit the appropriateness of that system, they are not capable, however, of rendering the said system inappropriate for the purpose of contributing to the attainment of the objective of combating terrorist offences and serious crime. As is apparent from the Commission working document referred to in paragraph 106 above, automated processing carried out under the said directive have indeed already made it possible to identify air passengers presenting a risk in the context of the fight against terrorist offences and serious crime.

124 In addition, having regard to the margin of error inherent in the automated processing of PNR data and, in particular, the fairly substantial number of 'false positives', the appropriateness of the system established by the PNR Directive essentially depends on the proper functioning of the subsequent verification of the results obtained under those processing operations, by non-automated means, which, pursuant to that directive, is task for the PIU. The provisions laid down to that effect by the said directive thus contribute to the attainment of those objectives.

(c) Whether the interferences from the PNR Directive are necessary

125 According to the case-law recalled in paragraphs 115 to 118 above, it must be determined whether the interferences resulting from the PNR Directive are limited to what is strictly necessary and, inter alia, whether that directive lays down clear and precise rules governing the scope and application of the measures provided for and whether the system it establishes continues to meet objective criteria that establish a connection between PNR data, closely linked to booking for and engaging in air travel, and the objectives pursued by that directive, namely the fight against terrorist offences and serious crime.

(1) *Air passenger data covered by the PNR Directive*

126 It is necessary to assess whether the data headings in Annex I to the PNR Directive define in a clear and precise manner the PNR data which air carriers are required to provide to the PIU.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

127 As a preliminary point, it must be recalled that, as is apparent from recital 15 of the PNR Directive, the EU legislature intended for the list of the PNR data to be obtained by a PIU to be drawn up 'with the objective of reflecting the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime, thereby improving internal security within the [European] Union as well as protecting the fundamental rights, in particular privacy and the protection of personal data'. In particular, under that same recital, those data 'should only contain details of passengers' reservations and travel itineraries that enable competent authorities to identify air passengers representing a threat to internal security'. In addition, the PNR Directive prohibits, in the first sentence of Article 13(4) thereof, 'the 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'.

128 Consequently, PNR data collected and provided in accordance with Annex I to the PNR Directive must relate directly to the flight operated and the passenger concerned and must be limited in such a way as to, on the one hand, meet solely the legitimate requirements of public authorities to prevent, detect, investigate and prosecute terrorist offences or serious crime and, on the other, exclude sensitive data.

129 Headings 1 to 4, 7, 9, 11, 15, 17 and 19 of Annex I to the PNR Directive meet those requirements as well as those of clarity and precision, in that they concern clearly identifiable and circumscribed information directly related to the flight operated and the passenger concerned. As noted by the Advocate General in point 165 of his Opinion, the same is true of headings 10, 13, 14 and 16, despite their 'open-ended' wording.

130 However, clarifications are needed for the purposes of interpreting headings 5, 6, 8, 12 and 18.

131 Heading 5, entitled 'address and contact information (telephone number, email address)', does not expressly specify whether the said address and contact information refer to the air passenger alone or also cover third parties who made the flight reservation for the air passenger, third parties through whom an air passenger may be contacted, or indeed third parties who are to be informed in the event of an emergency. However, as noted by the Advocate General, in essence, in point 162 of his Opinion, given the requirements of clarity and precision, that heading cannot be interpreted as allowing, implicitly, also the collection and transfer of personal data of such third parties. Consequently, that heading should be interpreted as referring only to the postal address and contact information, namely the telephone number and email address, of the air passenger on behalf of whom the reservation is made.

132 As to heading 6, which relates to 'all forms of payment information, including billing address', that heading, in order to meet the requirements of clarity and precision, must be interpreted as covering solely information relating to the payment methods for, and billing of, the air ticket, to the exclusion of any other information not directly relating to the flight (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 159).

133 Heading 8, which relates to 'frequent flyer information', must be interpreted, as noted by the Advocate General in point 164 of his Opinion, as referring exclusively to data relating to the status of the passenger concerned in the context of a customer loyalty programme of a given airline or a given group of airlines as well as the number identifying that passenger as a 'frequent flyer'. Heading 8 thus does not permit the collection of information relating to transactions through which that status was acquired.

134 Heading 12 concerns '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)'.

135 In that regard, it must be noted from the outset that whereas the phrase 'general remarks' does not meet the requirements of clarity and precision in that it does not set, as such, any limitation on the nature and scope of the information that may be collected and provided to a PIU under heading 12 (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 160), the list in brackets does.

136 Consequently, in order to interpret heading 12, in accordance with the case-law recalled in paragraph 86 above, in a manner that complies with the requirements of clarity and precision and, more generally, with Articles

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

7 and 8 as well as Article 52(1) of the Charter, it is appropriate to consider that only the collection and provision of information expressly listed under that heading are allowed, namely the name and gender of minor air passengers, their age, language(s) spoken, the name and contact details of the guardian on departure and relationship to the minor, the name and contact details of the guardian on arrival and relationship to the minor, departure and arrival agent.

137 Lastly, heading 18 refers to '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)'.

138 As noted, in essence, by the Advocate General, in points 156 to 160 of his Opinion, it is apparent from that heading 18, read in the light of recitals 4 and 9 of the PNR Directive, that the information to which it refers is exhaustively the API data listed in the said heading as well as in Article 3(2) of the API Directive.

139 Thus heading 18, in so far as it is construed as covering only the information expressly referred to in that heading and in Article 3(2) of the API Directive, may be regarded as meeting the requirements of clarity and precision (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 161).

140 Accordingly, it must be held that, interpreted in accordance with the considerations set out inter alia in paragraphs 130 to 139 above, Annex I to the PNR Directive is of a sufficiently clear and precise nature overall, thus defining the scope of the interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

(2) *The purposes for which PNR data may be processed*

141 As is apparent from Article 1(2) of the PNR Directive, the PNR data collected in accordance with that directive are to be processed for the purposes of combating 'terrorist offences' and 'serious crime'.

142 As to whether the PNR Directive provides, in that context, for clear and precise rules that limit the application of the system established by that directive to what is strictly necessary for those purposes, it should be borne in mind, first, that the phrase 'terrorist offences' is defined in Article 3(8) of the said directive by reference to the 'offences under national law referred to in Articles 1 to 4 of Framework Decision [2002/475]'.

143 In addition to the fact that that framework decision, in Articles 1 to 3 thereof, defined in a clear and precise manner 'terrorist offences', 'offences related to a terrorist group' and 'offences related to terrorist activities', which Member States had to ensure were made punishable as criminal offences under that framework decision, Directive 2017/541, in Articles 3 to 14 thereof, also defines those same offences in a clear and precise manner.

144 Secondly, Article 3(9) of the PNR Directive defines 'serious crime' by reference to the 'offences listed in Annex II [to that directive] that are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State'.

145 However, first of all, that annex lists exhaustively the different categories of offences that might be covered by the notion of 'serious crime' referred to in Article 3(9) of the PNR Directive.

146 Next, having regard to the particular features, at the time that directive was adopted, of the criminal justice systems of the Member States in the absence of harmonisation of the offences thus referred to, it was possible for the EU legislature merely to refer to categories of offences without defining the constitutive elements thereof, especially since those elements are necessarily defined under the national law to which Article 3(9) of the PNR Directive refers, in that Member States are bound by the respect for the principle of legality of criminal offences and penalties as a component of the common value, shared with the European Union, of the rule of law under Article 2 TEU (see, by analogy, judgment of 16 February 2022, *Hungary* v *Parliament and Council*, C-156/21, EU:C:2022:97, paragraphs 136, 160 and 234), which principle is, moreover, is enshrined in Article 49(1) of the Charter, which Member States are required to observe when they implement an EU measure such as the PNR Directive (see, to that effect, judgment of 10 November 2011, *QB*, C-405/10, EU:C:2011:722, paragraph 48 and the case-law cited). Thus, in the light of the

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

usual meaning of the terms used in that annex, it must be found that the said annex determines, in a sufficiently clear and precise manner, the offences that may constitute serious crime.

147 It is true that paragraphs 7, 8, 10 and 16 of Annex II relate to categories of offences that are very general (fraud, laundering of the proceeds of crime and counterfeiting of currency, environmental crime, illicit trafficking in cultural goods) while nonetheless referring to specific offences falling within those general categories. In order to ensure the requisite level of precision under Article 49 of the Charter also, those paragraphs must be interpreted as referring to the said offences, as defined in the relevant area of national and/or EU law. When interpreted that way those paragraphs can be regarded as meeting the requirements of clarity and precision.

148 Lastly, it is important also to bear in mind that, although, in accordance with the principle of proportionality, the objective of combating serious crime is capable of justifying the serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which the PNR Directive entails, the same is not true of the objective of combating criminality in general, since the latter objective may justify solely non-serious interferences (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 59 and the case-law cited). Thus, that directive must ensure, by means of clear and precise rules, that the application of the system established by the said directive is limited to offences amounting to serious crime and thereby excludes those amounting to ordinary crime.

149 In that regard, as noted by the Advocate General in point 121 of his Opinion, many of the offences listed in Annex II to the PNR Directive – such as human trafficking, the sexual exploitation of children and child pornography, illicit trafficking in weapons munitions and explosives, money laundering, cybercrime, illicit trade in human organs and tissue, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in nuclear or radioactive materials, unlawful seizure of aircraft/ships, serious crimes within the jurisdiction of the International Criminal Court, murder, rape, kidnapping, illegal restraint and hostage-taking – are inherently and indisputably extremely serious.

150 In addition, although other offences, also referred to in that Annex II, are less likely, a priori, to be associated with serious crime, it is nevertheless apparent from Article 3(9) of the PNR Directive that those offences may be considered to amount to serious crime only if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of the Member State concerned. The requirements flowing from that provision, which relate to the nature and severity of the penalty applicable, are, in principle, such as to limit the application of the system established by that directive to offences that have the requisite level of seriousness to justify the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter stemming from the system established by the said directive.

151 Nonetheless, since Article 3(9) of the PNR Directive refers to the maximum rather than the minimum penalty applicable, it cannot be ruled out that PNR data may be processed for the purposes of combating offences which, although meeting the criterion laid down by that provision relating to the threshold of severity, amount to ordinary crime rather than serious crime, having regard to the particular features of the domestic criminal justice system.

152 It is thus for the Member States to ensure that the application of the system established by the PNR Directive is effectively limited to combating serious crime and that that system does not extend to offences that amount to ordinary crime.

(3) The link between PNR data and the purposes for which those data are processed

153 It is true that, as noted, in essence, by the Advocate General in point 119 of his Opinion, the wording of Article 3(8) and Article 3(9) of the PNR Directive, read in conjunction with Annex II thereto, does not expressly refer to a criterion that is capable of confining the scope of that directive solely to offences that may, by their nature, have an objective link, even if only indirect one, with air travel and, therefore, with the categories of data transferred, processed and retained pursuant to that directive.

154 Nevertheless, as pointed out by the Advocate General in point 121 of his Opinion, certain offences listed in Annex II to the PNR Directive, such as human trafficking, illicit trafficking in narcotic drugs or weapons, facilitation

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

of unauthorised entry and residence and the unlawful seizure of aircraft, are, by their very nature, likely to have a direct link with the carriage of passengers by air. The same is true of certain terrorist offences, such as causing extensive destruction to a transport system or an infrastructure facility or seizure of aircraft, offences under Article 1(1)(d) and (e) of Framework Decision 2002/475, to which Article 3(8) of the PNR Directive refers, or travelling for the purpose of terrorism and organising or otherwise facilitating such travelling, offences under Articles 9 and 10 of Directive 2017/541.

155 Against that background, it must also be borne in mind that the Commission provided reasons for its Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime of 2 February 2011 (COM (2011) 32 final), which became the PNR Directive, emphasising the fact that 'the terrorist attacks in the United States in 2001, the aborted terrorist attack in August 2006 aimed at blowing up a number of aircraft on their way from the United Kingdom to the United States, and the attempted terrorist attack on board a flight from Amsterdam to Detroit in December 2009 showed the ability of terrorists to mount attacks, targeting international flights, in any country' and that 'most terrorist activities are transnational in character and involve international travel, inter alia to training camps outside the [European Union]'. In addition, in order to justify the need for analysis of PNR data for the purposes of combating serious crime, the Commission referred, by way of example, to the case of a group of human traffickers who had used fake documents to check in for a flight as well as that of a human and drug trafficking network which, for the purposes of importing drugs to several destinations in Europe, had used persons who were themselves trafficked persons and had bought their air tickets with stolen credit cards. All of those cases concerned offences having a direct link with the carriage of passengers by air in that they were offences targeting the carriage of passengers by air as well as offences committed during or through travel by air.

156 In addition, it is important to note that even offences that have no such direct link with the carriage of passengers by air may, depending on the circumstances of the case, have an indirect link with the carriage of passengers by air. Such is the case, in particular, when air transport is used as a means of preparing such offences or evading criminal prosecution after committing such offences. By contrast, offences having no objective link, not even an indirect one, with the carriage of passengers by air cannot justify the application of the system established by the PNR Directive.

157 In those circumstances, Article 3(8) and (9) of that directive, read in conjunction with Annex II thereto and in the light of the requirements stemming from Articles 7 and 8 as well as Article 52(1) of the Charter, requires Member States, in particular upon individual review by non-automated means as referred to in Article 6(5) of that directive, to ensure that the application of the system established by it be limited to terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

(4) *The air passengers and flights concerned*

158 The system established by the PNR Directive covers the PNR data of anyone who meets the definition of 'passenger' within the meaning of Article 3(4) of that directive on a flight falling within the scope thereof.

159 According to Article 8(1) of the said directive, those data are transferred to the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart, regardless of whether there is any objective evidence from which it may be inferred that the passengers concerned may present a risk of being involved in a terrorist offence or serious crime. The data thus transferred are, inter alia, processed by automated means in connection with the advance assessment under Article 6(2)(a) and (3) of the PNR Directive, the objective of that assessment, as is apparent from recital 7 of that directive, being the identification of persons who were not suspected of involvement in terrorist offences or serious crime prior to that assessment and who should be subject to further examination by the competent authorities.

160 Specifically, it is apparent from Article 1(1)(a) and Article 2 of the PNR Directive that the latter distinguishes between passengers of extra-EU flights, operated between the European Union and third countries, and those of intra-EU flights, operated between different Member States.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

161 As regards passengers of extra-EU flights, it must be recalled that, in respect of passengers flying between the European Union and Canada, the Court has already held that the automated processing of their PNR data, before their arrival in Canada, facilitates and expedites security checks, in particular at borders. Furthermore, the exclusion of certain categories of persons, or of certain areas of origin, would be liable to prevent the achievement of the objective of automated processing of PNR data, namely identifying, through verification of that data, persons liable to present a risk to public security from amongst all air passengers, and make it possible for that verification to be circumvented (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 187).

162 Those considerations can be applied *mutatis mutandis* to the situation of passengers flying between the European Union and all third countries, whom Member States are required to subject to the system established by the PNR Directive pursuant to Article 1(1)(a) of that directive, read in conjunction with Article 3(2) and (4) of the said directive. The transfer and advance assessment of the PNR data of air passengers entering or leaving the European Union cannot be restricted to a particular group of air passengers, given the very nature of the threats to public security that may stem from terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air between the European Union and third countries. Thus, it must be found that the necessary connection between those data and the objective of combating such offences exists, with the result 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.

163 As regards passengers flying between different Member States of the European Union, Article 2(1) of the PNR Directive, read in conjunction with recital 10 thereof, provides only that Member States may extend the application of the system established by that directive to intra-EU flights.

164 Thus, the EU legislature did not intend to oblige Member States to extend the application of the system established by the PNR Directive to intra-EU flights but, as is apparent from Article 19(3) of that directive, reserved its decision concerning such an extension, while taking the view that it should be preceded by a detailed assessment of the legal implications thereof, in particular for the fundamental rights of the data subjects.

165 In that regard, it should be noted that, by stating that the Commission's review report referred to in Article 19(1) of the PNR Directive must 'also include a review of the necessity, proportionality, and effectiveness of including within the scope of th[at] Directive the mandatory collection and transfer of PNR data relating to all or selected intra-EU flights' and that it must, in that regard, take into account 'the experience gained by Member States, especially those Member States that apply th[at] Directive to intra-EU flights in accordance with Article 2', Article 19(3) of that directive makes apparent that, for the EU legislature, the system established by the said directive must not necessarily extend to all intra-EU flights.

166 In a similar vein, Article 2(3) of the PNR Directive provides that Member States may decide to apply that directive only to selected intra-EU flights when they consider it necessary in order to pursue the objectives of the said directive, while being able to change the selected flights at any time.

167 In any event, the Member States' power to extend the application of the system established by the PNR Directive to intra-EU flights is to be exercised, as is apparent from recital 22 thereof, in full respect for the fundamental rights guaranteed in Articles 7 and 8 of the Charter. In that regard, while, according to recital 19 of the directive, it is for the Member States to assess the threats linked to terrorist offences and serious crime, the fact remains that the exercise of that power presupposes that, upon that assessment, Member States find that there is a threat related to those offences which is capable of justifying the application of the said directive to intra-EU flights also.

168 In those circumstances, a Member State, when it wishes to exercise the power provided for in Article 2 of the PNR Directive, either for all intra-EU flights under paragraph 2 of that article or only for such selected flights under paragraph 3 of the said article, is not exempt from the requirement to verify that the extension of the application of that directive to selected or all intra-EU flights is effectively necessary and proportionate for the purposes of attaining the objective set out in Article 1(2) of the said directive.

169 Thus, given recitals 5 to 7, 10 and 22 of the PNR Directive, the Member State must verify that the processing, under that directive, of the PNR data of passengers of intra-EU flights or selected such flights is strictly necessary, having regard to the seriousness of the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, in order to ensure the internal security of the European Union or, at least, that of that Member State and, thus, protect the life and safety of persons.

170 As regards, in particular, the threats related to terrorist offences, it is apparent from the Court's case-law that terrorist activities are amongst those capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, particularly, of directly threatening society, the population or the State itself, and that it is of paramount interest for each Member State to prevent and punish those activities to protect the essential functions of the State and the fundamental interests of society in order to safeguard national security. Such threats are distinguishable, by their nature, their particular seriousness and the specific nature of the circumstances of which they are constituted, from the general and permanent risk of serious criminal offences being committed (see, to that effect, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 135 and 136, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraphs 61 and 62).

171 Thus, in a situation where it is established, on the basis of the assessment carried out by a Member State, that there are sufficiently solid grounds for considering that the latter is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the fact that that Member State makes provision for the application of the PNR Directive, pursuant to Article 2(1) of that directive, to all intra-EU flights from or to the said Member State, for a limited period of time, does not appear to go beyond what is strictly necessary. The existence of that threat is, in itself, capable of establishing a connection between, on the one hand, the transfer and processing of the data concerned and, on the other, the fight against terrorism (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 137).

172 The decision providing for that application must be open to effective review, either by a court or by an independent administrative body whose decision is binding, in order to verify that that situation exists and that the conditions and safeguards which must be laid down are observed. The period of application must also be limited in time to what is strictly necessary but may be extended if that threat persists (see, by analogy, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 58).

173 By contrast, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, the indiscriminate application by that Member State of the system established by the PNR Directive not only to extra-EU flights but also to all intra-EU flights would not be considered to be limited to what is strictly necessary.

174 In such a situation, the application of the system established by the PNR Directive to selected intra-EU flights must be limited to the transfer and processing of the PNR data of flights relating, inter alia, 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. It is for the Member State concerned, in that situation, to select the intra-EU flights, according to the outcome of the assessment which it must carry out on the basis of the requirements set out in paragraphs 163 to 169 above, and to review that assessment regularly in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of the system established by that directive to intra-EU flights continues to be limited to what is strictly necessary.

175 It follows from the foregoing that the interpretation, thus followed, of Article 2 and Article 3(4) of the PNR Directive, in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, is capable of ensuring that those provisions are within the limits of what is strictly necessary.

(5) *Advance assessment of PNR data by automated processing*

176 Under Article 6(2)(a) of the PNR Directive, the objective of the advance assessment provided for therein is to identify persons who require further examination, inter alia by the competent authorities referred to in Article 7 of that directive, in view of the fact that such persons may be involved in a terrorist offence or serious crime.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

177 That advance assessment is carried out in two stages. As a first step, the PIU of the Member State concerned, pursuant to Article 6(3) of the PNR Directive, processes PNR data by automated means by comparing them against databases or pre-determined criteria. As a second step, should that processing by automated means lead to a positive match ('hit'), that unit, pursuant to Article 6(5) of the said directive, is to carry out an individual review by non-automated means to verify whether the competent authorities referred to in Article 7 of the said directive need to take action under national law ('match').

178 As recalled in paragraph 106 above, automated processing necessarily presents a fairly substantial margin of error, since it is carried out on the basis of unverified personal data and is based on pre-determined criteria.

179 In those circumstances, and given the need, highlighted in the fourth recital of the preamble to the Charter, to strengthen the protection of fundamental rights in the light, inter alia, of scientific and technological developments, it must be ensured, as stated in recital 20 and Article 7(6) of the PNR Directive, that no decision that produces an adverse legal effect on a person or significantly affects a person may be taken by the competent authorities only by reason of the automated processing of PNR data. Moreover, in accordance with Article 6(6) of that directive, the PIU itself may transfer PNR data to those authorities only after individual review by non-automated means. Lastly, in addition to those verifications which the PIU and the competent authorities are to carry out themselves, the lawfulness of all automated processing must be open to review by the data protection officer and the national supervisory authority, in accordance with Article 6(7) and Article 15(3)(b), respectively, of that directive as well as by the national courts in the context of the judicial redress referred to in Article 13(1) of that same directive.

180 As noted, in essence, by the Advocate General in point 207 of his Opinion, the national supervisory authority, the data protection officer and the PIU must be provided with the material and human resources necessary to carry out their review under the PNR Directive. Furthermore, it is important that the national legislation transposing that directive into domestic law and authorising the automated processing provided for by the directive lays down clear and precise rules for the determination of the databases and criteria for analysis used, without relying, for the purposes of advance assessment, on other methods not referred to expressly in Article 6(2) of that directive.

181 Moreover, it follows from Article 6(9) of the PNR Directive that the consequences of advance assessment under Article 6(2)(a) thereof do not jeopardise the right of entry of persons enjoying the right of free movement within the territory of the Member State concerned as laid down in Directive 2004/38 and must, also, comply with Regulation No 562/2006. Thus, the system established by the PNR Directive does not allow the competent authorities to limit that right beyond what is prescribed by Directive 2004/38 and Regulation No 562/2006.

(i) *Comparing PNR data against databases*

182 Under Article 6(3)(a) of the PNR Directive, the PIU 'may', when carrying out the assessment referred to in Article 6(2)(a) of that directive, compare PNR data against '[relevant] databases' for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, 'including databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases'.

183 Although it follows from the very wording of that Article 6(3)(a) of the PNR Directive, in particular from the word 'including', that the databases on persons or objects sought or under alert are among the 'relevant databases' referred to in that provision, that provision does not specify which other databases could also be considered to be 'relevant' in the light of the objectives pursued by that directive. As noted by the Advocate General in point 217 of his Opinion, that provision does not expressly indicate the nature of the data that those databases may contain or their relationship to those objectives nor does it mention whether PNR data must be compared exclusively against databases managed by public authorities or whether they may also be compared against databases managed by private individuals.

184 In those circumstances, Article 6(3)(a) of the PNR Directive could, prima facie, lend itself to an interpretation according to which PNR data may be used as mere search criteria for the purposes of conducting analyses using various databases, including databases managed and exploited by the security and intelligence agencies of Member States in order to pursue objectives other than those referred to in that directive, and that those analyses may take the form of 'data mining'. The fact that such analyses can be conducted and PNR data compared to such databases may

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

give rise in the minds of passengers of carriage by air to the feeling that their private life is under a form of surveillance. Thus, while the advance assessment provided for in that provision relies on a relatively limited set of PNR data, such an interpretation of that Article 6(3)(a) cannot be adopted, since it would lead to a disproportionate use of those data providing the means of establishing a detailed profile of the individuals concerned solely because they intend to travel by air.

185 Therefore, according to the case-law recalled in paragraphs 86 and 87 above, Article 6(3)(a) of the PNR Directive must be interpreted in such a way as to ensure full respect for the fundamental rights enshrined in Articles 7 and 8 of the Charter.

186 In that regard, it is apparent from recitals 7 and 15 of the PNR Directive that the automated processing provided for in Article 6(3)(a) of that directive must be limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, while ensuring a high level of protection of those fundamental rights.

187 In addition, as observed, in essence, by the Commission in response to a question put by the Court, the wording of that provision, that the PIU 'may' compare PNR data against the databases referred to therein, allows the PIU to choose a processing method that is limited to what is strictly necessary, depending on the particular situation. In the light of the obligation to comply with the requirements of clarity and precision necessary to ensure the protection of the fundamental rights enshrined in Articles 7 and 8 of the Charter, the PIU must limit the automated processing provided for in Article 6(3)(a) of the PNR Directive to the databases identifiable under that provision. In that regard, whereas the reference, in the latter provision, to 'relevant databases' does not lend itself to an interpretation defining in a sufficiently clear and precise manner the databases thus referred to, the same is not true of the reference to 'databases on persons or objects sought or under alert, in accordance with [EU], international and national rules applicable to such databases'.

188 Accordingly, as noted, in essence, by the Advocate General in point 219 of his Opinion, Article 6(3)(a) of the PNR Directive must, in the light of those fundamental rights, be interpreted as meaning that the latter databases are the only databases against which the PIU may compare PNR data.

189 As regards the requirements which those databases must satisfy, it is appropriate to note that, under Article 6(4) of the PNR Directive, advance assessment against pre-determined criteria must, pursuant to Article 6(3)(b) of that directive, be carried out in a non-discriminatory manner, those criteria must be targeted, proportionate and specific, and must be set and regularly reviewed by the PIUs in cooperation with the competent authorities referred to in Article 7 of the directive. If, by referring to Article 6(3)(b) of that directive, the wording of Article 6(4) thereof covers only the processing of PNR data against pre-determined criteria, the latter provision must be interpreted, in the light of Articles 7, 8 and 21 of the Charter, as meaning that the requirements it lays down apply *mutatis mutandis* to the comparison of those data against the databases referred in the preceding paragraph, especially since those requirements correspond, in essence, to those adopted by the case-law arising from Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017 (EU:C:2017:592, paragraph 172), for the purposes of cross-checking PNR data against databases.

190 In that regard, it should be stated that the requirement as to the non-discriminatory nature of those databases implies, inter alia, that entry into the databases on persons sought or under alert is based on objective and non-discriminatory factors, defined in EU, international and national rules applicable to such databases (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 78).

191 In addition, in order to satisfy the requirement as to the targeted, proportionate and specific nature of the pre-determined criteria, the databases referred to in paragraph 188 above must 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.

192 Moreover, the databases used pursuant to Article 6(3)(a) of the PNR Directive must, in view of the considerations set out in paragraphs 183 and 184 above, be managed by the competent authorities referred to in Article 7 of that directive or, with regard to EU databases as well as international databases, be exploited by those authorities in

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

the context of their mission to combat terrorist offences and serious crime. That is the case of the databases on persons or objects sought or under alert, in accordance with the EU, international and national rules applicable to such databases.

(ii) *Processing PNR data against pre-determined criteria*

193 Article 6(3)(b) of the PNR Directive provides that the PIU may also process PNR data against pre-determined criteria. As is apparent from Article 6(2)(a) of that directive, the advance assessment and, accordingly, the processing of PNR data against pre-determined criteria is intended, in essence, to identify persons who may be involved in a terrorist offence or serious crime.

194 As regards the criteria that the PIU may use to that end, it should be noted, first, that according to the very wording of Article 6(3)(b) of the PNR Directive those must be 'pre-determined' criteria. As noted by the Advocate General in point 228 of his Opinion, that requirement precludes the use of artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.

195 It is important to add that use of such technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive. As observed, in essence, by the Advocate General in point 228 of his Opinion, given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.

196 Concerning, next, the requirements flowing from Article 6(4) of the PNR Directive, that provision states, in its first sentence, that any advance assessment against pre-determined criteria is to be carried out in a non-discriminatory manner and indicates, in its fourth sentence, that those criteria are in no circumstances to 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.

197 Thus Member States cannot use, as pre-determined criteria, criteria that are based on the characteristics referred to in the preceding paragraph and use of which may result in discrimination. In that regard, it follows from the wording of the fourth sentence of Article 6(4) of the PNR Directive, according to which pre-determined criteria are 'in no circumstances' to be based on those characteristics, that that provision covers both direct and indirect discrimination. That interpretation is, moreover, confirmed by Article 21(1) of the Charter, in the light of which the said provision must be read, which prohibits 'any' discrimination based on the said characteristics. In those circumstances, pre-determined criteria must be defined in such a way that, while worded in a neutral fashion, their application does not place persons having the protected characteristics at a particular disadvantage.

198 As to the requirements relating to the targeted, proportionate and specific nature of pre-determined criteria, referred to in the second sentence of Article 6(4) of the PNR Directive, it follows from those requirements that the criteria used for the purposes of advance assessment must be determined in such a way as to target, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime covered by that directive. That reading is supported by the very wording of Article 6(2)(a) thereof, which emphasises the 'fact' that the persons concerned 'may' be involved in 'a' terrorist offence or serious crime. In the same vein, recital 7 of the said directive states that the creation and application of assessment criteria should be limited to terrorist offences and serious crime 'for which the use of such criteria is relevant'.

199 In order to target in that way the persons thus referred to and given the risk of discrimination that criteria based on the characteristics set out in the fourth sentence of Article 6(4) of the PNR Directive entail, the PIU and the competent authorities cannot, generally, rely on those characteristics. By contrast, as pointed out by the German Government at the hearing, they can inter alia take into consideration specific features in the factual

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

conduct of persons when preparing and engaging in air travel which, following the findings of and experience acquired by the competent authorities, might suggest that the persons acting in that way may be involved in terrorist offences or serious crime.

200 In that context, as noted by the Commission in response to a question put by the Court, pre-determined criteria must be defined in such a way as to take into consideration both 'incriminating' as well as 'exonerating' circumstances, since that requirement may contribute to the reliability of those criteria and, in particular, ensure that they are proportionate, as required by the second sentence Article 6(4) of the PNR Directive.

201 Lastly, the third sentence of Article 6(4) of that directive provides that pre-determined criteria must be reviewed regularly. In the context of that review, those criteria must be updated in accordance with changes in the circumstances that justified their being taken into consideration for the purposes of advance assessment, thus making it possible, inter alia, to react to developments in the fight against terrorist offences and serious crime referred to in paragraph 157 above (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 82). In particular, that review must take into account the experience acquired in the context of the application of pre-determined criteria, in order to reduce, as much as possible, the number of 'false positives' and, thereby, contribute to the strictly necessary nature of the application of those criteria.

(iii) *Safeguards surrounding the automated processing of PNR data*

202 Compliance with the requirements to which the automated processing of PNR data is subject under Article 6(4) of the PNR Directive is required not only when determining and reviewing the databases as well as the pre-determined criteria provided for in that provision, but also, as noted by the Advocate General in point 230 of his Opinion, throughout the process of processing those data.

203 As regards pre-determined criteria specifically, it is appropriate, first of all, to specify that, although the PIU, as stated in recital 7 of the PNR Directive, must define the assessment criteria in a manner which keeps to a minimum the number of innocent people wrongly identified by the system established by that directive, that unit must still, in accordance with Article 6(5) and (6) of the said directive, individually review any positive match by non-automated means in order to identify, as much as possible, any 'false positives'. In addition, notwithstanding the fact that they must set the assessment criteria in a non-discriminatory manner, the PIU is required to carry out such a review for the purposes of excluding any discriminatory results. The PIU must comply with that same review obligation when comparing PNR data against databases.

204 Thus, the PIU must refrain from transferring the results of those automated processing operations to the competent authorities referred to Article 7 of the PNR Directive when, having regard to the considerations set out in paragraph 198 above, they do not, following that review, have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory results.

205 As regards the verifications which the PIU must carry out to that end, it follows from Article 6(5) and (6) of the PNR Directive, read in conjunction with recitals 20 and 22 thereof, that Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the agents in charge of the individual review, for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination.

206 In particular, given the fairly substantial number of 'false positives', mentioned in paragraph 106 above, Member States must ensure that the PIU establishes, in a clear and precise manner, objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match ('hit') concerns effectively an individual who may be involved in the terrorist offences or serious crime referred to in paragraph 157 above and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of that directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations under that directive and, in particular, the pre-determined criteria and databases used.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

207 In that context, Member States are required to ensure that, in accordance with Article 13(5) of the PNR Directive, read in conjunction with recital 37 thereof, the PIUs maintain documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring.

208 Next, the competent authorities, pursuant to the first sentence of Article 7(6) of the PNR Directive, cannot take any 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, which means, in connection with the advance assessment, that they must take into consideration and, where applicable, give preference to the result of the individual review conducted by non-automated means by the PIU over that obtained by automated processing. The second sentence of that Article 7(6) specifies that those decisions must not be discriminatory.

209 In that context, the competent authorities must ensure the lawfulness of the automated processing, in particular its non-discriminatory nature, as well as that of the individual review.

210 In particular, the competent authorities must ensure that the person concerned – without necessarily allowing that person, during the administrative procedure, to become aware of the pre-determined assessment criteria and programs applying those criteria – is able to understand how those criteria and those programs work, so that it is possible for that person to decide with full knowledge of the relevant facts whether or not to exercise his or her right to the judicial redress guaranteed in Article 13(1) of the PNR Directive, in order to call in question, as the case may be, the unlawful and, inter alia, discriminatory nature of the said criteria (see, by analogy, judgment of 24 November 2020, *Minister van Buitenlandse Zaken*, C-225/19 and C-226/19, EU:C:2020:951, paragraph 43 and the case-law cited). The same must apply to the review criteria mentioned in paragraph 206 above.

211 Lastly, in the context of redress introduced pursuant to Article 13(1) of the PNR Directive, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the persons concerned themselves must have had an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken (see, by analogy, judgment of 4 June 2013, *ZZ*, C-300/11, EU:C:2013:363, paragraphs 54 to 59), including the pre-determined assessment criteria and the operation of the programs applying those criteria.

212 Moreover, according to Article 6(7) and Article 15(3)(b), respectively, of the PNR Directive, it is for the data protection officer and the national supervisory authority to ensure the monitoring of the lawfulness of the automated processing carried out by the PIU in connection with the advance assessment, monitoring which covers, inter alia, whether those operations are not discriminatory. While the first of those provisions states, to that end, that the data protection officer has access to all data processed by the PIU, that access must necessarily cover the pre-determined criteria and databases used by that unit in order to guarantee effectivenes and a high level of data protection that that officer must ensure in accordance with recital 37 of that directive. Similarly, the investigations, inspections and audits that the national supervisory authority conducts pursuant to the second of those provisions may also concern those pre-determined criteria and those databases.

213 It follows from all of the foregoing that the provisions of the PNR Directive governing the advance assessment of PNR data under Article 6(2)(a) of that directive lend themselves to an interpretation that is consistent with Articles 7, 8 and 21 of the Charter and comes within the limits of what is strictly necessary.

(6) *The disclosure and subsequent assessment of PNR data*

214 According to Article 6(2)(b) of the PNR Directive, PNR data may also, on request of the competent authorities, be provided to the latter and assessed subsequently to the scheduled arrival in or departure from the Member State.

215 As regards the circumstances in which that disclosure and assessment may occur, it is apparent from the wording of that provision that the PIU may process PNR data in order to respond 'on a case-by-case basis' to 'a duly reasoned request based on sufficient grounds' from the competent authorities to have those data disclosed to them and processed 'in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime'. In addition, where a request is introduced more than six months after the transfer of the

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

PNR data to the PIU, a period upon the expiry of which the PNR data are depersonalised through masking out of certain elements, pursuant to Article 12(2) of that directive, Article 12(3) of the said directive provides that disclosure of the full PNR data and, therefore, a non-depersonalised version thereof, is permitted only under the dual condition that, first, it is reasonably believed that it is necessary for the purposes referred to in Article 6(2)(b) of the said directive and, secondly, it is approved by a judicial authority or another national authority competent under national law.

216 In that regard, it is apparent, first of all, from the very wording of Article 6(2)(b) of the PNR Directive that the PIU cannot systematically proceed to the subsequent disclosure and assessment of the PNR data of all air passengers and that it can only respond 'on a case-by-case basis' to requests relating to such processing operations 'in specific cases'. Having said that, in so far as that provision referred to 'specific cases', those processing operations must not necessarily be limited to the PNR data of a single air passenger but may, as noted by the Commission in response to a question put by the Court, also concern groups of persons provided that the persons concerned share a certain number of characteristics allowing them to be considered to constitute together a 'specific case' for the purposes of the intended data disclosure and assessment.

217 Concerning, next, the substantive conditions required for the PNR data of air passengers to be disclosed and assessed subsequently, although Article 6(2)(b) and Article 12(3)(a) of the PNR Directive use 'sufficient grounds' and 'reasonably', respectively, without expressly specifying the nature of such grounds, it nonetheless follows from the very wording of the first of those provisions, which refers to the purposes mentioned in Article 1(2) of the said directive, that PNR data can be disclosed and assessed subsequently only in order to verify whether there are indications that the data subject may be involved in terrorist offences or serious crime having, as follows from paragraph 157 above, an objective link, even if only an indirect one, with the carriage of passengers by air.

218 In the context of the system established by the PNR Directive, the disclosure and processing of PNR data under Article 6(2)(b) of that directive concern the data of persons who have already been subject to advance assessment prior to their scheduled arrival in or departure from the Member State concerned. In addition, a request for subsequent assessment may relate, inter alia, to persons whose PNR data have not been transferred to the competent authorities following an advance assessment, in so far as the latter has revealed nothing to suggest that those persons may be involved in terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. In those circumstances, the disclosure and processing of those data for the purposes of their subsequent assessment must be based on new circumstances justifying that use (see, to that effect, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, *EU:C:2017:592*, paragraph 200 and the case-law cited).

219 As to the nature of the circumstances capable of justifying the disclosure and processing of PNR data for the purposes of their subsequent assessment, it is settled case-law that, since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the legislation concerned, be it EU legislation or a national rule intended to transpose the latter, must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of combating crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be inferred that that data might, in a specific case, make an effective contribution to combating such activities (judgments of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, C-746/18, EU:C:2021:152, paragraph 50 and the case-law cited, and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 105).

220 Thus, the terms 'sufficient grounds' and 'reasonably' in Article 6(2)(b) and Article 12(3)(a), respectively, of the PNR Directive must be interpreted, in the light of Articles 7 and 8 of the Charter, as referring to objective evidence capable of giving rise to a reasonable suspicion that the person concerned is involved in one way or another in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, whereas, as

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

regards terrorist offences having such a link, that requirement is satisfied when there is objective evidence from which it can be inferred that the PNR data could, in a given case, contribute effectively to combating such offences.

221 Lastly, as regards the procedural conditions governing the disclosure and processing of PNR data for the purposes of their subsequent assessment, Article 12(3)(b) of the PNR Directive requires, where the request is introduced more than six months after their transfer to the PIU, that is to say when, pursuant to paragraph 2 of that article, those data have been depersonalised through masking out of the elements referred to in that paragraph 2, that the disclosure of the full PNR data and, therefore, of a non-depersonalised version thereof, must be approved by a judicial authority or by another national authority competent under national law. In that context, it is for those authorities to examine in full the merits of the request and, in particular, to ascertain whether the evidence in support of that request is likely to substantiate the substantive condition for the existence of 'reasonabl[e]' grounds referred to in the preceding paragraph.

222 It is true that, where a request for the subsequent disclosure and assessment of PNR data is introduced before the expiry of the period of six months after the transfer of those data, Article 6(2)(b) of the PNR Directive does not expressly provide for such a procedural requirement. Nonetheless, the interpretation of the latter provision must take into consideration recital 25 of that directive, from which it is apparent that, by laying down the said procedural requirement, the EU legislature intended 'to ensure the highest level of data protection' concerning access to PNR data in a form which permits direct identification of the data subject. Any request for subsequent disclosure and assessment implies such access to those data, irrespective of whether that request is introduced before the expiry of the period of six months after the transfer of the PNR data to the PIU or whether it is introduced after the expiry of that period.

223 In particular, in order to ensure, in practice, that fundamental rights are fully observed in the system put in place by the PNR Directive and, in particular, the conditions set out in paragraphs 218 and 219 above, it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority, and that the decision of that court or body be 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. In the event of duly justified urgency, the review must take place within a short time (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 202 and the case-law cited, and judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 110).

224 In those circumstances, the requirement for prior review under Article 12(3)(b) of the PNR Directive, for requests for the disclosure of PNR data introduced after the expiry of a period of six months following the transfer of those data to the PIU must also apply, *mutatis mutandis*, where the request for disclosure is introduced before the expiry of that period.

225 Moreover, if Article 12(3)(b) of the PNR Directive does not expressly specify the requirements which the authority responsible for carrying out the prior review must satisfy, it is settled case-law that, in order to ensure that the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter which results from access to personal data is limited to what is strictly necessary, that authority must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that authority must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 107 and the case-law cited).

226 For that purpose, such an 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. That requirement of independence means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review, free from any external influence. In particular, in the criminal field, the requirement of independence entails that the said authority, first, should not be involved in the conduct of

the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 108 and the case-law cited).

227 Accordingly, the provisions of the PNR Directive governing the subsequent disclosure and assessment of PNR data pursuant to Article 6(2)(b) of that directive lend themselves to an interpretation that is consistent with Articles 7 and 8 as well as Article 52(1) of the Charter and comes within the limits of what is strictly necessary.

228 In the light of all the foregoing, given that an interpretation of the PNR Directive in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter ensures that that directive is consistent with those articles of the Charter, the examination of Questions 2 to 4 and Question 6 has revealed nothing capable of affecting the validity of the said directive.

C. QUESTION 5

229 By its Question 5, the referring court seeks to ascertain whether Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises PNR data collected in accordance with that directive to be processed for the purposes of monitoring activities by the intelligence and security services.

230 It follows from the request for a preliminary ruling that, by that question, the referring court refers specifically to the activities covered by the Sûreté de l'État (State Security Services, Belgium) and the Service général du renseignement et de la sécurité (General intelligence and security services, Belgium), in the context of their respective duties relating to the protection of national security.

231 In that regard, in order to comply with the principles of legality and proportionality referred to in Article 52(1) of the Charter, the EU legislature provided clear and precise rules governing the purposes of the measures provided for by the PNR Directive which interfere with the fundamental rights guaranteed in Articles 7 and 8 of the Charter.

232 Article 1(2) of the PNR Directive states expressly that the PNR data collected in accordance with that directive may be processed 'only for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime, as provided for in points (a), (b) and (c) of Article 6(2) [of the said directive]'. The latter provision confirms the principle set out in that Article 1(2), by referring systematically to the concepts of 'terrorist offence' and 'serious crime'.

233 It is thus clear from the wording of those provisions that the list included therein of the objectives pursued by the processing of PNR data under the PNR Directive is exhaustive.

234 That interpretation is supported, inter alia, by recital 11 of the PNR Directive, according to which the processing of PNR data should be proportionate to 'the specific security goals' pursued by that directive, and by Article 7(4) thereof, according to which the PNR data and the result of processing those data received by the PIU may be further processed 'only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime'.

235 Moreover, the exhaustive nature of the purposes set out in Article 1(2) of the PNR Directive means also that PNR data may not be retained in a single database that may be consulted both for those as well as other purposes. Retention of those data in such a database would entail the risk that those data be used for purposes other than those referred to in that Article 1(2).

236 In the present case, in so far as, according to the referring court, the national legislation at issue in the main proceedings includes, among the purposes for which PNR data is to be processed, monitoring activities within the remit of the intelligence and security services, thus treating that purpose as an integral part of the prevention, detection, investigation and prosecution of terrorist offences and serious crime, that legislation is liable to disregard the exhaustive nature of the list of the objectives pursued by the processing of PNR data under the PNR Directive, which is a matter for the referring court to verify.

237 Accordingly, the answer to Question 5 is that Article 6 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which authorises

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

PNR data collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.

D. QUESTION 7

238 By its Question 7, the referring court asks, in essence, whether Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

239 As a preliminary point, it must be noted that the Belgian Government harbours doubts as to whether the Court has jurisdiction to answer that question, as formulated by the referring court, given that the latter court is the only one with jurisdiction to interpret provisions of national law and, in particular, assess the requirements stemming from the Law of 25 December 2016 in the light of Article 12(3)(b) of the PNR Directive.

240 In that regard, suffice it to note that, by that question, the referring court is seeking the interpretation of a provision of EU law. In addition, if, in proceedings brought on the basis of Article 267 TFEU, the interpretation of provisions of national law is a matter for the courts of the Member States, not for the Court of Justice, and the Court has no jurisdiction to rule on the compatibility of rules of national law with EU law, the Court does have jurisdiction to provide the national court with all the guidance as to the interpretation of EU law necessary to enable that court to determine whether those national rules are compatible with EU law (judgment of 30 April 2020, *CTT – Correios de Portugal*, C-661/18, EU:C:2020:335, paragraph 28 and the case-law cited). It follows that the Court has jurisdiction to answer Question 7.

241 As to the substance, it should be noted that the wording of Article 12(3)(b) of the PNR Directive, which in its points (i) and (ii) refers to 'a judicial authority' and 'another national authority competent under national law to verify whether the conditions for disclosure are met', respectively, places both authorities on the same footing as is apparent from the use of the conjunction 'or' between those points (i) and (ii). It thus follows from that wording that the 'other' competent national authority thus referred to is an alternative to the judicial authority and, accordingly, must have a level of independence and impartiality similar to the latter.

242 That analysis is supported by the objective of the PNR Directive, mentioned in recital 25 thereof, to ensure the highest level of data protection concerning access to the full PNR data, which enable direct identification of the data subject. That same recital specifies, moreover, that that access should be granted only under very strict conditions after the period of six months following the transfer of PNR data to the PIU.

243 That analysis is also corroborated by the history of the PNR Directive. Whereas the proposal for a directive mentioned in paragraph 155 above, which became the PNR Directive, simply provided that 'access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit', the version of Article 12(3)(b) of that directive finally adopted by the EU legislature designates, placing them on the same footing, the judicial authority and 'another national authority' competent to verify whether the conditions for disclosure of the full PNR data are met and approve such disclosure.

244 In addition and, most importantly, according to the settled case-law recalled in paragraphs 223, 225 and 226 above, it is essential that access to retained data by the competent authorities be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. The requirement of independence that the body responsible for carrying out the prior review must satisfy also means that that body must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially, and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority responsible for that prior review, first, should not be involved in the conduct of the criminal investigation in question and, secondly, must have a neutral stance vis-a-vis the parties to the criminal proceedings.

245 As noted by the Advocate General in point 271 of his Opinion, Article 4 of the PNR Directive, in paragraphs 1 and 3 thereof, provides that the PIU established or designated in each Member State is an authority competent for

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

the prevention, detection, investigation and prosecution of terrorist offences and of serious crime, and that its staff members may be agents seconded from the competent authorities referred to in Article 7 of that directive, so that the PIU appears necessarily linked to those authorities. The PIU may also, pursuant to Article 6(2)(b) of the said directive, process PNR data and disclose the results to the said authorities. In the light of the foregoing, the PIU cannot be considered to be a third party in relation to those authorities and, accordingly, to have all the qualities of independence and impartiality required to carry out the prior review mentioned in the preceding paragraph and verify whether the conditions for disclosure of the full PNR data are met, as provided for in Article 12(3)(b) of that directive.

246 Furthermore, the fact that the latter provision requires, in its point (ii), where disclosure of the full PNR data has been approved by 'another [competent] national authority', that the data protection officer of the PIU '[is] inform [ed] and [carries out] an *ex post* review', whereas this is not the case for approval by the judicial authority, is not such as to call that assessment into question. In accordance with well-established case-law, a subsequent review, such as that carried out by the data protection officer, does not enable the objective of a prior review, consisting in preventing the authorisation of access to the data in question that exceeds what is strictly necessary, to be met (see, to that effect, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 110 and the case-law cited).

247 In the light of all of those considerations, the answer to Question 7 is that Article 12(3)(b) of the PNR Directive must be interpreted as precluding national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

E. QUESTION 8

248 By its Question 8, the referring court asks, in essence, whether Article 12 of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, without drawing any distinction based on whether or not the passengers concerned present a risk that relates to terrorist offences or serious crime.

249 It must be recalled that, under Article 12(1) and (4) of that directive, the PIU of the Member State on the territory of which the flight concerned is landing or departing retains the PNR data provided by the air carriers in a database for a period of five years after their transfer to that unit and deletes such data permanently upon expiry of that period of five years.

250 As recalled in recital 25 of the PNR Directive, 'the period during which PNR data are to be retained should be as long as is necessary for and proportionate to the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime'.

251 Consequently, the retention of PNR data pursuant to Article 12(1) of the PNR Directive cannot be justified in the absence of an objective connection between that retention and the objectives pursued by that directive, namely 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.

252 In that regard, as is apparent from recital 25 of the PNR Directive, a distinction must be drawn between, on the one hand, the initial retention period of six months, referred to in Article 12(2) of that directive, and, on the other hand, the later period referred to in Article 12(3) of the said directive.

253 The interpretation of Article 12(1) of the PNR Directive must take into account the provisions in paragraphs 2 and 3 of that article, which lay down a set of rules for the retention of and access to PNR data retained after expiry of the initial retention period of six months. As is apparent from recital 25 of that directive, those provisions reflect, on the one hand, the objective of ensuring 'that the PNR data be retained for a sufficiently long period to carry out analysis and for use in investigations', which may be carried out already during the initial retention period of six months. On the other hand, according to that recital 25, they seek to 'avoid disproportionate use' through masking out of those data and to 'ensure the highest level of data protection' by granting access to those data in a form which permits direct identification of the data subject 'only under very strict and limited conditions after

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

that initial period', thus having regard to the fact that the longer the period for the retention of PNR data, the more serious the resulting interference.

254 The distinction between the initial retention period of six months referred to in Article 12(2) of the PNR Directive and the later period referred to in Article 12(3) of that directive applies also to the obligation to comply with the requirement referred to in paragraph 251 above.

255 Thus, in view of the aims pursued by the PNR Directive and of the needs of the investigation and prosecution of terrorist offences and serious crime, the Court finds that the retention, during the initial period of six months, of the PNR data of all air passengers subject to the system established by that directive, 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, in so far as it allows the necessary searches to be carried out for the purposes of identifying the persons who were not suspected of involvement in terrorist offences or serious crime.

256 By contrast, as to the later period, set out in Article 12(3) of the PNR Directive, the retention of the PNR data of all air passengers subject to the system established by that directive, in addition to the fact that, by reason of the significant quantity of data that may be retained continuously, it entails an inherent risk of disproportionate use and abuse (see, by analogy, judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, *EU:C:2020:791*, paragraph 119), runs counter to the requirement in recital 25 of the said directive that the period during which those data are to be retained should be as long as is necessary for and proportionate to the objectives pursued, since the EU legislature intended to establish the highest level of protection of PNR data allowing direct identification of the data subjects.

257 As regards air passengers for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out during the period of six months referred to in Article 12(2) of that directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers' air travel, there would not appear to be, in such circumstances, any connection – even a merely indirect one – between the PNR data of those passengers and the objective pursued by the said directive which would justify the retention of those data (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraphs 204 and 205).

258 The continued storage of the PNR data of all air passengers after the initial period of six months is not therefore limited to what is strictly necessary (see, by analogy Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 206).

259 However, in so far as, in specific cases, objective evidence, such as the PNR data of passengers which gave rise to a verified positive match, is identified from which it may be inferred that certain passengers may present a risk that relates to terrorist offences or serious crime, it seems permissible to store their PNR data beyond that initial period (see, by analogy, Opinion 1/15 *(EU-Canada PNR Agreement)* of 26 July 2017, EU:C:2017:592, paragraph 207 and the case-law cited).

260 Identification of that objective evidence is capable of establishing a connection with the objectives pursued by processing under the PNR Directive, with the result that the retention of the PNR data of those passengers is justified during the maximum period permitted by the said directive, namely during five years.

261 In the present case, in so far as the legislation at issue in the main proceedings appears to prescribe a general retention period of five years for PNR data, applicable indiscriminately to all passengers, including those for whom neither the advance assessment under Article 6(2)(a) of the PNR Directive nor any verification carried out in the initial period of six months nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime, that legislation is liable to infringe Article 12(1) of that directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, unless it may be interpreted in a manner that is consistent with those provisions, which is a matter for the referring court to ascertain.

262 In the light of the foregoing, the answer to the Question 8 is that Article 12(1) of the PNR Directive, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter, must be interpreted as precluding national

legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.

F. QUESTION 9(A)

263 By its Question 9(a), the referring court raises the question, in essence, of the validity of the API Directive in the light of Article 3(2) TEU and Article 45 of the Charter, based on the premiss that the obligations introduced by that directive apply to intra-EU flights.

264 As noted by the Advocate General in point 277 of his Opinion and as observed by the Council, the Commission and several governments, that premiss is incorrect.

265 Article 3(1) of the API Directive provides that Member States are to take the necessary steps to establish an obligation for carriers to transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State. Those data are to be communicated, pursuant to Article 6(1) of the said directive, to the authorities responsible for carrying out checks at external borders through which the passenger will enter that territory and are to be processed in accordance with the latter provision.

266 It is clear from those provisions, read in the light of Article 2(a), (b) and (d) of the API Directive, where the concepts of 'carrier', 'external borders' and 'border crossing point', are defined, respectively, that that directive imposes the obligation, for air carriers, to transmit the data referred to in Article 3(2) thereof, to the authorities responsible for carrying out external border checks only in the case of flights transporting passengers to an authorised crossing point for crossing the Member States' external borders with third countries and provides that only the data relating to those flights are to be processed.

267 By contrast, the said directive does not impose any obligation concerning the data of passengers travelling on flights that cross only internal borders between Member States.

268 It should be added that the PNR Directive, by including among PNR data, as is apparent from recital 9 and Article 8(2) thereof, the data referred to in Article 3(2) of the API Directive collected in accordance with that directive and retained by certain air carriers, and by granting Member States the power to apply the PNR Directive, pursuant to Article 2 thereof, to the intra-EU flights selected by them, altered neither the scope of the provisions of the API Directive nor the limitations stemming from that directive.

269 In the light of the foregoing, the answer to Question 9(a) is that the API Directive must be interpreted as not applying to intra-EU flights.

G. QUESTION 9(B)

270 While, by its Question 9(b), the referring court refers to the API Directive, read in conjunction with Article 3(2) TEU and Article 45 of the Charter, it is apparent from the request for a preliminary ruling that that court has doubts as to whether the system for the transfer and processing of passenger data established by the Law of 25 December 2016 is compatible with the free movement of persons and the abolition of internal border control provided for by EU law, in that that system applies not only to transport by air, but also transport by rail, by road or even by sea, departing from or going to Belgium and carried out within the European Union, without crossing external borders with third countries.

271 As is apparent from paragraphs 265 to 269 above, the API Directive, which does not apply to intra-EU flights and does not impose any obligation to transfer and process the data of passengers travelling by air or by another mode of transport within the European Union, without crossing external borders with third countries, is irrelevant for the purposes of answering that question.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

272 However, and whereas, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons, Article 2 of the PNR Directive, on which the Belgian legislature relied to adopt the Law of 25 December 2016 at issue in the main proceedings, as is apparent from the request for a preliminary ruling, authorises Member States to apply that directive to intra-EU flights.

273 In those circumstances, in order to provide a useful answer to the referring court, it is appropriate to reformulate Question 9(b) as seeking to clarify, in essence, whether EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding national legislation which provides for a system for the transfer, by carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through the Member State which adopted the said legislation.

274 First of all, Article 45 of the Charter enshrines the free movement of persons, which is, moreover, one of the fundamental freedoms of the internal market (see, to that effect, judgment of 22 June 2021, *Ordre des barreaux francophones et germanophone and Others (Preventive measures for removal)*, C-718/19, EU:C:2021:505, paragraph 54).

275 That article guarantees, in paragraph 1 thereof, the right of every citizen of the European Union to move and reside freely within the territory of the Member States, a right which, according to the Explanations relating to the Charter of Fundamental Rights (OJ 2007 C 303, p. 17), corresponds to that guaranteed in the first subparagraph of Article 20(2) TFEU, under (a), and is to be exercised, under the second subparagraph of Article 20(2) TFEU and Article 52(2) of the Charter, in accordance with the conditions and the limits defined by the Treaties and by the measures adopted thereunder.

276 Next, Article 3(2) TEU provides that the European Union is to offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect, inter alia, to external border controls and the prevention and combating of crime. Similarly, according to Article 67(2) TFEU, the European Union is to ensure the absence of internal border controls for persons and to frame a common policy on, inter alia, external border control.

277 In accordance with the Court's established case-law, national legislation which places certain nationals at a disadvantage simply because they have exercised their freedom to move and to reside in another Member State is a restriction of the freedoms conferred by Article 45(1) of the Charter to every Union citizen (see, to that effect, concerning Article 21(1) TFEU, judgments of 8 June 2017, *Freitag*, C-541/15, EU:C:2017:432, paragraph 35 and the case-law cited, and of 19 November 2020, *ZW*, C-454/19, EU:C:2020:947, paragraph 30).

278 National legislation such as that at issue in the main proceedings, which applies the system provided for by the PNR Directive not only to extra-EU flights but also, pursuant to Article 2(1) of that directive, to intra-EU flights as well as, beyond what is envisaged under that provision, to transport by other means within the European Union, results in the systematic and continuous transfer and processing of the PNR data of any passenger travelling by those means within the European Union while exercising his or her freedom of movement.

279 As noted in paragraphs 98 to 111 above, the transfer and processing of data of passengers of extra-EU and intra-EU flights stemming from the system established by the PNR Directive entail undeniably serious interferences with the fundamental rights of the data subjects enshrined in Articles 7 and 8 of the Charter. The seriousness of those interferences is even greater where the application of that system covers other means of transport within the European Union. Such interferences are, for the same reasons as those set out in those paragraphs, also such as to place at a disadvantage and, therefore, deter from exercising their freedom of movement, within the meaning of Article 45 of the Charter, the nationals of the Member States which adopted such a legislation as well as, generally, Union citizens travelling by those means of transport within the European Union from or to those Member States, with the result that that legislation entails a restriction of that fundamental freedom.

280 In accordance with settled case-law, an obstacle to the freedom of movement of persons can be justified only where it is based on objective considerations and is proportionate to the legitimate objective of the national

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

provisions. A measure is proportionate if, while appropriate for securing the attainment of the objective pursued, it does not go beyond what is necessary in order to attain that objective (see, to that effect, judgment of 5 June 2018, *Coman and Others*, C-673/16, EU:C:2018:385, paragraph 41 and the case-law cited).

281 It should be added that a national measure that is liable to obstruct the exercise of freedom of movement for persons may be justified only where such a measure is consistent with the fundamental rights guaranteed by the Charter, it being the task of the Court to ensure that those rights are respected (judgment of 14 December 2021, *Stolichna obshtina, rayon 'Pancharevo'*, C-490/20, EU:C:2021:1008, paragraph 58 and the case-law cited).

282 In particular, in accordance with the case-law recalled in paragraphs 115 and 116 above, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue. In that regard, the possibility of Member States justifying a limitation of the right guaranteed in Article 45(1) of the Charter must be assessed by measuring the seriousness of the interference which such a limitation entails and by verifying that the importance of the objective of general interest pursued by that limitation is proportionate to that seriousness.

283 As recalled in paragraph 122 above, the objective of combating terrorist offences and serious crime that the PNR Directive pursues is undoubtedly an objective of general interest of the European Union.

284 As to the question whether national legislation adopted for the purposes of transposing the PNR Directive that extends the system provided for by that directive to intra-EU flights and other modes of transport within the European Union is appropriate for securing the attainment of the objective pursued, it is apparent from the information in the file before the Court that use of PNR data allows identification of persons who were unsuspected of involvement in terrorist offences or serious crime and who should be subject to further examination, so that such legislation appears to be appropriate for the purpose of attaining the intended objective of combating terrorist offences and serious crime.

285 As to whether such legislation is necessary, the exercise by the Member States of the power provided for in Article 2(1) of the PNR Directive, read in the light of Articles 7 and 8 of the Charter, must be limited to what is strictly necessary for securing the attainment of that objective in the light of the requirements mentioned in paragraphs 163 to 174 above.

286 Those requirements apply, a fortiori, where the system provided for by the PNR Directive is applied to other means of transport within the European Union.

287 Moreover, as follows from the information in the request for a preliminary ruling, the national legislation at issue in the main proceedings transposes, in a single act, the PNR Directive, the API Directive and, in part, Directive 2010/65. To that end, it provides for the application of the system laid down in the PNR Directive to all intra-EU flights and transport by train, by road or even by sea carried out within the European Union departing from, going to or transiting through Belgium, and applies also to tour operators, while also pursuing objectives other than the fight against terrorist offences and serious crime. Following the said information, it appears that all the data collected in the context of the system established by that national legislation are retained by the PIU in a single database encompassing the PNR data, including the data covered by Article 3(2) of the API Directive, for all the passengers of the transport operations covered by that legislation.

288 In that regard, in so far as the referring court referred to the objective of improving border controls and combating illegal immigration in its Question 9(b), which is the objective of the API Directive, it should be borne in mind that, as follows from paragraphs 233, 234 and 237 above, the list of objectives pursued by the processing of PNR data under the PNR Directive is an exhaustive list with the result that national legislation authorising the processing of PNR data collected in accordance with that directive, for purposes other than those provided for therein, namely for the purposes of improving border controls and combating illegal immigration, is contrary to Article 6 of the said directive, read in the light of the Charter.

289 In addition, as is apparent from paragraph 235 above, Member States cannot create a single database containing both the PNR data collected under the PNR Directive and relating to extra-EU and intra-EU flights and the

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

data of passengers of other means of transport as well as the data covered by Article 3(2) of the API Directive, in particular where that database can be consulted not only for the purposes referred to in Article 1(2) of the PNR Directive but for other purposes also.

290 Lastly and in any event, as noted by the Advocate General in point 281 of his Opinion, Articles 28 to 31 of the Law of 25 December 2016 can only be compatible with EU law, and with Article 67(2) TFEU in particular, if they are interpreted and applied as relating only to the transfer and processing of the API data of passengers crossing Belgium's external borders with third countries. A measure whereby a Member State would extend the provisions of the API Directive, for the purposes of improving border controls and combating illegal immigration, to intra-EU and, a fortiori, other modes of transport carrying passengers within the European Union departing from, going to or transiting through that Member State, in particular the obligation to provide the data covered by Article 3(1) of that directive, would amount to allowing the competent authorities, when internal borders of the said Member State are crossed, to ensure systematically that those passengers can be authorised to enter its territory or to leave it and would thus have an effect equivalent to the checks carried out at external borders with third countries.

291 In view of all of those considerations, the answer to Question 9(b) is that EU law, in particular Article 2 of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, must be interpreted as precluding:

– national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union and departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by the PNR Directive must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and

– national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.

H. QUESTION 10

292 By its Question 10, the referring court asks, in essence, whether EU law must be interpreted as meaning that a national court may limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by land as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter.

293 The principle of the primacy of EU law establishes the pre-eminence of EU law over the law of the Member States. That principle therefore requires all Member State bodies to give full effect to the various provisions of EU law, and the law of the Member States may not undermine the effect accorded to those various provisions in the territory of those States. In the light of that principle, where it is unable to interpret national legislation in compliance with the requirements of EU law, the national court which is called upon within the exercise of its jurisdiction to apply provisions of EU law is under a duty to give full effect to those provisions, if necessary refusing of its own motion to apply any conflicting provision of national legislation, even if adopted subsequently, and it is not necessary for that court to request or await the prior setting aside of such provision by legislative or other constitutional means

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

(judgments of 15 July 1964, Costa, 6/64, EU:C:1964:66, pp. 593 and 594; of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, *EU:C:2020:791*, paragraphs 214 and 215; and of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 118).

294 Only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto. Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested. The primacy and uniform application of EU law would be undermined if national courts had the power to give provisions of national law primacy in relation to EU law contravened by those provisions, even temporarily (judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 119 and the case-law cited).

295 Unlike a breach of a procedural obligation such as the prior assessment of the impact of a project on the environment, at issue in the case that gave rise to the judgment of 29 July 2019, *Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen* (C-411/17, *EU:C:2019:622*, paragraphs 175, 176, 179 and 181), in which the Court accepted the temporary suspension of that ousting effect, a failure to comply with the provisions of the PNR Directive, read in the light of Articles 7, 8 and 45 as well as Article 52(1) of the Charter, cannot be remedied by a procedure comparable to the procedure allowed in that case. Maintaining the effects of national legislation such as the Law of 25 December 2016 would mean that that legislation would continue to impose on air carriers and other carriers as well as tour operators obligations which are contrary to EU law and which seriously interfere with the fundamental rights of the persons whose data have been transferred, retained and processed as well as restrictions on the freedom movement of those persons going beyond what is necessary (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 122 and the case-law cited).

296 Therefore, the referring court cannot limit the temporal effects of a declaration of illegality which it is bound to make under national law in respect of the national legislation at issue in the main proceedings (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 123 and the case-law cited).

297 Lastly, in so far as the referring court raises the question of the impact of a finding of incompatibility, if any, of the Law of 25 December 2016 with the provisions of the PNR Directive, read in the light of the Charter, on the admissibility and use of the evidence and information secured from the data transferred by the carriers and tour operators concerned in the context of criminal proceedings, it suffices to refer to the Court's case-law on that subject, in particular to the principles recalled in paragraphs 41 to 44 of the judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152), from which it follows that that admissibility is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness (see, by analogy, judgment of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 127).

298 In the light of the foregoing, the answer to the Question 10 is that EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of the PNR Directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Articles 7, 8 and 45 as well as Article 52(1) of the Charter. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

IV. Costs

299 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 2(2)(d) and Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), must be interpreted as meaning that that regulation applies to the processing of personal data envisaged by national legislation intended to transpose, into domestic law, the provisions of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, those of Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC and also those of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, in respect of, on the one hand, data processing operations carried out by private operators and, on the other hand, data processing operations carried out by public authorities covered, solely or in addition, by Directive 2004/82 or Directive 2010/65. By contrast, the said regulation does not apply to the data processing operations envisaged by such legislation which are covered only by Directive 2016/681 and are carried out by the passenger information unit (PIU) or by the authorities competent for the purposes referred to in Article 1(2) of that directive.**

2. **Given that an interpretation of Directive 2016/681 in the light of Articles 7, 8 and 21 as well as Article 52(1) of the Charter of Fundamental Rights of the European Union ensures that that directive is consistent with those articles of the Charter of Fundamental Rights, the examination of Questions 2 to 4 and Question 6 referred for a preliminary ruling has revealed nothing capable of affecting the validity of the said directive.**

3. **Article 6 of Directive 2016/681, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which authorises passenger name records (PNR data) collected in accordance with that directive to be processed for purposes other than those expressly referred to in Article 1(2) of the said directive.**

4. **Article 12(3)(b) of Directive 2016/681 must be interpreted as precluding national legislation pursuant to which the authority put in place as the passenger information unit (PIU) is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.**

5. **Article 12(1) of Directive 2016/681, read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers, including those for whom neither the advance assessment under Article 6(2)(a) of that directive nor any verification carried out during the period of six months referred to in Article 12(2) of the said directive nor any other circumstance have revealed the existence of objective evidence capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air.**

6. **Directive 2004/82 must be interpreted as not applying to flights, whether scheduled or non-scheduled, carried out by an air carrier flying from the territory of a Member State and that are planned to land on the territory of one or more of the other Member States, without any stop-overs in the territory of a third country (intra-EU flights).**

7. **EU law, in particular Article 2 of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter of Fundamental Rights, must be interpreted as precluding:**

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press

– **national legislation which, in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted, establishes a system for the transfer, by air carriers and tour operators, as well as for the processing, by the competent authorities, of the PNR data of all intra-EU flights and transport operations carried out by other means within the European Union, departing from, going to or transiting through that Member State, for the purposes of combating terrorist offences and serious crime. In such a situation, the application of the system established by Directive 2016/681 must be limited to the transfer and processing of the PNR data of flights and/or transport operations relating, inter alia, to certain routes or travel patterns or to certain airports, stations or seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the intra-EU flights and/or the transport operations carried out by other means within the European Union for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection, for the purposes of ensuring that the application of that system to those flights and/or those transport operations continues to be limited to what is strictly necessary, and**

– **national legislation providing for such a system for the transfer and processing of those data for the purposes of improving external border controls and combating illegal immigration.**

8. **EU law must be interpreted as precluding a national court from limiting the temporal effects of a declaration of illegality which it is bound to make under national law in respect of national legislation requiring carriers by air, by rail and by road as well as tour operators to transfer PNR data, and providing for the processing and retention of those data, in breach of the provisions of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU, Articles 7, 8 and 45 as well as Article 52(1) of the Charter of Fundamental Rights. The admissibility of the evidence thus obtained is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.**

[Signatures]

https://doi.org/10.1017/ilm.2023.8 Published online by Cambridge University Press